# CAPÍTULO I
# EL PROYECTO
# MEJORAR LA SEGURIDAD Y ACCESO AL INTERNET DE LOS USUARIOS DE LA RED PRIVADA VIRTUAL

# CAPÍTULO I: EL PROYECTO

## I.1 Presentación del proyecto

### I.1.1 Título

MEJORAR LA SEGURIDAD Y CONEXIÓN AL INTERNET MEDIANTE LA IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL BASADA EN SOFTWARE LIBRE: FAST TUNNEL VPN

### I.1.2 Responsabilidad del proyecto

Carrera de Ingeniería Informática – Taller III.

### I.1.3 Entidades asociadas

Universidad Autónoma Juan Misael Saracho – Carrera de Ingeniería Informática.

### I.1.4 Compromiso del director del proyecto

| | |
|---|---|
| Yo, Kevin Tambo Sossa, director del proyecto, acepto las bases y condiciones del proyecto, así mismo asumo la responsabilidad de cumplir los compromisos de ejecución del proyecto titulado "MEJORAR LA SEGURIDAD Y CONEXIÓN AL INTERNET MEDIANTE LA IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL BASADA EN SOFTWARE LIBRE: FAST TUNNEL VPN". | |
| Nombre del director | Firma |

*Tabla 1 – 1 Compromiso del director del proyecto*

### I.1.5 Grupo responsable del proyecto

Universitario: Kevin Tambo Sossa

### I.1.6 Duración

La ejecución del proyecto será de ocho meses de acuerdo a lo establecido.

### I.1.7 Área/línea de investigación priorizada

Redes y Telecomunicaciones.

### I.1.8 Director responsable del proyecto

| **Apellido Paterno** | **Apellido Materno** | **Nombre** | **Cédula de Identidad** |
|---|---|---|---|
| Tambo | Sossa | Kevin | 7258882 |
| **Profesión** | **Carrera** | **Facultad** | |
| Estudiante | Ingeniería Informática | Ciencias y Tecnología | |
| **Celular** | **Correo** | | **Firma** |
| 78707985 | kevintambososa@gmail.com | | |

*Tabla 1 – 2 Director responsable del proyecto*

### I.1.9 Actividades previstas para los integrantes del equipo de investigación

| **Responsable** | **Actividad** |
|---|---|
| **Jefe de Proyecto**<br>Kevin Tambo Sossa | El jefe de proyecto es el encargado de supervisar el Proyecto en todas las áreas del mismo, desde la programación hasta el cumplimiento en las fases de la Metodología RUP en la parte analítica del sistema.<br>• Control y Planificación del cronograma del proyecto.<br>• Organizar un equipo de proyecto adecuado y focalizarlos siempre en los objetivos.<br>• Seguimiento a cada etapa del proyecto.<br>• Controlar y supervisar el desarrollo del proyecto<br>• Presentación final del sistema. |
| **Analista de Sistemas**<br>Kevin Tambo Sossa | Captura, especificación y validación de requisitos, interactuando con el cliente y los usuarios mediante entrevistas. |

| | |
|---|---|
| | • Realización y especificación de<br>• Requerimientos.<br>• Elaboración del Análisis.<br>• Elaboración del Diseño.<br>• Diseño de los Diagramas UML.<br>• Construcción de la base de datos. |
| **Programador**<br>Kevin Tambo Sossa | Construcción de prototipos. Colaboración en la elaboración de las pruebas funcionales, modelo de datos y en las validaciones con el usuario.<br>La programación del código debe ir de acuerdo a las especificaciones<br>que se maneja el analista del sistema. |
| **Ingeniero de Software**<br>Kevin Tambo Sossa | Gestión de requisitos, gestión de configuración y cambios, elaboración del modelo de datos, preparación de las pruebas funcionales, elaboración de la documentación. Elaborar modelos de implementación y despliegue |

*Tabla 1 – 3 Integrantes del equipo de investigación*

## I.2 Perfil del Proyecto

### I.2.1 Introducción

Internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP, El Internet junto con la globalización permitió que compartir información sea más fácil que nunca y empezó una revolución modelando lo que hoy en día es la sociedad moderna. El sistema se transformó en un pilar de las comunicaciones, el entretenimiento y el comercio en todos los rincones del planeta.

Las estadísticas indican que, en 2018, los usuarios de Internet (conocidos como internautas) superaron los 4.54 billones de usuarios únicos. Se espera que en la próxima década esa cifra se duplique gracias a los avances tecnológicos que reducen los costos de los dispositivos que se pueden conectar y mejorando su velocidad y consume de energía drásticamente este último es muy importante dado que con la automatización de las cosas o IOT prácticamente todo se conecta al internet y a una red para ser controlado.

Este crecimiento en los usuarios del Internet aumenta exponencialmente con la situación actual en la que el mundo vive donde todos necesitan quedarse en sus hogares y evitar salir haciendo que la mayoría de las actividades cotidianas se realicen virtualmente.

Mucho de estos usuarios nuevos que vinieron por la Pandemia del COVID-19 que sufre el mundo son usuarios que no estaba familiarizados o que usaban al internet para cosas básicos, este grupo de usuarios son muy susceptibles a terminar en páginas no segura o caer en otro tipo de peligros que corremos todos al conectarnos a mejorar la situación de todos los usuarios de la Internet llegan los VPN de las siglas en inglés Virtual Private Network o RPV en español. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital. Por

tanto, dichas redes deben cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Los datos que viajan a través de una VPN parten del servidor dedicado y llegan a un firewall que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan a una nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad y ancho de banda garantizado lleguen a su vez al firewall remoto y terminen en el servidor remoto. Se muestra una imagen a continuación que ilustra el proceso:

El presente proyecto de redes y comunicación sobre redes privadas virtuales se plantea resolver la inseguridad a la que se exponen cada vez más usuarios del internet mientras navegan y realizan sus actividades, este incremento al agravarse por la actual pandemia en la que vive el mundo a forzado también a compañías y negocios a mover sus actividades en lo posible al internet.

Esto ocasiona que necesiten proteger a sus trabajadores y a la empresa mientras realizan sus actividades, cualquier empleado podría necesitar acceder al sistema de la compañía, archivos, etc. Y estas solicitudes y muchas otras necesitan estar protegidas mientras viajan por el internet como así también los datos e información personal de los usuarios de la “Red de Redes” son muy importantes, ya que al conectarnos está riego nuestra privacidad e identidad misma.

Para ello, se necesita usar una red privada virtual que protegerá nuestra conexión y nuestras solicitudes que es lo que se plantea en el proyecto, crear como un servicio disponible en el mercado un VPN Comercial para las empresas y público en general.

### I.2.2 Descripción del Proyecto

#### I.2.2.1 Antecedentes

El uso de VPN no es algo muy común por la falta de conocimiento de las personas, pero ahora que cada vez más personas están usando el internet para poder realizar sus actividades que antes se realizaban en el exterior previo a la pandemia actual. Este acrecentamiento de usuarios incrementara la necesidad de servicios de protección.
Existen diferentes tipos de arquitecturas que son usados actualmente por empresas y compañías como así también tipos de conexión.

**Arquitecturas**

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN.

VPN over LAN

Este esquema es el menos difundido, pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP,

MacAddress, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN internas o externas.

La implementación de Redes Virtuales Privadas en compañías ya existía desde hace bastante tiempo atrás dado que las seguridades de su información es una prioridad para ellos, pero ahora que más gente que nunca a empezado a usar el uso y la demanda para servicios VPN como la que el proyecto plantea ofrecer a crecido considerablemente el estimado en el reporte de Statista para el marzo del 2020 al inicio de la epidemia vio un crecimiento promedio del 36% del uso de esta tecnología como se puede apreciar en la figura 1 – 1.

Statista (18 de Marzo de 2020). Re: EPIDEMIA DEL COVID-19 El uso de las tecnologías VPN se dispara por el coronavirus [Reportaje Noticias Tecnológicas]. https://es.statista.com/grafico/21151/aumento-de-uso-de-la-vpn-en-paises-afectados-por-el-coronavirus/.


*Figura 1 – 1 Crecimiento del uso de VPNs*

Este crecimiento de los usuarios de la tecnología demuestra que ella puede ser implementada como un servicio de seguridad para todas las personas aportando una mejora en la seguridad y conexión de ellos a la "Red de Redes". Pero con este incremento de usuarios también significa un crecimiento en los usuarios que caen en los riegos que existen en la internet como el phishing, spam, recolección de información, entre otros.

La INTERPOL reporta mediante Trend Micro ahora incluso "los autores de las amenazas han visto en la pandemia una oportunidad para aumentar las probabilidades de éxito de sus ataques y han aprovechado la ocasión para revisar sus sistemas habituales de estafas por internet y phishing. Ahora envían a sus víctimas unos correos electrónicos de phishing sobre la COVID-19, a menudo haciéndose pasar por autoridades gubernamentales y sanitarias, en los que les incitan a facilitar sus datos personales y a descargarse contenidos maliciosos. INTERPOL, ha detectado 907.000 mensajes relacionados con la COVID-19 desde enero de 2020. Los ciberdelincuentes han aprovechado la recesión económica y la ansiedad que padecen las personas para perfeccionar sus tácticas de ingeniería social, utilizando la COVID-19 como eje de sus ataques".

Ainoa Guillén González. (20 de Marzo de 2021). Re: Alarmante aumento de phishing durante la pandemia global: el coronavirus [Reportaje Noticias Tecnológicas]. https://atalayar.com/content/alarmante-aumento-de-phishing-durante-la-pandemia-global-el-coronavirus-el-pretexto.

#### I.2.2.2 Justificación del Proyecto

TECNOLÓGICO: Existen VPNs comerciales con bastantes años en funcionamientos estos no son locales, son extranjeros y el manejo de nuestra información de parte de ellos no es muy transparente hecho que se volvió evidente cuando 3 de los más grandes VPN PIA, NORDVPN, TUNNELBEAR. Tuvieron escándalos donde se confirmó que mantenían registros de los lugares visitados de sus usuarios y otros tipos de información más para la venta.

Dado que estas empresas que también brindan el mismo servicio que el proyecto busca dar abre espacio para nuevos competidores que puedan aprovechar el incremento de internautas y la necesidad que ellos tendrán de mejorar su seguridad y conexión al internet. El Protocolo para redes virtuales privada de código abierto OpenVPN permitirá que el proyecto pueda lanzar sus servicios.

SOCIAL: Con la actual pandemia afectando al país y al mundo muchas más personas están ingresando al internet sin tener mucha experiencia o ignorando las buenas políticas que se deben tener en cuenta al usarlo, poniendo en peligro su información y sus dispositivos. Por esto es que un VPN proveerá de Integridad, confidencialidad y seguridad de los datos de todos sus usuarios y son sencillos de usar.

DESARROLLO SOSTENIBLE: Usando como base OpenVPN se puede crear un VPN totalmente funcional y contratar servidores en otros países no puede ser más fácil y cada vez la conexión es más estable y se pueden obtener anchos de banda mayores.

Mediante la cantidad de usuarios del VPN crezca se puede ir escalando gracias a la simplicidad que presenta para ello OpenVPN reduciendo costos también para el proyecto y incrementando las ganancias en las suscripciones por el servicio

MEDIO AMBIENTAL: Protegiendo los dispositivos conectados por un VPN al internet reducirá la posibilidad de que estos se dañen por alguno tipo de virus o malware y sean desechados aumentando la cantidad de desechos electrónicos que son muy difíciles de reciclar dado a los diferentes tipos de componentes que tienen y al tamaño diminuto de los mismos.

### I.2.2.3 Planteamiento del problema

En la actualidad las personas que recurren al internet para entretenimiento y trabajo lo cual hace que inviertan gran parte de su día a ello, la cantidad de personas que tienen acceso a la internet también incrementa cada vez más gracias a la reducción de los costos en los servicios de Internet

como así también en la de los dispositivos capaces de conectarse. Dicho crecimiento tomo una escala logarítmica después de que la pandemia del 2020 Covid -19 llegara a afectar al mundo entero obligando a todos a quedarse casa.

Estos crecimientos en usuarios también incremento el número de persona que caen en problemas de seguridad o ataques en la red como fishing, spam entre otros lo cual representa un peligro para la información de los usuarios pudiendo llegar a costar millones de dólares en pérdidas.

**Análisis de involucrados**

| Grupo | Intereses | Problemas | Recursos/Mandatos |
|---|---|---|---|
| Empresa | Que sus trabajares tenga conexiones seguras hacia afuera<br>Proteger sus sistemas de ataques internos<br>Resguardar Información y Datos de la empresa | Cuenta con una intranet pero que los usuarios todavía tienen salida al internet sin protección | R: Presupuesto anual<br>M: Determinar políticas seguridad de la empresa |
| Familias | Proteger los datos personales de la familia y los menores<br>Evitar propaganda tipo target estafas | El proveedor ISP no cuenta con VPN<br>Salidas dispositivas no es directa | M: Priorizar la seguridad de la familia<br><br>R: Presupuesto |
| Personas | Proteger datos personales<br>Acceder a contenidos restringidos | El proveedor ISP no cuenta con VPN<br>Contenidos restringidos por area | M: Priorizar la seguridad<br><br>R: Presupuesto |

*Tabla 1 – 4 Análisis de involucrados*

**Árbol de Problemas:**

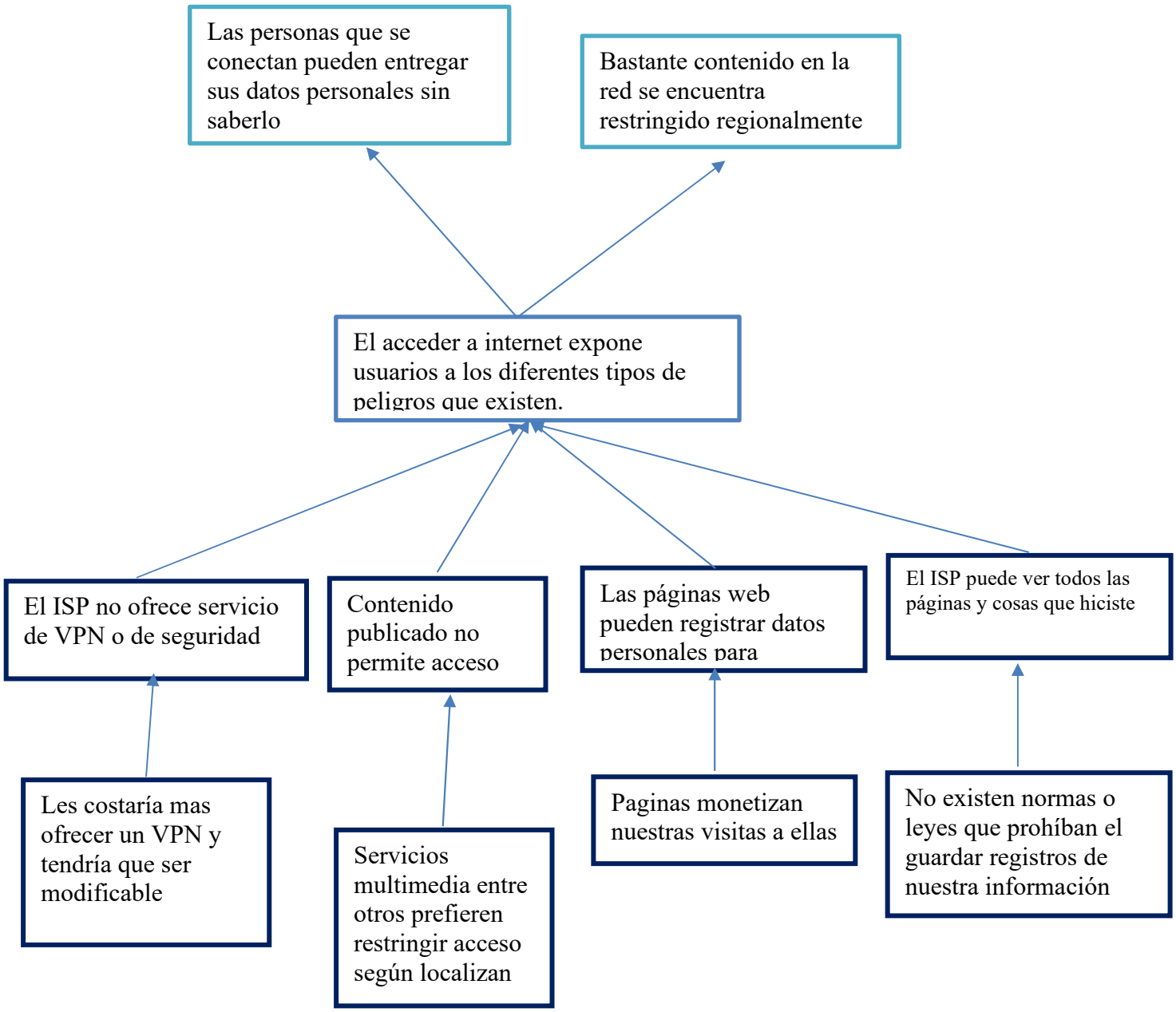


*Figura 1 – 1 Árbol de Problemas*

**Árbol de Objetivos:**

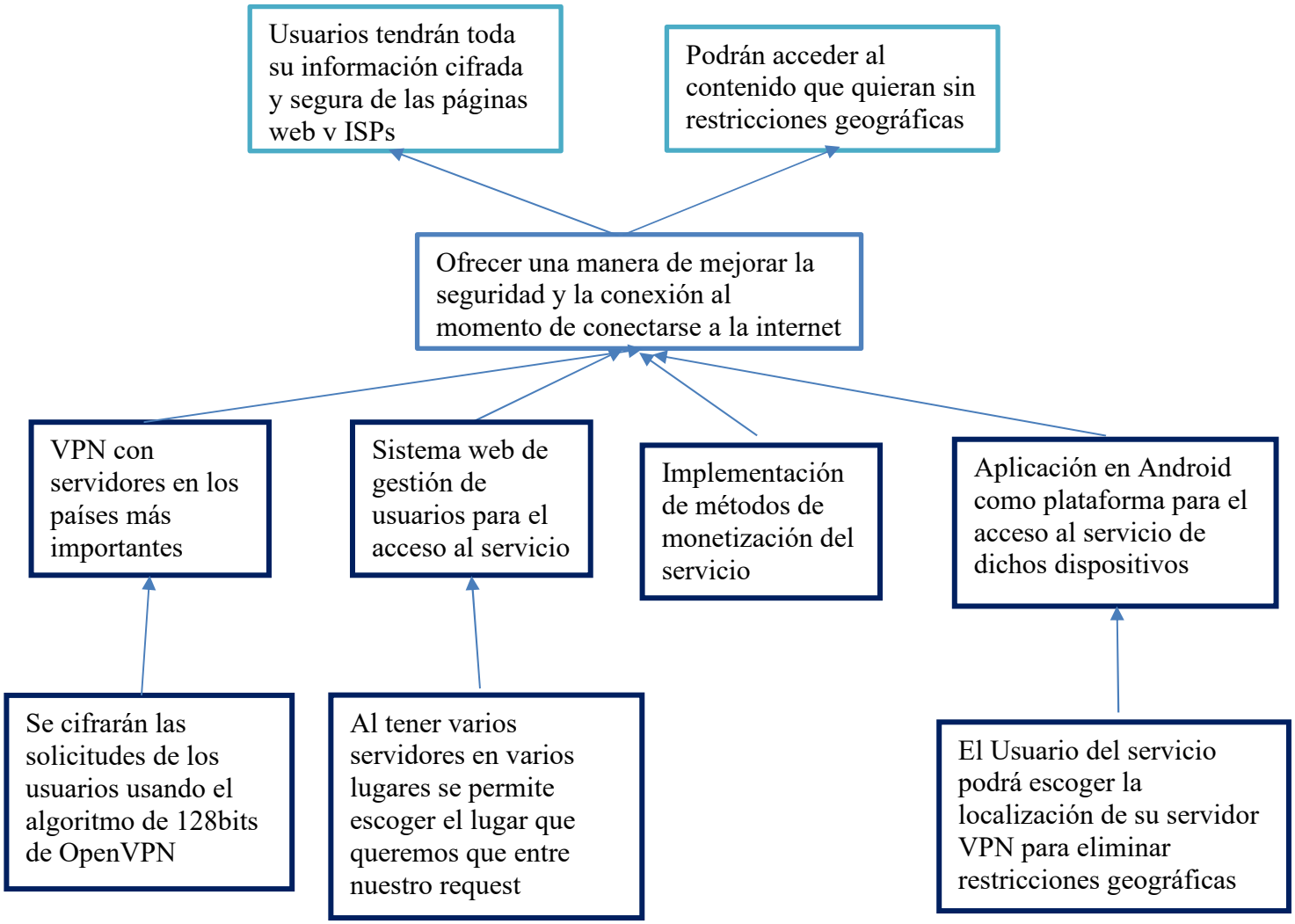


*Figura 1 – 2 Árbol de Objetivos*

### I.2.2.4 Objetivos

#### I.2.2.4.1 Objetivo General

Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual.

#### I.2.2.4.2 Objetivos Específicos

- Red privada virtual basada en OpenVPN con servidores en los países más demandados
- Sistema web de gestión de usuario para el control de inicio de sesión.
- Aplicación en Android como plataforma para que los usuarios de ese proyecto puedan usar el servicio VPN.
- Aplicación con in-app purcharses IAPs basada en suscripciones.

### I.2.2.5 Alcances

- Instalación y configuración de servidores VPS en los países más importantes.
- Creación de una plataforma para la conexión de los usuarios en Android.
- Aplicación para el uso del servicio en el sistema operativo de Android con in-app purchases IAPs.
- Brindar seguridad a los usuarios que estén usando el VPN mediante las encriptación y bloque de contenidos peligrosos.
- El sistema informático de gestión de usuarios incluye los siguientes módulos:
    - Modulo Gestión de Usuarios
    - Modulo Gestión de Roles
    - Módulos Gestión de Suscripciones

### I.2.2.6 Limitaciones

- La plataforma para el uso del VPN en Android no requerirá uno cuenta para el uso.
- El proyecto no contara con plataformas en otros sistemas operativos aparte de Android
- El sistema informático no contara con módulo de contabilidad
- La aplicación en Android no manejara Creaciones de Usuarios o un Módulo de Usuarios solo redireccionara al sistema web.

### I.2.2.7 Metodología de desarrollo del proyecto

Cada componente del proyecto cuenta con su metodología dentro de su respectivo capitulo per se manejarán dos metodologías RUP para el sistema web y la aplicación. Para la red una Por Pasos Estructurada.

Objetivos de las metodologías

- Definir actividades a llevar a cabo en un proyecto
- Unificar criterios en la organización para el desarrollo del proyecto
- Proporcionar puntos de control y revisión.

Tipos de Metodologías

- Estructurada
- Prototipos
- Orientada a objetos

### I.2.2.8 Resultados Esperados

- Los dispositivos que usen el VPN estarán protegidos de todos ni el VPN guardara registros.
- Las páginas y sitios visitados por los usuarios con el VPN podrán cambiar la región de la que consumen el contenido de la página.
- La velocidad de algunos sitios o paginas será mejorada encontrando la cantidad mínima de saltos y menor concurrencia mediante DNS pining.

### I.2.2.9 Beneficiarios

#### I.2.2.9.1 Beneficiarios Directos

- Empresas
- Instituciones
- Familias
- Personas

#### I.2.2.9.2 Beneficiarios indirectos

- Proveedores de Internet
- Medio Ambiente
- Páginas y sitios Web

### I.2.2.10 Matriz del marco Lógico (MML)

| Enunciado del Objetivo | Indicadores | Medios de Verificación | Supuestos |
|---|---|---|---|
| **Fin (Objetivo de Desarrollo)**<br><br>Ofrecer una opción para la mejora de seguridad y acceso al internet mediante el servicio VPN en la plataforma de Android. | Al año de lanzar el servicio en Android en la tienda de Play Store, alcanzaremos al menos una cantidad de 1000 descargas de la aplicación. | Los informes que la plataforma de Play Store sobre las visitas y descargas de la aplicación. | Las condiciones tecnológicas están aseguradas para el funcionamiento del software desarrollado. |
| **Propósito (Objetivo General)**<br><br>Mejorar la seguridad y acceso al internet de los usuarios de la red privada virtual. | A la finalización del proyecto los usuarios de la red privada virtual tendrán sus información y dispositivos seguros.<br><br>A la finalización del proyecto se buscará la opinión de la población en general sobre los VPN y su interés en ellos. | Los comentarios sobre el servicio que brinda la aplicación y las calificaciones al mismo dentro de la plataforma de Play Store.<br><br>Encuesta realizada a la población en general sobre la tecnología y su interés en la misma. | Las personas sean conscientes de los peligros que existen en el internet y se preocupen por su seguridad. |
| **Componentes (Objetivos Específicos)**<br><br>Red privada virtual basada en OpenVPN con servidores en los países más demandados | Al finalizar el proyecto, se contará con una red privada virtual configurada para priorizar la seguridad de la | Usuarios del servicio podrán a acceder a contenido restringido basado en localización | La cantidad de población que necesita acceder al internet para realizar sus actividades diarias |

| | | | |
|---|---|---|---|
| Sistema web de gestión de usuario del servicio de red privada virtual.<br><br>Aplicación en Android para que los usuarios de ese sistema operativo puedan usar el VPN. | información de los usuarios de la misma.<br><br>Al finalizar el proyecto, los usuarios que decidan usar el servicio con una cuenta podrán crearla en el sistema Web y manejar su información.<br><br>Al finalizar el proyecto, los usuarios que decidan mejorar su seguridad y conexión a la internet podrán hacerlo en sus dispositivos Android | Usuarios podrán enmascarar su ubicación mediante saltos de servidores<br><br>Usuarios tendrán todas sus solicitudes encriptadas al salir de su dispositivo<br><br>Usuarios del servicio podrán crear su cuenta para el acceso del servicio. | solo va a aumentar por la situación actual del país. |
| **Actividades**<br><br>1. Red privada virtual basada en OpenVPN con servidores en los países más demandados<br>1.1. Diseño de la red.<br>1.2. Instalación y Configuración de los servidores para que trabajen la red priva virtual bajo OpenVPN.<br>2. Sistema web de gestión de usuario.<br>2.1. Diseño de la base de datos.<br>2.2. Diseño de las pantallas<br>2.3. Compra del Dominio<br>2.4. Compra del Hosting<br>2.5. Diseño del sitio web | 12100 Personal Eventual **36500**<br>23200 Alquiler de Equipos y Maquinarias **5550**<br>43120 Equipo de Computación **4500** Varios **4329**<br>**Total: Bs: 50879** | Protocolos de Seguridad Web<br><br>Manual de Usuario Impreso<br><br>Stress Test Servicio | Disponibilidad de herramientas para el desarrollo del sistema. |

| | | | |
|---|---|---|---|
| 3. Aplicación en Android para que los usuarios de ese sistema operativo puedan usar el VPN con IAPs.<br>3.1. Diseño de la Aplicación<br>3.2. Elaboración de la Aplicación | | | |

*Tabla 1 – 5 Matriz del marco Lógico (MML)Resultados Esperados*

### I.2.2.11 Cronograma de Actividades

| Nº | Actividad | Nº días | Fecha inicio | Fecha Finaliz. | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | Investigación | | **01/05/2020** | **30/07/2020** | | | | | | | | |
| **2** | Diseño | | **01/07/2020** | **30/09/2020** | | | | | | | | |
| **3** | Desarrollo | | **01/08/2020** | **30/11/2020** | | | | | | | | |
| **4** | Prueba Alfa | | **01/10/2020** | **30/10/2020** | | | | | | | | |
| **5** | Prueba Beta Cerrada | | **01/11/2020** | **30/11/2020** | | | | | | | | |
| **6** | Prueba Beta Abierta | | **01/12/2020** | **20/12/2020** | | | | | | | | |
| **7** | Lanzado de Servicio | | **01/12/2020** | **20/12/2020** | | | | | | | | |

*Tabla 1 – 6 Cronograma de Actividades*

# CAPÍTULO II
# COMPONENTE I
# RED PRIVADA VIRTUAL

# CAPÍTULO II: Componentes del Proyecto

## II.1 Componente 1: Red Privada Virtual

El diseño de la red será basado en OpenVPN con servidores en por lo menos 2 diferentes países de los más demandados en este tipo de servicios, el acceso a la red privada virtual requerirá una cuenta ya sea gratis o paga con las respectivas credenciales de inicio de sesión proveídos por el sistema de gestión de usuarios.

### II.1.1 Marco Teórico

Este capítulo se centrará en la presentación de las redes privadas virtuales como una solución de seguridad y de alta escalabilidad. Seguidamente se describirán las arquitecturas utilizadas en las VPN y también las diferentes tecnologías que existen en la actualidad, así como sus ventajas y desventajas.

#### II.1.1.1 VPN (Virtual Prívate Network)

##### II.1.1.1.1 Definición VPN

Una red privada virtual, por sus siglas en inglés VPN (Virtual Private Network), es una tecnología que permite una extensión de la red local sobre una red pública imitando un vínculo privado punto a punto, como se ilustra en la Figura 2 - 1. Esta red pública o compartida comúnmente es Internet.

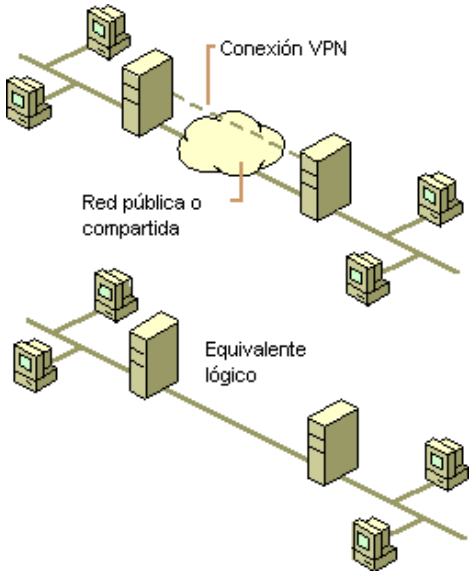


*Figura 2 – 1 Conexión VPN*

Una manera de construir VPNs es estableciendo túneles virtuales entre los dos extremos. En este caso, un túnel es la ruta de información lógica que representa una transferencia segura a través del cual viajan los paquetes encapsulados de un equipo a otro, como se muestra en la Figura 2 - 2. Para los usuarios de origen y destino, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. Los usuarios desconocen los routers, switches, servidores proxy u otros gateways de seguridad, que pueda haber entre los extremos del túnel

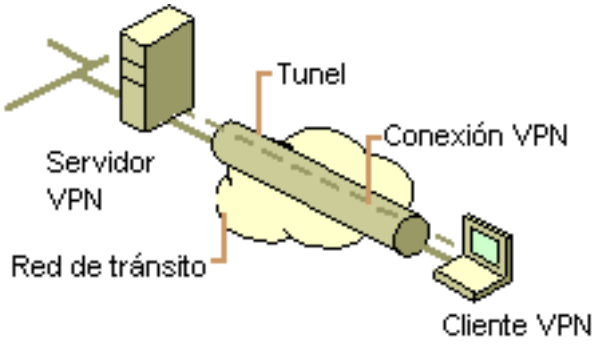


*Figura 2 – 2 Túnel VPN*

El proceso de encapsulamiento se efectúa a la entrada del túnel y consiste en la adición al paquete original de un header (cabecera) que contiene la dirección IP pública de la red remota. Una vez recibido el nuevo paquete por el dispositivo de enrutamiento propietario de la IP pública de destino, éste retira el header adicionado anteriormente y entrega el paquete original a la estación destino identificada por la IP privada.

La tecnología de VPN conforma un canal de comunicación seguro para oficinas remotas, usuarios móviles y socios comerciales que permitirá trabajar al usuario como si estuviera en la misma red local.

### II.1.1.1.2 Elementos de una VPN

Una conexión VPN consta de los siguientes elementos, que se pueden observar en la Figura 3:

- **Servidor VPN:** Un equipo que acepta conexiones VPN y puede configurarse para proporcionar acceso a toda la red o restringir el acceso sólo a sus propios recursos.

- **Cliente VPN:** Un equipo que inicia una conexión segura a un servidor VPN. Un cliente VPN puede ser un equipo individual o un router.
- **Túnel:** La parte de la conexión en la que se encapsulan los datos.
- **Conexión VPN:** La parte de la conexión en la que se cifran los datos.
- **Protocolos de túnel:** Los protocolos utilizados para administrar túneles y encapsular datos privados. Los datos que se envían por el túnel también deben estar cifrados.
- **Datos en túnel:** Los datos que normalmente se envían a través de un vínculo punto a punto privado.
- **Conjunto de redes públicas o privadas de tránsito:** La red compartida o privada que atraviesan los datos encapsulados. El conjunto de redes públicas o privadas de tránsito puede ser Internet o una intranet privada basada en IP (Internet Protocol).

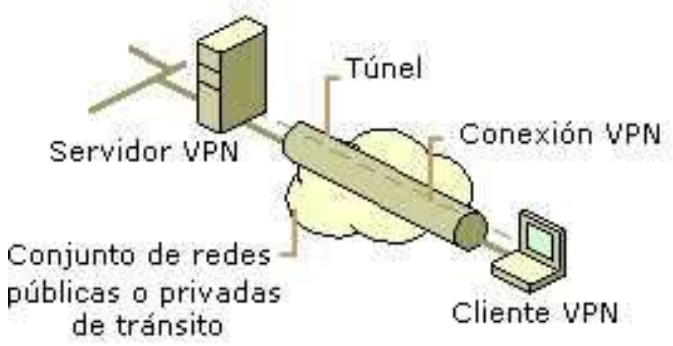


*Figura 2 – 3 Elementos de una VPN*

### II.1.1.1.3 Tipos de VPN

De manera general, los tipos de VPN describen los dispositivos que se encuentran involucrados en la conexión [10]. Existen cuatro tipos de VPN: sitio-a-sitio, acceso remoto, firewall y usuario-a-usuario.

#### II.1.1.1.3.1 VPN Sitio-a-Sitio (Site-to-Site VPN)

Una VPN sitio-a-sitio utiliza una conexión en modo túnel entre dispositivos VPN (gateway VPN) para proteger el tráfico entre dos o más sitios o localidades. Las conexiones sitio-a- sitio también son conocidas como conexiones L2L (LAN-to-LAN). Con este tipo de conexiones, un dispositivo central ubicado en cada localidad provee protección al tráfico entre sitios. Este

proceso de protección, así como la red de transporte ubicada entre los dos dispositivos VPN, es transparente para el dispositivo final en los dos sitios.

#### II.1.1.1.3.2 VPN de Acceso Remoto o VPDN (Virtual Private Dial-up Network)

Es uno de los modelos más usados, donde los usuarios remotos acceden a la red corporativa, típicamente desde distintas ubicaciones (oficinas comerciales, domicilios, hoteles, etc.). Para ello se deben tomar en cuenta ciertos aspectos de seguridad en los extremos de la comunicación, tales como el cifrado y uso de contraseñas. Los requerimientos de seguridad para los servicios VPDN nunca son tan altos como los requerimientos para las comunicaciones sitio-a-sitio. Actualmente la mayoría de los servicios VPDN están implementados sobre IP o usando el backbone privado de un proveedor de servicio. Los protocolos usados para implementar este servicio sobre IP incluyen L2F (Layer 2 Forwarding) o L2TP (Layer 2 Transport Protocol), entre otros, que serán descritos más adelante.

#### II.1.1.1.3.3 VPN Firewall

Las VPN basadas en firewall por lo general son sólo módulos que se añaden al firewall que se esté ejecutando. Habitualmente tienen muchas funciones necesarias para la implementación de VPN como la autenticación, autorización y amplias funciones de conexión, que simplifican la supervisión de lo que sucede. Estas VPN refuerzan también al sistema operativo del host porque inhabilitan o eliminan servicios innecesarios que son susceptibles a ser atacados. La mayoría tiene una interfaz adicional, llamada interfaz DMZ (Demilitarized Zone), con sus propios controles de acceso. La DMZ permite un acceso controlado a los servidores, proxies y otros servicios en un entorno que se puede comprometer sin afectar a la seguridad de la red interna.

#### II.1.1.1.3.4 VPN Usuario-a-Usuario (User-to-User VPN)

Una VPN de tipo usuario-a-usuario es básicamente una conexión VPN entre dos dispositivos finales. Este tipo de conexión se implementa cuando se necesita proteger un tipo de tráfico específico entre dispositivos determinados.

#### II.1.1.1.4 Topologías de VPN

Desde una perspectiva de diseño, a continuación, se describen varias de las topologías implementadas en una VPN. Estas topologías incluyen punto-a-punto, hub-and-spoke, y fully meshed.

##### II.1.1.1.4.1 Punto-a-Punto (Point-to-Point)

Existen dos tipos básicos de conexiones VPN punto-a-punto:

- Dispositivo-a-Dispositivo (Device-to-Device).
- Red-a-Red (Network-to-Network).

##### II.1.1.1.4.2 Dispositivo-a-Dispositivo (Device-to-Device)

Una conexión VPN dispositivo-a-dispositivo es una VPN de tipo usuario-a-usuario, donde sólo dos dispositivos están involucrados en la VPN. Esta topología es usualmente implementada cuando sólo un tipo de tráfico específico entre dos dispositivos necesita ser protegido. Una de las preocupaciones de las conexiones de dispositivo-a-dispositivo es que agregan una carga adicional sobre el dispositivo VPN final, como se puede observar en la Figura 2 - 4.

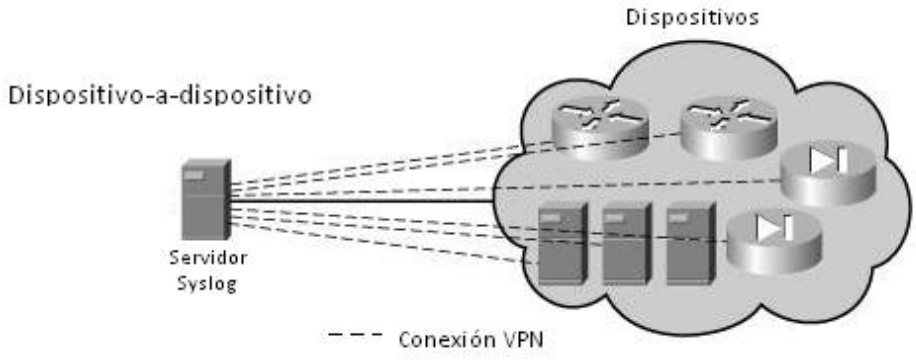


*Figura 2 – 4 Conexión dispositivo-a-dispositivo.*

##### II.1.1.1.4.3 Red-a-Red (Network-to-Network)

Una conexión VPN red-a-red podría ser considerada como una VPN de tipo L2L. Con una conexión red-a-red, dos gateways VPN proporcionan protección al tráfico entre dos o más redes. Una ventaja de este tipo de conexión es que el tráfico de varios dispositivos puede ser protegido por una misma conexión VPN. Además, se puede escoger un dispositivo apropiado

como gateway VPN para manejar la sobrecarga y el procesamiento del tráfico VPN, quitando este trabajo a los clientes finales. En la se muestra una topología red-a-red.

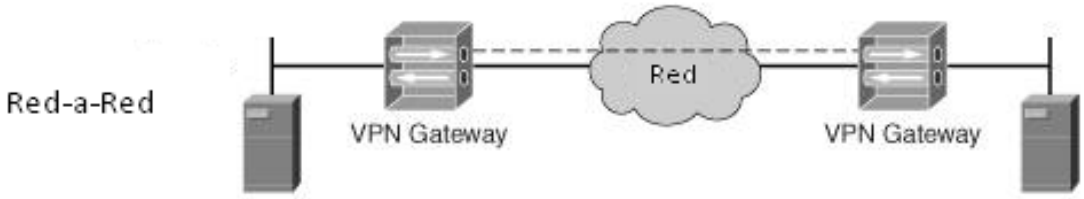


*Figura 2 – 5 Conexión red-a-red.*

Las VPN red-a-red se pueden dividir en dos categorías:

- **Fully-Meshed:** En una red VPN fully-meshed todos los dispositivos o redes VPN se encuentran conectados entre sí. La parte izquierda de la Figura 2.6 [10], muestra un ejemplo de un diseño fully-meshed, conectando múltiples redes entre sí. Una ventaja de este diseño es que un dispositivo o red puede enviar tráfico directamente a través de una VPN hasta un destino remoto sin tener que implementar más conexiones VPN. Sin embargo, la principal desventaja de esta solución es la escalabilidad.

- **Hub-and-Spoke (Partially-Meshed):** En este diseño, no todo dispositivo VPN tiene una conexión con otros dispositivos VPN, como se muestra en la sección derecha de la Figura 2 - 6. El diseño hub-and-spoke es común en redes corporativas, donde el hub es típicamente la empresa y los spokes son las oficinas remotas.

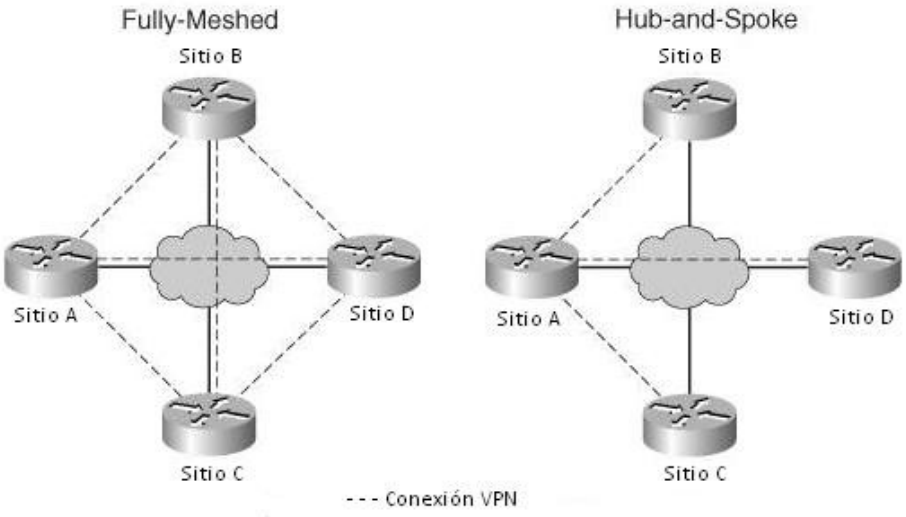


*Figura 2 – 6 Diseños de redes VPN fully/partially-meshed.*

#### II.1.1.1.5 Categorías de VPN

Cada organización tiene su propia clasificación. Cisco Systems define tres categorías básicas que describen dónde es implementada una VPN: intranet, extranet e Internet.

##### II.1.1.1.5.1 Intranet

Una VPN intranet conecta recursos de la misma empresa a través de la infraestructura de la compañía ofreciendo altos niveles de seguridad y aislamiento de zonas y servicios de la red interna. También requieren garantía de calidad de servicio para los procesos de misión crítica. Las VPN para comunicaciones intranet son usualmente implementadas con tecnologías como Frame Relay, MetroEthernet o ATM (Asynchronous Transfer Mode). Un ejemplo clásico es un equipo VPN que proporcione autenticación y cifrado a la información de un servidor de nóminas de sueldo, haciendo posible que sólo el personal autorizado pueda acceder a la misma.

##### II.1.1.1.5.2 Extranet

Una VPN extranet conecta recursos de una empresa a otra mediante el uso de dispositivos de seguridad dedicados, como firewalls o técnicas de cifrado. Estas comunicaciones pueden tener requerimientos menos estrictos de calidad de servicio, por lo que hacen que Internet sea el medio más adecuado para las comunicaciones inter-organizacionales ya que permite eliminar los costosos enlaces punto-a-punto tradicionales.

##### II.1.1.1.5.3 Internet

Una VPN Internet utiliza una red pública como backbone para transportar tráfico VPN entre dos dispositivos. Por ejemplo, se podría utilizar Internet para conectar dos sitios entre sí (conexión sitio-a-sitio), o tener usuarios de acceso remoto usando su ISP (Internet Service Provider) local para conectarse a la red corporativa a través de una conexión VPN.

#### II.1.1.1.6 Componentes de una conexión VPN

En esta sección se describirán los componentes de una VPN tradicional. No todas las implementaciones de VPN incluirán todos estos componentes. Dependerá de las

necesidades de seguridad de la empresa determinar cuál implementación de VPN (o implementaciones) posee los componentes necesarios para cubrir todos sus requerimientos de seguridad.

- **Autenticación:** Asegura que el intercambio de información se lleve a cabo con el usuario o dispositivo correcto, es decir, verifica la identidad de los usuarios. Se realiza normalmente al inicio de una sesión, y luego aleatoriamente durante el transcurso de la sesión, para asegurar que no haya algún tercer usuario no autorizado. La mayor parte de los sistemas de autenticación de dispositivos usados en VPN están basados en sistema de claves compartidas. También se utilizan las firmas digitales o certificados.
- **Integridad:** Garantiza que los datos enviados no han sido alterados, a través del uso de algoritmos de hash como MD5 (Message Digest Algorithm 5) y el SHA (Secure Hash Algorithm).
- **Confidencialidad:** Se garantiza a través del cifrado de los datos. El cifrado protege los datos transportados para que no sean interpretados por nadie más que sus destinatarios. Esta tarea se realiza con algoritmos de cifrado como DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), entre otros. En las redes virtuales, el cifrado debe ser realizado en tiempo real, de esta manera las claves son válidas únicamente para la sesión usada en un determinado momento.
- **No repudio:** Involucra dos componentes, autenticación y contabilización (accounting). La autenticación se refiere a que los mensajes deben estar firmados, y quien los firma no puede negar su autoría [14]. La contabilización es el registro de la sesión VPN, esto puede incluir la identidad de los dispositivos que establecieron la conexión, su duración, la información transmitida a través de ella, y así sucesivamente. Esto puede ser utilizado posteriormente para detectar ataques de acceso y para propósitos de gestión de la conexión.

- **Método de Encapsulado:** Define cómo la información del usuario será encapsulada y transportada a través de la red, así como las aplicaciones o protocolos contenidos en la carga útil del paquete VPN.

Además de garantizar los aspectos de seguridad mencionados anteriormente, se debe cumplir con:

- **Soporte a protocolos múltiples:** Manejo de los protocolos comunes utilizados en las redes públicas, como IP, IPX (Internetwork Packet Exchange), etc.
- **Administración de direcciones:** Asignación de una dirección al cliente en la red privada, asegurando que las direcciones privadas se conserven así.
- **Administración de claves:** Las claves de codificación se deben generar y renovar periódicamente.

#### II.1.1.1.7 Ventajas de una VPN

- **Bajo costo:** Una forma de reducir costo en las VPN es eliminando la necesidad de largos enlaces dedicados de costo elevado, líneas alquiladas, equipos de acceso dial-up, etc.
- **Escalabilidad:** Las redes VPN son arquitecturas de red más escalables y flexibles que las WAN (Wide Area Network) tradicionales, debido a que permiten a las corporaciones agregar o eliminar sus sistemas localizados remotamente, usuarios móviles o aliados comerciales de forma fácil y poco costosa en función de las necesidades del negocio.
- **Compatibilidad**: Como aceptan la mayor parte de los protocolos de red más comunes, incluidos TCP/IP (Transmission Control Protocol/Internet Protocol), IPX (Internetwork Packet Exchange) y NetBEUI (NetBIOS Extended User Interface), las VPN puede ejecutar de forma remota cualquier aplicación que dependa de estos protocolos de red específicos.
- **Movilidad:** Las VPN utilizan Internet para comunicarse con la intranet por lo que el acceso puede llevarse a cabo prácticamente desde cualquier lugar que tenga acceso a Internet.

- **Seguridad:** Utilizan mecanismos para transmitir información a través de redes inseguras, lo que garantiza la confidencialidad, integridad y autenticación de los datos transmitidos.
- **Administración centralizada:** Algunos proveedores soportan la característica de administración centralizada de sus productos VPN. Esto representa una fuerte característica de seguridad y un buen mecanismo para la resolución de problemas.
- **Prioridad de tráfico:** Algunos proveedores ofrecen la funcionalidad de priorizar tráfico en sus productos VPN. Esto agrega gran flexibilidad a la corporación en cuanto a la utilización de los enlaces de Internet, debido a que se puede decidir en qué orden se preserva el ancho de banda según el tipo de tráfico permitido y de acuerdo a su importancia.
- **Transparencia:** Interconectar distintos equipos es transparente para el usuario final.
- **Simplicidad**: Son de fácil instalación y uso en cualquier equipo.
- **Control de Acceso:** Basado en políticas de la organización.

#### II.1.1.1.8 Desventajas de una VPN

- El rendimiento de la red basada en VPN es dependiente del rendimiento de Internet, se puede garantizar un ancho de banda pero no su rendimiento. Una sobrecarga de Internet puede afectar negativamente el rendimiento de toda la VPN.
- Debido a las distintas soluciones disponibles para implementar una VPN, se pueden encontrar incompatibilidades entre las usadas en los distintos nodos de la misma. Además, no todos los equipos actualmente instalados poseen facilidades para realizar VPNs y se rigen por distintas normas y estándares.
- El tiempo de respuesta no está garantizado y, por lo tanto, no son recomendables para aplicaciones críticas.
- Son propensas a ataques de negación de servicio, dado que los túneles están sobre Internet.
- La posibilidad de pérdida de paquetes en tránsito es alta.

### II.1.1.1.9 Implementaciones de VPN

Actualmente se dispone de una gran variedad de protocolos para VPN, cada uno con sus ventajas y desventajas en cuanto a los parámetros de seguridad, facilidad, mantenimiento y tipos de clientes soportados. En esta sección se describen los más utilizados.

#### II.1.1.1.9.1 PPTP (Point-to-Point Tunneling Protocol)

PPTP es un protocolo normalizado por la IETF (Internet Engineering Task Force) [8] y desarrollado originalmente por Microsoft como una solución de acceso remoto para permitir transferencias seguras desde un cliente, a través de una red pública, a un servidor Microsoft. PPTP es una extensión del PPP (Point-to-Point Protocol) lo que permite encapsular múltiples protocolos como NetBEUI, IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange), etc., en un paquete IP, para luego poder encaminarlos a través de un túnel VPN.

La autenticación PPTP está basada en el sistema de acceso de Windows, en el cual todos los clientes deben proporcionar un par usuario/contraseña. En el caso de Microsoft, la autenticación de clientes PPTP soporta los protocolos CHAP (Challenge Handshake Authentication Protocol), MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol versión 2), y PAP (Password Authentication Protocol). Para el cifrado de los datos, PPTP utiliza MPPE (Microsoft Point-to-Point Encryption) donde sólo los extremos de la conexión comparten la clave. Esta clave es generada empleando el estándar RSA RC-4 (Rivest-Shamir-Adleman Rivest Cipher 4) a partir de la contraseña del usuario. La longitud de la clave puede ser 128 bits o 40 bits

El establecimiento de conexiones PPTP se divide en tres fases que se describen a continuación:

- Fase 1 PPTP: En la fase 1, se utiliza el LCP (Link Control Protocol) para iniciar la conexión. Esto incluye la negociación de parámetros de capa 2, tales como el uso de autenticación, cifrado con MPPE, entre otros protocolos.
- Fase 2 PPTP: En la fase 2, el usuario es autenticado ante el servidor. PPP soporta cuatro tipos de autenticación: PAP, CHAP, MS-CHAPv1 y MS-CHAPv2.

- Fase 3 PPTP: En la fase 3, son invocados los protocolos utilizados por la conexión de datos negociados durante la fase 1. Una vez completada la fase 3, los datos pueden ser enviados a través de la conexión PPP.

  Componentes de PPTP

  PPTP se basa en una arquitectura cliente-servidor para conectividad de acceso remoto que involucra dos entidades, como se observa en la Figura 7.

  El cliente es comúnmente referido como PAC (PPTP Access Concentrator). El PAC es responsable de establecer una conexión segura hacia un servidor y enviar los datos en paquetes PPP a través del túnel hacia el servidor.

  El servidor es conocido como PNS (PPTP Network Server). El servidor toma los paquetes protegidos PPP que viajan a través del túnel, verifica la protección, descifra los paquetes, y reenvía la información de la carga útil PPP encapsulada, por ejemplo un paquete IP, al destino.

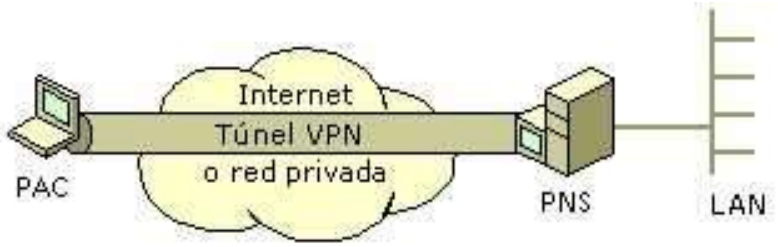


*Figura 2 – 7 Conexión PPTP.*

El PAC es responsable de iniciar la conexión con el PNS, utilizando LCP para la negociación, y participando en el proceso de autenticación de PPP. El PNS es responsable de autenticar al PAC y de enrutar el tráfico encapsulado del PAC hacia otras localidades.

Funcionamiento de PPTP

PPTP es un protocolo orientado a conexión, en donde el PAC y el PNS mantienen un estado de su comunicación. Dos conexiones son establecidas para la sesión: una conexión de control entre cada pareja PAC-PNS y una conexión de datos sobre la misma pareja PAC- PNS. Una vez que la sesión es establecida, el PAC y el PNS pueden utilizar GRE (Generic Routing Encapsulation) a través de la conexión de

datos para transmitir el tráfico de usuario. Generalmente, la conexión de datos es llamada túnel.

Conexión de datos

La conexión de datos o túnel transporta todos los paquetes PPP de la sesión de usuario. Utiliza una versión extendida de GRE como protocolo de transporte para los paquetes PPP. Este protocolo proporciona el envío, control de flujo y control de congestión de los paquetes PPP. Algunos de los parámetros que necesitan ser negociados son la asignación de dirección del PAC, el algoritmo de cifrado a usar, y el uso de compresión, de ser necesario.

PPTP permite a los usuarios y a los ISPs crear varios tipos de túneles, basados en la capacidad del equipo del usuario final y en el soporte del ISP para implementar PPTP. De esta manera, el equipo del usuario final determina el lugar de terminación del túnel, bien sea en su equipo, si está ejecutando un cliente PPTP, o en el servidor de acceso remoto del ISP, si su equipo solo soporta PPP y no PPTP.

Dado lo anterior, los túneles se pueden dividir en dos clases, voluntarios y permanentes. Los túneles voluntarios son creados por requerimiento de un usuario y para un uso específico. Los túneles permanentes son creados automáticamente sin la acción de un usuario y no le permite escoger ningún tipo de privilegio.

En los túneles voluntarios, la configuración del mismo depende del usuario final, cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el equipo del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un
túnel permanente. La Figura 2 - 8 muestra un escenario de túneles voluntarios creados desde dos clientes distintos a un mismo servidor PPTP a través de Internet.

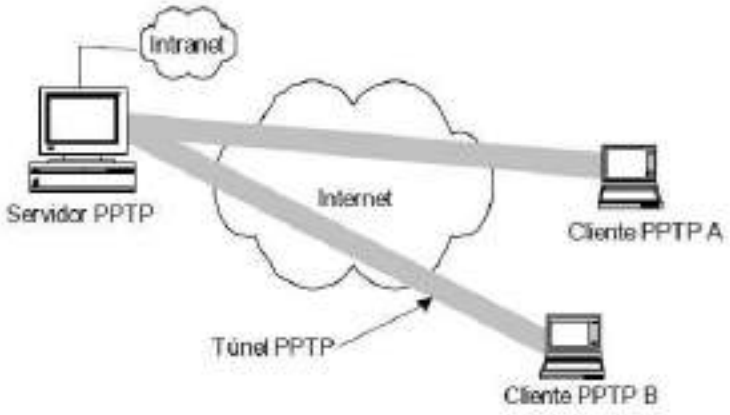


*Figura 2 – 8 Túneles voluntarios.*

Los túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el RAS (Remote Access Server) del ISP al que se conectan los usuarios finales. En este caso la conexión del usuario se limita solo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel. La Figura 2 - 9 muestra un túnel permanente entre un servidor PPTP y por medio del cual van multiplexadas dos sesiones de clientes A y B.

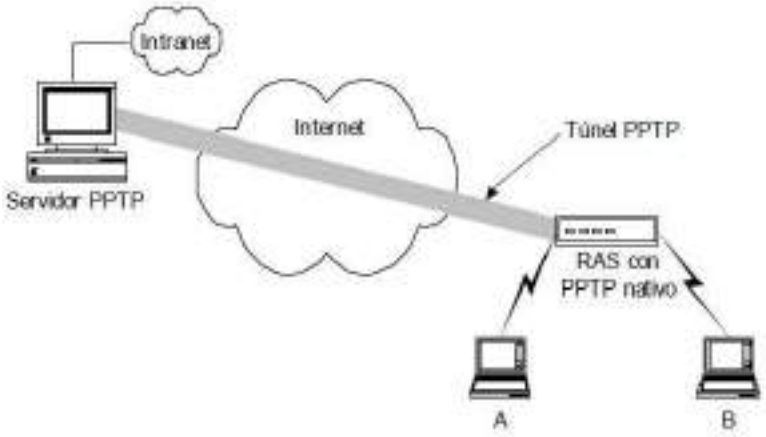


*Figura 2 – 9 Túneles permanentes.*

Encapsulado de la carga útil

PPTP encapsula los paquetes PPP en datagramas IP con un GRE header y un IP header, como se muestra en la Figura 2 - 10. En el IP header están las direcciones IP de origen y destino que corresponden al PAC y al PNS. Cuando los datagramas llegan al PNS, son desencapsulados con la finalidad de obtener el paquete PPP y descifrados de acuerdo al protocolo de red transmitido. El paquete PPP contiene los datos del usuario.

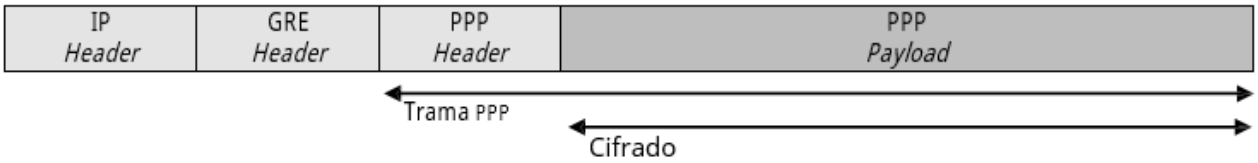


*Figura 2 – 10 Estructura de un paquete PPTP.*

**II.1.1.1.9.2 L2TP (Layer 2 Tunneling Protocol)**

L2TP fue diseñado y aprobado por un grupo de trabajo de la IETF como una evolución y combinación de los protocolos PPTP y L2F (Layer-2 Forwarding) para corregir así las deficiencias de ambos.

L2TP es un protocolo orientado a conexión y utiliza PPP para encapsular los datos de usuario, permitiendo el envío de múltiples protocolos a través del túnel. A diferencia de PPTP, L2TP utiliza UDP como método de encapsulación tanto para el túnel de control como para el de datos de usuario. Mientras PPTP utiliza MPPE como método de cifrado, L2TP posee una solución más segura donde los paquetes L2TP son protegidos por ESP (Encapsulation Security Payload) de IPSec (IP Security) en modo túnel. Aunque puede utilizarse sin IPSec, L2TP por sí sólo no realiza cifrado y por eso debe apoyarse en otros métodos, es por esto que la mayoría de las implementaciones de L2TP incluyen IPSec.

L2TP es considerado como una solución de acceso remoto y consiste de dos dispositivos, un cliente y un servidor. Los túneles de datos y de control utilizados entre estos dos dispositivos usan la misma estructura de paquete, simplificando así su implementación.

Al utilizar PPP para el establecimiento del enlace, L2TP aprovecha las ventajas de los procesos de autenticación y compresión de este protocolo, así como también permite la

utilización de protocolos de autenticación como PAP, CHAP, MS-CHAP, RADIUS (Remote Authentication Dial-In User Server) y servicios de autenticación actuales como EAP (Extensible Authentication Protocol) y sus derivados.

L2TP envía los paquetes por UDP al puerto 1701. La Figura 2 - 11, contiene la estructura de un paquete L2TP, donde se encapsulan las tramas PPP con un L2TP header, un UDP header y IP header.

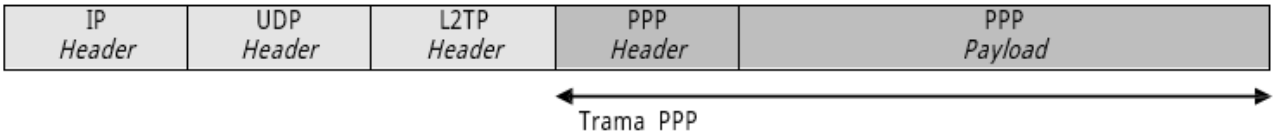


*Figura 2 - 11 Estructura de un paquete L2TP.*

La configuración de túneles L2TP consiste de dos pasos:

- Establecimiento de la conexión de control para el túnel.
- Establecimiento de sesión para la transmisión de los datos de usuario a través del túnel.

Al igual que en PPTP, existen dos tipos de túneles:

- **Voluntario:** El equipo de usuario y el servidor son los puntos extremos del túnel.
- **Obligatorio:** El equipo de usuario no es un punto extremo del túnel, en lugar de este, algunos otros dispositivos ubicados frente al equipo de usuario, como un RAS, actúan como punto extremo del túnel.

Con el túnel voluntario, el cliente de acceso remoto utiliza un software L2TP y crea una conexión con el servidor. Con el túnel obligatorio, otro dispositivo en nombre del usuario es responsable de establecer el túnel. El dispositivo que inicia el túnel es conocido como LAC (L2TP Access Concentrator). El servidor es llamado LNS (L2TP Network Server).

Generalmente, los LAC son utilizados en situaciones donde una empresa no puede manejar las funcionalidades de L2TP en los equipos de usuario, y necesita contratar el

servicio de L2TP VPN en un ISP. De esta manera los clientes establecerán una conexión PPP con el ISP y un dispositivo LAC dentro del mismo ISP será el encargado de enviar a través de un túnel el tráfico PPP a las oficinas corporativas.

El LAC tiene la capacidad de enviar tráfico hacia un destino particular, basado en el número telefónico o nombre de usuario. A través de cualquiera de estos dos métodos, el ISP sabrá qué conexión de túnel LNS utilizar (en el caso de que el ISP preste este servicio a múltiples clientes). El primer usuario que realice una llamada al ISP hará que el LAC plantee la creación de un túnel al LNS ubicado en la oficina corporativa de usuario. Todos los clientes de esta empresa se conectarán a través del mismo LAC utilizando el mismo túnel. Una vez que todos los usuarios se han desconectado del ISP, el LAC terminará el túnel con el LNS.

Como se mencionó anteriormente, el protocolo no posee cifrado de datos y para lidiar con esto L2TP puede ser colocado en la carga útil de un paquete IPSec, combinando las ventajas de seguridad que provee IPSec y los beneficios de la autenticación de usuario, asignación y configuración de direcciones de túnel y soporte a protocolos múltiples con PPP. Esta combinación es comúnmente conocida como L2TP sobre IPSec o L2TP/IPSec.

### II.1.1.1.9.3 L2TP/IPSEC

Debido a que L2TP utiliza IPSec como transporte, la conexión IPSec se establece entre el LAC y el LNS. Primero, debe ser construida una conexión de manejo de claves ISAKMP/IKE (Internet Security Association and Key Management Protocol/Internet Key Exchange), luego debe establecerse una conexión de datos ESP en modo transporte. La información de L2TP es finalmente encapsulada en la carga útil de ESP.

**Mensajes de control L2TP**

L2TP utiliza una sola conexión para transmitir tanto información de control como datos de usuario. Tanto el LAC como el LNS usan el puerto UDP número 1701 como origen y destino.

La estructura típica de un paquete de control L2TP se puede observar en la Figura 2 - 12. IPSec utiliza ESP en modo transporte para compartir mensajes y datos de usuario entre dispositivos. Cuando el LAC y el LNS necesitan establecer, mantener, o cerrar un túnel, la fase 2 de la conexión de datos ESP IPSec es utilizada. Se puede observar que el UDP header, el mensaje L2TP y el ESP trailer son cifrados por ESP y que opcionalmente puede utilizarse la autenticacion ESP para verificar que el origen de los paquetes y que los componentes ESP del paquete IP no han sido alterados.

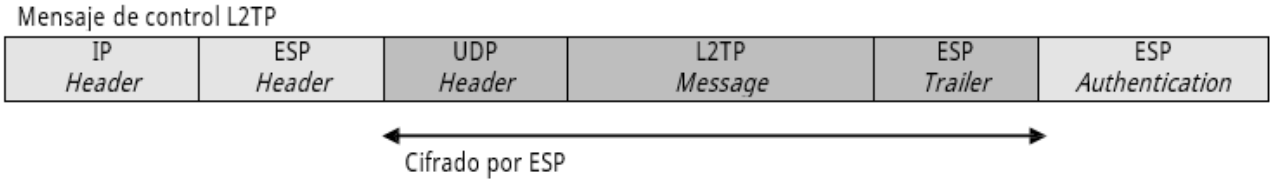


*Figura 2 - 12 Mensaje de control L2TP.*

L2TP se apoya en UDP para asegurarse del envío de mensajes de control. Dentro del mensaje de control existe un campo de Next-Received, este campo funciona de la misma manera que el campo Acknowledgment del TCP header. Otro campo, Next-Sent, cumple la misma función que el campo Sequence Number del TCP header. Estos campos pueden ser usados para control de flujo y de secuencia de los mensajes de control y los paquetes de datos, por ende, cualquier mensaje de control Out-of-Sequence recibido es automaticamente eliminado.

L2TP utiliza los mismos mensajes de control que utiliza PPTP, y como es orientado a conexión, el LNS y el LAC mantienen información de estado por cada llamada de túnel y control. Además de esto, cada sesión entre el LAC y el LNS tendrá un identificador de túnel único (tunnel-ID). Este identificador es empleado para diferenciar las distintas conexiones de túnel entre el LNS y los distintos LACs.

Cuando el túnel es obligatorio, se le asigna un identificador de llamada o sesión único a cada sesión de usuario a través del túnel. Este es empleado para diferenciar a los distintos usuarios (sesiones PPP) que están usando el LAC para conectarse con el LNS a través del

túnel. En caso de que el equipo de usuario cumpla las funciones del LAC, este será un solo valor de identificador de sesión.

**Túnel de datos L2TP**

La Figura 2 - 13, muestra el método de encapsulación utilizado para el tráfico de usuario a través de una conexión L2TP/IPSec. Se puede observar que los datos de usuario son encapsulados en paquetes PPP, y luego son adheridos los headers de L2TP y PPTP para sucesivamente ser encapsulados y protegidos en paquetes ESP.

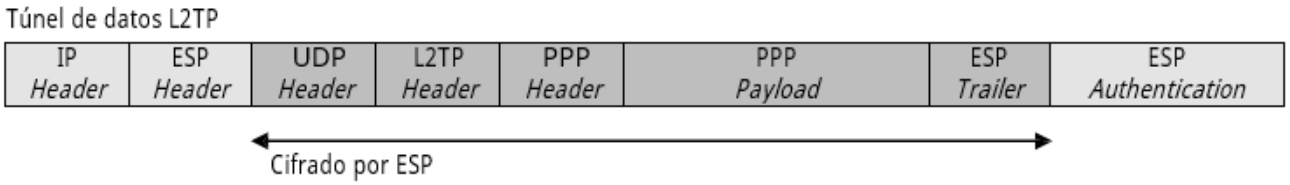


*Figura 2 - 13 Túnel de datos L2TP.*

Cuando un paquete L2TP/IPSec es recibido por el destino, el IP header es removido y la firma digital del paquete ESP es validada. Si la firma es válida, el contenido de L2TP es descifrado. El UDP header es procesado y el paquete L2TP es remitido a proceso L2TP del dispositivo. L2TP revisa los identificadores de túnel y de sesión para determinar el túnel L2TP específico que manejará el paquete. Una vez que el túnel es determinado, el PPP header es utilizado para identificar el tipo de información de la carga útil en el paquete PPP y remitir esta información encapsulada, por ejemplo, un paquete IP, a la pila de protocolos apropiada para su procesamiento.

Dos situaciones comunes para L2TP/IPSec son la protección de comunicaciones entre clientes de acceso remoto y la red corporativa, y la protección de las comunicaciones entre sucursales.

**Clientes de acceso remoto con L2TP/IPSec**

Un requisito habitual es proteger las comunicaciones entre los clientes de acceso remoto y la red corporativa a través de Internet.

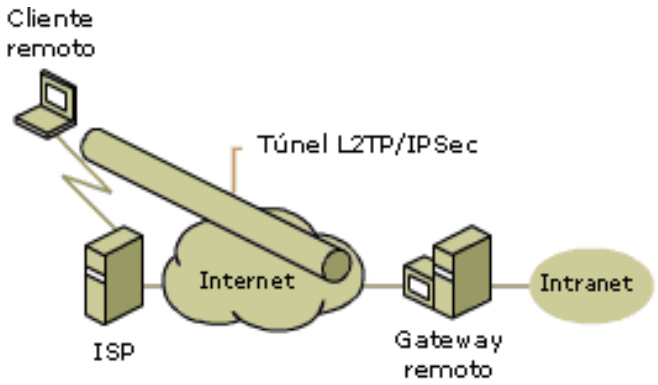


*Figura 2 - 14 Ejemplo de acceso remoto con L2TP/IPSec.*

En el ejemplo de la Figura 2 - 14, el gateway remoto es un servidor que proporciona alta seguridad para la intranet corporativa. El cliente remoto representa un usuario itinerante que precisa obtener acceso frecuente a los recursos y la información de la red. El cliente utiliza un ISP para el acceso a Internet. L2TP se combina con IPSec para proporcionar un modo sencillo y eficaz de construir el túnel y proteger la información a través de Internet.

**Conectar sucursales con L2TP/IPSec**

Las grandes compañías suelen disponer de varias sucursales que necesitan comunicarse.

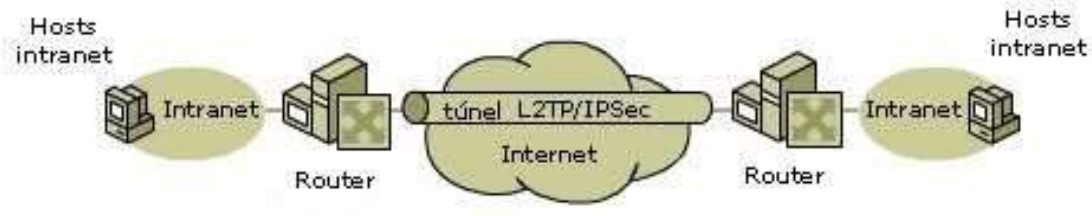


*Figura 2 - 15 conexión de sucursales con L2TP/IPSec.*

En el ejemplo de la Figura 2 - 15, el router proporciona alta seguridad. Es posible que los routers utilicen una línea alquilada, acceso telefónico u otro tipo de conexión a Internet. La AS (Asociación de Seguridad) de IPSec y el túnel L2TP se establecen entre los routers, y permiten la comunicación segura a través de Internet.

### II.1.1.1.9.4 GRE

GRE es una tecnología VPN desarrollada originalmente por Cisco como un método para tomar paquetes de un protocolo, encapsularlos en paquetes IP, y transportarlos a través de una red IP sin tener que configurarla para que soporte protocolos adicionales. Tiene el identificador de protocolo 47 en el paquete IP.

GRE es un protocolo de capa 3 y puede encapsular protocolos como IP, IPX, entre otros. Los paquetes GRE que se utilizan para encapsular los datos tiene el formato que se muestra en la Figura 2 - 16.


*Figura 2 - 16 Estructura de un paquete GRE.*

El header de los paquetes GRE tiene el formato que se muestra en la Figura 2 - 17 . La longitud mínima del GRE header es de 4 octetos.

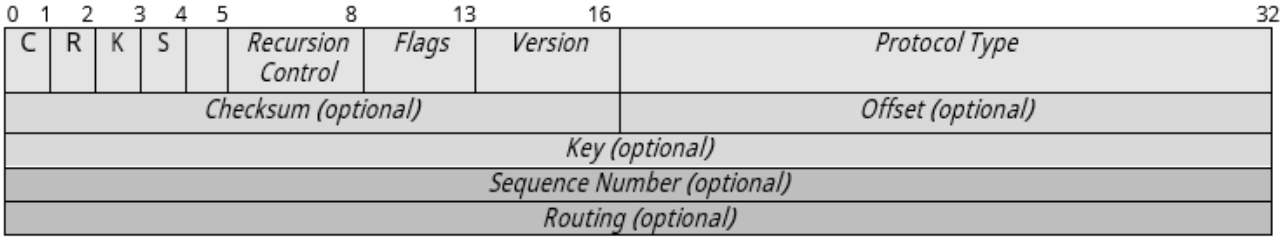


*Figura 2 - 17 GRE header.*

**Descripción de los campos**

- **C:** Presencia del campo de integridad de la trama o Checksum (1 bit). Si el valor es 1 los campos Checksum y Offset están presentes y contienen información válida.
- **R:** Presencia del campo Routing (1 bit). Cuando el valor es 1 el campo Routing está presente y contiene información válida y los campos Checksum y Offset están presentes.
- **K:** Presencia del campo Key (1 bit). Si el valor es 1 el campo Key existe y tiene información válida.
- **S:** Presencia del campo Sequence Number (1 bit). Si el valor es 1 el campo sequence number existe y tiene información válida.

- **s:** Campo Strict Source Route (1 bit). Se recomienda configurar su valor a 1 sólo si toda la información de enrutamiento está formada por rutas estrictas.
- **Recursion Control: (3 bits).** Número de encapsulaciones recursivas permitidas. Por defecto cero.
- **Flags: (5 bits).** Reservado. Por defecto cero.
- **Version: (3 bits).** Versión del protocolo GRE. Debe ser cero.
- **Protocol Type: (16 bits).** Indica el protocolo contenido en el paquete GRE. Para ello utiliza los mismos indicadores que Ethernet.
- **Checksum: (16 bits).** Opcional. Contiene la suma en complemento a 1 de los datos y el GRE header.
- **Offset: (16 bits).** Opcional. Indica el primer octeto a examinar dentro del campo
- routing para conocer la entrada de enrutamiento activa.
- **Key: (32 bits).** Opcional. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizar el destino para propósitos de comprobación del remitente correcto.
- **Sequence Number: (32 bits).** Opcional. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizar el destino para controlar el orden de los paquetes.
- **Routing: (Longitud variable).** Opcional. Este campo consiste en una lista de rutas.

GRE posee dos grandes desventajas. En primer lugar, desde la perspectiva de los productos Cisco, GRE sólo funciona con routers Cisco. En segundo lugar, GRE no realiza tareas de autenticación, cifrado ni chequeo de integridad. Debido a estas dos limitaciones, GRE no es usado como una tecnología VPN completa; sin embargo, puede combinarse con otras soluciones, como IPSec, para crear una solución VPN más robusta y escalable.

### II.1.1.1.9.5 IPSec

IP Security o IPSec, es un conjunto de estándares que proveen las siguientes características claves de seguridad a la capa de red entre dos pares de dispositivos:

- **Confidencialidad:** Utilizando el cifrado para proteger los datos de ataques de escuchas; soporta algoritmos como DES, 3DES y AES.

- **Integridad y autenticación de los datos:** A través de funciones HMAC (Hash-based Message Authentication Code) incluyendo MD5 y SHA-1.
- **Autenticación de dispositivos:** Es soportada con claves pre-compartidas simétricas, claves pre-compartidas asimétricas y certificados digitales.

La IETF define los estándares para IPSec en varios RFCs (Request For Comments). IPSec es comúnmente utilizado en las redes IPv4 e IPv6 de hoy en día, ya que provee protección a nivel de la capa de red entre dispositivos o redes, y es un estándar abierto.

Las dos grandes agrupaciones de estándares que IPSec utiliza son:

- **ISAKMP (Internet Security Association and Key Management Protocol)/IKE (Internet Key Exchange):** Estos estándares son usados para crear una conexión de gestión segura, determinan información clave para el cifrado, y utilizan firmas para la autenticación de dicha conexión para que los dos dispositivos IPSec puedan compartir mensajes entre sí.
- **AH (Authentication Header) y ESP (Encapsulation Security Payload):** Estos estándares son utilizados para proveer protección de los datos de usuario. Pueden proveer confidencialidad (sólo ESP), integridad de los datos, autenticación de origen de los datos, y servicios de anti-replay.

Normalmente, ambas partes de la comunicación requieren una configuración de IPSec (denominada directiva IPSec) para establecer las opciones y los parámetros de seguridad que permitirán que ambos sistemas acuerden el modo de proteger el tráfico entre ellos. Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro.

La seguridad ofrecida por el uso de IPSec es críticamente dependiente en muchos aspectos del entorno de operaciones en el que se ejecuta la implementación de IPSec. Por ejemplo, defectos en la seguridad en el sistema operativo, prácticas y protocolo de manejo de sistemas descuidado, entre otros aspectos, pueden todos degradar la seguridad proporcionada por IPSec.

**Modos de conexión IPSec**

IPSec fue proyectado para proporcionar seguridad en modo transporte o extremo a extremo del tráfico de paquetes, en el que los equipos de los extremos finales llevan a cabo el proceso de seguridad, o en modo túnel o gateway a gateway en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas, incluso a toda la red de área local, por un único nodo. A continuación se describen los modos de conexión IPSec.

**Modo transporte**

En el modo transporte sólo la carga útil del paquete IP es cifrada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra el IP header. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas. El modo transporte se utiliza para comunicaciones end-to-end.

**Modo túnel**

En el modo túnel, todo el paquete IP (es decir, los datos más los headers del mensaje) es cifrado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza principalmente para comunicaciones sitio-a-sitio (túneles seguros entre routers o firewalls).

El motivo principal por el que se utiliza el modo de túnel IPSec es la interoperabilidad con otros routers, gateways o sistemas finales que no son compatibles con los túneles de VPN L2TP/IPSec o PPTP.

**Protocolos de seguridad IPSec**

Los servicios IPSec son llevados a cabo mediante el uso de protocolos de seguridad, así como también mediante un conjunto de protocolos necesarios para la gestión de claves criptográficas que se definirán en la siguiente sección .

**AH (Authentication Header)**

El protocolo AH proporciona únicamente mecanismos de autenticación. Como se ilustra en la Figura 2 - 18, en modo transporte los datos de autenticación AH son insertados entre el IP header y los datos referentes al paquete de nivel superior (TCP, UDP, ICMP).

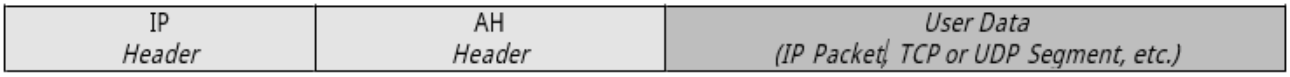


*Figura 2 - 18 Paquete IPSec con el AH header.*

AH tiene asignado el número de protocolo 51. Éste es el número que lleva el IP header en el campo Protocol, en lugar de los valores 6 o 7 que corresponden a TCP y UDP, respectivamente.

En la Figura 2 - 19 se pueden observar los campos del AH header.

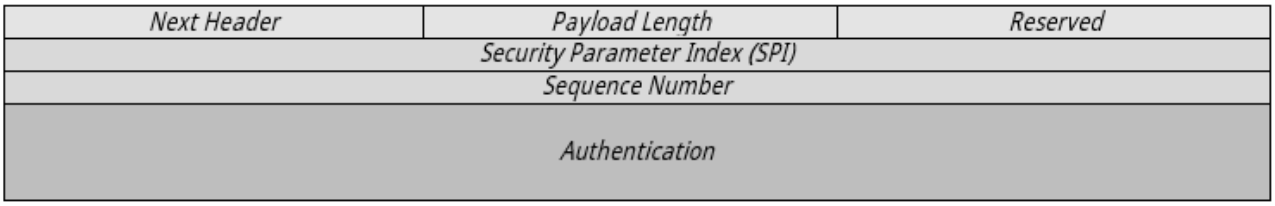


*Figura 2 - 19 AH header.*

El AH header está formado por los siguientes campos:

- Un campo Next Header el cual identifica el protocolo que se está llevando, como por ejemplo TCP.
- El campo Payload Length indica el tamaño del AH header.
- El campo Security Parameter Index (SPI) es utilizado para identificar la asociación de seguridad con la que se protege el paquete.
- Con el Sequence Number se provee protección contra ataques de réplicas de los paquetes.
- El campo Authentication es de tamaño variable, y contiene el Integrity Check Value (ICV) o Message Authentication Code (MAC) para ese datagrama, utilizando una función hash que puede ser MD5 o SHA.

En la Figura 20, se puede observar el mecanismo de autenticación AH en donde se tiene un mensaje original al cual se le aplica una función de hash con una clave y se obtiene un MAC y esa información es colocada en el AH header para posteriormente agregarlo entre el IP header y la carga útil de IP. Luego cuando el mensaje es recibido el receptor le aplica un hash con la misma clave y obtiene el MAC del mensaje recibido y lo compara con el MAC que se encuentra en el header de AH y si son iguales el paquete es autenticado y en caso contrario se asume que el paquete está alterado.

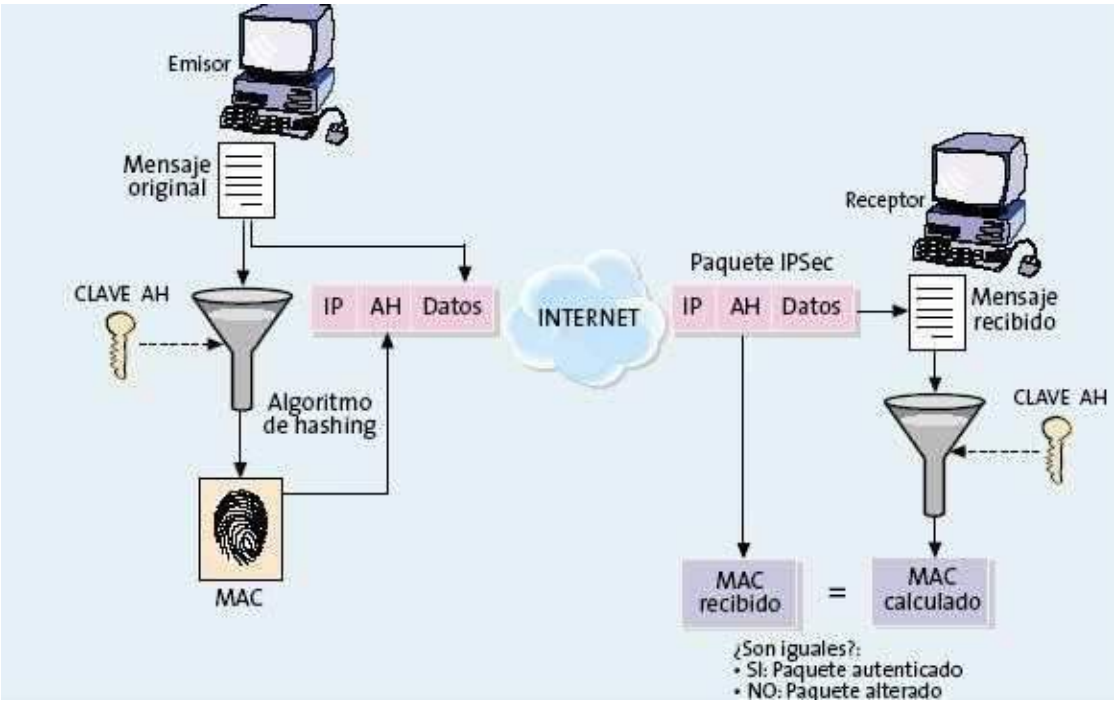


*Figura 2 - 20 Mecanismo de autenticación AH.*

El modo de túnel AH encapsula un paquete IP con un AH header y un nuevo IP header y firma todo el paquete para asegurar su integridad y autenticación, como se muestra en la Figura 2 - 21.

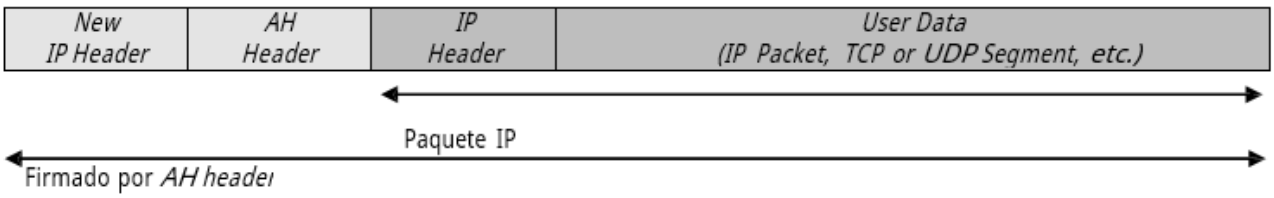


*Figura 2 - 21: Un datagrama IPSec-AH en modo túnel.*

**ESP (Encapsulation Security Payload)**

El protocolo ESP proporciona confidencialidad, autenticación, integridad y protección contra réplica para la carga útil IP. ESP hace uso de una amplia variedad de algoritmos de cifrado entre los cuales se encuentran DES, 3DES y Blowfish. La carga útil IP está cifrada para su confidencialidad y firmada para garantizar su integridad y autenticación. Al recibirse, una vez completado el proceso de comprobación de la integridad, se descifra la carga de datos del paquete.

ESP trabaja a nivel de la capa de enlace de datos y se identifica con el número de protocolo 50. En modo transporte, el ESP header se coloca delante de la carga IP, y tras ella se incluye un ESP trailer y un ICV, como se ilustra en la Figura 2 - 22.

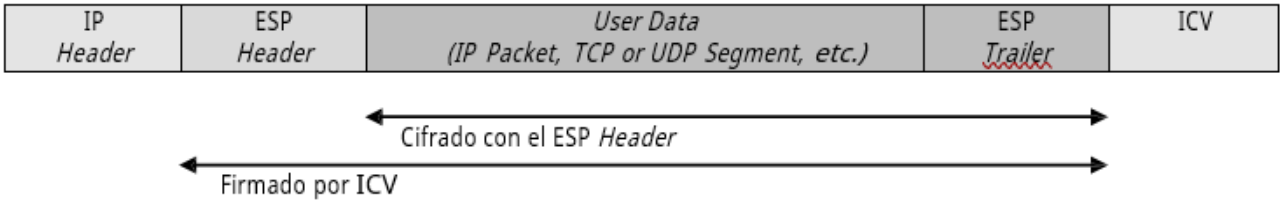


*Figura 2 - 22 Paquete IPSec con ESP header y ESP trailer.*

El IP header no se firma y no está necesariamente protegido frente a modificaciones. Para proporcionar integridad de datos y autenticación al IP header, puede utilizarse ESP conjuntamente con AH. En la Figura 23 se puede observar el ESP header.

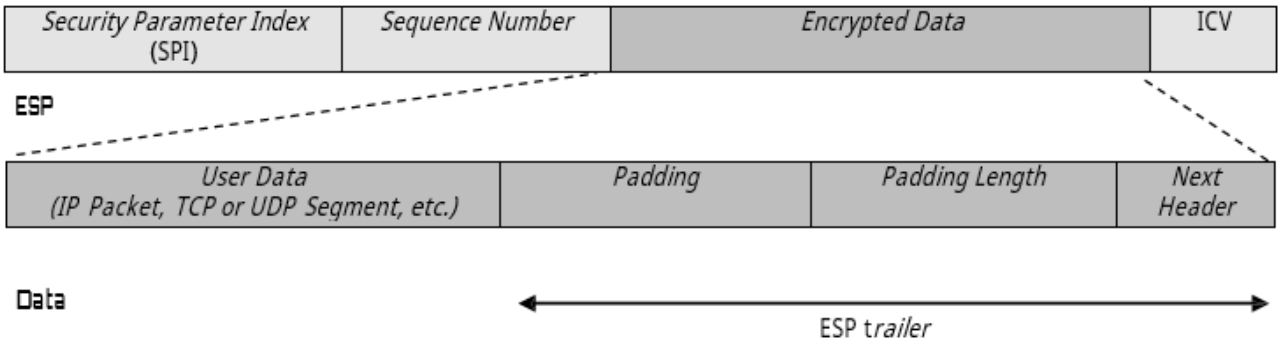


*Figura 2 - 23 Campos del paquete ESP.*

A continuación, se describen los campos del paquete ESP.

El campo SPI identifica la asociación de seguridad correcta para la comunicación cuando se utiliza junto con la dirección de destino y el protocolo de seguridad (AH o ESP). El receptor utiliza este valor para determinar la asociación de seguridad con la que se debe identificar este paquete.

El Sequence Number es un número de 32 bits que indica el número de paquetes enviados a través de la asociación de seguridad para una comunicación dada. El sequence number no se puede repetir mientras perdure la asociación de seguridad. El receptor comprueba este campo para asegurarse de que no ha recibido ya un paquete para una asociación de seguridad con este número; si se recibió alguno, se rechazará este paquete.

El ESP trailer contiene el campo de Padding en donde se coloca un valor entre 0 y 255 bytes y asegura que la carga cifrada junto con los bytes de relleno se ajuste a los límites de bytes que requieren los algoritmos de cifrado.

El campo Padding Length indica la longitud en bytes del campo Padding. El receptor utiliza este campo para eliminar los bytes de relleno una vez descifrada la carga que los contiene.

El campo Next Header identifica el tipo de datos de la carga, por ejemplo TCP o UDP.

El ESP Trailer contiene el ICV que se utiliza para comprobar la autenticación del mensaje y su integridad. El receptor calcula el valor del ICV y lo compara con este valor (calculado por el origen) para comprobar la integridad. El ICV se calcula para el ESP header, los datos de la carga y el ESP trailer.

El modo túnel ESP encapsula un paquete IP con un ESP header, un nuevo IP header y un ICV, como se ilustra en la Figura 2.24. Debido al nuevo header agregado al paquete para el túnel, todo lo que se encuentra a partir del ESP header está firmado, excepto el ICV. El IP header original se coloca después del ESP header. El paquete entero se anexará con un ESP trailer antes del cifrado. Todo lo que sigue al ESP header, salvo el ICV, se cifra. Esto incluye el IP header original, que ahora se considera parte de los datos del paquete.

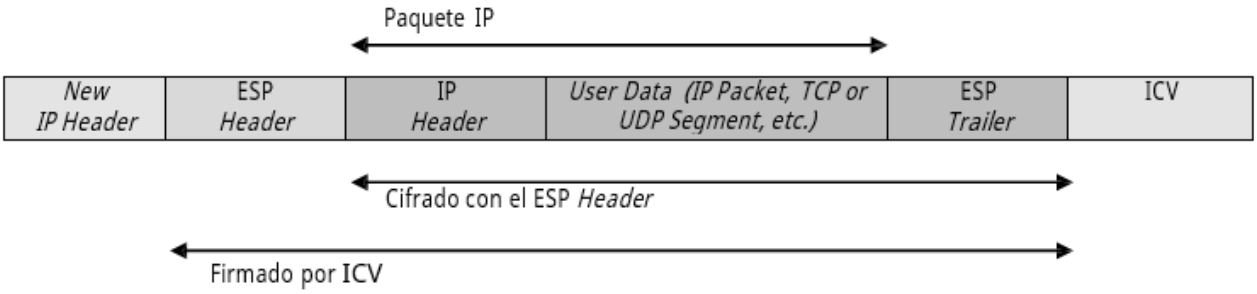


*Figura 2 - 24: Un paquete IPSec-ESP en modo túnel.*

Toda la carga ESP se encapsula dentro del nuevo header de túnel, el cual no se cifra. La información del nuevo header de túnel sólo se utiliza para enrutar el paquete desde el origen hasta el destino. Si el paquete se envía a través de una red pública, se enrutará hacia la dirección IP del servidor de túnel de la intranet receptora. En la mayoría de los casos, el paquete irá destinado a un equipo de una intranet. El servidor de túnel descifra el paquete, descarta el ESP header y utiliza el IP header original para enrutar el paquete hacia el equipo de la intranet.

AH y ESP pueden combinarse al utilizar túneles para lograr tanto la confidencialidad del paquete IP enviado por el túnel como la integridad y la autenticación de todo el paquete.

**Asociaciones de seguridad**

Las asociaciones de seguridad (AS) son acuerdos que se establecen entre dos equipos antes del intercambio de información protegida y especifican los servicios de seguridad que se aplicarán al tráfico correspondiente. Estos servicios son ofrecidos por una AS mediante el uso de los headers AH o ESP, pero no ambos. Una AS puede ser una conexión IPSec entre dos dispositivos finales, entre dos dispositivos VPN, o incluso entre un dispositivo final y un dispositivo extremo de un túnel IPSec. Dichos equipos establecen el modo de intercambiar y proteger la información, como se muestra en la Figura 2 - 25.

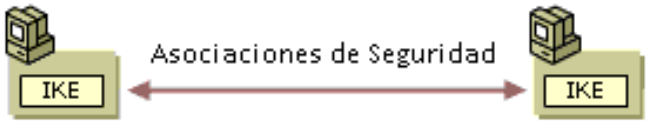


*Figura 2 - 25: Asociación de seguridad.*

Todos los parámetros necesarios para que los participantes de una comunicación puedan encapsular y desencapsular paquetes IPSec, se almacenan en la AS y estas a su vez se almacenan en bases de datos de asociaciones de seguridad.

Cada asociación de seguridad define los siguientes parámetros de una conexión IPSec que conjuntamente definen el método de seguridad utilizado para proteger la comunicación desde el origen hasta el destino:

- Dirección IP origen y destino de la comunicación, que normalmente es una dirección unicast, aunque también puede ser una dirección broadcast o una dirección multicast.
- Protocolo de seguridad, AH o ESP. Una AS permite protocolos de seguridad mediante el uso de AH o de ESP pero no de ambos.
- Algoritmo de cifrado y autenticación a usar en las comunicaciones.
- Clave secreta.
- Tiempos de vida de las claves y de la propia AS.
- Modo IPSec, modo transporte o modo túnel.
- SPI, es un número de 32 bits elegido aleatoriamente que identifica la asociación de seguridad.

Como se mencionó anteriormente, en una AS se definen las direcciones IP de origen y destino de la comunicación, por ello mediante una única AS sólo se puede proteger un sentido del tráfico en una comunicación IPSec full duplex. Para proteger ambos sentidos de la comunicación, IPSec necesita de dos AS unidireccionales, es decir, habrá dos AS por cada conexión (una en cada sentido). Además, dos mismos extremos pueden establecer múltiples pares de AS, uno para cada sesión de comunicaciones.

Básicamente, cada AS se identifica por medio del SPI y por la dirección de destino correspondiente, algunos incluyen también un identificador de protocolo de seguridad (AH o ESP). El número en cuestión se inserta en el encabezamiento IPSec. En el otro extremo dicho número permite identificar la AS correspondiente y por lo tanto, su procesamiento.

Es importante mencionar que las AS sólo especifican cómo se supone que IPSec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad. Para establecer o mantener las AS se utiliza un protocolo denominado ISAKMP/IKE.

**Protocolo ISAKMP/IKE**

ISAKMP (Internet Security Association and Key Management Protocol) es utilizado para negociar AS de manera segura y autenticada, y las políticas para proteger la comunicación, a través de un intercambio seguro de claves. De esta manera proporciona un método para centralizar la administración y creación de AS.

IKE (Internet Key Exchange) es un protocolo estándar de asociación de seguridad y resolución de intercambio de claves, establecido por la IETF.

ISAKMP e IKE trabajan juntos para establecer conexiones seguras entre dos dispositivos. ISAKMP define el formato del mensaje, el mecanismo del protocolo de intercambio de claves y el proceso de negociación para construir conexiones. ISAKMP, sin embargo, no define como las claves son creadas, compartidas, o manejadas para proteger las conexiones seguras; IKE es responsable de esto.

ISAKMP/IKE presentan tres características principales:

- Asegura que la comunicación IPSec y el intercambio de claves se lleve a cabo entre partes autenticadas.
- Negocia los protocolos, algoritmos, y claves que serán utilizados en la comunicación IPSec.
- Proporciona un método seguro para actualizar y renegociar asociaciones una vez que éstas han expirado.

De este modo, se resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. IPSec implementa ISAKMP/IKE en dos fases. En la primera fase, los dos

extremos crean una conexión de gestión, estableciendo así un canal seguro entre ellos. Ya en la segunda fase, esta conexión será empleada para establecer la conexión de datos. La confidencialidad y la autenticación se aseguran durante cada una de las fases mediante el uso del cifrado y los algoritmos de autenticación acordados entre los dos equipos durante las negociaciones de seguridad. Al estar las tareas divididas entre las dos fases se agiliza la creación de claves.

**Fases ISAKMP/IKE**

En la Figura 2 - 26, se resumen los pasos de las dos fases de IKE.


*Figura 2 - 26: Fases de ISAKMP/IKE.*

**Fase 1 ISAKMP/IKE**

Esta fase se realiza a través del intercambio de 6 mensajes, es por ello que se dice que se realiza en modo principal y puede verse como el establecimiento de la política básica de seguridad.

En una primera parte (mensajes 1 y 2) se negocian las características de las AS ISAKMP/IKE, mediante la definición de directivas. Una directiva es una lista de aspectos de seguridad que deben ser utilizados para proteger la conexión, estos son:

- Algoritmo de cifrado: DES, 3DES o AES.
- Algoritmo de integridad: MD5 o SHA1.

- Grupo Diffie-Hellman: Grupo 1, 2, 5 o 7 que se utilizará para el material base de generación de claves.
- Método de autenticación: Certificados digitales o autenticación por claves pre-compartidas.

La segunda parte del modo principal (mensajes 3 y 4) se refiere especialmente al intercambio Diffie-Hellman, las claves reales no se intercambian en ningún momento. Sólo se intercambia la información básica que requiere el algoritmo de determinación de la clave Diffie-Hellman para generar la clave secreta compartida. Después de este intercambio, el servicio ISAKMP/IKE de cada equipo genera la clave principal utilizada para proteger la autenticación.
Finalmente (mensajes 5 y 6) los dispositivos proveen una autenticación mutua (se aseguran de que su interlocutor es quien dice ser). Si se produce un error en la autenticación, no se continuará con la comunicación. Para autenticar las identidades se utiliza la clave principal junto con los algoritmos y métodos de negociación. Los algoritmos de hash y cifrado se aplican a toda la carga de identidad mediante las claves generadas a partir del intercambio Diffie-Hellman del segundo paso.

El origen presenta una oferta para establecer una posible asociación de seguridad con el destino. El destino no puede modificar la oferta. En caso de que se modifique la oferta, el origen rechazará el mensaje del destino. El destino envía una respuesta para aceptar la oferta o bien una respuesta con alternativas, de esta manera se establece un canal seguro. Una vez que un dispositivo reconoce la identidad del otro y viceversa, los intercambios de información bajo ISAKMP/IKE se realizan por medio de mensajes en el puerto 500 de UDP.

Esta primera fase también suele soportar un modo agresivo (sólo usa la mitad de los mensajes para alcanzar su objetivo), aunque este no proteja identidades. Sea cual sea el modo, los participantes son autenticados.

**Fase 2 ISAKMP/IKE**

Una vez establecido un canal seguro en la fase 1 se inicia la fase 2 que se realiza en el modo agresivo o rápido por medio de tres mensajes. Esta fase define las AS y las claves de IPSec.

En el primer mensaje el dispositivo origen indica al destino el tipo de protocolo de seguridad a utilizar (ESP, AH o ESP+AH) incluyendo el SPI, así como los algoritmos de hash para la integridad y autenticación (MD5 o SHA1) y para el cifrado, si se solicita (DES, 3DES o AES). De esta manera, se llega a un acuerdo y se establecen dos AS, una para la comunicación entrante y otra para la comunicación saliente.

Con el segundo mensaje, y previa autenticación, el destino reconoce y acepta el uso de lo establecido en el primer mensaje. Si es necesario, el material de clave de sesión se actualiza generando nuevas claves compartidas e intercambiándolas para la integridad de los datos, la autenticación y el cifrado.

Finalmente, el tercer mensaje simplemente indica que el origen está en funcionamiento, tras lo cual ambos dispositivos pueden comenzar a usar los protocolos en cuestión.

Esta segunda negociación de la configuración de seguridad y el material de claves (con el fin de proteger los datos) está protegida por la conexión de gestión. Mientras que la primera fase protege la identidad, la segunda fase proporciona protección mediante la actualización del material de las claves antes de enviar los datos. Mientras la conexión de gestión no caduque, no es necesario volver a negociar o a autenticar.

**Conexiones IPSec**

En la siguiente sección se describirá el proceso de comunicación para compartir de manera segura los datos entre dos dispositivos IPSec.

Un administrador o usuario inicia el proceso de IPSec manualmente desde uno de los dos dispositivos.

Si no existe una conexión VPN, IPSec utilizará la fase 1 ISAKMP/IKE para construir una conexión de gestión segura. Esta conexión es usada para que los dispositivos puedan comunicarse entre ellos de manera segura, vía IPSec, y puedan construir conexiones de datos.

A través de la conexión gestión, los dispositvos IPSec negociarán los parámetros de seguridad que son usados para construir las conexiones de datos; dichas conexiones son utilizadas para transmitir los datos de usuario como archivos, mensajes de correo electrónico, video, y voz.

Una vez que las conexiones de datos son creadas, los dispositivos IPSec pueden utilizarlas para compartir datos de usuario de manera segura. Si son usadas funciones HMAC por la fuente para crear firmas, el destino las verifica para la integridad de los datos y autenticación; además, si los datos están cifrados por el origen, el destino descifrará los datos.

Tanto la conexión de gestión como la conexión de datos tienen un tiempo de vida asociado a ellas. Esto asegura que la información clave es regenerada para proveer mayor seguridad en caso de que alguien esté tratando de romper las claves de seguridad. Una vez que el tiempo de vida de una conexión es alcanzado, esta es terminada. Por supuesto, si aun se necesita enviar datos, la conexión será reconstruida dinámicamente.

### II.1.1.1.9.6 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. SSL/TLS permite la autenticación tanto de cliente como 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.

Hay que destacar que SSL/TLS se compone de cuatro protocolos, como se muestra en la Figura 27. En la siguiente sección se definen estos cuatro protocolos:

- **Record Protocol:** Encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro.
- **Handshake Protocol:** Se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para cifrar.
- **Change Cipher Spec Protocol:** Utiliza un mensaje de un byte para notificar cambios en la estrategia de cifrado.
- **Alert Protocol:** Señaliza alertas y errores en la sesión establecida.

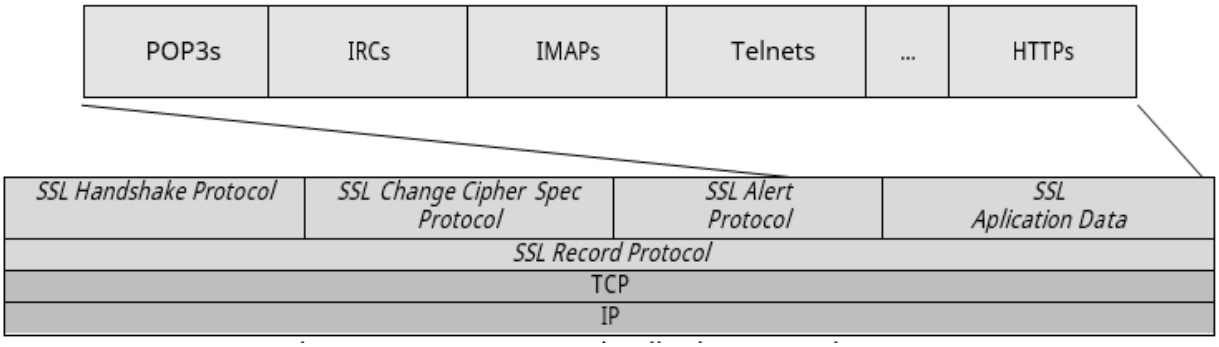


*Figura 2 - 27: SSL/TLS en la pila de protocolos OSI.*

Existen diversas implementaciones del protocolo, tanto comerciales como de libre distribución siendo una de las más populares la biblioteca OpenSSL.

SSL es capaz de interactuar con la mayoría de protocolos que trabajan sobre TCP de tal manera que la IANA les tiene asignado un número de puerto por defecto, por ejemplo el protocolo HTTP sobre SSL ha sido denominado HTTPS (Hypertext Transfer Protocol Secure) y utiliza el puerto TCP 443.

SSL se basa en un esquema de clave pública para el intercambio de claves de sesión. En primer lugar, el cliente y el servidor intercambian una clave mediante un algoritmo de cifrado asimétrico como RSA (Rivest-Shamir-Adleman) o Diffie-Hellman utilizando certificados. Mediante esa clave se establece un canal seguro, utilizando para ello un algoritmo simétrico previamente negociado. Los mensajes a ser transmitidos se fragmentan en bloques, se comprimen y se les aplica un algoritmo hash para obtener un resumen que asegure la integridad.

**Funcionamiento de SSL/TLS**

El funcionamiento de SSL/TLS está comprendido por una sesión y una conexión. En SSL/TLS una sesión es una asociación entre un cliente y un servidor. Las sesiones se crean mediante el protocolo Handshake y coordina los estados del cliente y del servidor. El estado de una sesión incluye la siguiente información:

- **Identificador de Sesión:** Consiste en una secuencia arbitraria de bytes elegida por el servidor para identificar una sesión activa.
- **Certificado de la Entidad Par:** El certificado del otro extremo de la comunicación (puede ser nulo).
- **Método de Compresión:** Indica el algoritmo usado para comprimir los datos antes de cifrarlos.
- **Especificación de Cifrado:** Especifica el algoritmo de cifrado de datos (DES, AES, etc.) y el algoritmo HMAC (MD5 o SHA-1). También define atributos como el tamaño del Hash.
- **Clave Maestra:** Una clave secreta de 48 bytes intercambiada entre cliente y servidor.

En SSL/TLS una conexión es transitoria y está asociada solamente a una sesión, mientras que una sesión puede tener múltiples conexiones. En otras palabras, las sesiones se usan para evitar la costosa negociación de los parámetros de cada conexión. El estado de una conexión incluye la siguiente información:

- **Valores aleatorios del servidor y del cliente:** Secuencia de bytes elegidos por el servidor y el cliente para cada conexión.
- **Clave secreta HMAC de escritura del servidor:** Secreto utilizado en operaciones HMAC sobre los datos del servidor.
- **Clave secreta HMAC de escritura del cliente:** Secreto utilizado en operaciones HMAC sobre los datos del cliente.
- **Clave de escritura del servidor:** Clave secreta para el cifrado de datos por el servidor y descifrado de datos por el cliente.
- **Clave de escritura del cliente:** Clave secreta para el cifrado de datos por el cliente y descifrado de datos por el servidor.

- **Vector de Inicialización (IV) del cliente y servidor:** Vectores de inicialización utilizados para bloques de cifrado.
- **Número de secuencia:** Cada estado de conexión contiene un número de secuencia que se mantiene independientemente para los estados de lectura y escritura. El número de secuencia debe ser inicializado en cero cada vez que un estado de conexión pasa a estado activo.

EL SSL/TLS Record Protocol es el protocolo de transporte que proporciona a cada conexión:

- **Confidencialidad:** Utilizando una clave compartida generada durante el protocolo Handshake para el cifrado convencional de los datos.
- **Integridad del mensaje:** El protocolo de Handshake también genera una clave secreta común que se usa para formar el HMAC o código de autenticación del mensaje.

En el funcionamiento del SSL Record Protocol intervienen mecanismos criptográficos, para los cuales son necesarios ciertos parámetros como la clave secreta para el cifrado. Estos parámetros se negocian durante el establecimiento del protocolo Handshake, que además permite la autenticación de cliente y servidor.

Como se muestra en la Figura 2 - 28, el proceso que sigue el SSL/TLS Record Protocol es el siguiente:

- Los mensajes se fragmentan en bloques de 214 bytes o menos.
- Se aplica compresión opcionalmente.
- Se calcula un HMAC o una función hash sobre los datos comprimidos.
- El HMAC junto con el mensaje se cifra con un algoritmo simétrico.
- Finalmente se le añade un header de registro o SSL Record Header

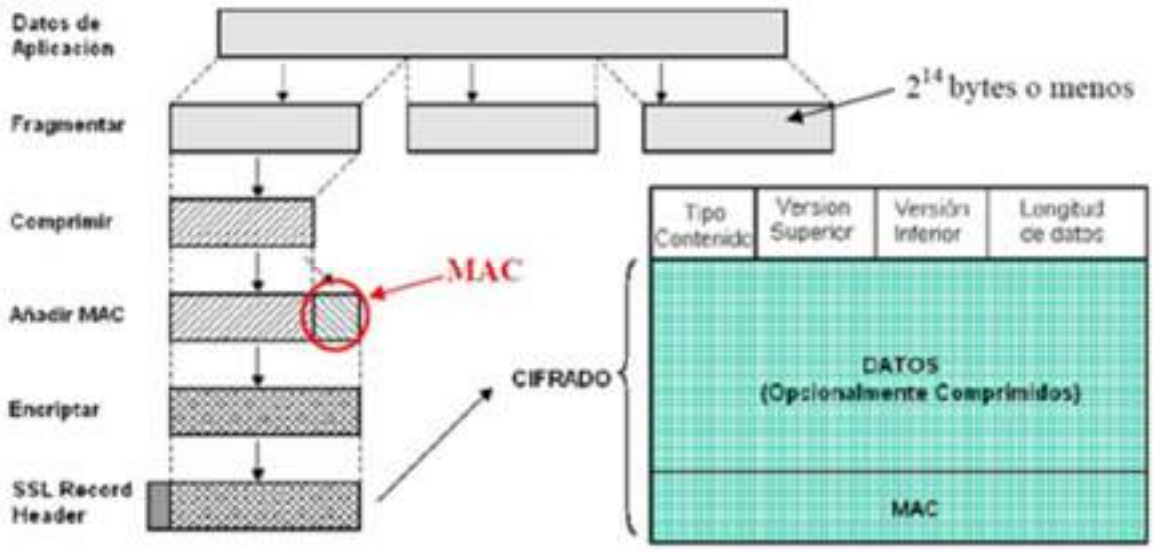


*Figura 2 - 28: Cifrado y formato de datos de aplicación con Récord Protocol.*

Los algoritmos de cifrado soportados por SSL son los que se muestran en la Tabla 1.

| Tipo de Cifrado | Algoritmo | Tamaño K |
|---|---|---|
| Cifrado Bloque | IDEA | 128 |
| | DES | 56 |
| | 3DES | 112 |
| | RSA | 1024 |
| | DSA | 1024 |
| Cifrado Flujo | RC4-40 | 40 |
| | RC4-128 | 128 |

*Figura 2 - 29 Algoritmos de cifrado soportados por SSL/TLS.*

El protocolo Change Cipher Spec utiliza un único mensaje de un byte de valor 1 que tiene como objetivo pasar del modo pendiente, para negociar los parámetros de una conexión, al modo operativo, en el que los parámetros ya se han establecido y la comunicación es totalmente segura.

El tercer protocolo de SSL/TLS, Alert Protocol, tiene como objetivo transmitir alertas mediante mensajes de 2 bytes.

El cuarto protocolo y más importante que forma SSL/TLS es el Handshake Protocol, mediante este protocolo se generan los parámetros criptográficos que van a definir el estado de una sesión (una sesión SSL/TLS siempre empieza con el Handshake). Este

protocolo permite la autenticación entre el cliente y el servidor y la negociación de los algoritmos de cifrado y las claves y subclaves. Este protocolo consta de cuatro fases en los que se negocian los parámetros de una sesión:

- **Fase 1:** Se establecen las características de seguridad (versión de protocolo, identificador de sesión, suite de cifrado, método de compresión y números aleatorios iniciales).
- **Fase 2:** En esta fase el servidor puede enviar un certificado, intercambio de clave y solicitud de certificado.
- **Fase 3:** El cliente envía su certificado, en caso de habérselo solicitado, el intercambio de clave y puede enviar verificación de certificado.
- **Fase 4:** Se produce el intercambio de suite de cifrado y finalización del protocolo Handshake. En esta fase se completa el establecimiento de la conexión segura.

### II.1.1.1.9.7 OpenVPN

OpenVPN es una solución de conectividad basada en software de código abierto (publicado bajo la licencia GPL) para soluciones VPN SSL/TLS11, creada por James Yonan en el año 2001. OpenVPN ofrece conectividad punto a punto con validación de usuarios y host conectados remotamente, además de una variedad de configuraciones VPN basadas en SSL/TLS, incluyendo acceso remoto, sitio-a-sitio, seguridad para redes inalámbricas bajo el estándar IEEE 802.11, soluciones de balanceo de carga, respuesta ante fallos y diferentes técnicas de control de acceso. OpenVPN tiene asignado y reservado el puerto 1194 de manera oficial por la IANA.

Esta herramienta implementa redes seguras en la capa 2 o 3 del modelo de referencia OSI utilizando como extensión el protocolo SSL/TLS y soportando métodos de autenticación del cliente de manera flexible mediante dos factores: permite utilizar políticas de acceso a usuarios y grupos específicos, y reglas de firewall aplicadas a las interfaces virtuales utilizadas por OpenVPN para el filtrado de paquetes IP. OpenVPN no es una aplicación web Proxy ni opera a través de un navegador web.

OpenVPN es una herramienta multiplataforma, soportada en sistemas operativos como Linux, Windows 2000/XP, Vista y 7, OpenBSD, FreeBSD, NetBSD, Mac OS X, Solaris, entre otros. Ofrece compatibilidad con la infraestructura de clave pública (PKI, Public Key Infrastructure) mediante el uso de certificados X.509 y la técnica de intercambio de claves RSA, compatible con NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol) y con los dispositivos de red virtuales TUN/TAP. Por el contrario, OpenVPN no ofrece compatibilidad con estándares tales como IPSec, IKE, PPTP o L2TP.

Por otra parte, OpenVPN permite encapsular el tráfico en paquetes que utilicen como protocolo de transporte TCP o UDP, como se puede observar en la Figura 29. Otra característica en las versiones más recientes de OpenVPN es la posibilidad de utilizar un único puerto en el servidor para todas las conexiones VPN o de soportar más de una conexión TCP.

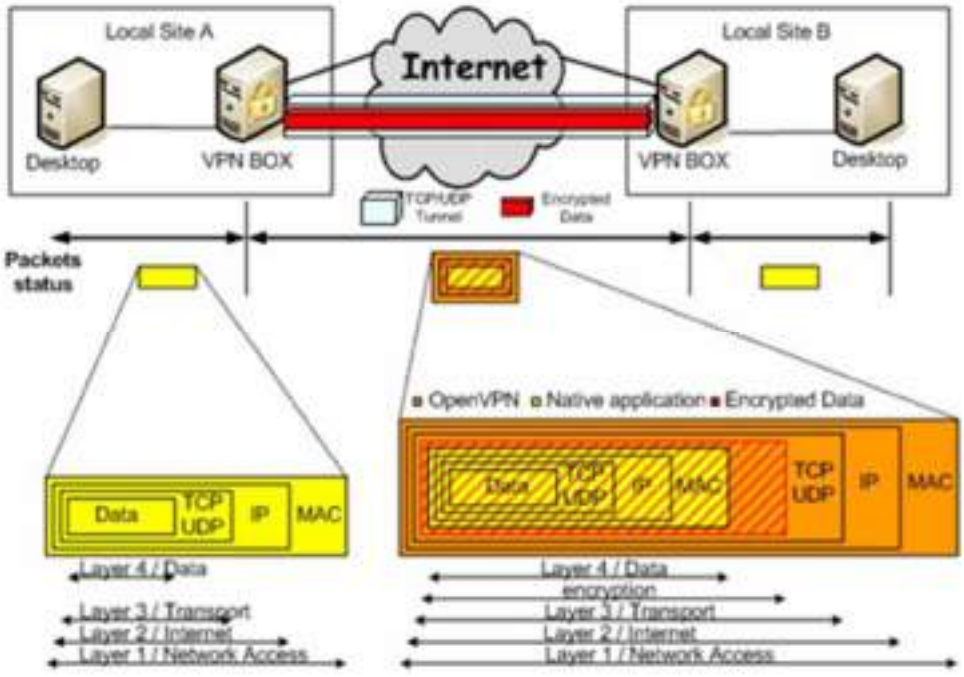


*Figura 2 - 30 Formato del paquete encapsulado por OpenVPN.*

OpenVPN encapsula en un mismo datagrama UDP (o TCP, pero no recomendado) los canales de control y datos. Es decir, utiliza el mismo puerto para ambos canales, por lo que un datagrama UDP puede contener un mensaje de control y de datos a la vez.
Además, un paquete de OpenVPN puede contener información IP o una trama Ethernet pudiendo operar a nivel IP o a nivel de enlace. Utilizando UDP como protocolo encapsulador se obtiene una encapsulación del paquete original como la que se observa en la Figura 2 - 31.

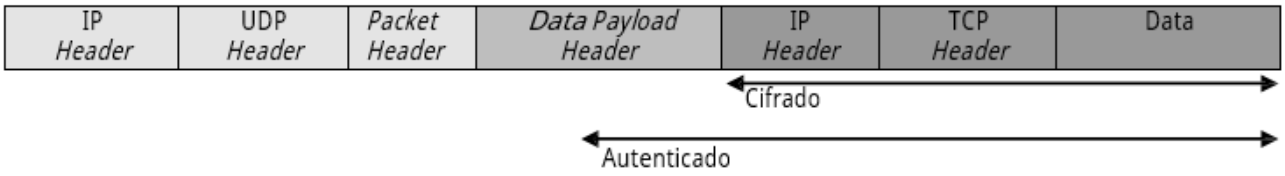


*Figura 2 – 31 Encapsulación del canal de datos en OpenVPN.*

OpenVPN divide el campo Data Payload Header en dos partes: el Packet Header, que identifica el tipo de paquete y los parámetros para las claves, y el Data Payload Header, que contiene parámetros de autentificación, vector de inicialización y campos de número de secuencia del paquete de datos.

El formato de un paquete de control de OpenVPN se observa en la Figura 2 - 32.

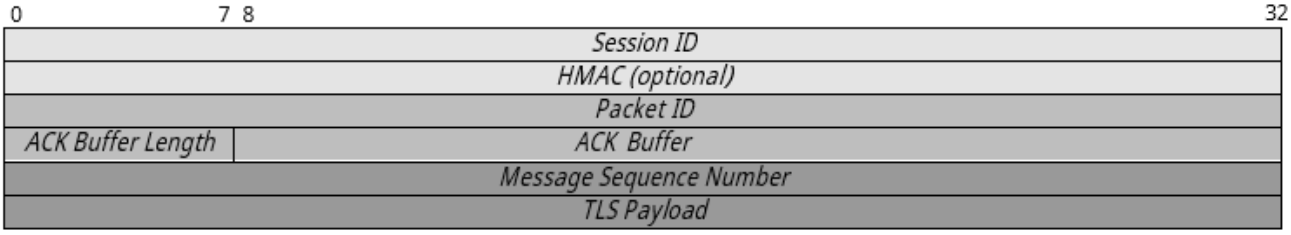


*Figura 2 – 32 Formato del paquete de control de OpenVPN.*

**Descripción de los campos:**

- **Session ID: (64 bits aleatorios).** Identifica la sesión TLS.
- **HMAC: (16 - 20 bytes).** Función que se aplica a todo el header de encapsulación para obtener integridad y poder prevenir ataques de denegación de servicio (DoS).

- **Packet ID: (32 – 64 bits).** Incluye el número de secuencia. Realiza la misma función en los paquetes de datos y en los paquetes de control.
- **ACK Buffer Length: (1 byte).** Indica el número de reconocimientos que hay en el buffer de ACK. Cuando este valor es cero, el buffer de reconocimientos ACK no existe.
- **ACK Buffer: (si ACK Buffer Length > 0).** Realiza el reconocimiento de paquetes entre ambos puntos de la comunicación.
- **ACK Remote Session ID: (si ACK Buffer Length > 0).** Representa el indicador de sesión (session ID) de los pares que componen la VPN. Estos participantes de la VPN utilizan el session ID para enlazar los reconocimientos ACK a una sesión VPN particular.
- **Message Sequence Number: (32 bits).** Número de secuencia del paquete.
- **TLS payload: (n bytes).** Carga TLS cifrada.

Cuando se inicia la conexión VPN, ambos extremos del túnel ejecutan la autenticación del cliente de SSL mediante el protocolo Handshake, donde cada uno presenta su certificado al otro extremo. Tras la autenticación, ambos lados saben que se están comunicando con quien dice ser y tienen un canal seguro mediante SSL sobre el cual pueden realizar el intercambio para generar las claves para el túnel seguro.

**Aplicaciones y características de OpenVPN**

De las aplicaciones y características que OpenVPN ofrece se pueden citar las siguientes:

- Enviar a través de un solo puerto TCP o UDP cualquier subred IP o adaptador de red virtual.
- Posibilidad de implementar dos modos básicos: bridge en la capa 2 o tunnel en la capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no IP como por ejemplo IPX.
- Configurar granjas de servidores VPN escalables y con balanceo de carga. Cada servidor puede mantener miles de conexiones dinámicas de clientes VPN.
- Uso de todos los protocolos de cifrado, autenticación y certificación que ofrece la librería OpenSSL para proteger el tráfico de la VPN.

- OpenVPN permite escoger entre el mecanismo de cifrado mediante claves compartidas o mediante clave pública basado en certificados.
- Uso de compresión en tiempo real y gestión del tráfico para manejar la utilización del ancho de banda.
- Funciona a través de proxy y puede ser configurado para ejecutarse como un servicio TCP o UDP y además como servidor (esperando conexiones entrantes) o como cliente (iniciando conexiones).
- Establecer túneles donde los extremos utilizan direcciones IP dinámicas con técnicas como DHCP.
- Tanto los clientes como el servidor pueden estar en la red usando solamente direccionamiento IP privado.
- Crear puentes Ethernet seguros utilizando para ello adaptadores Ethernet virtuales (o TAP).
- Controlar y monitorizar conexiones OpenVPN mediante interfaces gráficas de usuario (GUI, Graphical User Interface) para diferentes plataformas (Windows, Linux, MAC OS, etc.).
- Las interfaces virtuales (tun0, tun1,…) permiten la implementación de rutas y reglas de firewall específicas.

**Controladores virtuales TUN/TAP**

OpenVPN depende de los controladores virtuales TUN/TAP para poder establecer túneles punto a punto entre los dos extremos de la comunicación. Estos túneles fueron desarrollados por Maxim Krasnyansky en 1999 contenidos en la herramienta para creación de adaptadores virtuales VTUN, de libre distribución.

El modelo que utiliza OpenVPN para implementar una VPN se basa en utilizar el espacio de usuario y enlazar una interfaz de red virtual punto a punto llamada TUN con otra interfaz de red virtual punto a punto TUN remota. Un adaptador de red virtual TUN a su vez se podría ver como un enlace punto a punto entre la tarjeta de red del equipo y el sistema operativo. La interfaz TUN en lugar de entregar los bits al medio físico los entrega

al espacio de usuario del sistema operativo y éste abre, lee y/o escribe datos de paquete IP en la interfaz TUN como si se tratara de un archivo.

Cuando una interfaz virtual TUN/TAP recibe el nombre TUN significa que está trabajando en modo tunnel punto a punto, enlazando con otra interfaz virtual del mismo tipo. Por otro lado, si una interfaz virtual TUN/TAP recibe el nombre de TAP, significa que está trabajando en modo bridge, simulando de esta manera una interfaz de red Ethernet en lugar de una interfaz punto a punto.

**Seguridad con OpenSSL**

OpenVPN utiliza OpenSSL para implementar su modelo de seguridad. OpenSSL se compone de la herramienta de línea de comandos OpenSSL y de dos librerías, la librería SSL y la librería Crypto. Estas herramientas ayudan al sistema a implementar el protocolo SSL, así como otros protocolos relacionados con la seguridad, como el protocolo TLS. OpenSSL también permite crear certificados digitales que se pueden aplicar a servidores.

OpenSSL soporta varios algoritmos criptográficos diferentes según la finalidad:

- Algoritmos de cifrado: Blowfish, AES, DES, 3DES, RC2 (Rivest Cipher 2), RC4 (Rivest
- Cipher 4), RC5 (Rivest Cipher 5), IDEA (International Data Encryption Algorithm).
- Algoritmos para funciones hash: MD5, SHA-1, MD2 (Message Digest Algorithm 2).
- Algoritmos de intercambio de clave pública: RSA, Diffie-Hellman, entre otros.

**Compresión con LZO**

LZO (Lempel-Ziv-Oberhumer)12 es una librería multiplataforma de compresión de datos codificados en ANSI C13, creada bajo la GNU/GPL (General Public License). LZO ofrece gran velocidad en la compresión y descompresión de datos, requiere de algún tipo de buffer de 64 KB de memoria para la compresión y no demanda memoria para la descompresión.

**Modos de funcionamiento de OpenVPN**

OpenVPN puede trabajar en dos modos: modo TUN (tunnel) o modo TAP (bridge). Ambos modos utilizan el adaptador TUN/TAP, en concreto, utilizando el adaptador TUN para transmitir tráfico IP a lo largo del túnel o por el contrario, utilizando el adaptador TAP para transmitir tráfico Ethernet por el túnel.

La principal diferencia entre los adaptadores TUN y los adaptadores TAP es que un adaptador TUN es como un dispositivo virtual IP punto a punto entre los dos extremos de la comunicación (al igual que una línea dedicada) y un dispositivo TAP es como un dispositivo Ethernet virtual entre los dos extremos de la comunicación (al igual que una red Ethernet).

Las principales ventajas del modo TUN o tunnel son:

- Eficiencia y mayor escalabilidad.
- Permite un mejor establecimiento de la MTU (Maximum Transfer Unit) para una mayor eficiencia.

Entre sus principales desventajas se pueden encontrar:

- En algunas configuraciones los clientes necesitan tener un servidor WINS (Windows Internet Naming Service).
- Se deben establecer las rutas que unen cada subred.
- El software que dependa de tráfico broadcast no podrá ver a los equipos pertenecientes a la red del otro extremo de la VPN.
- Sólo funciona para los protocolos de nivel de red IPv4 e IPv6 siempre que en ambos extremos del túnel se use el mismo protocolo.

El modo TAP o bridge tiene como ventajas principales:

- Permite al tráfico broadcast.
- Admite cualquier protocolo de red como IPv4, IPv6, IPX, etc.

La principal desventaja de este modo es que es menos eficiente y escalable que el modo tunnel.

### II.1.1.2 Seguridad de Red Privada Virtual

Los computadores son hoy en día una parte fundamental de la sociedad de la información en la que vivimos, han supuesto una revolución total en la forma de comunicarnos, de llevar a cabo nuestras necesidades básicas diarias, y que sin ellos la vida, tal como la concebimos hoy por hoy, sería imposible.

Resulta increíble que con tan sólo pulsar un botón podamos acceder a fuentes de información inmensas, situadas en cualquier parte del planeta y suministradas por personas de cualquier tipo. Que nuestro confort y bienestar dependan de máquinas que la gran mayoría ni conoce ni sabe cómo funcionan.

Pero esta facilidad de acceso a cualquier tipo de información y esta comodidad lograda con el uso de los computadores precisa que estas máquinas estén cada vez más interrelacionadas entre sí, comunicadas en todo momento con otras muchas, y sin lugar a dudas es Internet el mejor medio para conseguir esto.

Pero si esta apertura a la red de nuestras máquinas facilita la intercomunicación, también es cierto que con ella las situamos al alcance de todo tipo de ataques y contaminaciones externas, y es en este contexto en el que adquiere toda su magnitud la palabra clave SEGURIDAD.

La seguridad general abarca un sinnúmero de aspectos de la organización y este capitulo solo esta enfocado a la seguridad de la información, el cual abarca la seguridad de redes, la seguridad de las computadoras, la seguridad de acceso y la seguridad física, entre otras.

Con toda esta seguridad, ¿es la administración superior de la organización quién decide que información es crítica y que información no lo es?,. Ya que es aquí donde se decide dar un valor a la información y proporcionar los recursos necesarios para protegerla. Además, no todos los datos son confidenciales y no todos los datos comerciales son críticos.

La seguridad informática se ocupa de elaborar las normas y procedimientos que hacen al procesamiento seguro de la información en todos sus aspectos.
La seguridad persigue tres objetivos básicos:

**Confidencialidad:**

- Proteger la revelación de información a personas no autorizadas.
- Restringir el acceso a información confidencial.
- Proteger el sistema contra usuarios curiosos internos y externos.

**Integridad:**

- Proteger los datos de cambios no autorizados.
- Restringir la manipulación de datos a programas autorizados.
- Proveer información verídica y consistente.

**Disponibilidad:**

- Asegurar la continuidad operativa del sistema y proveer planes alternativos de contingencia
- Proteger el sistema contra acciones o accidentes que detengan los servicios o destruyan la información que brinda.

La seguridad informática es asociada siempre con amenazas externas (como hackers o espías), pero la prevención de accidentes de usuarios autorizados (internos) es uno de los principales beneficios de una seguridad bien diseñada.

La seguridad es un gran problema, y lamentablemente pocos administradores de la seguridad están consientes de ello. Los sistemas informáticos están dispersos en toda la organización. Se dispone de numerosas máquinas de distinto tipo. Se interconectan en red con las sucursales y con otras empresas. Tenemos redes de área amplia, Internet, diversidad de plataformas, múltiples sistemas operativos, usuarios internos, externos, invitados, entre otros, computadoras personales, redes heterogéneas, computación móvil, virus, etc.

La seguridad es el tema central del tópico aplicaciones sobre Redes Privadas Virtuales, y cuando se piensa en la seguridad de redes, especialmente cuando se implemente en las Redes Privadas Virtuales, se debería revisar la pila de Interconexión de Sistemas Abiertos (OSI). La pila OSI consta de siete niveles: aplicación, presentación, sesión, transporte, red, enlace de datos y físico. Cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo, confiabilidad, configuración, corrección, entre otras. Pero es aquí donde surgen problemas de seguridad, ya que los ataques más comunes en la actualidad suceden a través de todos estos niveles. Cada nivel puede atacarse y verse comprometido, por lo tanto, para que una red privada virtual sea segura es hacer que ésta se ubique en los niveles más bajos posibles de la pila OSI. La figura 2 - 33 muestra una ubicación óptima para la tecnología VPN.

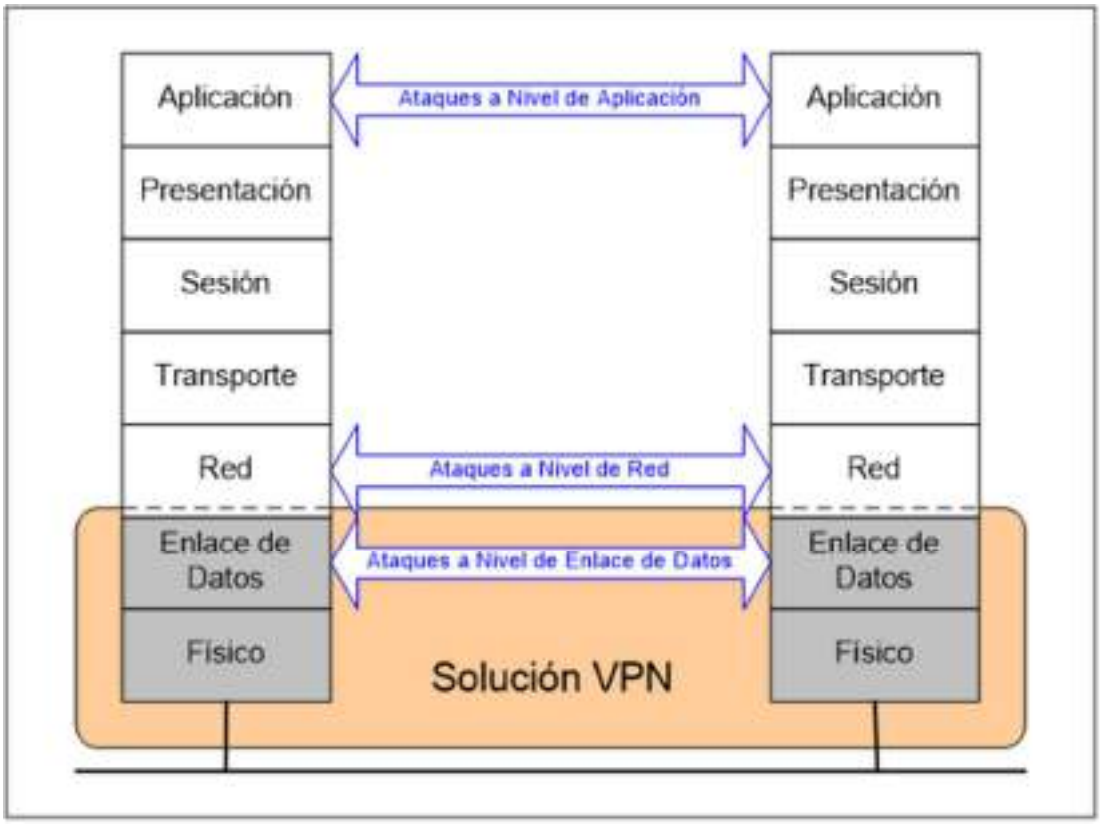


*Figura 2 – 33 Tecnología VPN en la pila de OSI*

Pero hay que tener presente que esta ubicación puede provocar problemas de compatibilidad. Al implementar el software de red privada virtual en los niveles más bajos de la pila OSI, la tecnología tiene la posibilidad de interactuar más con los componentes

específicos que forman el sistema operativo, y lamentablemente, los controladores de dispositivos, los optimizadores y los módulos cargados pueden tener problemas de interoperabilidad con la tecnología de red privada virtual instalada y esto puede ser un problema más grave con los usuarios remotos que utilizan equipos portátiles y equipos de escritorio.

**Control de acceso al usuario.**

El modo de control de acceso al usuario solo admite los derechos y permisos de usuario requeridos para que realicen su trabajo. El control de acceso al usuario es extremadamente importante cuando se implementa una tecnología de Red Privada Virtual. Primero se tiene que asegurar de que sólo se concede permiso a los usuarios autorizados. Después debe asegurarse de que esos usuarios tienen concedido el acceso a aquellos recursos que usted considera necesarios para ese usuario.

Un comentario acerca de la seguridad es que siempre esta cambiando, y la implementación de sistemas de seguridad tiene que estar al día con esta manera de pensar. Durante años, las contraseñas simples fueron suficientes para las máquinas individuales y otros dispositivos de red, pero ahora han terminado con su vida útil.

La seguridad tiene un costo. Mientras más seguridad implementa en la organización, mayores serán los costos, además, los requisitos de mantenimiento y la experiencia técnica necesaria para administrar ese aumento de seguridad, no solo serán mayores, sino que también aumentará la irritación de los usuarios finales.

Es muy frustrante para el usuario final que el servidor de seguridad de la red se caiga, que el cortafuego no pase el tráfico, que el servidor de autenticación se venga abajo, o que los servidores web no acepten los certificados.

#### II.1.1.2.1 Ataques a la red privada virtual

##### II.1.1.2.1.1 Ataques a los algoritmos criptográficos

Al igual que sucede en el software y el hardware, los algoritmos criptográficos también son vulnerables y están expuestos a ataques, y generalmente existen tres formas de atacar un algoritmo de este tipo y son las siguientes: Ataques contra el protocolo, Ataques contra el algoritmo, Ataques contra la implementación.

- **Ataques contra el protocolo**: Si al realizar el cifrado no se utilizan los generadores de números aleatorio correctos, la reutilización de valores y demás funciones transformaciones de código, la integridad del protocolo será verá comprometida.
- **Ataques contra el algoritmo:** Uno de los principales problemas con los ataques criptográficos es que es posible que el usuario no este consciente de que ha sido atacado, lo que hace es depositar toda su confianza al algoritmo de cifrado. Pero hay que estar concientes que los algoritmos criptográficos también son sujetos de ataques. A continuación se presentan varias categorías comunes de ataque a algoritmos.
- **Ataque de solo texto cifrado:** En un ataque de sólo texto cifrado, el agresor no sabe nada respecto al mensaje de texto simple, pero al obtener el texto cifrado, intenta obtener el texto simple. Lo que intenta el agresor es encontrar un patrón común donde puede identificar un conjunto de palabras de uso común. En la práctica esto es factible ya que la mayoría de documentos siguen ciertos formatos comunes, como por ejemplo, encabezados de formato fijo, las cartas, informes y memorando, comienzan de forma predecible.
- **Ataque de texto simple conocido:** En este ataque el agresor conoce parte del documento en texto simple o puede hacer conjeturas con cierta base sobre el mismo. Este texto simple puede adivinarse debido a que es posible que sea un saludo, encabezado o sinopsis estándar. Debido a que el atacante tiene el texto cifrado, puede utilizar el texto simple para decodificar el resto del texto.
- **Ataque de texto simple seleccionado:** En este tipo de ataque, el agresor toma algún texto y lo cifra con la clave desconocida. En una inferencia, el atacante intenta adivinar la clave utilizada para ese cifrado.
- **Ataque de texto cifrado seleccionado:** El agresor tiene la ventaja de elegir un texto cifrado seleccionado arbitrariamente y puede encontrar el texto simple descifrado correspondiente.
- **Ataque de intermediario:** Es práctico para comunicaciones criptográficas y protocolos de intercambio de claves. Aquí dos partes intercambian sus claves para comunicaciones posteriores. El intermediario secuestra las claves del emisor y del

receptor, y las sustituye por otras propias del intermediario, por lo cual tiene la capacidad de interceptar todas las comunicaciones futuras sin que el emisor y el receptor lo sepan. La única forma de impedir esto es con el uso de firmas digitales y con el mecanismo de claves secretas compartidas.

- **Ataque de sincronización:** Este tipo de ataque se basa en la medida de los tiempos de ejecución de una operación de exponenciación modular que se utiliza en los algoritmos criptográficos. Los criptosistemas toman cantidades de tiempo ligeramente diferentes para procesar entradas distintas. Cuando la CPU utiliza rutinas de optimización, ramificaciones, ciclos, instrucciones condicionales y demás, se utilizan distintas cantidades de ciclos de máquina. Es sabido que durante estos canales de sincronización los datos se pierden, aunque representan una cantidad mínima. Sin embargo los atacantes pueden explotar las medidas de tiempos o de sincronización de sistemas vulnerables para encontrar la clave secreta completa. Contra un sistema vulnerable, este ataque no es caro y a menudo requiere que se conozca el texto cifrado.
- **Ataque de fuerza bruta:** Un ataque de fuerza bruta es muy popular entre los agresores que tiene mucha capacidad de cómputo a su disposición. Lo que hace es simplemente tratar de ir probando una a una todas las claves posibles hasta encontrar la clave adecuada. Por ejemplo, el algoritmo DES tiene 256 posibles claves. ¿Cuánto tiempo nos llevaría probarlas todas si, supongamos, dispusiéramos de un computador capaz de hacer un millón de operaciones por segundo?. La respuesta es que tardaríamos más de 2200 años. Pero este algoritmo ya fue quebrantado por la Fundación de la Frontera Electrónica utilizando un método de fuerza bruta.
- **Criptoanálisis diferencial:** En los ataques de este tipo, el agresor utiliza la relación de la información que se basa en una información repetida. Al basar los resultados en un gran número de pares de texto cifrado, cuyas contrapartes de pares de texto simple satisfacen una diferencia XOR conocida en lo que respecta al componente, el atacante puede determinar la clave.
- **Solidez de los algoritmos criptográficos:** En teoría cualquier algoritmo criptográfico puede romperse al probar todas las claves posibles en secuencia (Un

ataque de fuerza bruta). Pero para poder romper el algoritmo el número de pasos requeridos crece en forma exponencial con la longitud de la clave. A continuación, se presenta el número de pasos requeridos para cada tamaño de clave.

- Clave de 32 bits requiere 232 pasos
- Clave de 40 bits requiere 240 pasos
- Clave de 56 bits requiere 256 pasos
- Clave de 64 bits requiere 264 pasos
- Clave de 80 bits requiere 280 pasos
- Clave de 128 bits requiere 2128 pasos
- Clave de 160 bits requiere 2160 pasos

Las claves de 32 y 40 bits pueden ser quebrantadas para cualquiera que tenga acceso a un computador de alto rendimiento, la clave de 56 bits están comprometidas y las claves de 64 y 80 bits pueden ser quebrantas por los gobiernos y las universidades. Las claves de 128 y 160 bits probablemente sean seguras ahora.

En los sistemas criptográficos de clave pública las longitudes de clave son mayores de aquellas que se utilizan en las cifras simétricas. En los sistemas de clave pública, la mayoría de las fallas de seguridad no vienen del método de fuerza bruta, sino de derivar la clave secreta de la clave pública. Por ejemplo, cualquiera con una computadora potente puede forzar un criptosistema de clave pública de un módulo de 256 bits con facilidad. Las universidades y gobiernos pueden forzar claves de módulos de 318 y 512 bits. Las claves con módulos de 768 y 1.024 bits probablemente son seguras por ahora.

Se debe tener presente que el algoritmo o las operaciones matemáticas que se ejecutan en los datos podrían debilitar todo el sistema, y por lo tanto los algoritmos de cifrados propietarios no hacen que un algoritmo sea seguro, la mayoría han mostrado ser débiles.

- **Ataques contra la implementación**: Este tipo de ataque es el más fácil de evitar, y se da cuando algunas implementaciones dejan archivos temporales, mensajes de texto simple y datos almacenados en la memoria intermedia de donde se puede extraer fácilmente.

### II.1.1.2.1.2 Ataques al generador de números aleatorios

Un generador de números aleatorios es un dispositivo que genera números al azar, pero lamentablemente solo existen en la naturaleza, por ejemplo, en la electricidad estática y en el ruido blanco de los circuitos eléctricos. Debido a que no se puede utilizar un generador de números aleatorios de la naturaleza, se emplean los generadores de números pseudo aleatorios para generar valores supuestamente aleatorios.

Ya que un generador de números aleatorios es un común denominador en muchas funciones criptográficas, y si sus algoritmos no están diseñados correctamente pueden ser el eslabón más débil en la cadena de seguridad. Al igual que existen categorías de ataque en las funciones criptográficas, también se presentan categorías de ataques al generador de números aleatorios, los cuales son:

- **Ataque criptoanalítico:** Este ataque ocurre si el agresor es capaz de observar una correlación entre el generador de números pseudo aleatorios y las salidas aleatorias. Es factible en las funciones criptográficas donde las salidas del generador de números pseudo aleatorios son visibles.

- **Ataque de entrada:** Ocurren cuando el agresor puede tener conocimiento sobre la entrada del generador de números pseudo aleatorios con el fin de producir algunas salidas del generador de números pseudo aleatorios. Este tipo de ataque puede ocurrir en sistemas que utilizan los diversos tipos de entradas predecibles, como contraseñas y frases.

- **Ataque de sincronización:** Es similar al que ocurre en una función criptográfica. Durante las operaciones matemáticas que cuentan el número de ciclos de máquina para cada operación, el agresor puede tener alguna información. Se cree que el agresor puede determinar cuando ocurren ciertas operaciones booleanas. Por ejemplo, las adiciones referentes a los bits pueden detectarse al contar los ciclos de máquina.

- **Confidencialidad adelantada perfecta:** Es un mecanismo mediante el cual si una clave se roba en algún momento del futuro no se puede revelar ninguna comunicación que se ha conducido en el pasado. Todo algoritmo criptográfico debería estar diseñado para la confidencialidad adelantada perfecta. Lamentablemente la implementación de este tipo de algoritmos consume muchos recursos, ya que cada paquete requiere una nueva clave.

#### II.1.1.2.1.3 Ataques a la recuperación de claves

En este método de recuperación de claves que es exigida por los gobiernos, especialmente por el de los Estados Unidos, se construye una puerta trasera a propósito y, si existe tal puerta alguien más puede entrar. Este concepto elimina cualquier oportunidad de confidencialidad adelantada perfecta que se menciono con anterioridad.

En la recuperación de claves, no solo esta en peligro la comunicación de datos futura sino cualquier información capturada previamente, ya que existe la clave para descifrarla. Los sistemas criptográficos confiables y seguros son muy difíciles de diseñar, y la implementación de recuperación de claves lo han más difícil aún.

Otro problema con la recuperación de claves es quién guardará las claves, será el gobierno, cuál?, empresas privadas, quienes tendrán accesos a sus claves, esto es seguro?, y si lo fuera, que sucede en el momento de requerir una clave, la persona que tiene la clave viajaría por todo el mundo entregando claves o se enviarían por la misma red, en el momento que viajan por la red están seguras? De hecho, ninguna solución se ve por el momento aceptable.

¿Y esto como le afecta a su Red privada Virtual?, de hecho, es muy simple ya que es susceptible de que sus datos y claves sean amenazados, no sólo por el gobierno, sino por los atacantes que rompen los algoritmos que utilizan recuperación de claves, interceptando los datos conforme pasan del departamento encargado de custodiar las claves, al agente encargado de custodiar las mismas.

### II.1.1.2.1.4 Ataques al Protocolo de Seguridad de Internet (IPSec)

El protocolo de seguridad de Internet (IPSec) no es un algoritmo de cifrado y tampoco es un algoritmo de autentificación. IPSec es un paradigma en el cual otros algoritmos protegen datos. Los principales tipos de ataques que ocurrirán con IPSec serán aquellos que caen en la categoría de ataques contra la implementación.

La norma IPSec solo requiere un algoritmo de cifrado (DES-CBC) y dos modos de autenticación (HMAC-MD5 y HMAC-SHA-1); sin embargo requiere los algoritmos NULL adicionales, ya que AH o ESP pueden ser opcionales, y cuando una norma requiere un algoritmo opcional está tratando de balancear la flexibilidad con la seguridad.

En el componente IKE del protocolo de administración de claves de IPSec, ambos extremos del canal de comunicación deciden que tan a menudo se deben cambiar las claves de cifrado. Debido a que muchos proveedores soportan claves de 40 bits débiles que se usan para compatibilidad con productos anteriores, cambiar estas claves se vuelve crítico.

También en la especificación de IKE, cualquiera de las dos partes podría terminar una sesión, pero no hay forma de que el otro extremo sepa de la sesión se ha terminado; el extremo emisor seguirá enviando datos. Si la estación todavía envía datos, ¿Cómo dejaría otra estación de recibirlos y, si se utilizan claves débiles, ¿cómo se burlaría la identidad del anfitrión original? Este tipo de ataque es similar a apropiarse de una sesión TCP.

Además IPSec no cuenta con ningún tipo de mecanismo para la autentificación de los usuarios: no incluye derechos de acceso, no existe verificación, etc. IPSec no se encarga del soporte para los clientes, ya que básicamente fue diseñado alrededor de una red privada virtual de LAN a LAN. Es por eso que queda la puerta abierta parea que los fabricantes ofrezcan su soporte de IPSec para la compatibilidad con los clientes.

La traducción de direcciones de red (NAT) existe en la norma IPSec. Cuando se utiliza el establecimiento de túneles en los modos ESP y AH, el encabezado IP original se reemplaza por uno nuevo encabezado IP. El problema es, ¿Dónde se esta ejecutando NAT? ¿En un enrutador, en un cortafuego o en un equipo de escritorio? ¿Qué dispositivo

cambiará físicamente la dirección IP del paquete? ¿Este dispositivo deberá ser compatible con IPSec?

Una deficiencia de IPSec es que sólo soporta un conjunto muy pequeño de algoritmos y protocolos en su escenario predeterminado. Con el propósito de que IPSec se vuelva una entidad administrativa de corriente principal, tendrá que incluir más soporte, como el soporte para cliente, LDAP y múltiples algoritmos de cifrado predeterminados, así como otros mecanismos de autentificación. Al momento, IPSec sólo soporta firmas y certificados digitales. También tendrá que incluir un mayor soporte para los navegadores y equipos de escritorio con el fin de continuar haciéndolo una verdadera norma Internet interoperable. Lamentablemente la flexibilidad y la seguridad se sacrifican.

#### II.1.1.2.1.5 Ataques al protocolo PPTP

El protocolo PPTP sufre ataques contra su implementación, y actualmente Microsoft, su diseñador, esta trabajando en esto. La red privada virtual de PPTP está formada por varios componentes y, de manera similar a IPSec, PPTP es un marco de referencia. No exige los algoritmos de cifrado y autentificación, esto se deja a los otros protocolos, como PAP, CHAP y MS-CHAP (detallados en el capitulo 3). Los protocolos utilizados son los siguientes:

- GRE. Protocolo de encapsulamiento de enrutamiento genérico.
- PPP. Protocolo de red punto a punto utilizado para proporcionar servicios TCP/IP sobre líneas de conexión serial por marcación.
- PPTP. Este protocolo utiliza GRE para establecer un túnel PPP y añade una instalación de conexiones y un protocolo de control.
- MS-CHAP. Es responsable del algoritmo de autentificación.
- MPPE. El protocolo de cifrado de punto a punto de Microsoft es el protocolo que se encarga de generar una clave y cifrar la sesión.

PPTP encapsula los paquetes PPP, los cuales a su vez son encapsulados en paquetes de encapsulamiento de enrutamiento genérico (GRE). PPTP crea una instalación de conexión

y controla el canal al servidor PPTP sobre el puerto TCP 1723. Además esta conexión no se autentifica de ninguna forma.

Un tipo de ataque puede darse al encapsulamiento de enrutamiento genérico (GRE), ya que los paquetes GRE pueden trasportar un número se secuencia y un número de reconocimiento y pueden utilizar una ventana deslizable para evitar la congestión. Y esto tiene algunas implicaciones, ya que si se desea burlar los paquetes PPP encapsulados en GRE, simplemente se necesita desincronizar el canal de GRE. Esto puede evitarse con el número de secuencia, pero el GRE no tiene forma de que el anfitrión final reaccione ante un número de secuencia erróneo o duplicado. Es posible que simplemente se ignore y después, los paquetes PPP pueden burlarse.

La implementación de autentificación PPTP soporta tres tipos, de los cuales dos están relacionados con la seguridad y son: El método de transformación de código y le método de respuesta de pruebas. Cuando se utiliza el método de transformación de código se esta exponiendo al los ataques de diccionario. Cuando se utiliza el método de respuesta de pruebas utilizando el protocolo de reconocimiento de pruebas (CHAP), el cual trabaja con el cliente contactando al servidor, y el servidor envía de regreso una prueba. El cliente entonces ejecuta una función de transformación del código, añade alguna información extra y la envía de regreso al servidor. El servidor busca en su propia base de datos y compara el valor de transformación del código con la prueba. Si son iguales, la autentificación es satisfactoria. Mientras esto elimina los ataques de diccionario, las funciones de transformación del código aún podrían ser atacadas.

Un punto vulnerable de PPTP es que se basa en PPP. Antes de cualquier comunicación, PPP establece e inicia los parámetros de comunicación, y debido a que no tiene autentificación contra estos paquetes, pueden ocurrir ataques como los de intermediario y de falsificación.

#### II.1.1.2.1.6 Ataques a la autoridad emisora de certificados

Las autoridades emisoras de certificados no son diferentes de cualquier otro dispositivo en la cadena de comunicación de terceras partes validadas. Si ocurre un ataque a una autoridad emisora de certificados, los agresores pueden hacerse pasar por quién ellos deseen, al unir cualquier clave de su elección al nombre de otro usuario, y utilizar a la autoridad emisora de certificados para verificarla.

#### II.1.1.2.1.7 Ataques a Radius

El servicio de usuarios de autentificación remota por marcación (RADIUS) se diseño teniendo dos protocolos en mente, el de autenticación y el de asignación de cuentas.

En la tecnología RADIUS se encontró un punto débil que provocó un problema de desbordamiento de la memoria intermedia, el cuál permitía que un agresor obtuviera acceso de superusuario de forma remota a una máquina que ejecutará al servidor RADIUS. El problema se manifestó como resultado de una operación de resolución inversa de direcciones IP a nombres de anfitrión. El software copiaría el nombre de anfitrión a una memoria intermedia en su pila sin revisar primer su longitud. En un ataque, un agresor establecería un nombre de anfitrión sumamente largo y el software RADIUS colocaría el nombre en la pila provocando que invadiera su memoria intermedia. Cualquier código malicioso podría entonces ejecutarse en el servidor.

#### II.1.1.2.1.8 Ataques a Kerberos

Kerberos es un sistema de autentificación distribuida que permiten que las organizaciones manejen seguridad de contraseñas para toda una organización. Lamentablemente estos protocolos son vulnerables a los ataques de diccionario. Un atacante puede agredir a un sistema Kerberos con la ayuda de una máquina local y un husmeador de paquetes ayudará para el ataque.

### II.1.1.2.1.9 Ataques a pretty good privacy (PGP)

PGP es muy seguro, probablemente se trata de una de las mejores estructuras de seguridad. Lo más interesante sobre PGP no es su solidez, sino la actitud que tiene el gobierno de los Estados Unidos hacia él.

PGP utiliza cuatro componentes: una cifra simétrica (IDEA), una cifra asimétrica (RSA), una función de transformación de código (MD5) y un generador de números pseudoaleatorios (PRGN). Cada uno de estos dispositivos podría ser atacado.

**Idea.-** La cifra de IDEA utiliza una clave de 128 bits, y la única forma de ataque conocida que podría intentarse contra ella sería un ataque de fuerza bruta. Por lo tanto, alguien tendría que intentar con al menos la mitad del espacio de clave, lo cual aproximadamente es 2127.

**RSA.-** Obtiene su solidez de la dificultad que implica factorizar números primos grandes. Ningún ataque a RSA ha tenido éxito hasta ahora. Y con tamaños de clave lo suficientemente grandes, se espera que ningún ataque pueda lograrlo.

**MD5.-** Se encontró que la función de transformación del código MD5 es vulnerable si se utiliza un número de ciclos pequeños. Se han presentado intentos de forzar MD5 utilizando los métodos de criptoánalisis diferencial, de aniversario y de fuerza bruta. De éstos, el criptoanálisis diferencial ha tenido cierto éxito fuera del ciclo de MD5 y sólo afectó a una operación que no estaba relacionada con la seguridad de MD5.

**PRNG.-** PGP utiliza dos generadores de números pseudoaleatorios: el generador ANSI X9.17 y el generador trueRand. Este último mide la latencia de la entrada del usuario y después utiliza ese grupo para establecer una semilla en el generador X9.17. Al utilizar dos generadores, PGP ha añadido mecanismos de seguridad para producir una aleatoriedad verdadera.

Parecería que PGP es un algoritmo muy seguro que no ha experimentado ataques de ningún tipo; sin embargo esta es una suposición incorrecta. Después de todo, si no se puede atacar el protocolo, puede atacar la implementación.

#### II.1.1.2.1.10 Ataques de negación de servicio

Los ataques de negación de servicio provocan que el sistema o la red dejen de dar servicio a los usuarios legítimos, y entre los más conocidos se encuentran los siguientes:

**Jamming o Flooding.-** Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

**Syn Flood.-** El protocolo TCP se basa en una conexión en tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto". El Syn Flood es el más famoso de los ataques del tipo Denial of Service. Se basa en un "saludo" incompleto entre los dos hosts.

El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado. Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el Syn Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

La potencia de este ataque reside en que muchos sistemas operativos fijan un límite del orden de 5 a 30 conexiones "semiabiertas", y que éstas caducan alcabo de un par de minutos. Para mantener el servidor fuera de servicio, un atacante sólo necesita enviar un paquete SYN cada 4 segundos (algo al alcance de, incluso, un módem de 300 baudios).

**Connection Flood.-** La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del Syn Flood) para mantener fuera de servicio el servidor.

**Land Attack.-** Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows. El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino. Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la máquina termina colgándose.

**E-Mail Bombing-Spamming.-** El E-Mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así mailbox del destinatario.

El Spamming, en cambio se refiere a enviar el e-mail a miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming esta siendo actualmente tratado por las leyes como una violación de los derechos de privacidad del usuario.

#### II.1.1.2.1.11 Ataques de Autentificación

Consisten en la suplantación de una persona con autorización por parte del atacante. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema. Para realizar ataques de este tipo se utilizan varias técnicas, las cuales pasamos a describir a continuación.

**Simulación de identidad.-** Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él teclea su login y password, el programa los captura y muestra una pantalla de "error en el acceso" al usuario. El usuario vuelve a teclear su login y password, entrando esta vez sin problemas. El usuario cree que en el primer intento se equivocó al teclear, sin embargo, su login y password han sido capturados por el atacante.

**Spoofing (Engaño).-** Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Consiste en sustituir la fuente de origen de una serie de datos (por ejemplo, un usuario) adoptando una identidad falsa para engañar a un firewall o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing , el Web Spoofing y el fake-mail.

- **IP Spoofing.-** Sustituir una IP. El atacante logra identificarse con una IP que no es la suya, con lo que a ojos del atacado, el agresor es una tercera persona, que nada tiene que ver en el asunto, en vez de ser el atacante real.

- **DNS Spoofing.-** Sustituir a un servidor DNS (Domain Name Server) o dominio. Se usan paquetes UDP y afecta a sistemas bajo Windows NT. Se aprovecha de la capacidad de un servidor DNS resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos, ya que éste es su método de trabajo por defecto.

- **Web Spoofing.-** El atacante crea un sitio web (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima: datos, contraseñas, números de tarjeta de créditos, etc. El atacante también es capaz de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

- **Fake-mail.-** Es otra forma de spoofing y consiste en el envío de e-mails con remitente falso. Aquí el atacante envía E-Mails en nombre de otra persona con cualquier motivo y objetivo. Muchos de estos ataques se inician utilizando la Ingeniería Social para hacerse con el nombre y contraseña de una víctima.

**Looping.-** El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente. Este proceso se llama looping y tiene como finalidad hacer imposible localizar la identificación y la ubicación del atacante, de perderse por la red.

**IP splicing-hijacking.-** Es un método de sustitución que consiste en que el atacante espera a que la víctima entre en una red usando su nombre, contraseña y demás y una vez que la víctima ha superado los controles de identificación y ha sido autorizada la "saca" del sistema y se hace pasar por ella.

**Utilización de backdoors (puertas traseras).-** Las puertas traseras son trozos de código en un programa que permiten a quien los conocen saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. No es por tanto un método de suplantación, si no de saltarse los controles de autentificación o, como su nombre indica, entrar por la "puerta de atrás".

Son fallas de seguridad que se mantienen, voluntariamente o no, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

**Obtención de contraseñas.-** Es la obtención por "Fuerza Bruta" de nombres de usuarios y claves de acceso. Casi todas las contraseñas que utilizamos habitualmente están vinculadas a nuestros nombres reales, nombres de familiares y/o mascotas, fechas significativas, .... etc. Además, no las solemos cambiar periódicamente. También se suele realizar este tipo de ataques usando una clase de programas llamados diccionarios.

**Diccionarios.-** Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números encriptados, incluso con caracteres especiales hasta descubrir la combinación correcta de nombre y usuario de la víctima. Son entonces programas de fuerza bruta.

#### II.1.1.2.2 Como identificar los ataques

Una buena política de seguridad tiene auditorias y registros como pasos principales de sus procesos, ya que nunca se sabe de antemano cuando se va ha ser atacado. Es por esta razón que es bueno tener registros de quién ha ingresado o ha intentado introducirse y no tuvo éxito. Cuando se tiene intrusiones extrañas es necesario rastrear la intrusión y ver si los archivos de registro pueden identificar de donde vino el intruso, cuál es su dirección IP, y si es posible quién es su proveedor de Internet.

Las auditorias y los registros son herramientas adecuadas y necesarias para intentar revelar la identidad de potenciales violaciones a la seguridad. Sin embargo, el monitoreo es la vista en tiempo real de los paquetes mientras pasan el límite entre la red interna de la empresa y las redes externas. Este monitoreo controla que tráfico permite entrar, que tipo de tráfico permite salir, que servicios están permitidos. El monitoreo en tiempo real es la única forma efectiva de observar las desviaciones contra la política de seguridad establecida por la organización.

El problema con el monitoreo en tiempo real para un administrador de red es que pueden haber cientos de alertas, y es probable que el administrador se canse de todas estas alertas y desactive el monitoreo de una estación.

### II.1.1.2.3 Importancia de la Seguridad en las VPN

Para que las Redes Privadas Virtuales puedan ser un medio efectivo para el comercio electrónico, para las aplicaciones de Intranet, Extranet y para las transacciones financieras a través de Internet, deben utilizarse tecnologías de autenticación seguras, las más recientes y sofisticadas, así como criptografía y cifrado en cada extremo del túnel de las Redes Privadas Virtuales. Por los motivos expuestos con anterioridad es importante para cualquier configuración de seguridad lo siguiente:

**Acceso solo a personas autorizadas. -** Sólo a las partes autorizadas se les permite el acceso a aplicaciones y servidores corporativos. Esté es un aspecto importante de la tecnología Red Privada Virtual, ya que se permite que personas entren y salgan de Internet o de otras redes públicas y se les ofrece acceso a los servidores.

**Imposibilidad de descifrar el mensaje. -** Cualesquiera que pase a través del flujo de datos cifrados de las Redes Privadas Virtuales no debe estar capacitado para descifrar el mensaje, ya que los datos de las VPN viajarán a través de una red pública, y cualquiera tendrá la capacidad de interceptarlos. El resguardo de la información está en el cifrado, incluyendo su solidez y la implementación específica del proveedor.

**Datos íntegros. -** Los datos deben permanecer intocables al cien por ciento, esto se debe a que algunas personas verán el tráfico cifrado e intentarán leerlo, sin embargo, otro problema, es que intenten modificarlo y enviarlo a su destino original. La integridad es un tema diferente cuando se trata de la tecnología VPN, ya que existen normas de cifrado que proporcionan autenticación, cifrado e integridad de datos.

**Distintos niveles de acceso. -** Los usuarios individuales deben tener un distinto nivel de acceso cuando entren al sitio desde redes externas.

**Interoperabilidad. -** Los aspectos de interoperabilidad deben tomarse en consideración, ya que es un problema cuando existen diferentes plataformas y sistemas operando en conjunto para lograr una meta común.

Las redes privadas virtuales deben funcionar en todas las plataformas y para logra este objetivo si es necesario, es probable que se tenga que instalar software adicional para estas plataformas, y se debe tener presente que cuando se aumenta algo nuevo, aumenta el riesgo de que se presenten consecuencias infortunadas.

**Facilidad de administración. -** Los dispositivos de las redes privadas virtuales deben proporcionar una administración fácil, la configuración debe ser directa, el mantenimiento y la actualización de las VPN deben estar asegurados. Una de estas facilidades de administración debe ser el acceso de los usuarios, es decir debe haber una manera sencilla para agregar/eliminar usuarios sin esperar demasiado tiempo.

#### II.1.1.2.4 Requisitos de seguridad en las Redes Privadas Virtuales

Una red Privada Virtual esta basada en una red tradicional, así que los requisitos de seguridad son los mismos que se utilizan en las redes tradicionales y de algunas técnicas más, propias de la Red Privada Virtual. El mismo hecho de querer instalar una Red Privada Virtual significa que se quiere añadir un nivel más de seguridad a la red que se posee actualmente.

La seguridad de las Redes Privadas Virtuales es de suma importancia para cualquier compañía que realice negocios a través de Internet o de cualquier red pública. Estos requisitos de seguridad incluyen el cifrado, los dispositivos de Red Privada Virtual, la autenticación, el proceso sin rechazos, el cifrado punto a punto, la administración centralizada de la seguridad y los procedimientos de respaldo restauración. A continuación se revisarán algunos de estos componentes.

##### II.1.1.2.4.1 Criptografía

Criptografía puede parecerse a magia negra para una persona promedio, pero en realidad está basada en principios matemáticos. El cifrado es sencillamente el procedimiento de convertir texto legible en un texto ilegible. La meta es permitir que sólo la persona a la que

se le envía lo convierta en un texto legible. Un mensaje o archivo de datos es llamado texto-plano antes de ser encriptado y texto-cifrado luego de ser encriptado. El proceso de "scrambling" del texto-plano es llamado encriptación. El proceso de "Unscrambling" del texto-cifrado al texto plano original es llamado desencriptación. A veces las palabras cifrar y descifrar son usadas en su lugar.

La ciencia de encriptar datos es llamada criptografía. La ciencia de romper datos encriptados es llamada criptoanálisis. La criptología es la ciencia combinada de estas dos.

Algunos de los mejores criptoanalístas del mundo trabajan en la Agencia nacional de Seguridad (NSA), una agencia muy secreta creada por el presidente Truman en 1952. Su propósito es desencriptar comunicaciones foráneas que son de interés para la seguridad nacional de los Estados Unidos.

Las claves se miden en bits. Una clave de un bit tiene dos combinaciones posibles 0 y 1. Cada bit adicional dobla la cantidad de combinaciones. Una clave de 8 bits tiene 256 combinaciones, una de 40 bits tiene más de un trillón de combinaciones y una de 160 bits tiene 1048 combinaciones. Probar cada posible clave hasta encontrar la correcta se denomina ataque de fuerza bruta. Una computadora personal que pueda probar 50.000 combinaciones por segundo puede testear todas las combinaciones de una clave de 40bits en alrededor de 255 días. Estadísticamente el usuario solo tendría que probar la mitad de las claves para encontrar la correcta. La clave de 40 bits puede ser clasificada como poseedora de seguridad casual. La clave de 160 bits usada en el algoritmo blowfish puede ser clasificada como poseedora de seguridad militar. Un trillón de supercomputadoras que pudieran probar cada una un trillón de claves por segundo demorarían cerca de 463 trillones de centurias para probar todas las combinaciones posibles de una clave de 160 bits.

La criptografía es clasificada como munición en la U.S. Munitions list (USML) y está contemplada en el International Traffic in Arms Regulations (ITAR). La NSA a través del Departamento de Estado, controla la tecnología de encriptación que es exportada desde los Estados Unidos. El Shareware y las versiones internacionales registradas contienen la tecnología de encriptación más sólida permitida para exportar por los Estados Unidos (40 bits). Las versiones registradas en Canadá no están sujetas a estos controles y por consiguiente contienen mejor tecnología de encriptación.

Básicamente hay dos tipos de algoritmos de encriptación en uso hoy, de clave privada o simétrico y de clave pública o asimétrico.

**Algoritmos Simétricos.-** Son sistemas convencionales basados en password (clave) que la mayoría de la gente conoce. El usuario suministra una clave y el archivo es cifrado con la clave. Para descifrar el archivo, el usuario debe suministrar la misma clave nuevamente y el proceso es reversado. La clave es la llave de encriptación. El principal problema aquí es la clave; el emisor y el receptor no solamente deben de estar de acuerdo en usar la misma clave, sino que también deben idear alguna manera para intercambiarla, especialmente si están en diferentes áreas geográficas. En los sistemas de clave privada, la integridad de la clave es sumamente importante. Por lo tanto, es importante reemplazar periódicamente esta clave.

Ejemplos de los esquemas de encriptación simétrica son el algoritmo RSA RC4 (que proporciona la base de Microsoft Point-to-Point Encription (MPPE), el Estándar de encriptación de datos (DES), el Algoritmo de encriptación de datos internacional (IDEA) y la tecnología de encriptación Skipjack propuesta por el gobierno de Estados Unidos (e implementada en el Chip Clipper).

En este punto es necesarios aclarar que existen dos técnicas de cifrado simétrico, las cuales son: cifrado por bloques y cifrado por flujo.

- **Cifras de Bloque. -** Una cifra de bloque es un cifrado que repite varias operaciones débiles como sustitución, transposición, adición modular, multiplicación y transformación lineal en un algoritmo mucho más sólido. Este algoritmo de cifrado se efectúa con la clave del usuario especificada. Una cifra de bloque codifica un bloque de datos, por ejemplo 64 bits a la vez, y luego va al siguiente bloque. DES es un ejemplo de una cifra de 64 bits. Una desventaja de la cifra de bloque es que el uso del mismo algoritmo y la misma clave generan el mismo texto cifrado que se puede utilizar como un ataque de análisis de datos sostenido.
    - **El cifrado Feistel.-** Es una cifra de bloques que opera sobre la mitad del texto cifrado en cada repetición y luego intercambia las mitades del texto cifrado después de cada ciclo. Utiliza 64 bits con 16 ciclos.

- **DES.-** La norma de cifrado de datos (DES) utiliza un tamaño de 64 bits y una clave de 56 bits durante la ejecución (los 8 bits de paridad se quitan de la clave de 64 bits completa). DES es un criptosistema simétrico, específicamente una cifra Feistel de 16 ciclos. En una cifra de ciclo se aplica el algoritmo varias veces; en este caso, el algoritmo se completa 16 veces. Durante cada ciclo (transformación) se utiliza una subclave con el proceso de repetición. Esta subclave es un derivado de la clave principal que el usuario suministró mediante una función especial en el algoritmo. Cabe aclarar que el cifrado DES de 56 bits fue violado en el lapso de un mes, por lo que el gobierno de los Estados Unidos permitió la exportación de DES de 56 bits.
- **El algoritmo Blowfish.-** Fue desarrollado por Bruce Scheneir en 1993. Blowfish es un cifrador de bloque de tamaño de clave variable para usuarios registrados que residen en los Estados unidos o Canadá. El tamaño de la clave de Blowfish varía de 32 a 448 bits. El algoritmo en sí mismo consta de dos partes: una parte de expansión de subclave y una parte de cifrado. La parte de generación de claves es complejo, ya que debe ejecutarse en 521 repeticiones para generar todas las subclaves. Esto debe hacerse antes de que se realice el proceso de cifrado. Blowfish no requiere licencia para la implementación y su desempeño es superior al de DES y al de IDEA con el mismo tamaño de clave. La ventaja principal sobre otros algoritmos se deriva de sus tamaños de clave de longitud variable.
- **El algoritmo IDEA.-** Es un cifrado de bloque que se creó en 1990 por una compañía suiza. Utiliza 64 bits con ocho ciclos. Este cifrado se diseño para una implementación fácil en hardware y software. La seguridad de IDEA se basa en la utilización de tres tipos incompatibles de operaciones aritméticas en palabras de 16 bits. En este algoritmo, las operaciones de tres grupos algebraicos diferentes se mezclan (XOR, modulo de adición 216 y módulo de multiplicación 216+1). IDEA utiliza 52 subclaves, cada una de las cuales comienza con una longitud de 16 bits. La generación de subclaves es como sigue: la clave de 128 bits de IDEA se utiliza como las primeras ocho

subclaves K1 a K8. Las ocho siguientes se obtienen de la misma manera, después de una rotación circular a la izquierda de 25 bits. Este proceso se repite hasta que todas las subclaves de cifrado se hayan calculado.

- IDEA es un cifrado sólido que ha enfrentado muchos retos en su contra. Se considera inmune al criptoanálisis diferencial y no se han reportado ataques criptoanalíticos lineales. De cualquier modo existen una gran clase de claves débiles, 251, que en el proceso de cifrado podrían permitir que se recuperara la clave. Sin embargo, IDEA todavía tiene 2128 claves posibles, lo que hace que sea seguro.
- **Skipjack.-** El algoritmo de cifrado por bloques Skipjack utiliza una clave de 80 bits para cifrar bloques de 64 bits y emplea 32 ciclos. Se espera que Skipjack sea más seguro que DES en la ausencia de cualquier ataque analítico, ya que utiliza claves de 80 bits contra los 56 bits en DES.

- **Cifras de flujo.-** Una cifra de flujo son algoritmos simétricos que normalmente son más rápidos que los de bloque. Mientras que las cifras de bloque trabajan con partes de datos (64 bits), las de flujo trabajan sobre bits individuales, una buena característica de seguridad con las cifras de flujo es que aunque se utilice el mismo algoritmo y la misma clave, es posible que no aparezca el mismo texto cifrado; esto depende del momento en que los bits se encuentran en el proceso de cifrado.

    - **RC4.-** RC4 (una marca registrada de RSA Data Securities, Inc.), utiliza una cifra de flujo de tamaño de clave variable con operaciones algebraicas orientadas a bytes. El algoritmo se basa en la utilización de permutación aleatoria. El cifrado se diseño para ejecutarse rápidamente en el software y utiliza de 8 a 16 operaciones por byte. Fue desarrollado en 1987 por Ron Rivest. Este es un algoritmo no patentado que fue mantenido en secreto durante 7 años hasta que fue sacado a la internet por una persona anónima a la lista de correo de Cypherpunks. RC4 posee un status de exportación especial. Es el único algoritmo (junto con el RC2) permitido para la exportación desde los Estados Unidos con un tamaño de clave de 40 bits

usando el requerimiento del State Departament's Commodity Jurisdiction. Otros algoritmos (como el Blowfish) están actualmente limitados a claves de 32 bits para exportación.

**Algoritmos Asimétricos. -** También se los conoce como algoritmos de clave pública. Cada parte obtiene un par de claves, una pública y una privada. La clave pública esta hecha para que todos la conozcan mientras que la privada no. La ventaja de utilizar criptografía de clave pública es la seguridad y la conveniencia. La clave privada nunca necesita transmitirse o confiarse a alguien más. Por lo tanto no hay ninguna posibilidad de que la clave se comprometa ni de que la transmisión sea interceptada o decodificada.
Es necesario aclarar que la clave privada utilizada en estos algoritmos no es la misma clave utilizada en los criptosistemas de clave privada; la clave privada sólo descifra los mensajes que han sido cifrados con la clave pública asociada.
Entre los algoritmos más representativos de esta categoría son el algoritmo Diffie-Hellman y el algoritmo RSA.

- **Algoritmo Diffie-Hellman. -** El protocolo de acuerdo de claves Diffie-Hellman es una generación de claves negociada. Su fortaleza radica en le campo matemático finito de exponenciación de los logaritmos. El protocolo permite que dos usuarios intercambien una clave secreta en un medio inseguro sin secreto previo alguno. El algoritmo Diffie-Hellman también ha establecido la función de seguridad de un acuerdo de claves secretas, por lo tanto aunque sea un algoritmo asimétrico (clave pública), tanto el emisor como el receptor pueden utilizar un cifrado simétrico.
  Existen dos valores globales en el intercambio de claves Diffie-Hellman: P (que es un número primo) y G (llamado generador). G tiene una propiedad especial: es un entero menor que P y puede generar todos los números entre 1 y P-1 al multiplicarse por sí mismo. Se hace referencia a G como módulo de P. Antes de que los usuarios puedan comunicarse entre sí utilizando el intercambio de claves Diffie-Hellman necesitan acordar las claves secretas.
  El intercambio de claves es vulnerable al ataque del intermediario, existe debido a que este algoritmo no autentifica a los usuarios. Por lo tanto, se necesitan otros

pasos para evitar estos ataques, tales como el empleo de firmas digitales y las autoridades emisoras de certificados.

- **Algoritmo RSA.-** Este algoritmo fue ideado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman (RSA). Es sencillo de comprender e implementar, aunque las longitudes de sus claves son bastante considerables (ha pasado desde sus 200 bits originales a 2048 actualmente).

  En este algoritmo se emplean las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo. En concreto, emplea la función exponencial discreta para cifrar y descifrar, y cuya inversa, el logaritmo discreto, es muy difícil de calcular.

  Los cálculos matemáticos de este algoritmo emplean un número denominado Módulo Público, N, que forma parte de la clave pública y que se obtiene a partir de la multiplicación de dos números primos, p y q, diferentes y grandes (del orden de 512 bits) y que forman parte de la clave privada. La gran propiedad de RSA es que, mientras que N es público, los valores de p y q se pueden mantener en secreto debido a la dificultad que entraña la factorización de un número grande.
- La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable.

**Algoritmo Híbrido (PGP).-** Pretty Good Privacy (PGP) de Philip Zimmermann es un criptosistema híbrido, con todas las ventajas. Combina un algoritmo de clave privada con uno de clave pública. Esto le da tanto la rapidez de un sistema simétrico como las ventajas de un sistema asimétrico. PGP utiliza cuatro componentes: una cifra simétrica (IDEA), una cifra asimétrica (RSA), una función de transformación de código (MD5) y un generador de números pseudoaleatorios (PRGN).

PGP genera claves criptográficas fuertes, una privada, otra pública. El usuario guarda la clave privada, y distribuye la clave pública... insertada en el correo electrónico usando un fichero de firma, colocada en una página web, o en cualquier otro lugar. Asimismo es importante obtener las claves públicas de los contactos e importarlas en tu PGP. Cuando quieres enviar un correo cifrado, lo cifras usando la clave pública del receptor y sólo esa persona podrá descifrarlo usando su clave privada. También se puede firmar los ficheros y correos electrónicos para que cualquiera que tenga tu clave pública en su 'keyring' (anillo de claves) pueda comprobar si ese fichero en concreto proviene de ti y no de otra persona que se hace pasar por ti.
PGP generalmente comprime el texto plano antes de encriptar el mensaje (y lo descomprime después de desencriptarlo) para disminuir el tiempo de cifrado, de transmisión y de alguna manera fortalecer la seguridad del cifrado ante el criptoanálisis que explotan las redundancias del texto plano.

**Otros Cifrados.-** Además de esos sistemas de cifrado basados en clave públicas o secretas existen otros sistemas de cifrado basados en algoritmos. Estos nuevos sistemas no emplean claves de ningún tipo, sino que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud arbitraria. Esto es, cada cierta cantidad de texto elegido de forma arbitraria, se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra longitud clave, esta palabra longitud tiene una extensión de x bits preestablecidos, de esta forma el texto es irreconocible ya que solo se pueden leer números secuénciales y no guardan relación alguna entre sí. Estos algoritmos normalmente se basan en complejas operaciones matemáticas de difícil resolución. Y el secreto esta en que operaciones matemáticas sigue el algoritmo.
Entre los sistemas desarrollados a partir de la creación de algoritmos cabe destacar al menos dos, por su complejidad e importancia: MD5 y SHA.

- **MD5.-** Este algoritmo fue desarrollado por el grupo RSA y es un intento de probar con otros sistemas criptográficos que no empleen claves. El algoritmo desarrollado es capaz de obtener 128 bits a partir de un determinado texto. Como es lógico hasta

el momento no se sabe cuales son las operaciones matemáticas a seguir, pero hay alguien que dice que es mas probable que se basen en factores de números primos.

- **SHA, SHA-1.-** Es un algoritmo desarrollado por el gobierno de los Estados Unidos y se pretende implantar en lo sistemas informáticos de alta seguridad del estado como estándar de protección de documentos. El algoritmo obtiene 160 bits de un texto determinado. Aún cuando es más lento que otras funciones de transformación del código, se considera más seguro ya que tiene mayor longitud.

#### II.1.1.2.4.2 Certificados Digitales

Con la encriptación simétrica, tanto el remitente como el destinatario cuentan con una llave secreta compartida. La distribución de la llave secreta debe ocurrir (con la protección adecuada) antes de cualquier comunicación encriptada. Sin embargo, con la encriptación asimétrica, el remitente utiliza una llave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una llave pública para descifrar estos mensajes. La llave pública puede distribuirse libremente a todos los que necesiten recibir mensajes encriptados o firmados digitalmente. El remitente necesita proteger cuidadosamente sólo la llave privada.

Para garantizar la integridad de la llave pública se publica con un certificado. Un certificado (o certificado de llave pública) es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA); una autoridad en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora. La CA utiliza su llave privada para firmar el certificado. Si el receptor conoce la llave pública de la autoridad certificadora, el receptor puede verificar que el certificado sea, en efecto, de esa CA y, por lo tanto, que contiene información confiable y una llave pública válida. Los certificados se pueden distribuir de manera electrónica (a través de acceso al Web o correo electrónico), en tarjetas inteligentes o en discos flexibles.

### II.1.1.2.4.3 Autenticación

La autentificación es el segundo factor más importante en la configuración de una Red Privada Virtual. Pero, así como existen distintas arquitecturas, topologías y esquemas de cifrado en las Redes privadas Virtuales, también hay muchos esquemas de autentificación. Además, hay dos aspectos que son necesarios aclarar; la autentificación es quién tiene el permiso y la autorización es a que tiene acceso.

En este punto el usuario debe estar conscientes de que en cualquier infraestructura de comunicaciones en red existe la necesidad de un proceso de autentificación que permita a que el usuario acceda a los servicios de red y que impida, al mismo tiempo, el acceso no garantizado de los usuarios sin autorización.
En un sistema de contraseñas normales, tanto el usuario como el servidor, conocen la contraseña, para el inicio de una sesión válida, el usuario ingresa la contraseña y el servidor la compra con la que tiene almacenada y si coinciden se permite el ingreso. Esto produce como resultado una debilidad en la seguridad, ya que, si asumimos que el usuario no revela su contraseña, está permanecerá guardada en el servidor, y puede ser susceptible de ataques.

**Contraseñas Del Sistema Operativo. -** En una organización existen varios servidores y aplicaciones protegidos con contraseñas. Los usuarios pueden tener varias contraseñas distintas para los diferentes servidores. A continuación, se presentan algunas recomendaciones para utilizar en una Red Privada Virtual.

- La identificación del usuario. - En lo posible debe ser Alfanumérica y de largo suficiente para que sea mnemotécnico, además, no deberían ser reutilizados en distintos usuarios ya que se pierde el control sobre las pistas de auditoria. Existen distintos métodos:
    - Apellido del usuario, si hay repeticiones apellido y parte del nombre. Ejemplo: JATON, JATONRE, RAMIREZ, RAMIREZO
    - Tres primeras letras del apellido y los nombres y el legajo (se utiliza en empresas grandes) Ejemplo: PAG81455 (Pablo Andrés Gietz)

- Tipo de usuario y legajo: ejemplo: EMP4517 (para empleado) GER7782 (para gerente). Desventajas: es difícil de administrar por que no se puede memorizar, además no permite el cambio de función sin cambiar el usuario.

- Contraseñas. - La contraseña es el método que sirve para autentificar a los usuarios. Es por lo general uno de los eslabones más débiles de la seguridad, ya que los usuarios no la utilizan correctamente, o no le dan la debida importancia. Las contraseñas deben ser secreta e intransferibles, mínimo de ocho caracteres, no debe ser escrita por el usuario para poder recordarla, el usuario puede cambiar su contraseña, debe caducar por lo menos en 45 días, el administrador del sistema no debe poder ver las contraseñas, y al tercer intento de ingreso no válido el sistema lo debe rechazar.
- Log de seguridad. - Se deben proteger contra accesos no autorizados, se deben controlar y respaldar diariamente. No es necesario imprimirlos. Estos son los registros que se tiene de los accesos, para en posterior poder realizar auditorías.

**S/KEY. -** Las contraseñas descartables del sistema S/KEY tienen una extensión de 64 bits. Esto se basa en la creencia de que son lo suficientemente extensas como para ser seguras y lo suficientemente cortas como para ser introducidas manualmente cuando sea necesario. El sistema S/KEY aplica funciones de transformación del código varias veces, produciendo una salida final de 64 bits. MD4 acepta un número arbitrario de bits como entrada y produce una salida de 128 bits. Las funciones de transformación del código seguras de S/KEY consisten en aplicar MD4 a una entrada de 64 bits y plegar la salida de MD4 con la función O exclusiva (XOR) para producir otra salida de 64 bits.
S/KEY, como se dijo anteriormente, es un sistema de contraseñas descartables, lo que significa que cada contraseña utilizada por el sistema se usa sólo para una autentificación. Las contraseñas no pueden volverse a utilizar, por lo tanto no pueden interceptarse ni usarse como una forma de predecir las contraseñas futuras.

**Radius. -** El protocolo de servicio de autenticación de usuario remoto de marcación (RADIUS) es un método basado en el UDP para administrar la autenticación y autorización

de usuarios remotos. Los servidores de RADIUS pueden localizarse en cualquier lugar de Internet y proporcionan autenticación (incluyendo PPP PAP, CHAP, MSCHAP y EAP) para su NAS de cliente. Al mismo tiempo, los servidores de RADIUS pueden proporcionar un servicio proxy para transmitir las solicitudes de autenticación a servidores distantes de RADIUS.

**Kerberos. -** Kerberos V5 es un protocolo de autentificación confiable fabricado por un tercero que permite que un proceso se ejecute en un cliente para demostrar su identidad frente a un servidor Kerberos [LIB02], sin tener que enviar los datos a través de la red, lo cuál permitiría que un atacante o un verificador se hiciera pasar por un director.
Kerberos es un sistema de cifrado DES simétrico. Utiliza una función de clave privada centralizada y en el núcleo del sistema se encuentra el centro de distribución de claves [RFC1510].

**LDAP. -** El protocolo ligero de acceso a directorio (LDAP) [RFC2251] es un protocolo estándar en la industria para acceder a servicios de directorio. Este es extensible, independiente del distribuidor y se basa en los estándares. Permitiendo que un administrador asigne una variedad de propiedades de conexión para sesiones de marcación o de VPN destinadas a usuarios individuales o grupos. Estas propiedades pueden definir los filtros por usuario, la autenticación requerida o los métodos de codificación, entre otras.

**EAP. -** El Protocolo de marcación extensible (EAP) es una extensión propuesta por la IETF para el PPP que permite que los mecanismos de autenticación arbitraria se utilicen para la validación de una conexión de PPP. EAP fue diseñado para permitir la adición dinámica de módulos de conexión de autenticación en ambos extremos de clientes y de servidor de una conexión, permitiendo a los distribuidores proveer un nuevo esquema de autenticación en cualquier momento, proporcionando la flexibilidad más alta en particularidad y variación de autenticación.
Con el EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor y el segundo proporciona certeza de que el

usuario ha contactado el servidor que esperaba. Ambos sistemas se basan en una cadena de autoridades confiables para verificar la validez del certificado ofrecido.

El certificado del usuario puede almacenarse en la PC de cliente de marcación o en una tarjeta inteligente externa, En cualquier caso, el certificado no puede ser accesado sin alguna forma de identificación de usuario entre el usuario y la PC del cliente.

**ISAKMP/Oakley. -** es el protocolo estándar para realizar una asociación de seguridad entre el transmisor y el receptor. Durante un intercambio de ISAKMP/Oakley, las dos máquinas acuerdan los métodos de autenticación y seguridad de datos, realizan una autenticación mutua y después generan una clave compartida para la codificación de datos subsecuente.

Después de establecer la asociación de seguridad, la transmisión de datos puede proceder para cada máquina aplicando tratamiento de seguridad de datos a los paquetes que transmite al receptor remoto. El tratamiento puede simplemente asegurar la integridad de los datos transmitidos o puede codificarlos también.

### II.1.1.2.4.4 Cifrado Punto a Punto

Los túneles cifrados de Red Privada Virtual aseguran los datos conforme pasan a través de la red pública. Existen por lo general dos términos que se asocian con la tecnología VPN que son cifrado y encapsulamiento. La principal diferencia es que el cifrado solo codifica los datos, mientras que el encapsulamiento hace un paquete de datos del paquete original, lo envuelve en su propio paquete y después codifica todo el paquete.

### II.1.1.2.4.5 Administración de seguridad centralizada

En cualquier momento en la arquitectura cliente/servidor hay distintas aplicaciones ejecutándose en varios servidores que soportan distintos clientes en redes diferentes. Imaginase lo que es administrar la seguridad en entornos tan heterogéneos y con varios tipos de aplicaciones corriendo en diferentes servidores.

Por las razones mencionadas anteriormente el ideal es poseer un especialista para cada Sistema Operativo o plataforma para administrar. La mayoría de las veces una persona puede atender varios sistemas operativos. La mínima dotación deseable es de dos personas

altamente capacitadas que puedan sustituirse una a la otra. Una persona para administrar la seguridad es importante para que los otros puedan investigar y desarrollar nuevas implementaciones.

Tengamos en cuenta que si la política es que todos los nuevos productos de Informatización tengan seguridad, el sector debe tener recursos suficientes para acompañar los desarrollos desde el momento cero.

Existen algunas funciones que tradicionalmente entran en conflicto con los administradores de seguridad, estas son: el DBA (Data base administrator - administrador de base de datos) el NA (Administrador de red - Network administrator), el SA (Administrador de sistema - System administrator) y el administrador de seguridad. En todos estos casos el conflicto surge por que el Sistema Operativo no permite la adecuada separación de funciones de los distintos perfiles, lo que conduce a que cada uno de los mencionados pueda eventualmente realizar funciones solo autorizadas a otro. Por ejemplo en el Unix el root es el usuario con máximo nivel de autorización, pero no solo administra la seguridad, sino también la configuración, las bases de datos, etc. En el caso de Windows NT, el usuario Administrador, se debe utilizar para instalar o para realizar ciertas tareas de configuración, por lo que se debe compartir para las distintas tareas.

Desde el punto de vista de seguridad el sistema operativo debería permitir configurar los siguientes perfiles.

- **SecAdmin:** Administrador de seguridad. Administra altas, bajas, y cambios de perfiles de usuarios. Otorga, permisos de acceso a los recursos. Puede auditar a los usuarios.
- **System Administrator:** Instalación de software de base, administración de recursos (capacidad, performance no permisos), capacity planning, etc. Sin acceso irrestricto a los datos. Con utilización controlada de utilitarios sensitivos.

- **Network Administrator:** Atiende y monitorea la red. Instala y configura los componentes de software y hardware. Resuelve problemas de performance y conexiones.
- **DBA:** Administra la base de datos. Genera las estructuras, los índices, el diccionario de datos, administra los espacios, la performance, etc. Debe permitir al SecADmin la administración de permisos (Grant y Revoke).
- **Desarrollador:** Puede modificar programas, compilar en librerías de test, y probar con datos de prueba. EL desarrollador puede tener línea de comandos restringidos.
- **Implementador:** Debe pasar los programas de desarrollo a Producción mediante un mecanismo que asegure la transparencia. Puede intervenir operaciones. El implementador puede tener línea de comandos restringidos.
- **Operador del sistema:** Puede operar el sistema, prenderlo, apagarlo, descolgar usuarios por terminales, etc. El operador no debe tener línea de comandos.
- **Usuarios finales:** Solo deben acceder a las aplicaciones mínimas que necesitan para desarrollar su tarea.

#### II.1.1.2.4.6 Procedimientos de respaldo/restauración

Las claves de los dispositivos de las redes privadas virtuales son lo que hace que esta tecnología sea segura. Si los dispositivos de las redes privadas virtuales presentan problemas, ¿cómo pueden reinstalarse? Las claves de dichos dispositivos son conocidas por las personas que configuraron el servicio de las Redes Privadas Virtuales: Si no es posible restaurar las claves, entonces las comunicaciones con las otras partes no podrán restablecerse. Por lo tanto, su política de respaldo y restauración debería tomar en cuenta los sistemas operativos, los niveles de reparación, la política de reglas implementadas, y las claves asociadas con la solución particular de las Redes Privadas Virtuales.

**Planes de contingencia. -** En lo posible se debe escribir uno, esto ayuda a pensar en cómo implementarlo, diseñarlo, entrenar al personal, implementarlo y probarlo.

Existe un equipo de especialistas que representa a las personas que conocen y que son imprescindibles para llevar adelante la ejecución del plan. Ellos entran en acción como un equipo del tipo SWAT.

Se debe poseer redundancia de los elementos críticos, array de discos, canales de comunicación, dispositivos de backup-restore de alta velocidad, o al menos contar con medios alternativos. Por ejemplo, si no se pueden disponer de dos servidores funcionando a la par, acordar el proceso en un servidor de terceros, o disponer de un plan de recuperación acorde con los tiempos de la empresa (reparación o cambio del servidor) esto debe ser probado.

SI no se dispone de dos links de comunicaciones del mismo ancho de banda disponer de un alternativo y probarlo.

En empresas grandes se dispone de planes de continuidad de negocio que preparan a la organización para cualquier tipo de contingencia. Se determina, por ejemplo: en caso de destrucción total de la casa matriz. Donde deben presentarse los empleados a trabajar. Donde se monta las oficinas de emergencia. Que se le debe decir a la prensa. Quien monta los sistemas de emergencia, etc.

### II.1.2 Metodología Implementación VPN

La información es una ventaja crítica para cualquier compañía, y poseer ésta a tiempo y con seguridad es fundamental para el desarrollo de cualquier organización. Además, se debe tomar en consideración que la fuerza laboral del futuro será móvil, y una compañía u organización no estarán en capacidad de construir o rentar suficientes líneas a través de todo el mundo para garantizar conexiones seguras. Y es aquí donde toma importancia la implementación de una red privada virtual, ya que como se mencionó en los capítulos anteriores, una red privada virtual utiliza Internet como medio de transmisión de datos, lo que permite un considerable ahorro en términos económicos.

Se debe tener presente también que en la actualidad muchas compañías utilizan Internet para enviar correo electrónico; sin embargo, la gran mayoría no toma en consideración que ese correo se envía en modo texto, es decir sin ningún tipo de seguridad, y cualquiera que tenga acceso a Internet puede leerlo. Es por esta razón que el presente trabajo trata de familiarizar a los lectores con la

tecnología de redes privadas virtuales, para hacer de sus redes más optimas y seguras al momento de transmitir y recibir datos desde el exterior, y por qué no también desde el interior.

La metodología que a continuación se va a describir ha sido realizada tomando como experiencia organizaciones pequeñas y tiene como objetivo ayudar al entendimiento y mejor manejo de la teoría y la práctica en el desarrollo de Redes Privadas Virtuales.

Para obtener una Red Privada Virtual exitosa es necesario tomar en cuenta algunos factores que son de vital importancia los mismos que se convertirán en pasos para el análisis y posterior implementación de una Red Privada Virtual.

#### II.1.2.1 Formación de un Equipo Ejecutor

Si se toma en consideración de que una Red Privada Virtual es un conjunto de aplicaciones de software cliente-servidor basados en tecnología Internet para la transmisión y recepción de datos, y que utilizan las plataformas de red local (LAN), redes a nivel mundial (WAN), protocolos TCP/IP y los servidores de su organización para prestar servicios de una red privada, entonces en el momento que se emprende la tarea de poner en marcha una Red Privada Virtual se hace necesario la formación de un Equipo Ejecutor, el cual debe ser conformado por un pequeño grupo de especialistas y a este agregar un número pequeño de personal con capacidad de decisión y conocimiento de la organización o empresa, de tal manera que se pueda asignar responsabilidades al personal, además que el equipo debe tener una gran capacidad de liderazgo y responsabilidad para asumir el reto de poner en marcha un proyecto de Redes Privadas Virtuales.

Los miembros recomendados para la conformación del Comité Ejecutor son: las direcciones de sistemas y recursos humanos. Deben concurrir además los gerentes cuyas divisiones vayan a tener contenido en la Red Privada Virtual. Se recomienda que al principio asistan todos los gerentes de la organización, para que estos decidan que tipo de información es confidencial y crucial para la compañía y encomienden ponerla en una red privada virtual, ya que como se explico en capítulos anteriores no es conveniente poner todo el tráfico de información que se genere en la organización en una Red Privada Virtual, ya que esta produce una sobrecarga de trabajo.

### II.1.2.2 Fijación del Alcance

Una vez que se ha tomado la decisión de implementar una Red Privada Virtual es necesario definir argumentos que serán tomados en cuenta para la implementación, y que deberán cumplirse en lo posterior. Temas como los que se describen a continuación deberían ser tomados en consideración:

- ¿Para qué tener una Red Privada Virtual?
- ¿Quiénes serán los usuarios?
- ¿Qué conocimientos, información o datos se van a poner en la Red Privada Virtual?
- ¿Utilizará la Redes Privadas Virtuales para comercio global?
- ¿Instalará una extranet?
- ¿Su organización posee la capacidad técnica adecuada para mantener e instalar una Red Privada Virtual?
- ¿Cómo se integrará la Red Privada Virtual con la Red de la compañía?
- ¿Qué respuesta o resultados se desea obtener?
- ¿Qué tipo de seguridad de utilizar en la red privada virtual?
- ¿Cómo se construirá?
- ¿Qué servicios se colocarán primero, cuáles después?
- ¿Su gobierno como considera al cifrado? Se debe tener en cuenta que algunos gobiernos consideran al cifrado como arma, por lo tanto, regula su uso.

El Comité Ejecutor será el organismo encargado de definir el "Por qué" y "Para qué" de una Red Privada Virtual. Para esto se analizará las expectativas creadas, las mismas que llevaron a la decisión de construirla, los problemas o retos que tienen factibilidad de resolverse con esta tecnología. Los objetivos buscados, a quienes se desea servir, el modelo administrativo con que se cuenta, y un punto muy importante a discutir, los parámetros que serán utilizados para medir el éxito. En este paso se debe definir la política de tecnología, recursos necesarios y los responsables de obtener la información que será entregada a los creadores de la Red Privada Virtual.

Es importante recalcar que el éxito del proyecto se fundamenta en la calidad del análisis de factibilidad y éste determina el grado de participación y compromiso de los miembros del Equipo Ejecutor, esto con la finalidad de que tenga éxito la implementación de la red privada virtual. En algunos casos es necesario obtener el permiso de los altos ejecutivos con la finalidad de que exista mayor seguridad en las acciones y obtener éxito en este paso.

### II.1.2.3 Estudio y Análisis

Luego de que se ha completado con la formación del equipo ejecutor, y la fijación del alcance del proyecto, es necesario realizar un estudio y análisis detenido para saber a ciencia cierta qué parámetros deben cumplir las Redes Privadas Virtuales que se desea implementar.

Durante el análisis el equipo que desarrolla la Red privada virtual intenta identificar qué información ha de ser procesada, que función y rendimiento se desea, cuál será el comportamiento de la red, que interfaces van a ser establecidas, que restricciones se pondrán, que tipo de seguridad de necesita, que parámetros se sacrificarán a favor de la seguridad y que criterios de validación se necesitan para definir una red privada virtual correcta. Es decir, durante el estudio y análisis deben identificarse los requisitos clave de la Red privada virtual.

El Análisis de factibilidad y la información en éste recolectada serán analizados por parte del Equipo Ejecutor asignado al proyecto y con esta base se propondrán los objetivos definitivos, como, por ejemplo, que aplicaciones se pondrán en las Redes Privadas Virtuales, que servicios se brindarán en línea y en que fases se construirá.

Durante la fase de estudio y análisis también se deben estudiar los sistemas y soluciones utilizados por la organización y el manual de identidad corporativo.

### II.1.2.4 Elección de la Plataforma

Para la implementación de una Red Privada Virtual es muy importante la elección de la plataforma en cual se la va a desarrollar. En el mercado existe una gran variedad de soluciones, por lo que se hace necesario elegir una. También es necesario mencionar que las Redes Privadas Virtuales pueden ser construidas tanto por software, como por hardware o una combinación de éstas. Para realizar la elección de qué tipo de Redes Privadas Virtuales instalar es necesario analizar los siguientes puntos:

- Software existente en la empresa.
- Aplicaciones existentes en la empresa.
- Plataforma existente en la empresa.
- Servicios que posee la plataforma.
- Seguridades que brinda la plataforma.
- Soporte técnico que posee la plataforma.

- Tipo de servidores que posee la empresa.
- Costo de la plataforma.

En el momento que se ha tomado la decisión de implementar una Red Privada Virtual, el Equipo Ejecutor deberá levantar un inventario del Hardware y Software existente en la empresa. Luego de levantado el inventario es necesario realizar un análisis para determinar que tipo de Red Privada Virtual se ajusta más a las necesidades de la organización.

Debido a que siempre será necesario contar con información y personal capacitado a tiempo y a mano, sobre todo en lo referente al manejo de la plataforma y a posibles dificultades que se encuentra en la configuración e implantación de una Red Privada Virtual, se ha visto necesario indicar que un punto de vital importancia para la selección de una Plataforma es el soporte técnico que tienen cada una de las empresas distribuidoras y dueñas de las diferentes plataformas.

Generalmente para implantar una red privada virtual no se empezará desde cero en lo que se refiere a Hardware y Software, en la actualidad la mayoría de las empresas poseen equipos computacionales y en algunos casos se encuentra redes ya configuradas, en este caso se debe analizar qué tipo de servidores tenemos y cuál será la plataforma que se debe utilizar. Es necesario comprender que, en algunos casos por costos de los servidores, o porque la tecnología es muy obsoleta, es muy probable que se tenga que empezar desde cero, es decir que se debe asumir que no existe nada.

Cuando se empieza desde cero el equipo ejecutor tiene más opciones para poder tomar la mejor decisión, ya que no se ve restringido a la tecnología existente, ya que, si existe algo, en lo posible se debe tratar de que las Redes Privadas Virtuales sean compatibles.

### II.1.2.5 Propuestas de Soluciones. (Diseño)

El diseño se lo pone como quinto punto, ya que luego de realizar el análisis se puede realizar el diseño, pero el diseño se ve afectado por la plataforma elegida, con esto se quiere decir que el diseño se lo debe realizar sólo después de haber realizado el análisis y de haber elegido una plataforma, ya que existen muchas opciones para instalar una red privada virtual.

Solo armados con el Análisis de factibilidad, la estructura general y la definición de los servicios a ser implementados, es posible acometer eficazmente la concepción, creación y construcción de la Red Privada Virtual. En esta etapa se definirán la filosofía y enfoque globales; se concebirá la

estructura lógica de la red privada virtual y se visualizará el conjunto general de la red, y esta deberá ser aprobada por el equipo ejecutor.

En la propuesta de soluciones se debe tener en consideración los siguientes aspectos:

- ¿Qué aplicaciones van a pasar por la Red Privada Virtual?
- ¿Qué tipo de infraestructura de hardware soporta su organización?
- ¿Cuántos usuarios estima que utilizarán la Red Privada Virtual?
- ¿El tráfico que pasará por la VPN es pesado?
- ¿Qué tipo de seguridades se utilizarán en la Red Privada Virtual?

#### II.1.2.6 Seguridades

Cómo la construcción de una Red Privada Virtual se basa en las seguridades, en este punto se debe ser muy exigente para poder disminuir a cero el riesgo de pérdida o daño de información en la Red Privada Virtual, y para esto se hace necesario la implantación de una política de Seguridad basándose en los siguientes parámetros:

- Fijación de Objetivos
- Relación Costos vs Riesgos

##### II.1.2.6.1 Fijación de Objetivos

Como se mencionó anteriormente, las seguridades es uno de los pasos de mayor importancia para la implantación de una Red Privada Virtual. Es necesario recalcar que con una buena política de seguridades se llegará al éxito en la propuesta, para lo cual se deben hacer algunas preguntas que permitirán conseguir el gran objetivo.

Si se toma en cuenta que es lo que se va a proteger, de que va a proteger y si se considera algunas sugerencias del equipo ejecutor (ya que éstos fueron escogidos precisamente para poder realizar un plan de seguridad), se encontrará en la capacidad de establecer cuales son las prioridades de seguridad corporativa, de tal manera que se pueda obtener una política de seguridad que brinde las mejores condiciones para la red implementada.

#### II.1.2.6.2 Relación Costos vs. Riesgos

Antes de fijarse objetivos y prioridades de seguridad es necesario levantar un inventario de las posibles amenazas y debilidades que existen, luego se someterá a un análisis en el cual se debe comparar costo de implantar la seguridad con el costo de la información que se desea proteger, el mismo que brindará un panorama bastante amplio, y se debe tomar la decisión de que es lo que va a proteger, porque realmente sería innecesario proteger algo que tenga menos costo que el valor de la seguridad a implantar.

### II.1.2.7 Plan de Contingencia

Cuando se tiene grandes volúmenes de información, y es de vital importancia para la organización el correcto funcionamiento de la red privada virtual, resulta necesario, por no decir imprescindible, el tener un plan de contingencia tanto durante la fase de desarrollo y durante el funcionamiento de la red privada virtual.

Durante el desarrollo se debe considerar un plan que garantice finalizar con éxito la implementación de la red privada virtual y para ello se debe tener en cuenta los siguientes aspectos:

- ¿El personal encargado de desarrollar las Redes Privadas Virtuales tiene la suficiente capacitación y experiencia en este tema?
- ¿En el medio en el que nos encontramos existen varios proveedores de Internet que puedan brindar soporte para las Redes Privadas Virtuales?
- ¿Todo el proyecto se está documentando?
- ¿Qué acciones se tomarán si el equipo de desarrollo se va?
- ¿Qué riesgos podrían hacer que nuestro proyecto fracasará?
- ¿Qué métodos y herramientas deberíamos emplear?
- ¿Cuánta importancia hay que darle a la calidad?
- ¿Tenemos aplicaciones que entren en conflicto con las Redes Privadas Virtuales?

Estas y otras preguntas más deberán ser analizadas para poder finalizar con éxito la realización de las Redes Privadas Virtuales.

Para cuando la Red privada virtual esté en funcionamiento también se deberá contar con un plan de contingencia, para garantizar a la organización su funcionamiento aún en casos extremos, para ello se deben analizar las siguientes preguntas.

- ¿Qué pasa si el proveedor de Internet cierra sus oficinas?
- ¿Qué acciones se realizarán en caso de que los servidores fallen?
- ¿El personal técnico que se tiene está en capacidad de resolver los problemas?
- ¿Se tiene servicios de emergencia?
- ¿Quién administrará la red en caso de que el personal a cargo salga de la organización?

#### II.1.2.8 Costos

Puesto que la parte económica juega un papel muy importante en el éxito de una Red Privada Virtual, se considera muy importante analizar los siguientes puntos para determinar los costos de implementar una Red privada virtual:

- Hardware
- Software
- Capacitación
- Contratación de Servicios

##### II.1.2.8.1 Hardware

Como se había mencionado anteriormente es necesario saber con qué Hardware cuenta la institución, de tal manera que después de haber levantado un inventario de los equipos existentes, se pueda determinar que equipos se van a adquirir y cuáles son los equipos existentes que se podrán utilizar, posteriormente se determina las características del hardware que se va adquirir de tal forma que se pueda hacer un concurso de ofertas para la adquisición de los diferentes implementos para la puesta en marcha de la Red Privada Virtual.

##### II.1.2.8.2 Software

Dependiendo de la plataforma elegida, los servicios y las aplicaciones que a determinado momento la Red Privada Virtual tenga a disposición de los usuarios, los costos de la implementación serán

elevados, moderados o bajos, pero lo que si hay que estar muy consiente es que el servicio que brindará la Red Privada Virtual debe ser de óptima calidad de tal manera que haya valido la pena la inversión, por esto el Equipo Ejecutor tiene que tener la capacidad para demostrar a las autoridades de que el costo de la implementación no es un gasto más bien es una inversión que mejorará la rentabilidad y los servicios que brinda la empresa.

#### II.1.2.8.3 Capacitación

Uno de los rubros que se debe tener presente en la implementación de una Red Privada Virtual es la capacitación, en vista de que el personal técnico que se encargara de realizar la implementación necesitará que se le ponga al día en la tecnología de Redes Privadas Virtuales.

Además, es necesario hacer conocer a las máximas autoridades que la capacitación siempre será una inversión y por tal motivo brindarle especial atención, para evitar posteriores inconformidades tanto de los usuarios como de las autoridades de la empresa.

#### II.1.2.8.4 Contratación de Servicios

Este es un rubro que en algunas empresas se lo puede evitar, en vista de que el personal existente en la institución puede estar en condiciones suficientes para llevar adelante un proyecto de esta magnitud. En el caso de no existir se hace necesario la contratación de personal especializado, en este caso diremos que será el rubro más elevado, en vista de que obtener mano de obra calificada y cualificada llevará una inversión bastante elevada.

### II.1.2.9 Implementación

Durante la implementación se utilizarán especialmente la fase del análisis y la fase del diseño, es necesario aclarar que antes de empezar con este punto, el personal que va a implementar la red privada virtual ya debe estar lo suficientemente capacitado acerca de esta tecnología para poder finalizar con éxito las Redes Privadas Virtuales.

En esta fase se configurarán los servidores, los clientes y demás equipos que sean necesarios para la red privada virtual.

### II.1.2.10 Mantenimiento

El mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno de la red privada virtual, y a cambios debidos a las mejoras producidas por los requisitos cambiantes de la organización.

Por lo delicado del asunto, una red privada virtual debe ser administrado apropiadamente, es decir, debe ser mantenido, actualizado y además renovado con regularidad para garantizar su uso, ya que es fundamental que siempre los usuarios se fíen en la confidencialidad que proporciona la red privada virtual, ya que, si un usuario sospecha que su información no está segura, talvez se restringa utilizar la Red Privada Virtual, especialmente si se está realizando negocios a través de ella.

#### II.1.2.10.1 El Mantenimiento preventivo

En si, se refiere a las actividades de orden técnico al nivel de hardware y software en producción, para garantizar la integridad de los archivos y sus respectivos enlaces y la verificación de la disponibilidad de la red privada virtual. Otra fase del mantenimiento consiste en la verificación constante de fallas en la seguridad, ya que es imposible determinar en un momento dado la inviolabilidad de la Red privada virtual.

#### II.1.2.10.2 El Mantenimiento correctivo

En este punto nos referimos a que, incluso llevando a cabo las mejores actividades de garantía de calidad, es muy probable que la organización descubra defectos en la red privada virtual. El mantenimiento correctivo modifica la red privada virtual para arreglar los defectos.

#### II.1.2.10.3 La Actualización

Se refiere a los pequeños cambios a servicios de acuerdo con la actualidad y el día a día de la organización, por ejemplo, el cambio de contraseñas, la implementación de un protocolo más seguro para la autentificación, el crecimiento de la organización, entre otros.

#### II.1.2.10.4 La Renovación

Basados en la realimentación y análisis de resultados que se obtengan de la actividad de medición, se realizará la renovación de la red privada virtual. Esta, se refiere a los cambios más profundos en el contenido, servicios, topologías y arquitectura de la red privada virtual. La renovación lleva a las Redes Privadas Virtuales más allá de sus requisitos funcionales originales.

Tanto el Mantenimiento, la Actualización y la Renovación pueden ser subcontratados con Personal externo, pero sólo en un comienzo y con el apoyo activo de su personal, de lo contrario su organización se perderá la oportunidad de recorrer la curva de aprendizaje de esta tecnología o lo que también se podría decir que el personal se perdería la oportunidad de capacitarse o de estar acorde a las necesidades actuales.

Esta tecnología está en su infancia, y como todo aquello que vale la pena, hay que comenzarlo temprano, antes que las barreras de entrada las construya su competencia.

### II.1.2.11 Medición de Resultados

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto, la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.

## II.1.3 Desplegado de Servicios

### II.1.3.1 Servicios de Hosting

Un hosting es un servicio de alojamiento web. Al igual que si se tratara de un alojamiento normal, los servicios de hosting en lugar de alojar personas alojan los contenidos de tu web y tu correo electrónico para que puedan ser visitados desde cualquier dispositivo conectado a Internet. Cuando quieres consultar un archivo o documento en tu ordenador, ese contenido está almacenado en algún sitio, puede ser en el disco duro de tu equipo o en un dispositivo de almacenamiento USB, por ejemplo.

Lo mismo sucede con el contenido de las webs, debe estar almacenado en algún sitio y para que pueda ser consultado desde cualquier dispositivo conectado a Internet tendrá que estar almacenado

en un servidor web. Un servidor es un equipo informático mucho más potente que un ordenador convencional, conectado a Internet las 24 horas para que en todo momento puedan ser visitados los contenidos que almacena.

#### II.1.3.1.1 Tipos de Hosting

Existen diferentes tipos de alojamiento web en función de sus características. Los tipos de hosting principales son el hosting compartido, los VPS y los servidores dedicados.

##### II.1.3.1.1.1 Hosting compartido

El hosting compartido es el tipo de alojamiento web más utilizado. En esta modalidad, las cuentas de hosting de diferentes usuarios se alojan en un mismo servidor físico, en el que comparten recursos como la memoria RAM y la CPU. Dentro del hosting compartido también existen diferentes tipos de servicio, en función de su configuración.

El hosting compartido más habitual en el mercado es un servicio básico, en el que los diferentes clientes comparten los recursos del servidor de forma que el comportamiento de la cuenta de un usuario puede afectar a las demás.

Los servicios de Hosting tienden a ofrecer otra modalidad de hosting compartido con aislamiento de cuentas. Utilizamos CloudLinux y CageFS para aislar cada cuenta de hosting, para garantizar la estabilidad, el rendimiento y la seguridad del servicio. Así conseguimos que posibles problemas en la cuenta de un usuario no afecten a las demás cuentas alojadas en ese servidor.

Todos sus servicios de hosting comparten esta característica, pero tenemos líneas especializadas para diferentes tipos de proyectos: Hosting WordPress optimizado para crear web con WordPress, Hosting WooCommerce para tiendas online y Hosting web para otro tipo de webs creadas con HTML y PHP.

##### II.1.3.1.1.2 Hosting VPS

Un VPS es un servidor privado virtual. En este tipo de hosting, los usuarios comparten un mismo servidor físico, pero a diferencia del hosting compartido no comparten los recursos.

El servidor físico se divide en una especie de compartimentos estancos mediante virtualización; y cada uno de esos compartimentos sería un VPS con sus propios recursos asignados y garantizados. A diferencia del hosting compartido, los VPS garantizan no solo los consumos de espacio y transferencia, sino también la RAM y la CPU asignada al servicio.

#### II.1.3.1.1.3 Hosting elástico

El hosting elástico es un tipo de hosting que reúne las ventajas de un hosting compartido y las de un VPS. En él compartiremos servidor físico con otros usuarios, pero tendremos recursos garantizados como en el VPS.

#### II.1.3.1.1.4 Hosting Cloud

El cloud o hosting en la nube es un tipo de alojamiento web que se ofrece desde una infraestructura compuesta por varios servidores que trabajan de forma conjunta. El servicio se distribuye en diferentes equipos conectados a una misma red, formando esa nube o cloud.

Es un tipo de alojamiento utilizado normalmente por empresas con necesidades inestables, que tienen variaciones frecuentes por altos picos de tráfico en diferentes períodos de tiempo. El cloud les ofrece una alta disponibilidad de recursos y garantías de uptime ante esas variaciones de demanda, mediante esa configuración en forma de clúster con balanceadores de carga.

#### II.1.3.1.1.5 Servidor dedicado

Un servidor dedicado es un tipo de hosting web en el que se ofrece un equipo físico completo para cada cliente. No se comparte el servidor con ningún otro usuario, por lo que todos los recursos están disponibles y garantizados para un único cliente.

### II.1.3.1.2 Políticas de Hosting

Las Empresas proveedoras de servicios de hosting mismo también tienen políticas para la obtención de sus servicios que están principalmente definidas por las reglas del país en las que dichas empresas residen, por ello al momento de escoger un servicio de hosting es muy importante tomarlas en cuenta.

Para la implementación de este proyecto las políticas que mas nos interesan son las políticas DMCA y las políticas de Información Reservada.

**II.1.3.1.2.1 DMCA**

¿Alguna vez se ha preguntado cómo algunos sitios web tienen contenido con derechos de autor en su sitio y no se les pide que lo eliminen? Si es así, siga leyendo mientras nos sumergimos en el concepto de Hosting Ignorado por DMCA.

DMCA son las siglas de Digital Millennium Copyright Act , que fue adoptada en 1998. La ley prohíbe que los sitios web carguen contenido que no sea legalmente suyo. Esto incluye materiales como videos, música y fotografías.

Por lo tanto, la DMCA puede obligar a los sitios web a eliminar o eliminar contenido protegido por derechos de autor de su página. Sin embargo, ciertos sitios web logran mantener contenido ilegal en sus sitios utilizando DMCA Ignored Hosting. Aquí encontrará todo lo que necesita saber sobre el servicio y cómo puede utilizarlo para proteger su sitio web.

**¿Cómo Funciona DMCA?**

DMCA bloquea o suspende cualquier contenido que se haya encontrado que contiene información con derechos de autor. Esto puede incluir textos, fotos o videos que no pertenecen legalmente al sitio web.

Una vez que el propietario de los derechos de autor se da cuenta de que su contenido se está utilizando en otro sitio web, envía un correo electrónico notificando al anfitrión de la infracción. Luego, el anfitrión procede a bloquear o suspender por completo el sitio web.

Aunque la DMCA es una ley destinada a proteger la propiedad individual, a menudo es utilizada indebidamente por partes con motivos ocultos.

**¿Cómo las empresas ignoran la DMCA?**

Ningún proveedor de alojamiento web puede ignorar la DMCA. Sin embargo, lo que hacen muchos servidores web es ubicar sus servidores en países que no cumplen con la DMCA. Esto ayuda a proteger cualquier contenido ilegal en su sitio web.

Además, un buen proveedor de alojamiento evita que varias partes los obliguen a eliminar su contenido. Esto facilita que su sitio web permanezca activo y obtenga un gran número de seguidores.

Si bien el host facilita el Hosting Ignorado de DMCA, es posible que deba lidiar con varias quejas que han sido fundamentadas con evidencia creíble. Esto no significa que deba eliminar el contenido, aunque garantiza que se aborden los intereses de todas las partes.

**¿Por qué Usar Hosting ignorado por DMCA?**

Por qué molestarse en conseguir un proveedor con Hosting Ignorado por DMCA cuando simplemente puede crear su sitio web con contenido auténtico. Sin embargo, el mundo se ha convertido en una aldea global donde la dura competencia puede llevar a varias partes a presentar quejas simplemente para cerrar o suspender su sitio web.

Esto sucede con más frecuencia de lo que imagina. Además, muchas quejas aún no están respaldadas por ninguna evidencia, su sitio web pagará el precio.

Esto se debe a la política común de “suspender primero, investigar después”. Por lo tanto, alojar su sitio web con un proveedor que no ignore la DMCA lo dejará vulnerable a varios ataques.

Tener un proveedor con DMCA Ignored Hosting ayudará a mantener vivo su sitio web. El alojamiento ignorado por DMCA también le dará más libertad para mostrar contenido que de otro modo podría estar prohibido. Esto asegura que su libertad de expresión esté protegida.

El Hosting Ignorado por DMCA también es muy bueno para su negocio. Estar protegido de ataques injustificados por parte de sus competidores ayudará a aumentar su base de clientes. Además, si desea abrir un casino en línea, DMCA Ignored Hosting funcionará para usted.

Un proveedor con DMCA Ignored Hosting también se ocupará de otros asuntos que afecten a sus sitios web, como disputas legales. Esto le dará tiempo para concentrarse en lo que es importante, su sitio web.

Además de ayudar con problemas legales, los proveedores de Hosting Ignorado de DMCA también tienen expertos que le brindarán apoyo. Esto es muy importante, especialmente si su sitio web contiene información muy sensible.

Un proveedor de Hosting Ignorado por DMCA también mejorará las características de seguridad de su sitio web. Esto se debe a que hay partes que harán todo lo posible para derribar su sitio. Tener un gran proveedor defenderá su sitio contra varios peligros, como los ataques DDoS.

Otra razón por la que necesitará Hosting ignorado por DMCA es que muchos proveedores aceptan métodos de pago alternativos. Aquí es donde entran las criptomonedas, aseguran el anonimato total. Esto protege su privacidad, especialmente si carga contenido muy sensible en su sitio.

**II.1.3.1.2.2 Reserva a la información (Confidentiality and NDA)**

Otro aspecto muy importante a la hora de escoger un servicio de hosting es sus políticas en cuanto al acceso que tienen a nuestra información, no solo a la información que les damos al adquirir sus servicios, sino que también a la información que tenemos alojada en su infraestructura de servidores, Servidores Hosting,

En el servicio mismo de una VPN las idea del servicio busca que la privacidad de los usuarios sea la prioridad así que aparte de tratar de reducir la cantidad de registros que manejamos de los movimientos de nuestros usuarios tenemos que hacer también porque la infraestructura no es nuestra donde están nuestros servicio alojados y podrán existir riesgos donde no solo la infraestructura podría sufrir ataques cibernéticos pero como así también la empresa que da el

servicio de hosting podría acceder a nuestra información si así lo quisiera. También existen casos como donde hablamos las empresas que brindan el servicio de hosting están obligados a seguir las leyes y reglas del país donde están establecidos y podría verse obligados a compartir información o cortar el servicio a solitud o busque de cumplimientos de dichas reglas y leyes, por ellos buscar hosting offshore es una de las maneras de asegurarse de evitar dichos riesgos.

**DMCA (Digital Millennium Copyright Act)**

La DMCA (Digital Millennium Copyright Act) es la ley que vela por los derechos de autor y lucha contra la piratería en los Estados Unidos.La Ley de Derechos de Autor de la Era Digital fue aprobada en el año 1998 y sanciona desde entonces las violaciones de derechos de autor a través de internet, tanto la reproducción en sí como la producción y distribución de tecnologías que posibiliten esquivar las medidas encaminadas a la protección de derechos de autor.El surgimiento de esta ley vino precedido del Tratado de la OMPI (Organización Mundial de la Propiedad Intelectual) sobre Derechos de Autor, cuyo fin fue mediar entre los derechos de los autores y los intereses de los usuarios dentro del marco de la nueva sociedad de la información.

No en vano, la Ley de Derechos de Autor de la Era Digital fue creada para implementar no solo el Tratado de la OMPI sobre Derechos de Autor, sino también el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas.

No es necesario que una página web que infringe los derechos de autor de otra se halle en un servidor estadounidense para que la que segunda pueda interponer una reclamación sobre la primera. El propietario del copyright puede solicitar a buscadores de internet como Google, Yahoo! o Bing que retiren links y páginas de cualquier parte del mundo que han copiado contenido que les pertenece. En el siguiente punto veremos cómo actúa Google en este sentido.

Eso sí, solamente puede un reportar un aviso el poseedor de los derechos de autor o bien un agente legalmente autorizado por el propietario de los mismos. Pero sí es posible que cualquier persona que detecte alguna violación de los derechos de autor de otra en la red le notifique a ésta para que pueda actuar en consecuencia.

### II.1.3.2 Servidores VPS

Un VPS es un servidor privado virtual (virtual private server, en inglés). Es un servicio de alojamiento web que se obtiene dividiendo un servidor físico en varios servidores virtuales, haciendo que cada uno de ellos cuente con recursos dedicados y esté aislado de los demás.

A nivel operativo, un Servidor Privado Virtual funciona igual que otros servicios de hosting web, ofreciendo un espacio conectado a internet de forma permanente al que podemos subir los contenidos de nuestra web para que otras personas puedan acceder a ellos.

Los VPS pueden ser administrados o no administrados. Para gestionar un VPS no administrado es necesario tener conocimientos avanzados de administración de sistemas; ya que el cliente es el responsable de instalar y mantener el software y la seguridad del servidor.

#### II.1.3.2.1 Ventajas de los VPS.

Recursos garantizados: en un VPS tendremos recursos garantizados como en un servidor dedicado. Un VPS tiene un entorno aislado con su propia RAM y CPU dedicada, por lo que ningún otro usuario podrá utilizar esos recursos.

Altamente personalizable: Los VPS comparten el mismo hardware con otros VPS, pero su software es totalmente independiente, lo que permite tener acceso y realizar cualquier cambio o mejora en la configuración.

La principal ventaja de un VPS es que tiene muchos de los beneficios de un servidor dedicado, pero pagando sólo por los recursos que necesites utilizar, siendo una buena opción para aquellos usuarios que requieran de una mayor libertad de uso y configuración.

Para la implementación de un VPN en especial uno nuevo esta modalidad de hosting que ofrecen casi todas las empresas es muy buena ya que podemos hacer crecer nuestros VPS dependiendo de las necesidades de nuestros servicios lo que permite que se tenga una escalabilidad en la atención de parte de la red misma excelente.

#### II.1.3.2.2 Inconvenientes de los VPS

La principal desventaja del VPS frente al hosting compartido es el precio. Un VPS supondrá pagar un precio más elevado no sólo por los recursos extras, sino que al precio base le deberás sumar tres costes adicionales: el panel de gestión (cPanel, Plesk, etc), el coste del servicio de administración del servidor, y el espacio para los Backups, aunque esto dependerá de la oferta de cada proveedor.

Se requieren conocimientos más avanzados de configuración y administración de servidores virtuales, siendo idóneo para proyectos con necesidades específicas, pero no recomendable para proyectos más sencillos o personas no especializadas en el tema.

Para la implementación de una VPN los VPS la principal desventaja que ofrecen es que en la mayoría de las empresas de hosting te limitan la cantidad de datos que pueden pasar por la IP privada que solicitas según tu plan, no se limita el ancho de banda lo que es bueno para los tiempos de reacción, pero puede ser un problema manejarlos

### II.1.3.3 Configuración Red Privada Virtual Basada en OpenVPN

#### II.1.3.3.1 Crear servidor VPS

La red privada virtual usara VPS de dos distintos servicios de hosting offshore los cuales serán Vultr y Linode.

En Linode usaremos el VPS más pequeño que ofrece con las siguientes características:

Características:

Nombre VPS: Nanode 1GB

CPU: 1CPU

RAM: 1GB

STORAGE: 25GB

BANDWIDTH: Unlimited

DATA: Unlimited

PRECIO: 5$/month

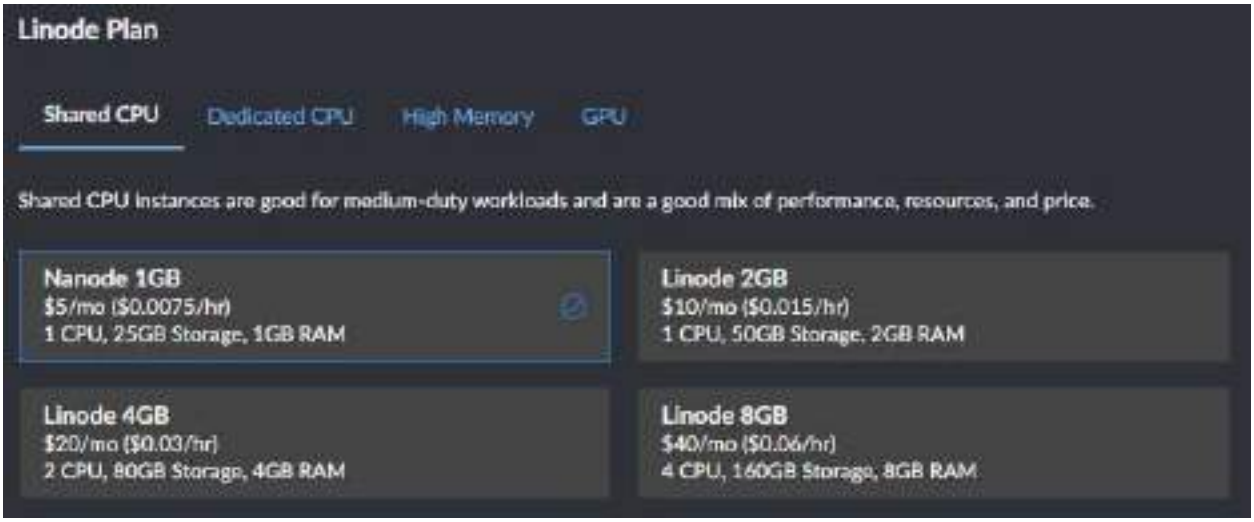


*Figura 2 – 34 Planes de hosting Linode*

En Vultr usaremos el VPS más pequeño que ofrece con las siguientes características:

Características:

Nombre VPS: 25 GB SSD

CPU: 1CPU

RAM: 1024 BB

STORAGE: 25GB SSD

BANDWIDTH: 10000GB

DATA: Unlimited

PRECIO: 5$/month

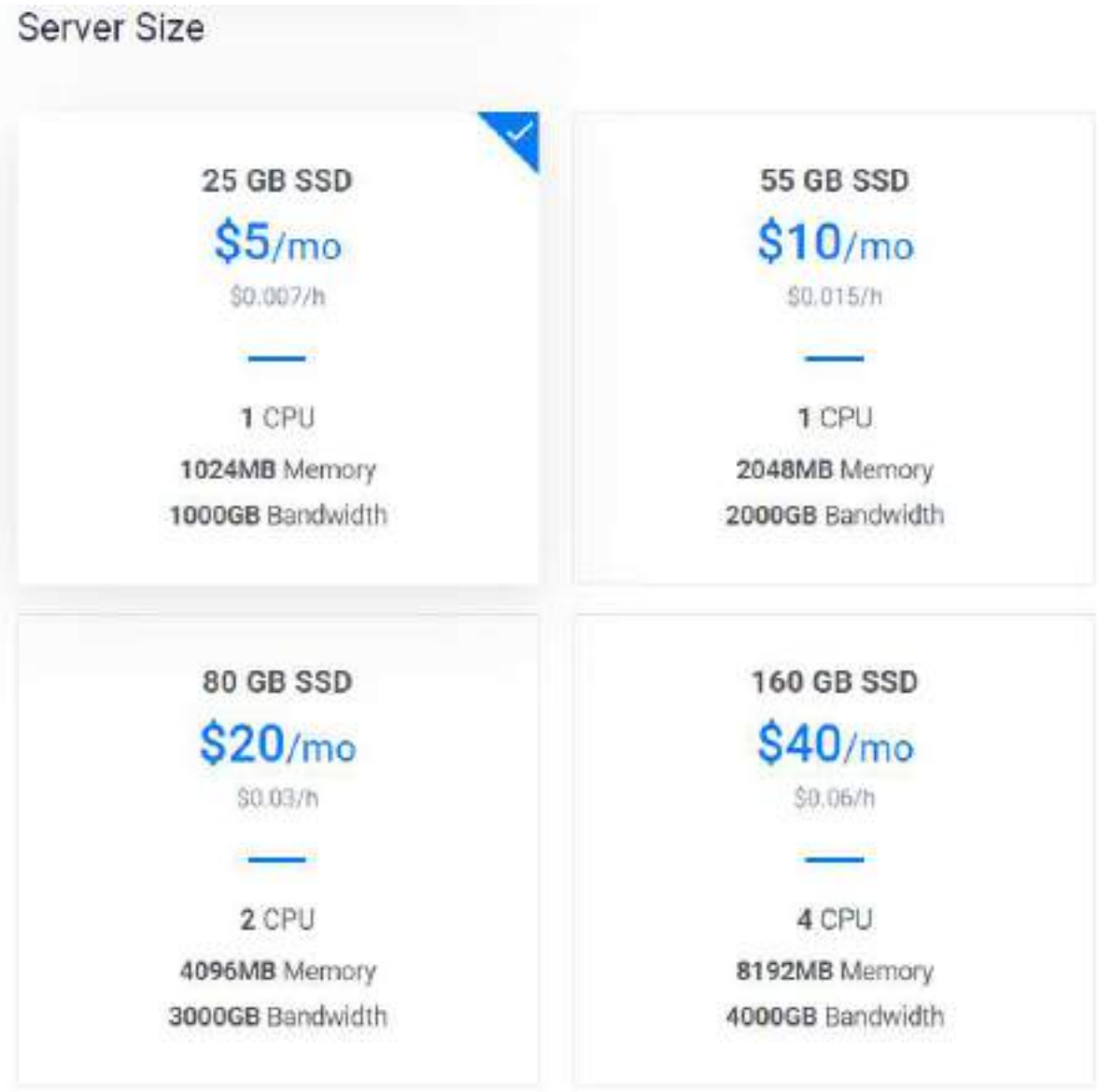


*Figura 2 – 35 Configuración de VPS "IP privada" Linode*

Todos los VPS estarán corriendo con la versión más reciente de Ubuntu, por motivos de seguridad y funcionalidad, la cual es al momento de la realización del proyecto Ubuntu 20.10.

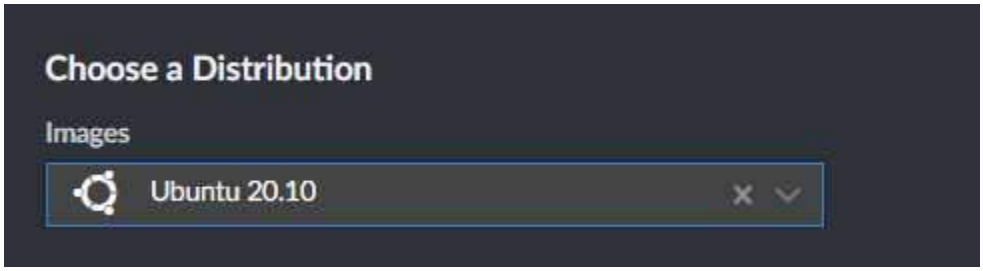


*Figura 2 - 36 Configuración de VPS "Distribución Linux" Linode*

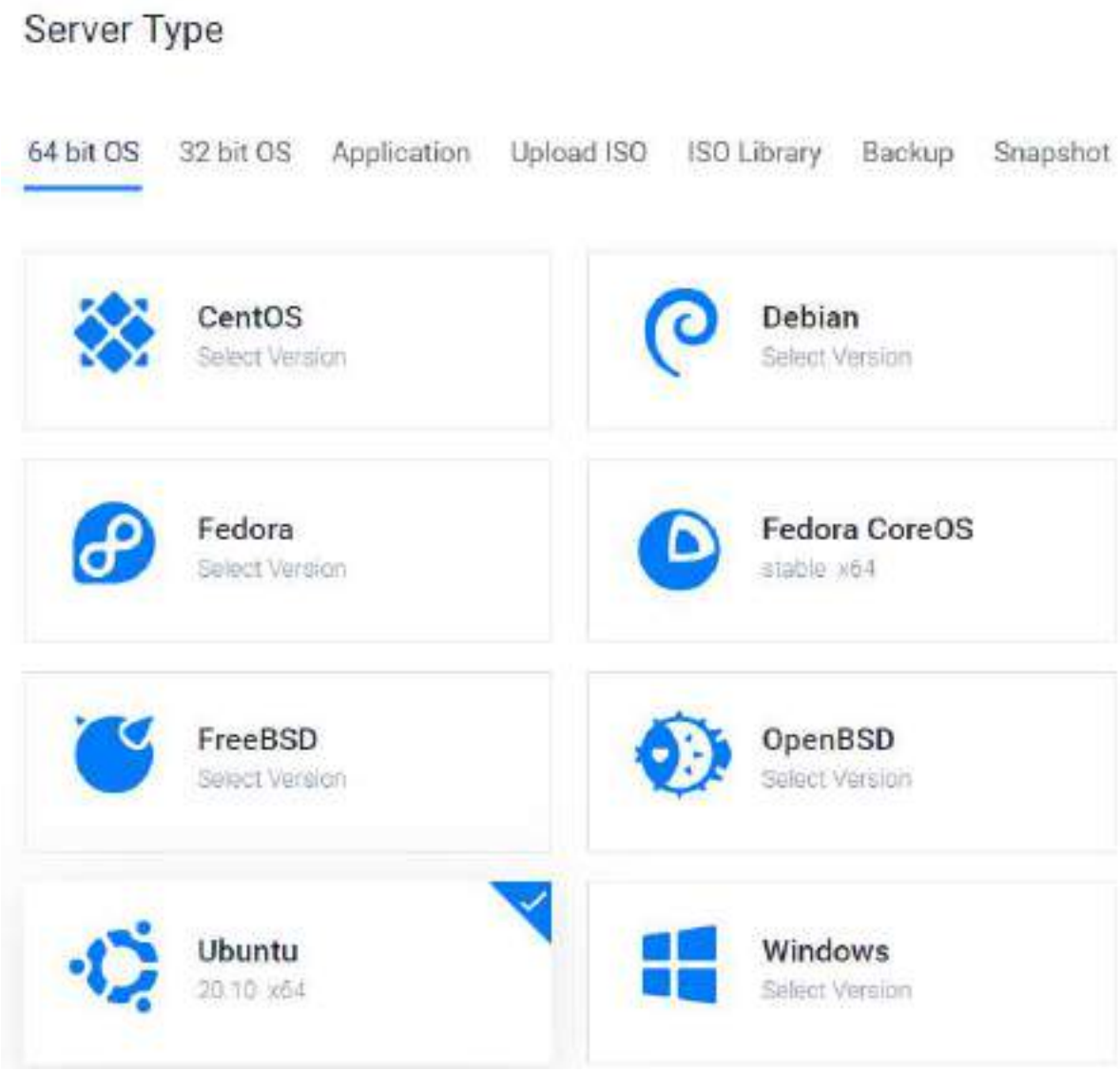


*Figura 2 - 37 Configuración de VPS "Distribución Linux" Vultr*

Al momento de la creación del VPS solicitar una IP privada es importante para evitar compartirla con otros usuarios del servicio.


*Figura 2 - 38 Configuración de VPS "IP privada" Linde*

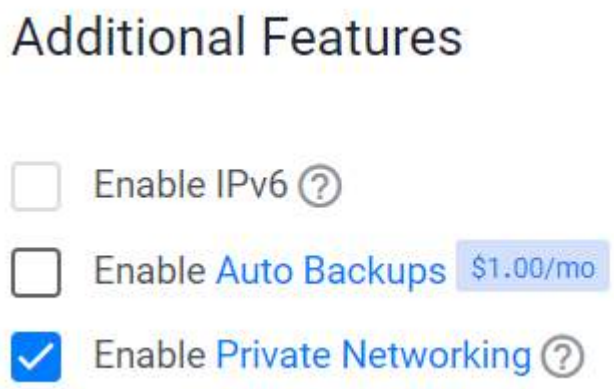


*Figura 2 – 39 Configuración de VPS "IP privada" Vultr*

Una vez concluida la creación de nuestro VPS el servicio creare el VM donde alojaremos los servicios que necesitemos, en nuestro caso nuestro servicio de VPN, La página del servicio de Hosting nos redirigirá al dashboard donde podremos ver nuestros servidores.

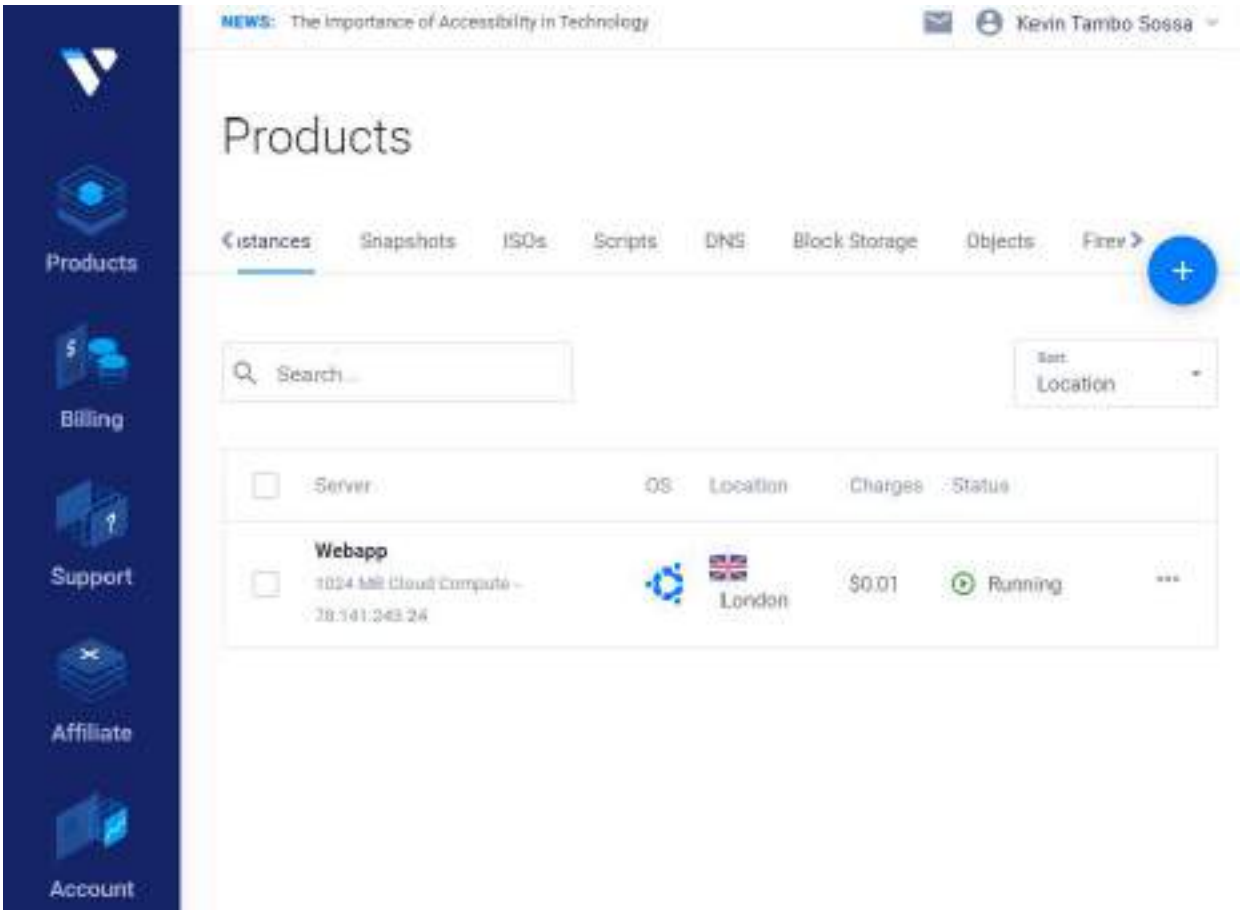


*Figura 2 – 40 Dashboard pantalla de Productos Vultr*

Ingresando dentro del servidor al que recién creamos obtendremos la información como la IP privada que solicitamos como así también la clave root para el SSH si la no configuramos.

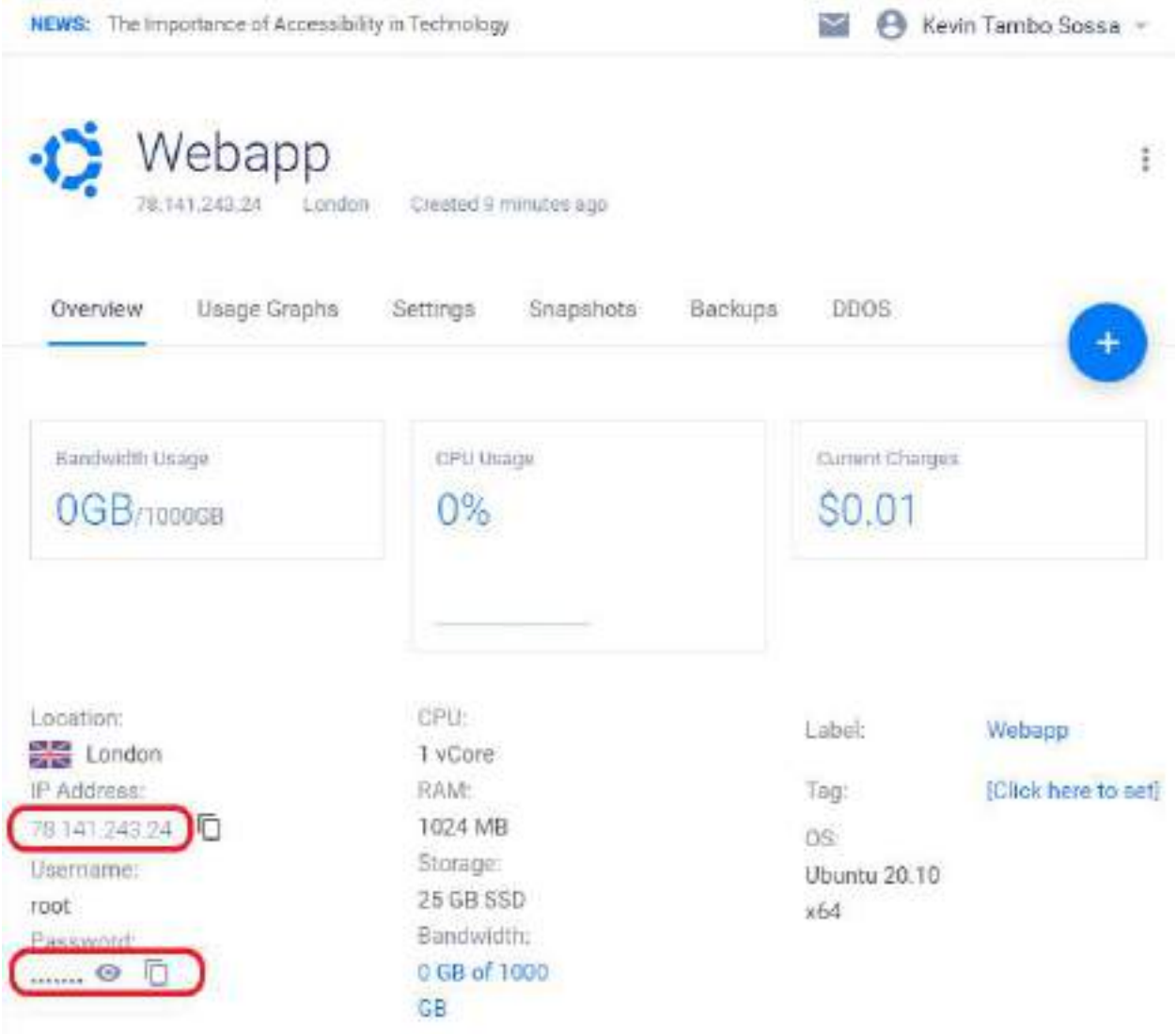


*Figura 2 – 41 Información servidor VPS Vultr*

### II.1.3.3.2 Configuración del servidor VPS

Una vez creado nuestro VPS y tengamos la IP privada y la clave accederemos mediante SSH a ellos desde la terminal de nuestra preferencia, también algunos servicios de Hosting tienen integrados dentro de su misma paginas terminales en las cuales podríamos ingresar a empezar la configuración de nuestros servidores.

#### II.1.3.3.2.1 Paso 1 Generando claves SSH

Usar una contraseña de texto sin cifrar para iniciar sesión en su servidor nunca es una buena idea, ya que la contraseña no está encriptada en tránsito y puede quedar expuesta en una red hostil. Al crear una clave SSH, lo haremos para que solo pueda iniciar sesión en el servidor si tiene el archivo de clave y la contraseña, y al mismo tiempo la contraseña está encriptada.

Si está utilizando Linux, probablemente ya sepa cómo abrir el terminal, si está en Mac, puede encontrar la aplicación Terminal en su carpeta Aplicaciones, y en Windows 10 deberá abrir PowerShell con privilegios de administrador e instalar SSH usando este comando:

```
PS C:\> Add-WindowsCapability -Online -Name OpenSSH.Client*
```

Este es el comando que generará nuestras claves SSH. El algoritmo RSA con un tamaño de clave de 4096 es lo que personalmente recomendaría, ya que es lo suficientemente seguro y ampliamente compatible.

```
ssh-keygen -t rsa -b 4096
```

Presione Enter cuando se le solicite la ubicación de la clave para guardarla en la predeterminada y luego ingrese la contraseña de su elección.

#### II.1.3.3.2.2 Paso 2 Iniciar sesión en el servidor

A estas alturas, nuestro servidor se ha iniciado y estamos listos para iniciar sesión. Copie la dirección IP del panel de control del servidor, vuelva a la terminal y escriba

```
ssh root@ip-address
```

Escriba sí, ingrese la contraseña de root que especificó en el primer paso y eso es todo, estamos dentro.

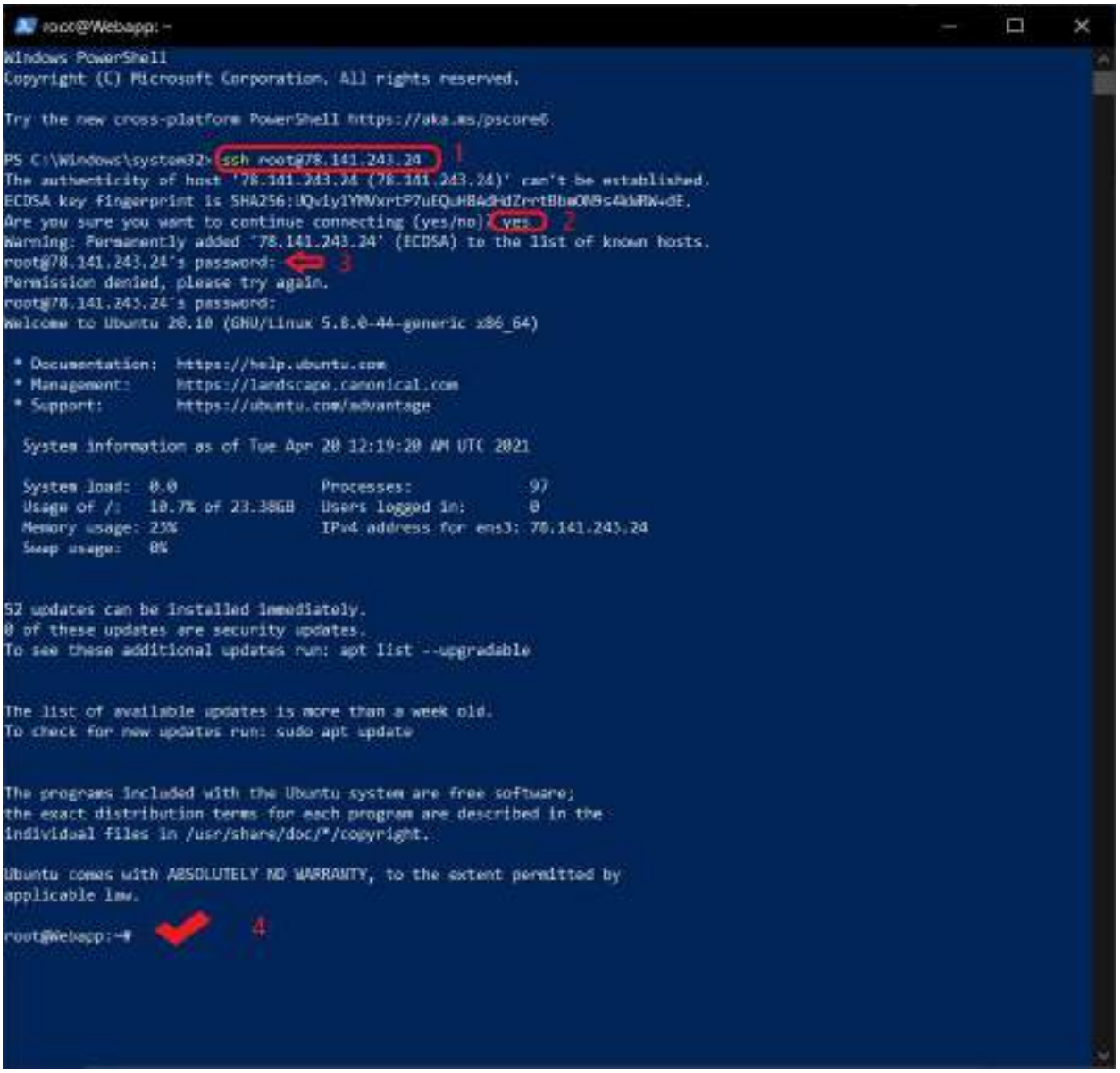


*Figura 2 – 42 Terminal Conectada a VPS SSH*

En la figura 2 – 40 usando Windows Powershell cargamos el comando ssh con la IP como lo primero resaltado después veremos que cuando tenemos una llave ssh local creada nos preguntara si queremos usarla y aceptamos. Ingresamos la contraseña y estamos ya dentro de nuestro servidor.

### II.1.3.3.2.3 Paso 3 Actualizar el sistema operativo

En primer lugar, actualice nuestro sistema operativo y software:

```
apt-get update && apt-get upgrade
```

Al ejecutar este comando Ubuntu buscara si existe alguna actualización para la distribución y luego reportara el tamaño de la misma pidiendo permiso para instalar las actualizaciones ocupando el espacio de almacenamiento que mencionara y luego recién iniciara la actualización.

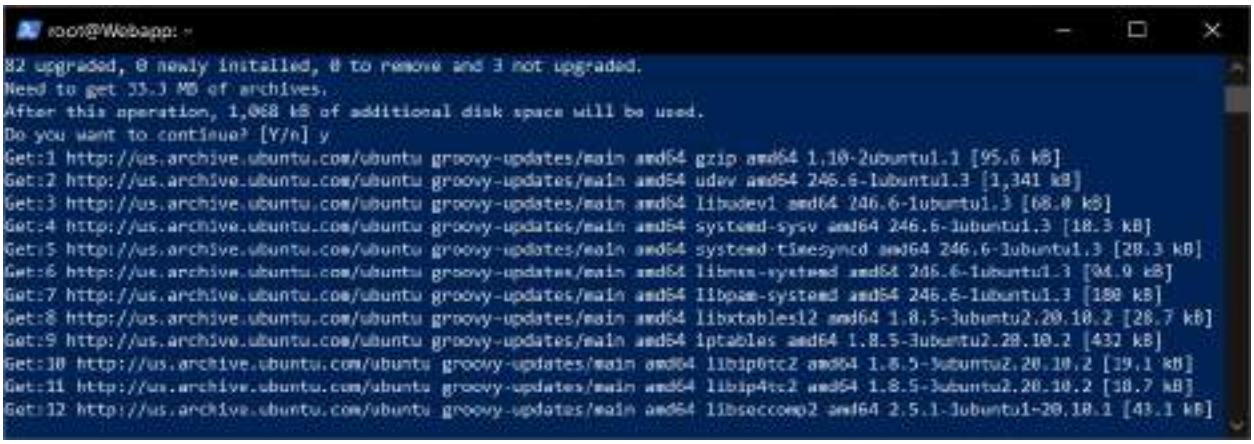


*Figura 2 – 43 Terminal Actualización de Distribución*

También instalaré mi editor de texto favorito, aunque siéntete libre de usar lo que quieras, por ejemplo, nano.

```
apt install neovim
```

Igualmente, que para las actualizaciones el comando para instalar el neovim pedirá de permiso después de el comando para ejecutar la instalación y ocupar el espacio en el almacenamiento

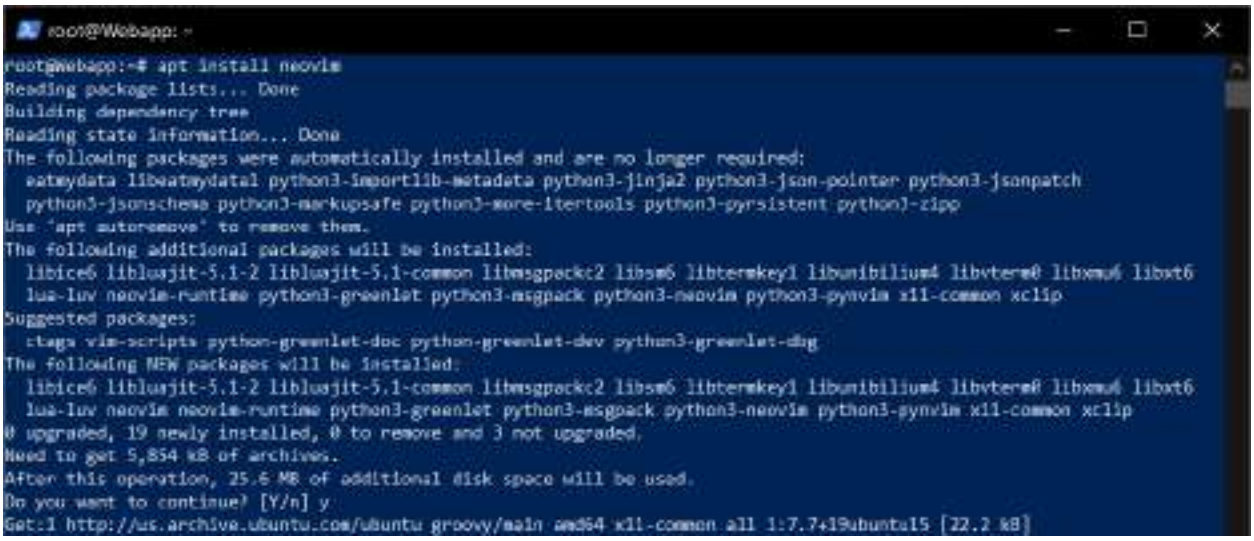


*Figura 2 – 44 Terminal Instalación Neovim (Editor de Texto)*

#### II.1.3.3.2.4 Paso 4 Creación de Usuario

Por mucho que sea conveniente no tener que ingresar una contraseña cada vez, necesitamos crear una cuenta de usuario que no sea root. Exponer el inicio de sesión de root en un servidor SSH probablemente no sea una buena idea, incluso si tiene autenticación de múltiples factores. Llámame paranoico, pero creo que tener que ingresar la contraseña de root a veces es el precio que estoy dispuesto a pagar por una sensación de seguridad. Tipo:

```
useradd -G sudo -m radarada14 -s /bin/bash
```

Eso creará un usuario, establecerá bash como shell predeterminado para él y permitirá el uso de sudo. Luego, necesitaremos crear una contraseña para nuestro usuario, usando

```
passwd radarada14
```

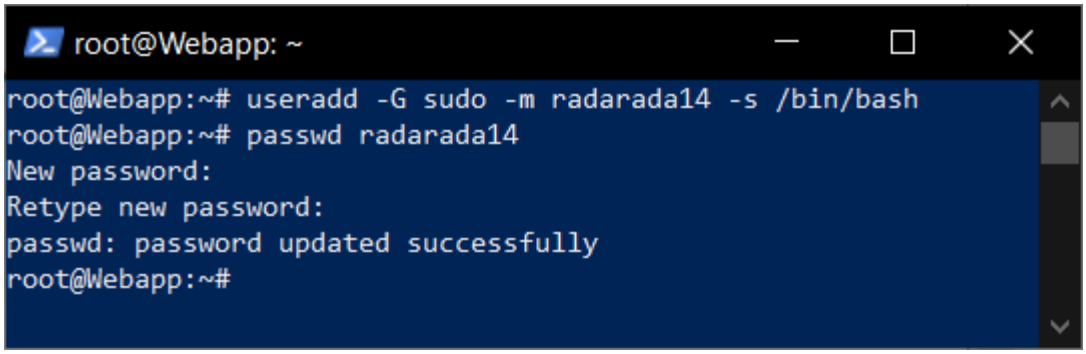


*Figura 2 – 45 Terminal Creación de Usuario*

Ingrese su contraseña dos veces y listo.

#### II.1.3.3.2.5 Paso 5 Copiar la clave SSH del host al servidor

Ahora que hemos creado nuestro usuario, es un buen momento para copiar la clave SSH pública al servidor. Abra una segunda ventana de terminal para su terminal local e ingrese:

```
ssh-copy-id radarada14@ip_address

type $env:USERPROFILE\.ssh\id_rsa.pub | ssh ip-address "cat >> .ssh/authorized_keys"
```

Se le pedirá que ingrese su contraseña y una vez que lo haga, regrese a la ventana de terminal con su servidor. No cierres la otra ventana todavía.

### II.1.3.3.2.6 Paso 6 Restringir SSH a la autenticación de claves

Ahora que hemos copiado las claves SSH en el servidor, tenemos que restringir la autenticación solo a la clave pública. Editemos el archivo de configuración sshd.

```
nvim /etc/ssh/sshd_config
```

En primer lugar, cambiemos el puerto predeterminado. Esto no hará mucho por la seguridad, pero ayudará con esos detestables escáneres SSH que intentan iniciar sesión con las credenciales predeterminadas. No mucho, pero los registros de seguridad definitivamente serán más fáciles de leer. Puede usar cualquier puerto que no esté en otros servicios, pero yo prefiero usar el 69.

```
# Port 22
Port 69
```

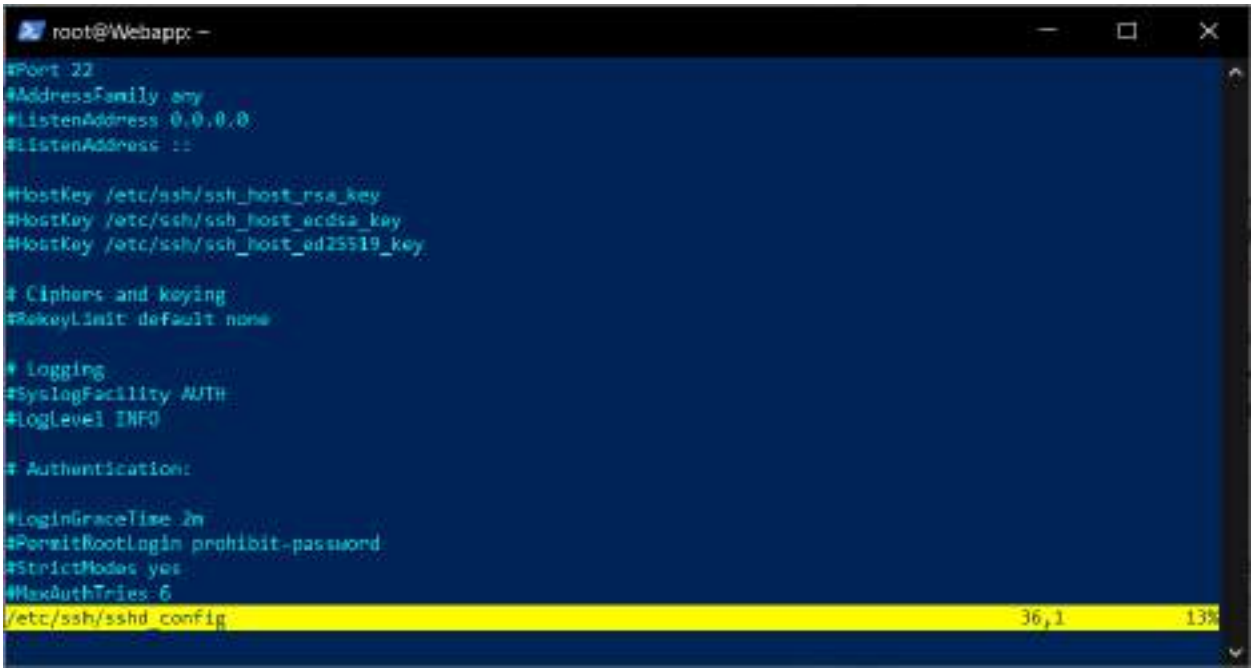


*Figura 2 – 46 Terminal sshd_config*

A continuación, debemos deshabilitar la autenticación de contraseña para que solo pueda iniciar sesión con una clave pública.

```
PasswordAuthentication no
```

Por último, pero no menos importante, también deshabilitemos el inicio de sesión de root.

```
PermitRootLogin no
```

Ahora guarde el archivo y reinicie el servicio sshd usando.

```
systemctl restart sshd
```

Ahora, sin cerrar esta ventana, regresemos a nuestra máquina local e intentemos iniciar sesión con nuestra clave:

```
ssh -i ~/.ssh/id_rsa radarada14@ip_address -p 69
```

Si ve el mensaje para ingresar su contraseña clave, eso significa que estamos listos para comenzar. También es una buena idea verificar que ya no podemos iniciar sesión con nuestra contraseña:

```
ssh radarada14@ip_address -p 69
```

Esto debería darnos "Permiso denegado".

#### II.1.3.3.2.7 Paso 7 Creando un alias de servidor

Este comando es un poco largo y molesto de escribir, así que arreglemos eso. Cree un archivo en la carpeta ".ssh" de su directorio personal llamado "config" y edítelo con su editor de texto favorito:

```
nvim ~/.ssh/config
```

Aquí vamos a crear un alias para nuestro VPS.

```
Host radaopenvpn # Escoge el nombre para el servidor
    User radarada14 # El nombre de usuario del usuario creado
    Port 69
    IdentityFile ~/.ssh/id_rsa # La localización de nuestra llave
    HostName ip_address # La ip de nuestro servidor
```

Guarde y cierre, y ahora podemos iniciar sesión en nuestro servidor simplemente escribiendo

```
ssh radaopenvpn
```

#### II.1.3.3.2.8 Paso 8 Configuración de OpenVPN

La configuración de un servidor OpenVPN lleva algún tiempo, ya que necesita instalar los paquetes, generar las claves, configurar IPTables, escribir los archivos de configuración para el servidor y el cliente. Pero usaremos un scrip personalizado con la configuración para nuestro servicio.

Inicie sesión en su servidor e instálelo wgetsi aún no lo ha hecho. A veces ya viene con la imagen de su sistema operativo, pero a veces no es así.

```
sudo apt install wget
```

A continuación, escriba wget, presione la barra espaciadora y pegue el enlace que copió anteriormente. Presione Enter.

```
wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh
```

lo cual correrá el código en bash para que se pueda configurar el OpenVPN preguntando parámetros al usuario donde escogeremos el deseado, este ya se encuentra configurado para el uso de solo una credencial de tipo llave.

```
#!/bin/bash
#
# https://github.com/radarada14/OpenVPNscript
#
# Copyright (c) 2013 Nyr. Released under the MIT License.


# Detect Debian users running the script with "sh" instead of bash
if readlink /proc/$$/exe | grep -q "dash"; then
	echo 'This installer needs to be run with "bash", not "sh".'
	exit
fi

# Discard stdin. Needed when running from an one-liner which includes a
newline
read -N 999999 -t 0.001

# Detect OpenVZ 6
if [[ $(uname -r | cut -d "." -f 1) -eq 2 ]]; then
	echo "The system is running an old kernel, which is incompatible
with this installer."
	exit
fi

# Detect OS
# $os_version variables aren't always in use, but are kept here for
convenience
if grep -qs "ubuntu" /etc/os-release; then
	os="ubuntu"
	os_version=$(grep 'VERSION_ID' /etc/os-release | cut -d '"' -f 2 |
tr -d '.')
	group_name="nogroup"
elif [[ -e /etc/debian_version ]]; then
	os="debian"
	os_version=$(grep -oE '[0-9]+' /etc/debian_version | head -1)
	group_name="nogroup"
```

```
elif [[ -e /etc/centos-release ]]; then
        os="centos"
        os_version=$(grep -oE '[0-9]+' /etc/centos-release | head -1)
        group_name="nobody"
elif [[ -e /etc/fedora-release ]]; then
        os="fedora"
        os_version=$(grep -oE '[0-9]+' /etc/fedora-release | head -1)
        group_name="nobody"
else
        echo "This installer seems to be running on an unsupported
distribution.
Supported distributions are Ubuntu, Debian, CentOS, and Fedora."
        exit
fi

if [[ "$os" == "ubuntu" && "$os_version" -lt 1804 ]]; then
        echo "Ubuntu 18.04 or higher is required to use this installer.
This version of Ubuntu is too old and unsupported."
        exit
fi

if [[ "$os" == "debian" && "$os_version" -lt 9 ]]; then
        echo "Debian 9 or higher is required to use this installer.
This version of Debian is too old and unsupported."
        exit
fi

if [[ "$os" == "centos" && "$os_version" -lt 7 ]]; then
        echo "CentOS 7 or higher is required to use this installer.
This version of CentOS is too old and unsupported."
        exit
fi

# Detect environments where $PATH does not include the sbin directories
if ! grep -q sbin <<< "$PATH"; then
        echo '$PATH does not include sbin. Try using "su -" instead of
"su".'
        exit
fi

if [[ "$EUID" -ne 0 ]]; then
        echo "This installer needs to be run with superuser privileges."
        exit
fi

if [[ ! -e /dev/net/tun ]] || ! ( exec 7<>/dev/net/tun ) 2>/dev/null; then
        echo "The system does not have the TUN device available.
TUN needs to be enabled before running this installer."
        exit
fi

new_client () {
        # Generates the custom client.ovpn
```

```
        {
        cat /etc/openvpn/server/client-common.txt
        echo "<ca>"
        cat /etc/openvpn/server/easy-rsa/pki/ca.crt
        echo "</ca>"
        echo "<cert>"
        sed -ne '/BEGIN CERTIFICATE/,$ p' /etc/openvpn/server/easy-
rsa/pki/issued/"$client".crt
        echo "</cert>"
        echo "<key>"
        cat /etc/openvpn/server/easy-rsa/pki/private/"$client".key
        echo "</key>"
        echo "<tls-crypt>"
        sed -ne '/BEGIN OpenVPN Static key/,$ p' /etc/openvpn/server/tc.key
        echo "</tls-crypt>"
        } > ~/"$client".ovpn
}

if [[ ! -e /etc/openvpn/server/server.conf ]]; then
        clear
        echo 'Welcome to this OpenVPN road warrior installer!'
        # If system has a single IPv4, it is selected automatically. Else,
ask the user
        if [[ $(ip -4 addr | grep inet | grep -vEc '127(\.[0-9]{1,3}){3}')
-eq 1 ]]; then
                ip=$(ip -4 addr | grep inet | grep -vE '127(\.[0-
9]{1,3}){3}' | cut -d '/' -f 1 | grep -oE '[0-9]{1,3}(\.[0-9]{1,3}){3}')
        else
                number_of_ip=$(ip -4 addr | grep inet | grep -vEc
'127(\.[0-9]{1,3}){3}')
                echo
                echo "Which IPv4 address should be used?"
                ip -4 addr | grep inet | grep -vE '127(\.[0-9]{1,3}){3}' |
cut -d '/' -f 1 | grep -oE '[0-9]{1,3}(\.[0-9]{1,3}){3}' | nl -s ') '
                read -p "IPv4 address [1]: " ip_number
                until [[ -z "$ip_number" || "$ip_number" =~ ^[0-9]+$ &&
"$ip_number" -le "$number_of_ip" ]]; do
                        echo "$ip_number: invalid selection."
                        read -p "IPv4 address [1]: " ip_number
                done
                [[ -z "$ip_number" ]] && ip_number="1"
                ip=$(ip -4 addr | grep inet | grep -vE '127(\.[0-
9]{1,3}){3}' | cut -d '/' -f 1 | grep -oE '[0-9]{1,3}(\.[0-9]{1,3}){3}' |
sed -n "$ip_number"p)
        fi
        # If $ip is a private IP address, the server must be behind NAT
        if echo "$ip" | grep -qE '^(10\.|172\.1[6789]\.|172\.2[0-
9]\.|172\.3[01]\.|192\.168)'; then
                echo
                echo "This server is behind NAT. What is the public IPv4
address or hostname?"
                # Get public IP and sanitize with grep
```

```
                get_public_ip=$(grep -m 1 -oE '^[0-9]{1,3}(\.[0-
9]{1,3}){3}$' <<< "$(wget -T 10 -t 1 -4qO- "http://ip1.dynupdate.no-
ip.com/" || curl -m 10 -4Ls "http://ip1.dynupdate.no-ip.com/")")
                read -p "Public IPv4 address / hostname [$get_public_ip]: "
public_ip
                # If the checkip service is unavailable and user didn't
provide input, ask again
                until [[ -n "$get_public_ip" || -n "$public_ip" ]]; do
                        echo "Invalid input."
                        read -p "Public IPv4 address / hostname: " public_ip
                done
                [[ -z "$public_ip" ]] && public_ip="$get_public_ip"
        fi
        # If system has a single IPv6, it is selected automatically
        if [[ $(ip -6 addr | grep -c 'inet6 [23]') -eq 1 ]]; then
                ip6=$(ip -6 addr | grep 'inet6 [23]' | cut -d '/' -f 1 |
grep -oE '([0-9a-fA-F]{0,4}:){1,7}[0-9a-fA-F]{0,4}')
        fi
        # If system has multiple IPv6, ask the user to select one
        if [[ $(ip -6 addr | grep -c 'inet6 [23]') -gt 1 ]]; then
                number_of_ip6=$(ip -6 addr | grep -c 'inet6 [23]')
                echo
                echo "Which IPv6 address should be used?"
                ip -6 addr | grep 'inet6 [23]' | cut -d '/' -f 1 | grep -oE
'([0-9a-fA-F]{0,4}:){1,7}[0-9a-fA-F]{0,4}' | nl -s ') '
                read -p "IPv6 address [1]: " ip6_number
                until [[ -z "$ip6_number" || "$ip6_number" =~ ^[0-9]+$ &&
"$ip6_number" -le "$number_of_ip6" ]]; do
                        echo "$ip6_number: invalid selection."
                        read -p "IPv6 address [1]: " ip6_number
                done
                [[ -z "$ip6_number" ]] && ip6_number="1"
                ip6=$(ip -6 addr | grep 'inet6 [23]' | cut -d '/' -f 1 |
grep -oE '([0-9a-fA-F]{0,4}:){1,7}[0-9a-fA-F]{0,4}' | sed -n
"$ip6_number"p)
        fi
        echo
        echo "Which protocol should OpenVPN use?"
        echo "   1) UDP (recommended)"
        echo "   2) TCP"
        read -p "Protocol [1]: " protocol
        until [[ -z "$protocol" || "$protocol" =~ ^[12]$ ]]; do
                echo "$protocol: invalid selection."
                read -p "Protocol [1]: " protocol
        done
        case "$protocol" in
                1|"")
                protocol=udp
                ;;
                2)
                protocol=tcp
                ;;
        esac
```

```
        echo
        echo "What port should OpenVPN listen to?"
        read -p "Port [1194]: " port
        until [[ -z "$port" || "$port" =~ ^[0-9]+$ && "$port" -le 65535 ]];
do
                echo "$port: invalid port."
                read -p "Port [1194]: " port
        done
        [[ -z "$port" ]] && port="1194"
        echo
        echo "Select a DNS server for the clients:"
        echo "   1) Current system resolvers"
        echo "   2) Google"
        echo "   3) 1.1.1.1"
        echo "   4) OpenDNS"
        echo "   5) Quad9"
        echo "   6) AdGuard"
        read -p "DNS server [1]: " dns
        until [[ -z "$dns" || "$dns" =~ ^[1-6]$ ]]; do
                echo "$dns: invalid selection."
                read -p "DNS server [1]: " dns
        done
        echo
        echo "Enter a name for the first client:"
        read -p "Name [client]: " unsanitized_client
        # Allow a limited set of characters to avoid conflicts
        client=$(sed
's/[^0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_-
]/_/g' <<< "$unsanitized_client")
        [[ -z "$client" ]] && client="client"
        echo
        echo "OpenVPN installation is ready to begin."
        # Install a firewall in the rare case where one is not already
available
        if ! systemctl is-active --quiet firewalld.service && ! hash
iptables 2>/dev/null; then
                if [[ "$os" == "centos" || "$os" == "fedora" ]]; then
                        firewall="firewalld"
                        # We don't want to silently enable firewalld, so we
give a subtle warning
                        # If the user continues, firewalld will be installed
and enabled during setup
                        echo "firewalld, which is required to manage routing
tables, will also be installed."
                elif [[ "$os" == "debian" || "$os" == "ubuntu" ]]; then
                        # iptables is way less invasive than firewalld so no
warning is given
                        firewall="iptables"
                fi
        fi
        read -n1 -r -p "Press any key to continue..."
        # If running inside a container, disable LimitNPROC to prevent
conflicts
```

```
        if systemd-detect-virt -cq; then
                mkdir /etc/systemd/system/openvpn-server@server.service.d/
2>/dev/null
                echo "[Service]
LimitNPROC=infinity" > /etc/systemd/system/openvpn-
server@server.service.d/disable-limitnproc.conf
        fi
        if [[ "$os" = "debian" || "$os" = "ubuntu" ]]; then
                apt-get update
                apt-get install -y openvpn openssl ca-certificates
$firewall
        elif [[ "$os" = "centos" ]]; then
                yum install -y epel-release
                yum install -y openvpn openssl ca-certificates tar
$firewall
        else
                # Else, OS must be Fedora
                dnf install -y openvpn openssl ca-certificates tar
$firewall
        fi
        # If firewalld was just installed, enable it
        if [[ "$firewall" == "firewalld" ]]; then
                systemctl enable --now firewalld.service
        fi
        # Get easy-rsa
        easy_rsa_url='https://github.com/OpenVPN/easy-
rsa/releases/download/v3.0.8/EasyRSA-3.0.8.tgz'
        mkdir -p /etc/openvpn/server/easy-rsa/
        { wget -qO- "$easy_rsa_url" 2>/dev/null || curl -sL "$easy_rsa_url"
; } | tar xz -C /etc/openvpn/server/easy-rsa/ --strip-components 1
        chown -R root:root /etc/openvpn/server/easy-rsa/
        cd /etc/openvpn/server/easy-rsa/
        # Create the PKI, set up the CA and the server and client
certificates
        ./easyrsa init-pki
        ./easyrsa --batch build-ca nopass
        EASYRSA_CERT_EXPIRE=3650 ./easyrsa build-server-full server nopass
        EASYRSA_CERT_EXPIRE=3650 ./easyrsa build-client-full "$client"
nopass
        EASYRSA_CRL_DAYS=3650 ./easyrsa gen-crl
        # Move the stuff we need
        cp pki/ca.crt pki/private/ca.key pki/issued/server.crt
pki/private/server.key pki/crl.pem /etc/openvpn/server
        # CRL is read with each client connection, while OpenVPN is dropped
to nobody
        chown nobody:"$group_name" /etc/openvpn/server/crl.pem
        # Without +x in the directory, OpenVPN can't run a stat() on the
CRL file
        chmod o+x /etc/openvpn/server/
        # Generate key for tls-crypt
        openvpn --genkey --secret /etc/openvpn/server/tc.key
        # Create the DH parameters file using the predefined ffdhe2048
group
```

```
        echo '-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEA//////////+t+FRYortKmq/cViAnPTzx2LnFg84tNpWp4TZBFGQz
+8yTnc4kmz75fS/jY2MMddj2gbICrsRhetPfHtXV/WVhJDP1H18GbtCFY2VVPe0a
87VXE15/V8k1mE8McODmi3fipona8+/och3xWKE2rec1MKzKT0g6eXq8CrGCsyT7
YdEIqUuyyOP7uWrat2DX9GgdT0Kj3jlN9K5W7edjcrsZCwenyO4KbXCeAvzhzffi
7MA0BM0oNC9hkXL+nOmFg/+OTxIy7vKBg8P+OxtMb61zO7X8vC7CIAXFjvGDfRaD
ssbzSibBsu/6iGtCOGEoXJf//////////wIBAg==
-----END DH PARAMETERS-----' > /etc/openvpn/server/dh.pem
        # Generate server.conf
        echo "local $ip
port $port
proto $protocol
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA512
tls-crypt tc.key
topology subnet
server 10.8.0.0 255.255.255.0" > /etc/openvpn/server/server.conf
        # IPv6
        if [[ -z "$ip6" ]]; then
                echo 'push "redirect-gateway def1 bypass-dhcp"' >>
/etc/openvpn/server/server.conf
        else
                echo 'server-ipv6 fddd:1194:1194:1194::/64' >>
/etc/openvpn/server/server.conf
                echo 'push "redirect-gateway def1 ipv6 bypass-dhcp"' >>
/etc/openvpn/server/server.conf
        fi
        echo 'ifconfig-pool-persist ipp.txt' >>
/etc/openvpn/server/server.conf
        # DNS
        case "$dns" in
                1|"")
                        # Locate the proper resolv.conf
                        # Needed for systems running systemd-resolved
                        if grep -q '^nameserver 127.0.0.53'
"/etc/resolv.conf"; then

        resolv_conf="/run/systemd/resolve/resolv.conf"
                        else
                                resolv_conf="/etc/resolv.conf"
                        fi
                        # Obtain the resolvers from resolv.conf and use them
for OpenVPN
                        grep -v '^#\|^;' "$resolv_conf" | grep '^nameserver'
| grep -oE '[0-9]{1,3}(\.[0-9]{1,3}){3}' | while read line; do
                                echo "push \"dhcp-option DNS $line\"" >>
/etc/openvpn/server/server.conf
                        done
                ;;
```

```
                2)
                        echo 'push "dhcp-option DNS 8.8.8.8"' >>
/etc/openvpn/server/server.conf
                        echo 'push "dhcp-option DNS 8.8.4.4"' >>
/etc/openvpn/server/server.conf
                ;;
                3)
                        echo 'push "dhcp-option DNS 1.1.1.1"' >>
/etc/openvpn/server/server.conf
                        echo 'push "dhcp-option DNS 1.0.0.1"' >>
/etc/openvpn/server/server.conf
                ;;
                4)
                        echo 'push "dhcp-option DNS 208.67.222.222"' >>
/etc/openvpn/server/server.conf
                        echo 'push "dhcp-option DNS 208.67.220.220"' >>
/etc/openvpn/server/server.conf
                ;;
                5)
                        echo 'push "dhcp-option DNS 9.9.9.9"' >>
/etc/openvpn/server/server.conf
                        echo 'push "dhcp-option DNS 149.112.112.112"' >>
/etc/openvpn/server/server.conf
                ;;
                6)
                        echo 'push "dhcp-option DNS 94.140.14.14"' >>
/etc/openvpn/server/server.conf
                        echo 'push "dhcp-option DNS 94.140.15.15"' >>
/etc/openvpn/server/server.conf
                ;;
        esac
        echo "keepalive 10 120
cipher AES-256-CBC
user nobody
group $group_name
persist-key
persist-tun
verb 3
crl-verify crl.pem" >> /etc/openvpn/server/server.conf
        if [[ "$protocol" = "udp" ]]; then
                echo "explicit-exit-notify" >>
/etc/openvpn/server/server.conf
        fi
        # Enable net.ipv4.ip_forward for the system
        echo 'net.ipv4.ip_forward=1' > /etc/sysctl.d/30-openvpn-
forward.conf
        # Enable without waiting for a reboot or service restart
        echo 1 > /proc/sys/net/ipv4/ip_forward
        if [[ -n "$ip6" ]]; then
                # Enable net.ipv6.conf.all.forwarding for the system
                echo "net.ipv6.conf.all.forwarding=1" >> /etc/sysctl.d/30-
openvpn-forward.conf
                # Enable without waiting for a reboot or service restart
                echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

```
        fi
        if systemctl is-active --quiet firewalld.service; then
                # Using both permanent and not permanent rules to avoid a
firewalld
                # reload.
                # We don't use --add-service=openvpn because that would
only work with
                # the default port and protocol.
                firewall-cmd --add-port="$port"/"$protocol"
                firewall-cmd --zone=trusted --add-source=10.8.0.0/24
                firewall-cmd --permanent --add-port="$port"/"$protocol"
                firewall-cmd --permanent --zone=trusted --add-
source=10.8.0.0/24
                # Set NAT for the VPN subnet
                firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -s
10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to "$ip"
                firewall-cmd --permanent --direct --add-rule ipv4 nat
POSTROUTING 0 -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to "$ip"
                if [[ -n "$ip6" ]]; then
                        firewall-cmd --zone=trusted --add-
source=fddd:1194:1194:1194::/64
                        firewall-cmd --permanent --zone=trusted --add-
source=fddd:1194:1194:1194::/64
                        firewall-cmd --direct --add-rule ipv6 nat
POSTROUTING 0 -s fddd:1194:1194:1194::/64 ! -d fddd:1194:1194:1194::/64 -j
SNAT --to "$ip6"
                        firewall-cmd --permanent --direct --add-rule ipv6
nat POSTROUTING 0 -s fddd:1194:1194:1194::/64 ! -d
fddd:1194:1194:1194::/64 -j SNAT --to "$ip6"
                fi
        else
                # Create a service to set up persistent iptables rules
                iptables_path=$(command -v iptables)
                ip6tables_path=$(command -v ip6tables)
                # nf_tables is not available as standard in OVZ kernels. So
use iptables-legacy
                # if we are in OVZ, with a nf_tables backend and iptables-
legacy is available.
                if [[ $(systemd-detect-virt) == "openvz" ]] && readlink -f
"$(command -v iptables)" | grep -q "nft" && hash iptables-legacy
2>/dev/null; then
                        iptables_path=$(command -v iptables-legacy)
                        ip6tables_path=$(command -v ip6tables-legacy)
                fi
                echo "[Unit]
Before=network.target
[Service]
Type=oneshot
ExecStart=$iptables_path -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d
10.8.0.0/24 -j SNAT --to $ip
ExecStart=$iptables_path -I INPUT -p $protocol --dport $port -j ACCEPT
ExecStart=$iptables_path -I FORWARD -s 10.8.0.0/24 -j ACCEPT
```

```
ExecStart=$iptables_path -I FORWARD -m state --state RELATED,ESTABLISHED -
j ACCEPT
ExecStop=$iptables_path -t nat -D POSTROUTING -s 10.8.0.0/24 ! -d
10.8.0.0/24 -j SNAT --to $ip
ExecStop=$iptables_path -D INPUT -p $protocol --dport $port -j ACCEPT
ExecStop=$iptables_path -D FORWARD -s 10.8.0.0/24 -j ACCEPT
ExecStop=$iptables_path -D FORWARD -m state --state RELATED,ESTABLISHED -j
ACCEPT" > /etc/systemd/system/openvpn-iptables.service
                if [[ -n "$ip6" ]]; then
                        echo "ExecStart=$ip6tables_path -t nat -A
POSTROUTING -s fddd:1194:1194:1194::/64 ! -d fddd:1194:1194:1194::/64 -j
SNAT --to $ip6
ExecStart=$ip6tables_path -I FORWARD -s fddd:1194:1194:1194::/64 -j ACCEPT
ExecStart=$ip6tables_path -I FORWARD -m state --state RELATED,ESTABLISHED
-j ACCEPT
ExecStop=$ip6tables_path -t nat -D POSTROUTING -s fddd:1194:1194:1194::/64
! -d fddd:1194:1194:1194::/64 -j SNAT --to $ip6
ExecStop=$ip6tables_path -D FORWARD -s fddd:1194:1194:1194::/64 -j ACCEPT
ExecStop=$ip6tables_path -D FORWARD -m state --state RELATED,ESTABLISHED -
j ACCEPT" >> /etc/systemd/system/openvpn-iptables.service
                fi
                echo "RemainAfterExit=yes
[Install]
WantedBy=multi-user.target" >> /etc/systemd/system/openvpn-
iptables.service
                systemctl enable --now openvpn-iptables.service
        fi
        # If SELinux is enabled and a custom port was selected, we need
this
        if sestatus 2>/dev/null | grep "Current mode" | grep -q "enforcing"
&& [[ "$port" != 1194 ]]; then
                # Install semanage if not already present
                if ! hash semanage 2>/dev/null; then
                        if [[ "$os_version" -eq 7 ]]; then
                                # Centos 7
                                yum install -y policycoreutils-python
                        else
                                # CentOS 8 or Fedora
                                dnf install -y policycoreutils-python-utils
                        fi
                fi
                semanage port -a -t openvpn_port_t -p "$protocol" "$port"
        fi
        # If the server is behind NAT, use the correct IP address
        [[ -n "$public_ip" ]] && ip="$public_ip"
        # client-common.txt is created so we have a template to add further
users later
        echo "client
dev tun
proto $protocol
remote $ip $port
resolv-retry infinite
nobind
```

```
persist-key
persist-tun
remote-cert-tls server
auth SHA512
cipher AES-256-CBC
ignore-unknown-option block-outside-dns
block-outside-dns
verb 3" > /etc/openvpn/server/client-common.txt
        # Enable and start the OpenVPN service
        systemctl enable --now openvpn-server@server.service
        # Generates the custom client.ovpn
        new_client
        echo
        echo "Finished!"
        echo
        echo "The client configuration is available in:" ~/"$client.ovpn"
        echo "New clients can be added by running this script again."
else
        clear
        echo "OpenVPN is already installed."
        echo
        echo "Select an option:"
        echo "   1) Add a new client"
        echo "   2) Revoke an existing client"
        echo "   3) Remove OpenVPN"
        echo "   4) Exit"
        read -p "Option: " option
        until [[ "$option" =~ ^[1-4]$ ]]; do
                echo "$option: invalid selection."
                read -p "Option: " option
        done
        case "$option" in
                1)
                        echo
                        echo "Provide a name for the client:"
                        read -p "Name: " unsanitized_client
                        client=$(sed
's/[^0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_-
]/_/g' <<< "$unsanitized_client")
                        while [[ -z "$client" || -e /etc/openvpn/server/easy-
rsa/pki/issued/"$client".crt ]]; do
                                echo "$client: invalid name."
                                read -p "Name: " unsanitized_client
                                client=$(sed
's/[^0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_-
]/_/g' <<< "$unsanitized_client")
                        done
                        cd /etc/openvpn/server/easy-rsa/
                        EASYRSA_CERT_EXPIRE=3650 ./easyrsa build-client-full
"$client" nopass
                        # Generates the custom client.ovpn
                        new_client
                        echo
```

```
                        echo "$client added. Configuration available in:"
~/"$client.ovpn"
                        exit
                ;;
                2)
                        # This option could be documented a bit better and
maybe even be simplified
                        # ...but what can I say, I want some sleep too
                        number_of_clients=$(tail -n +2
/etc/openvpn/server/easy-rsa/pki/index.txt | grep -c "^V")
                        if [[ "$number_of_clients" = 0 ]]; then
                                echo
                                echo "There are no existing clients!"
                                exit
                        fi
                        echo
                        echo "Select the client to revoke:"
                        tail -n +2 /etc/openvpn/server/easy-
rsa/pki/index.txt | grep "^V" | cut -d '=' -f 2 | nl -s ') '
                        read -p "Client: " client_number
                        until [[ "$client_number" =~ ^[0-9]+$ &&
"$client_number" -le "$number_of_clients" ]]; do
                                echo "$client_number: invalid selection."
                                read -p "Client: " client_number
                        done
                        client=$(tail -n +2 /etc/openvpn/server/easy-
rsa/pki/index.txt | grep "^V" | cut -d '=' -f 2 | sed -n
"$client_number"p)
                        echo
                        read -p "Confirm $client revocation? [y/N]: " revoke
                        until [[ "$revoke" =~ ^[yYnN]*$ ]]; do
                                echo "$revoke: invalid selection."
                                read -p "Confirm $client revocation? [y/N]: "
revoke
                        done
                        if [[ "$revoke" =~ ^[yY]$ ]]; then
                                cd /etc/openvpn/server/easy-rsa/
                                ./easyrsa --batch revoke "$client"
                                EASYRSA_CRL_DAYS=3650 ./easyrsa gen-crl
                                rm -f /etc/openvpn/server/crl.pem
                                cp /etc/openvpn/server/easy-rsa/pki/crl.pem
/etc/openvpn/server/crl.pem
                                # CRL is read with each client connection,
when OpenVPN is dropped to nobody
                                chown nobody:"$group_name"
/etc/openvpn/server/crl.pem
                                echo
                                echo "$client revoked!"
                        else
                                echo
                                echo "$client revocation aborted!"
                        fi
                        exit
```

```
                ;;
                3)
                        echo
                        read -p "Confirm OpenVPN removal? [y/N]: " remove
                        until [[ "$remove" =~ ^[yYnN]*$ ]]; do
                                echo "$remove: invalid selection."
                                read -p "Confirm OpenVPN removal? [y/N]: "
remove
                        done
                        if [[ "$remove" =~ ^[yY]$ ]]; then
                                port=$(grep '^port '
/etc/openvpn/server/server.conf | cut -d " " -f 2)
                                protocol=$(grep '^proto '
/etc/openvpn/server/server.conf | cut -d " " -f 2)
                                if systemctl is-active --quiet
firewalld.service; then
                                        ip=$(firewall-cmd --direct --get-
rules ipv4 nat POSTROUTING | grep '\-s 10.8.0.0/24 '"'"'!'"'"' -d
10.8.0.0/24' | grep -oE '[^ ]+$')
                                        # Using both permanent and not
permanent rules to avoid a firewalld reload.
                                        firewall-cmd --remove-
port="$port"/"$protocol"
                                        firewall-cmd --zone=trusted --remove-
source=10.8.0.0/24
                                        firewall-cmd --permanent --remove-
port="$port"/"$protocol"
                                        firewall-cmd --permanent --
zone=trusted --remove-source=10.8.0.0/24
                                        firewall-cmd --direct --remove-rule
ipv4 nat POSTROUTING 0 -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to "$ip"
                                        firewall-cmd --permanent --direct --
remove-rule ipv4 nat POSTROUTING 0 -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT
--to "$ip"
                                        if grep -qs "server-ipv6"
/etc/openvpn/server/server.conf; then
                                                ip6=$(firewall-cmd --direct --
get-rules ipv6 nat POSTROUTING | grep '\-s fddd:1194:1194:1194::/64
'"'"'!'"'"' -d fddd:1194:1194:1194::/64' | grep -oE '[^ ]+$')
                                                firewall-cmd --zone=trusted --
remove-source=fddd:1194:1194:1194::/64
                                                firewall-cmd --permanent --
zone=trusted --remove-source=fddd:1194:1194:1194::/64
                                                firewall-cmd --direct --
remove-rule ipv6 nat POSTROUTING 0 -s fddd:1194:1194:1194::/64 ! -d
fddd:1194:1194:1194::/64 -j SNAT --to "$ip6"
                                                firewall-cmd --permanent --
direct --remove-rule ipv6 nat POSTROUTING 0 -s fddd:1194:1194:1194::/64 !
-d fddd:1194:1194:1194::/64 -j SNAT --to "$ip6"
                                        fi
                                else
                                        systemctl disable --now openvpn-
iptables.service
```

```
                                        rm -f /etc/systemd/system/openvpn-
iptables.service
                                fi
                                if sestatus 2>/dev/null | grep "Current mode"
| grep -q "enforcing" && [[ "$port" != 1194 ]]; then
                                        semanage port -d -t openvpn_port_t -p
"$protocol" "$port"
                                fi
                                systemctl disable --now openvpn-
server@server.service
                                rm -rf /etc/openvpn/server
                                rm -f /etc/systemd/system/openvpn-
server@server.service.d/disable-limitnproc.conf
                                rm -f /etc/sysctl.d/30-openvpn-forward.conf
                                if [[ "$os" = "debian" || "$os" = "ubuntu" ]];
then
                                        apt-get remove --purge -y openvpn
                                else
                                        # Else, OS must be CentOS or Fedora
                                        yum remove -y openvpn
                                fi
                                echo
                                echo "OpenVPN removed!"
                        else
                                echo
                                echo "OpenVPN removal aborted!"
                        fi
                        exit
                ;;
                4)
                        exit
                ;;
        esac
fi
```

Ahora iniciemos el script

```
sudo bash openvpn-install.sh
```

El guion le hará algunas preguntas y, en la mayoría de los casos, querrá elegir la respuesta predeterminada. Para el puerto, puede elegir el puerto predeterminado, 1194, pero yo prefiero elegir 443, ya que 1194 se conoce como "el puerto OpenVPN" y, en algunos casos, se puede bloquear en su red. 443 es el mismo puerto que se usa para HTTPS, pero mientras que HTTPS usa TCP, OpenVPN (en esta configuración) usa UDP, por lo que no entrarán en conflicto entre sí.

También se le preguntará qué DNS desea utilizar. Siéntete libre de elegir lo que quieras, pero normalmente elijo 1.1.1.1

En cuanto al nombre del cliente, elige el que más te guste. Ahora que la configuración está hecha, presione cualquier tecla y el proceso de instalación comenzará. Es completamente automatizado.

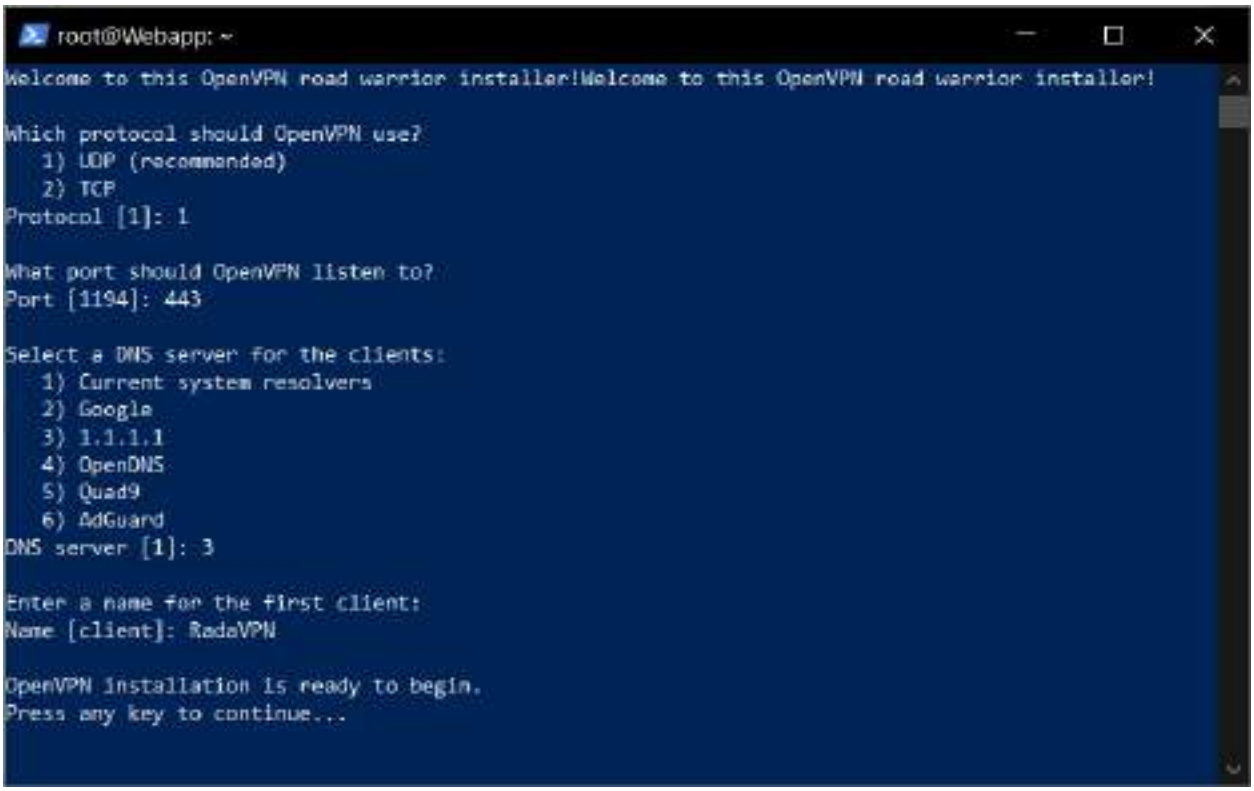


*Figura 2 – 47 Terminal Configuración Script Bash*

Al final obtendrás un archivo de configuración que descargaremos en nuestra máquina local más adelante. El problema es que el archivo RadaVPN.ovpn está en el directorio raíz por defecto, y para descargarlo más tarde, necesitamos moverlo al directorio de inicio de nuestro usuario y darnos los privilegios correctos:

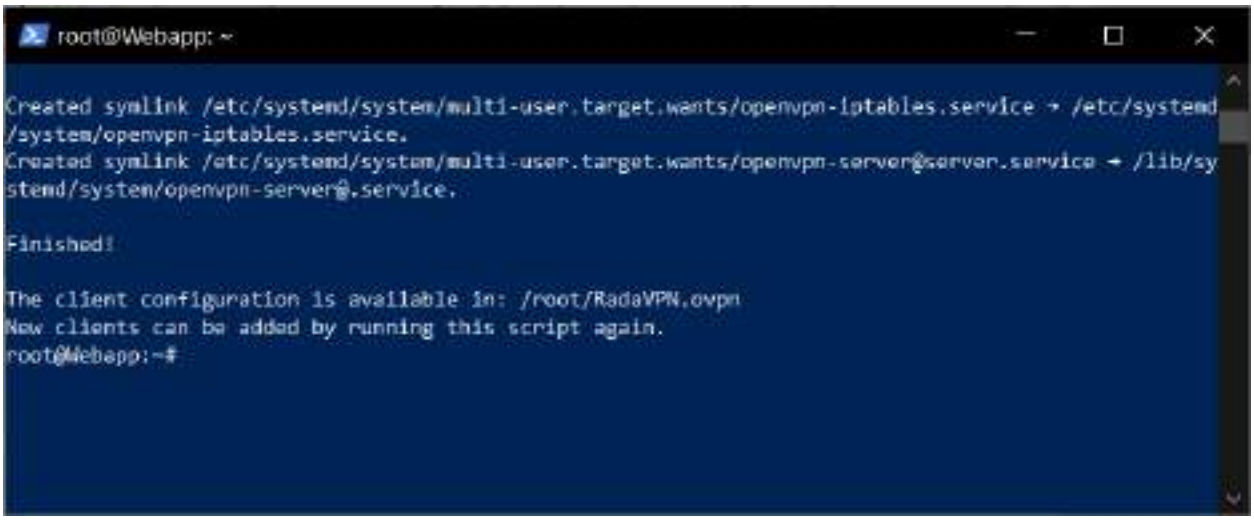


*Figura 2 – 48 Terminal Mensaje de Finalización OpenVPN*

Para poder copiar a la maquina necesitaremos correr los siguientes comandos

```
sudo mv /root/ RadaVPN.ovpn ~
sudo chown wolfgang RadaVPN.ovpn
```

Con esto fuera del camino, solo queda una cosa por hacer en el lado del servidor, y es deshabilitar los registros. Editemos el archivo de configuración:

```
sudo nvim /etc/openvpn/server/server.conf
```

Y cambia verb 3 a verb 0. Ahora reinicie el servicio OpenVPN:

```
systemctl restart openvpn-server@server.service
```

### II.1.3.3.2.9 Paso 9 Descargando el archivo de cliente

El archivo generado al momento de la culminación de la instalación del OpenVPN es el archivo cliente el cual contiene las credenciales para poder ingresar a la red privada virtual mediante el puerto que configuramos en el puerto 69.

Por lo que necesitamos descargarlo para poder ingresar y hacer las respectivas pruebas de la configuración ejecutando los siguientes comandos en la terminal o también se puede llegar a usar Programas de acceso SFTP como FileZilla entre otros.

*Figura 2 – 49 FileZilla Logo programa SFTP*

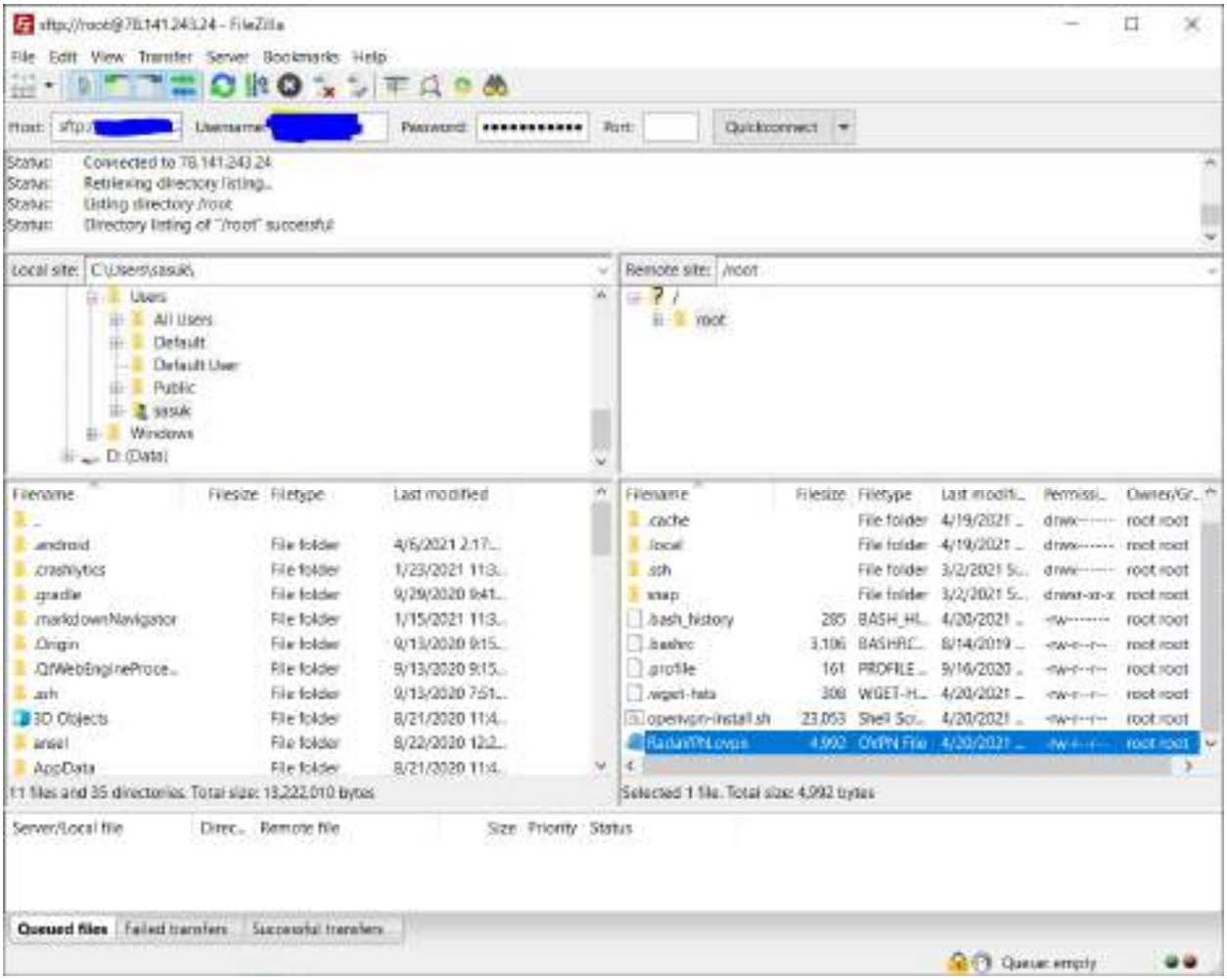


*Figura 2 – 50 FileZilla programa Conectado por SFTP puerto 22*

Ahora todo lo que tenemos que hacer es descargar el archivo de configuración a nuestra máquina local para que podamos usar la VPN. Abra una terminal en su máquina local y escriba.

```
sftp servername
```

Siguiente, descargue el archivo usando el comando:

```
get RadaVPN.ovpn
```

Y finalmente escribe:

```
exit
```

Deberíamos tener ahora el archivo en nuestras descargar ya que el SFTP lo pondrá ahí por defecto.

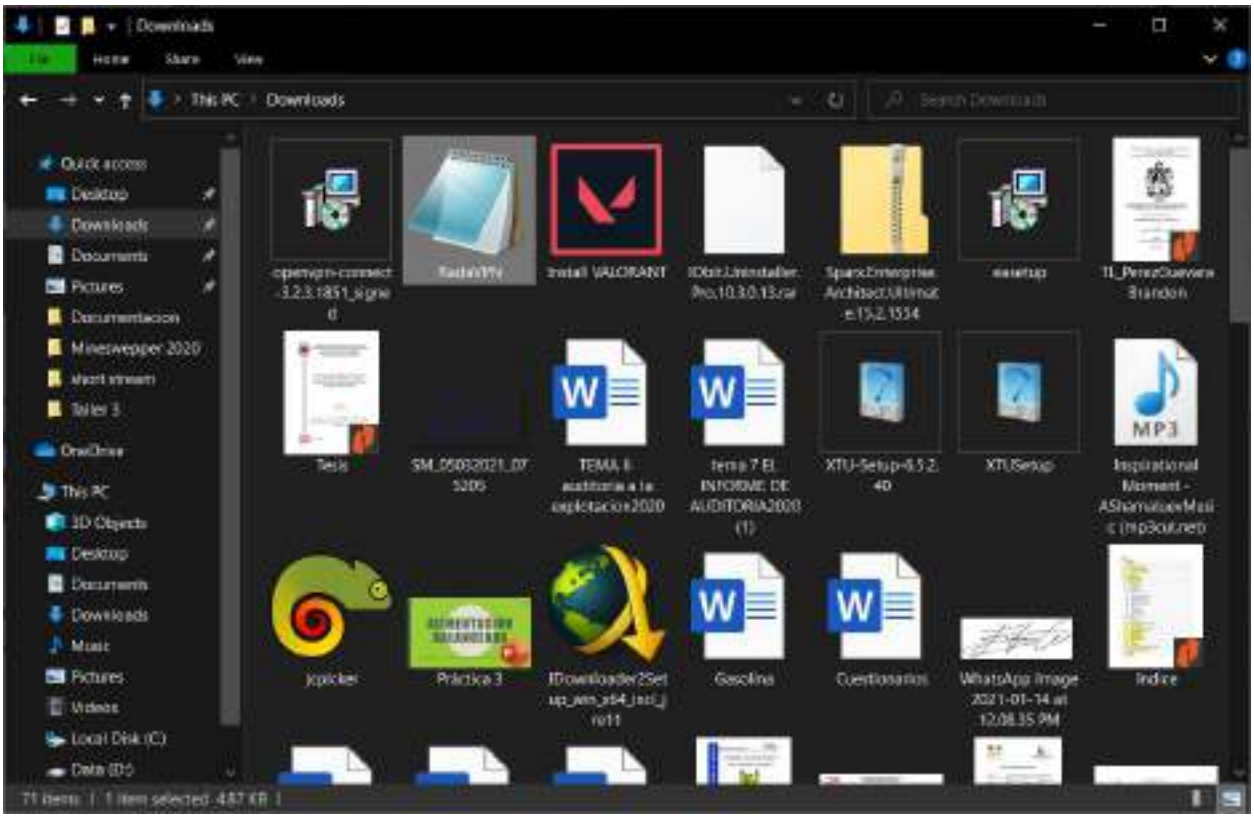


*Figura 2 – 51 Archivo Cliente OpenVPN*

### II.1.4 Estructura de Red Privada Virtual

| Localización Física/ País | Datos Servidor | Datos Red | SSL-VPN | L2TP/Ipsec | OvenVPN |
|---|---|---|---|---|---|
|  Japan | public-vpn-41.opengw.net 219.100.37.5 (219.100.37.5.vultr.com) | 3.49 Mbps Ping: 115 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1195 |
|  South Korea | vpn270196000.opengw.net 114.206.195.205 (114.206.195.205.vultr.com) | 64.42 Mbps Ping: 137 ms | TCP: 1313 UDP: Supported | UDP: Supported | TCP: 1313 UDP: 1654 |
|  United States | vpn607325998.opengw.net 207.148.91.158 (207.148.91.158.vultr.com) | 88.35 Mbps Ping: 118 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1195 |
|  United States | vpn224610463.opengw.net 45.32.8.100 (45.32.8.100.vultr.com) | 40.22 Mbps Ping: 120 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1195 |
|  United States | vpn733284746.opengw.net 45.32.29.3 (45.32.29.3.vultr.com) | 63.12 Mbps Ping: 122 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1195 |
|  United States | vpn408965850.opengw.net 198.13.36.179 (198.13.36.179.vultr.com) | 69.35 Mbps Ping: 118 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1195 |
|  Viet Nam | vpn171214815.opengw.net 14.241.119.9 (14.241.119.9.vultr.com) | 30.07 Mbps Ping: 138 ms | TCP: 1760 UDP: Supporte | UDP: Supported | TCP: 1760 UDP: 1916 |
|  Taiwan | kangfu.opengw.net 220.135.38.248 (220.135.38.248.vultr.com) | 25.33 Mbps Ping: 110 ms | TCP: 992 | UDP: Supported | TCP: 992 UDP: 1194 |
|  Thailand | vpn805124257.opengw.net 184.22.21.255 (184.22.21.255.vultr.com) | 29.69 Mbps Ping: 126 ms | UDP: Supported | UDP: Supported | UDP: 1671 |
|  Ukraine | vpn183085284.opengw.net 95.133.165.21 (184.22.21.255.linode.com) | 4.07 Mbps Ping: 133 ms | TCP: 443 UDP: Supported | UDP: Supported | UDP: 11981 |
|  Russian Federation | vpn636561501.opengw.net 46.187.2.203 (46.187.2.203.linode.com) | 8.93 Mbps Ping: 132 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1194 |
|  Singapore | vpn214769594.opengw.net 103.250.73.22 (103.250.73.22.linode.com) | 36.37 Mbps Ping: 211 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1194 |

| | | | | | |
|---|---|---|---|---|---|
|  United Kingdom | vpn797767052.opengw.net 217.138.212.46 (217.138.212.46.linode.com) | 297.70 Mbps Ping: 262 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1194 |
|  France | canadavpn1.opengw.net 54.39.64.209 (54.39.64.209.linode.com) | 22.13 Mbps Ping: 121 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1194 |
|  China | vpn828564105.opengw.net 101.33.33.219 (101.33.33.219.linode.com) | 66.20 Mbps Ping: 368 ms | TCP: 443 UDP: Supported | UDP: Supported | TCP: 443 UDP: 1194 |
|  Canada | vpn216865086.opengw.net 38.110.109.109 | 11.84 Mbps Ping: 186 ms | TCP: 1612 UDP: Supported | UDP: Supported | TCP: 1612 UDP: 1433 |

*Tabla 2 – 1 Estructura de Red Privada Virtual*

### II.1.5 Medios de verificación (Componente 1)

#### II.1.5.1 Pruebas de Seguridad Conexión Directa

Realizando la prueba de IP check podemos ver que la pagina detecta con facilidad todos nuestros datos y no solo los nuestros, sino que también los de nuestro ISP dejando ver que el está pasando por un DNS de Brasil para llegar al internet, lo cual es cierto ya que Bolivia no tiene una conexión directa a la internet, sino que pasamos por las conexiones marítimas en Brasil. Tambien Indicando que nuestra conexcion no es segura en la parte superior.

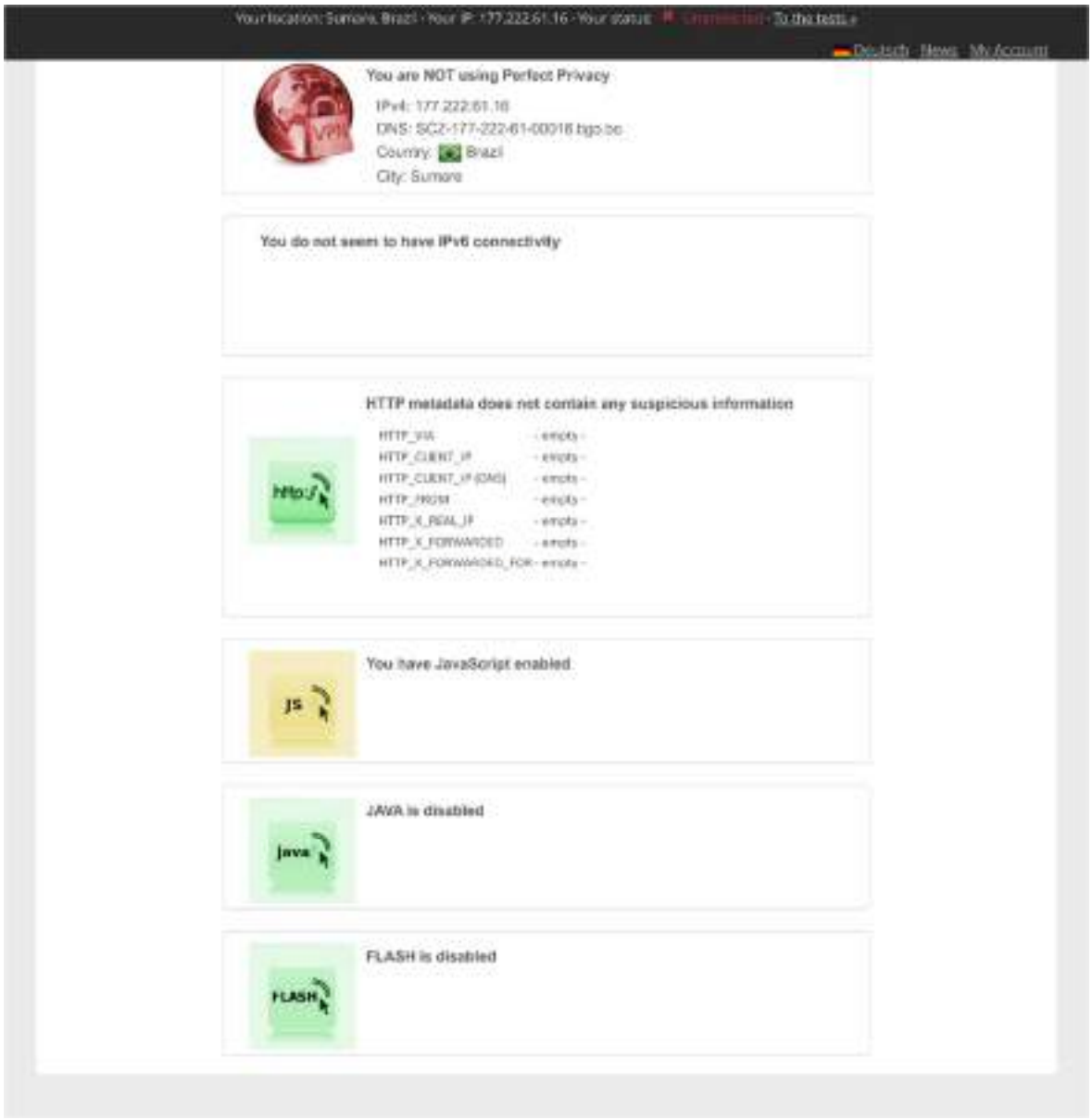


*Figura 2 – 52 Prueba IP Check página Perfect Privacy sin VPN*

Realizando la prueba de DNS se detectan los DNS del ISP que llegaría a ser Tigo brindando la información y mostrando que ellos usan 2 servidores DNS uno para paquetes locales y otro para quetes externos dado que también existen IP publican en Bolivia para servicio como llegan a ser las páginas y servicio de la universidad que usas como ISP a TIGO y Entel Simultáneamente.

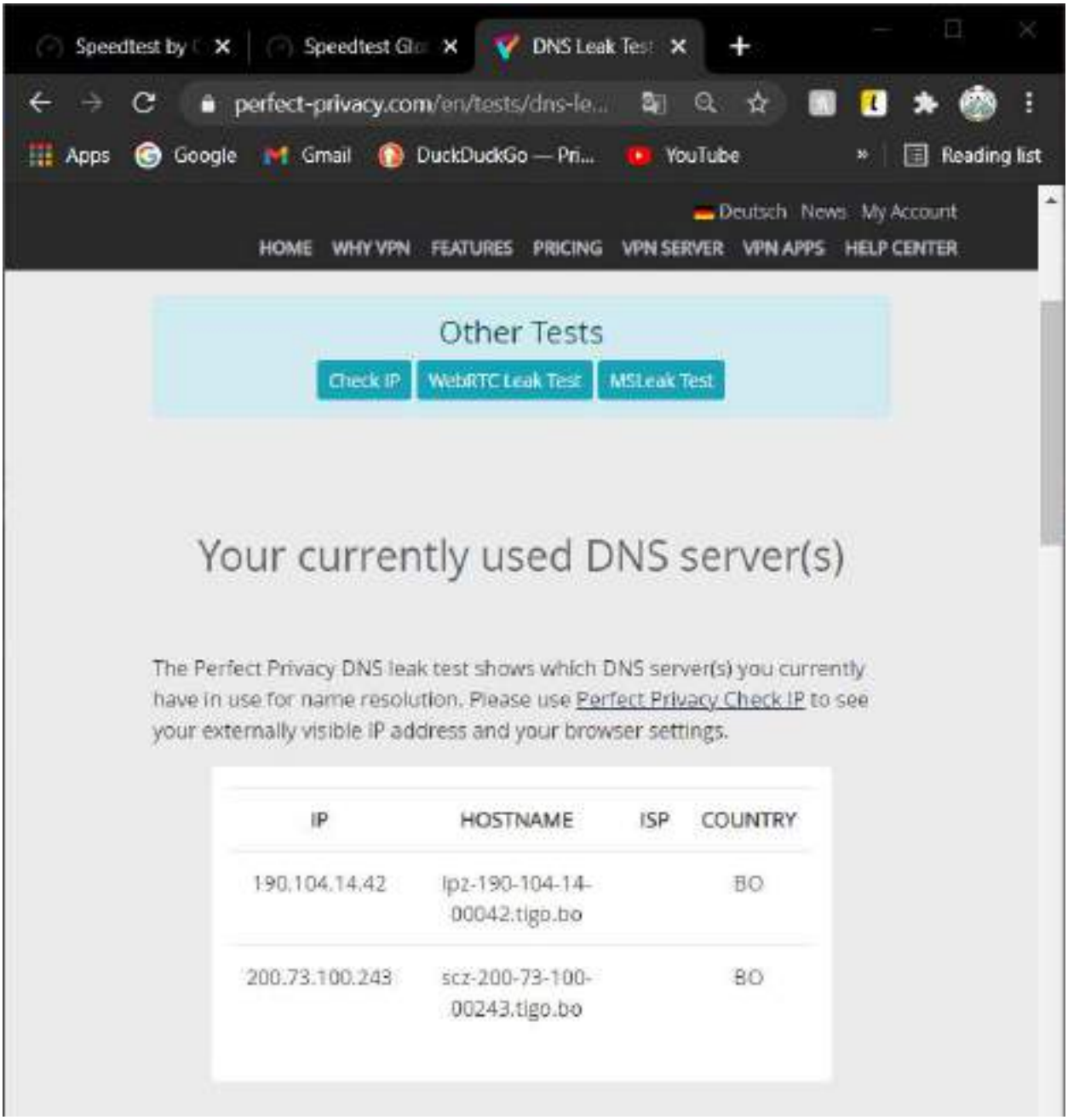


*Figura 2 – 53 Prueba DNS página Perfect Privacy sin VPN*

La última prueba es ver cuál es la velocidad de nuestra conexión a la internet cuando no estamos usando un VVPN para protegernos, el plan con el que cuento debería darnos 60MB de ancho de banda entre baja y subida.

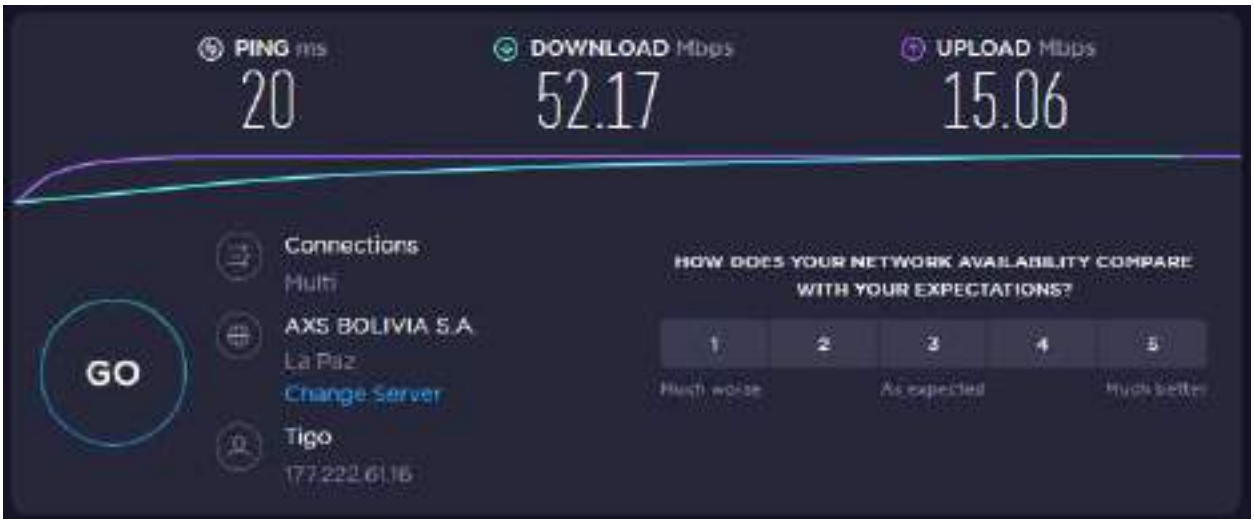


*Figura 2 – 54 Prueba velocidad Internet página SpeedTest by Ookla sin VPN*

### II.1.5.2 Pruebas de Seguridad Conexión OpenVPN

Luego Tener un servidor configurado verificaremos que podemos conectarnos a el usando la aplicación OpenVPN Connect de la página de OpenVPN el cual es una aplicación de Código Abierto que aceptara nuestro archivo de cliente en la siguiente dirección.

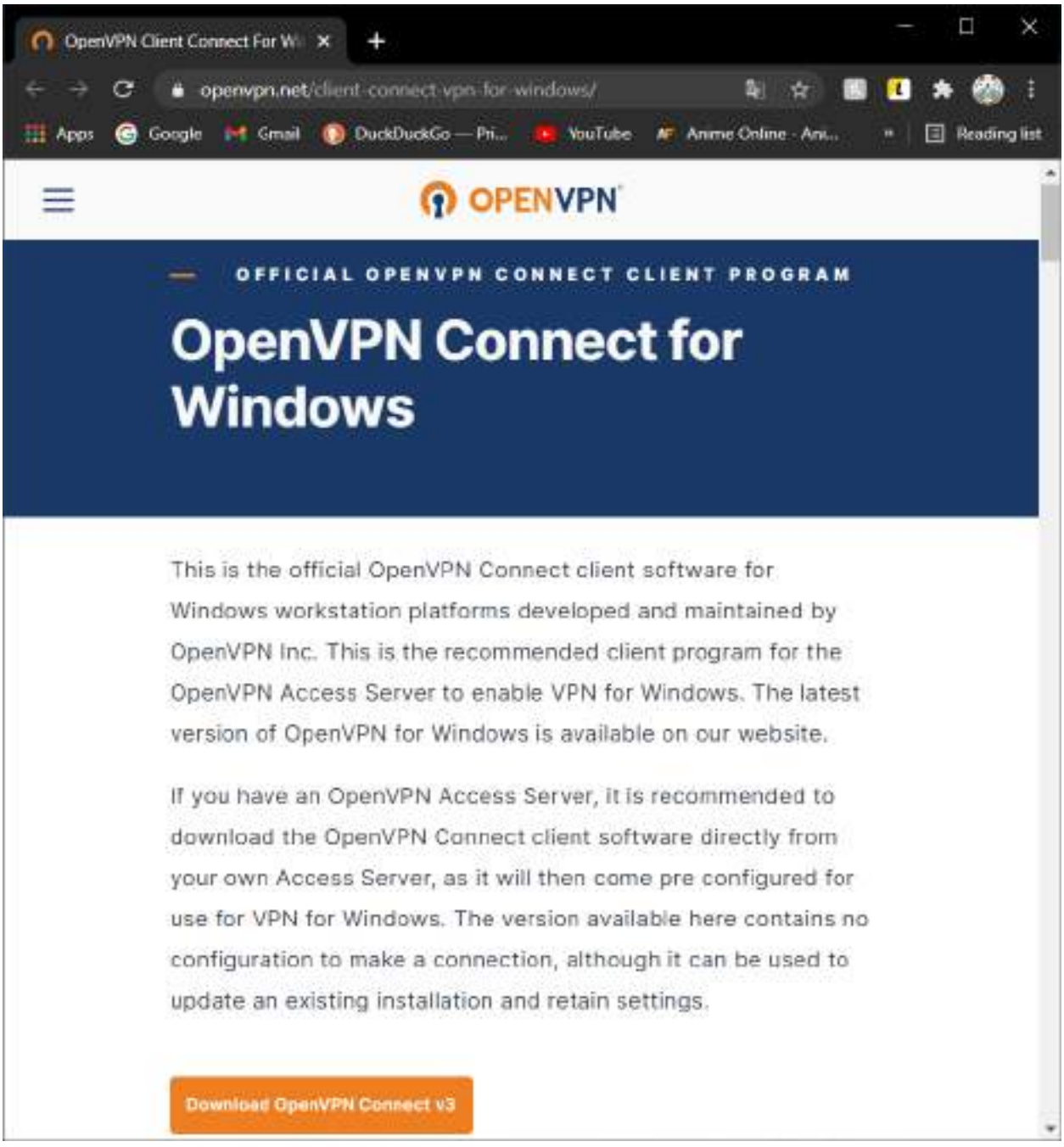


*Figura 2 – 55 OpenVPN Connect Pagina*

Instalamos y terminaremos con una pantalla donde nos pedirá ingresar la información de nuestro servidor OpenVPN en una pestaña pero en otra nos dará la opción de simplemente subir nuestro archivo de cliente llamada RadaVPN.ovpn .

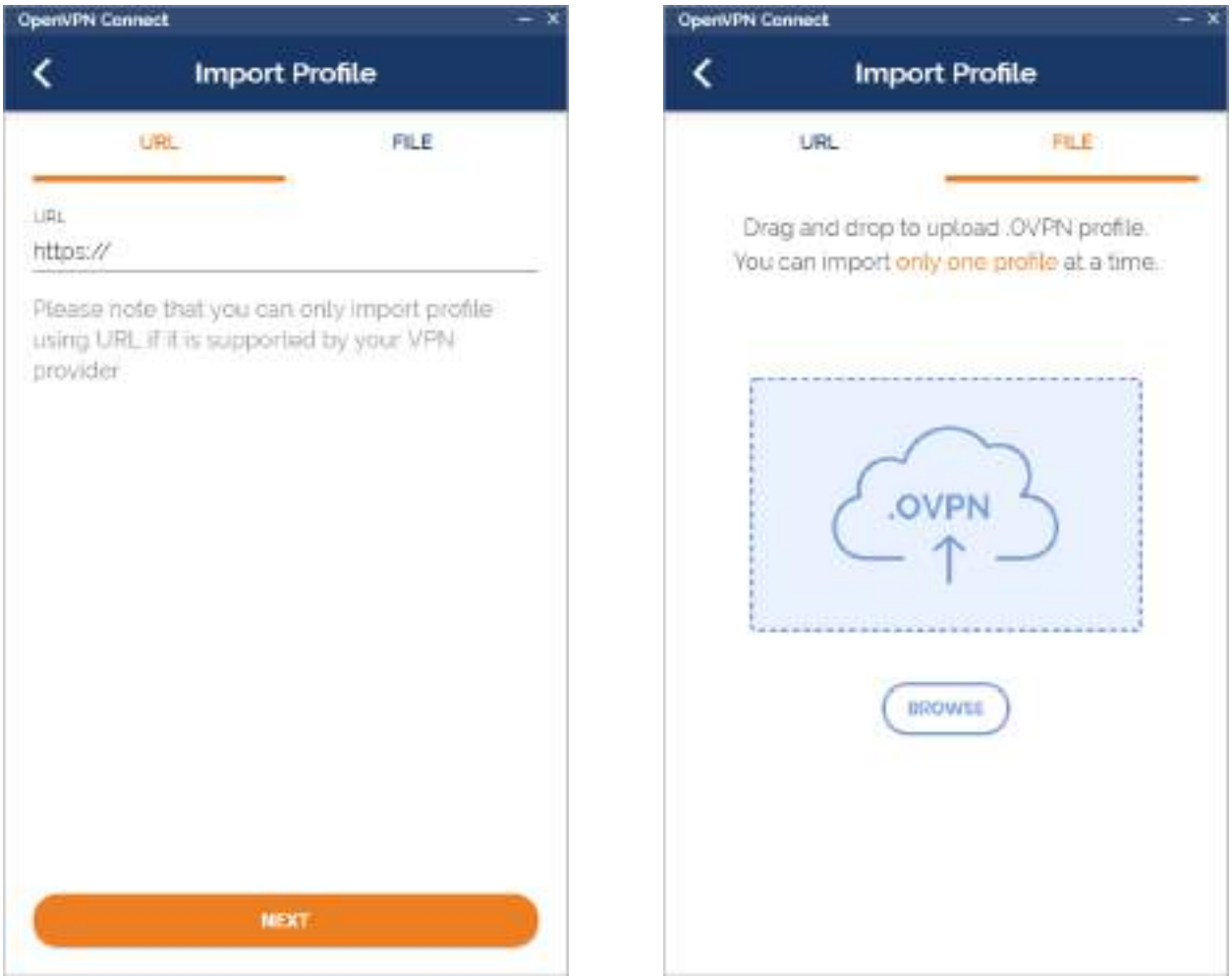


*Figura 2 – 56 Pantallas Inicio OpenVPN Connect*

Subiremos nuestro archivo en la pantalla file para no tener que ingresar la información de nuestro VPN además de que al haber cambiado el puerto del servicio OpenVPN 1194 por el puerto 443 no podremos usar la opción de conexión en la pantalla URL porque cambiamos el puerto a uno no estándar por motivos de seguridad.

Deberíamos terminar con una pantalla con un mensaje resaltado en verde que dice “Perfil exitosamente importado”.


*Figura 2 – 57 Pantalla Importación perfil OpenVPN Connect*

Luego de que el programa tenga un perfil de red OpenVPN dentro de ella ahora se abrirá directamente en la pantalla de perfiles el cual podremos activar la conexión a los perfiles que tengamos disponibles.

Activaremos la conexión al perfil que recién creado con el nombre de RadaVPN y se muestra la conexión la cantidad de datos que estamos consumiendo entre otras cosas más.

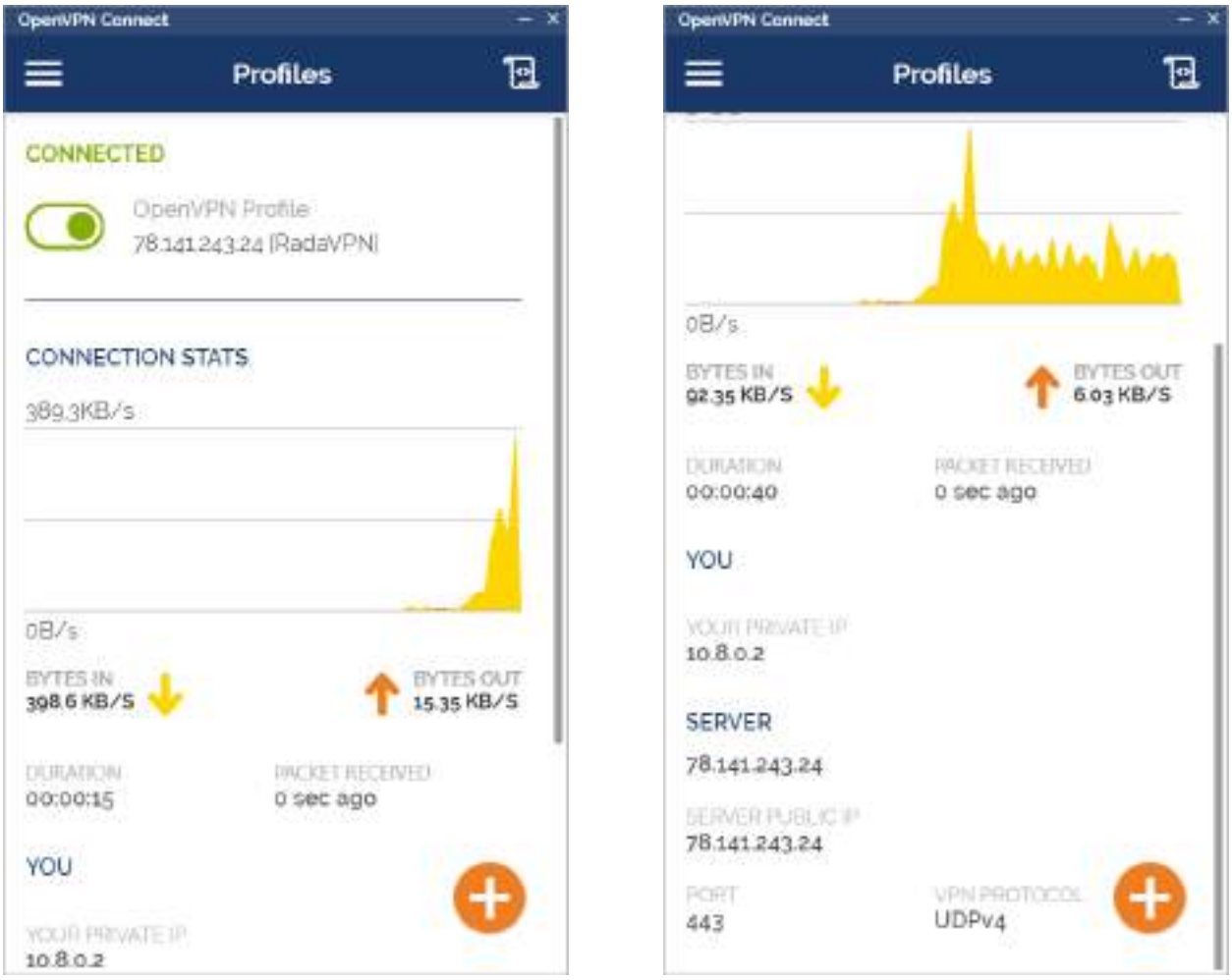


*Figura 2 – 58 Pantallas Conectado a Servidor OpenVPN Connect*

Ahora podremos verificar si nuestra tenemos conexión a la internet y con qué IP estamos saliendo a ella con una página que prueba la seguridad de nuestra conexión llamada Perfect-Privacy.com.

La prueba nos muestra que tenemos un IP en el país de nuestro servidor que es el Reino Unido además de cambiar nuestro DNS y no poder localizarnos en una ciudad en específico.

También muestra que nuestras solicitudes no contienen ningún tipo de rastreos o registros de navegación ni de tipo HTTP o HTTPS también indicando que solo tenemos activado JS y no así Java o Flash.

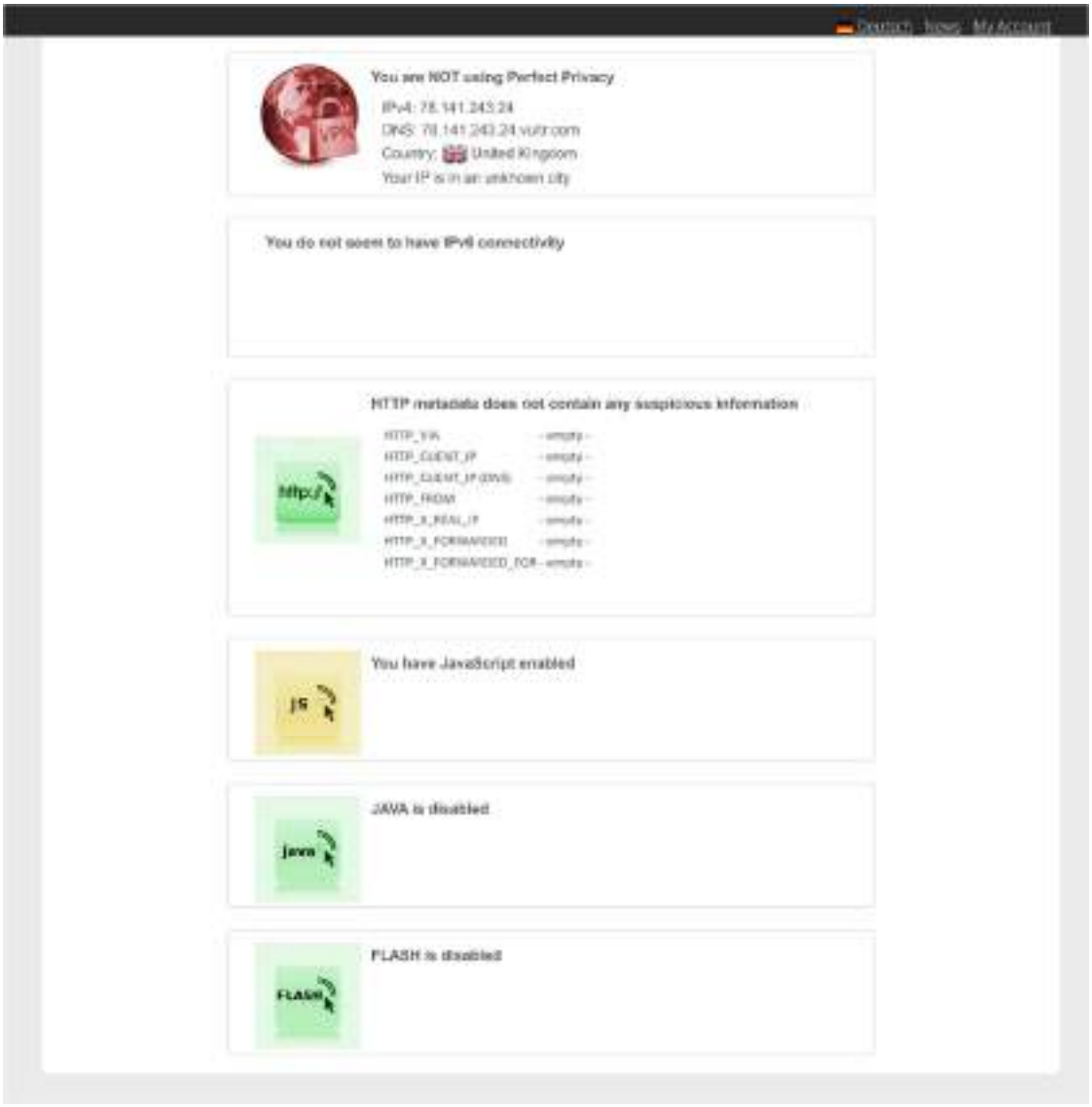


*Figura 2 – 59 Prueba IP Check página Perfect Privacy*

El DNS test nos muestra que tampoco ve que estemos haciendo más de 2 saltos en cuanto a nuestras solicitudes a su página lo que es bueno ya que ni siquiera puede ver nuestro DNS principal si no que solo los de nuestro servidor que e el ultimo por el que pasan.

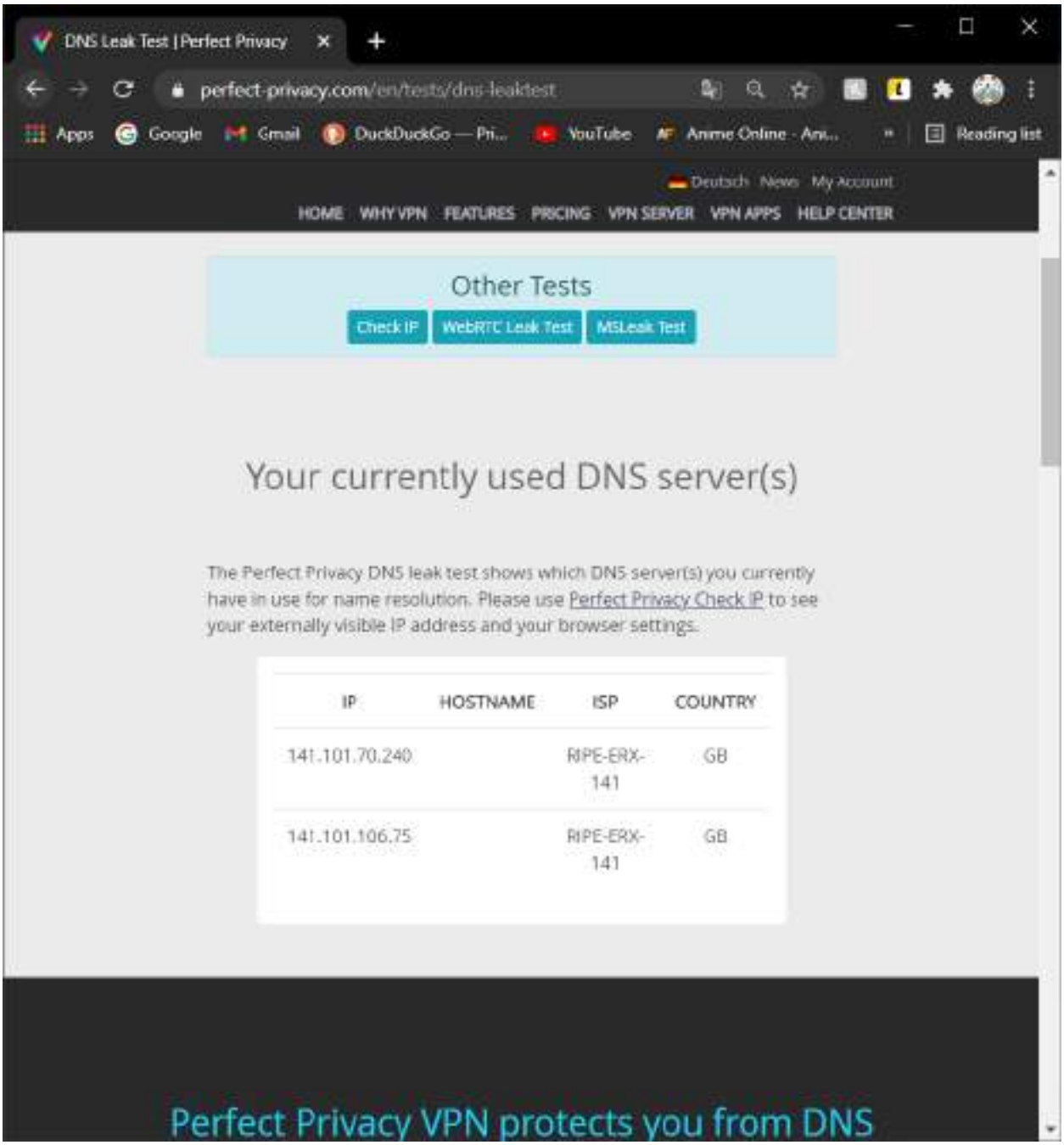


*Figura 2 – 60 Prueba DNS página Perfect Privacy*

Por último, el WebRTC Leak Test no muestra que no pueden encontrar rastro alguno de nuestra IP real por lo tanto el servicio de OpenVPN que instalamos está protegiendo nuestra identidad en la red a no permitir que nadie puede obtener nuestra IP real.

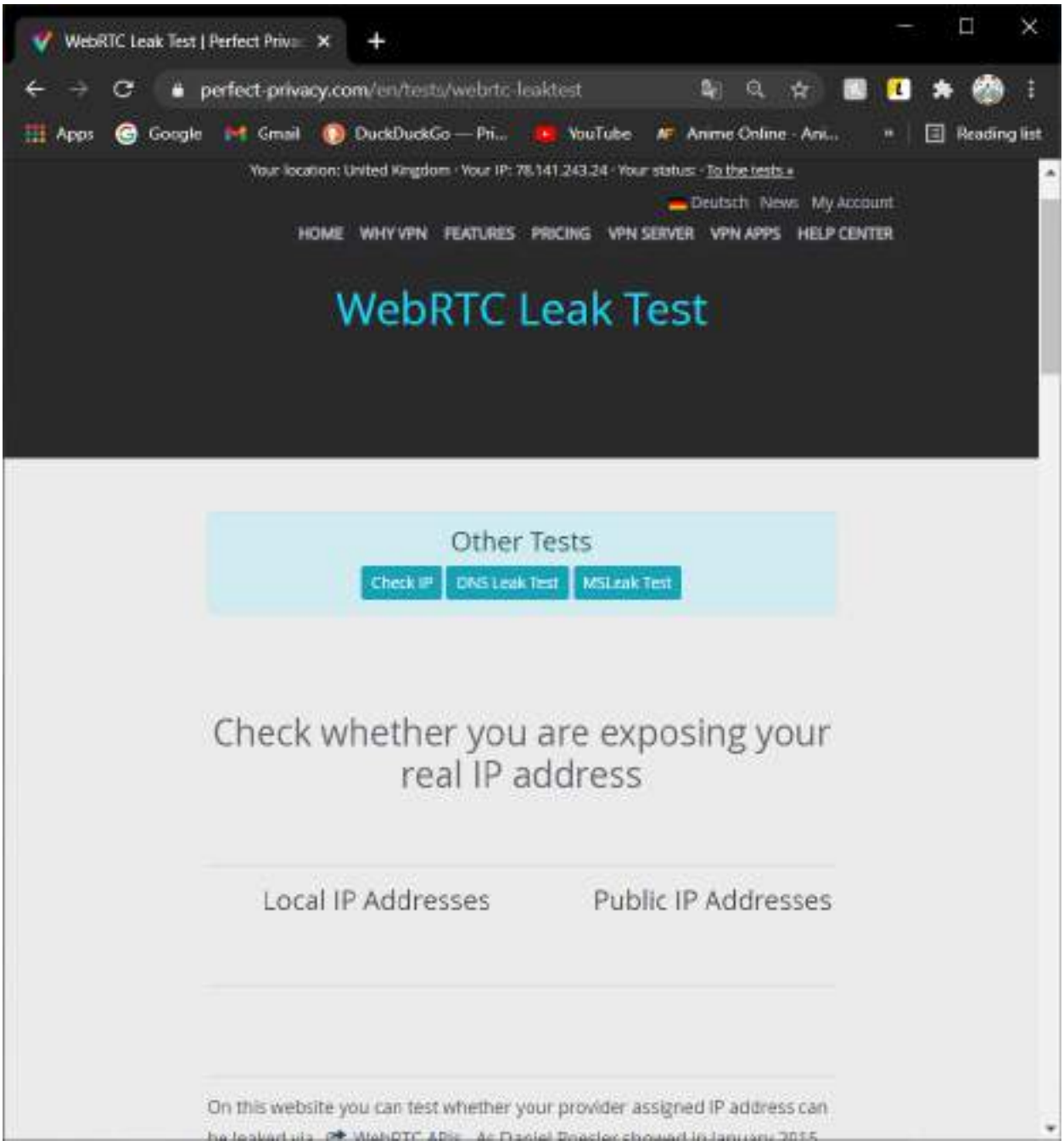


*Figura 2 – 61 Prueba WebRTC Leak Test página Perfect Privacy*

Para finalizar las pruebas al servicio OpenVPN que levantamos veremos en la localización actual cual es nuestra velocidad y ping dado que todo estos saltos y la encriptación de nuestras solicitudes tienen a reducir lastimosamente nuestra velocidad de conexión a cambio de brindarnos seguridad. Lo haremos en la página [SpeedTest by Ookla]


*Figura 2 – 62 Prueba velocidad Internet página SpeedTest by Ookla*

### II.1.5.3 Pruebas de propaganda y recolección de información

Una de las bondades de un VPN también es el poder evitar que las paginas recolecten información por ejemplo cuando uno busca un producto en alguna página como Amazon o también redes sociales como Facebook, porque ellas ahora también permiten promocionar productos para vender y comprar. Procederemos a Buscar en varias páginas información sobre aspiradoras para poder observar que estas páginas y todas las paginas en el internet, aunque una pueda pensar que su contenido esta gratis ahí para nosotros poder usarlo no nos damos cuenta que monetizan nuestra vistas información.

Este tipo de prácticas de recolección de información es muy común en el inter y las paginas se ven obligadas a hacerlo para monetizar el servicio que ofrecen, este tipo de propaganda personalidad de una característica bastante depredadora de parte de las páginas que compran esa información y nos precondicionan a pensar que queremos adquirir dichos productos que buscamos a veces solo por curiosidad en su página mediante anuncios. Estos también pueden ser para por programar y extensiones en navegadores llamados “ADD BLOCKERS” los cuales permiten bloquear el cargado los archivos de direcciones que son conocidas como páginas de propagandas mediante sus IP y dominios algo que el protocolo VPN ofrece ya incluido mediante la configuración del Firewall bloqueando paginas conocidas por ser de anuncios.

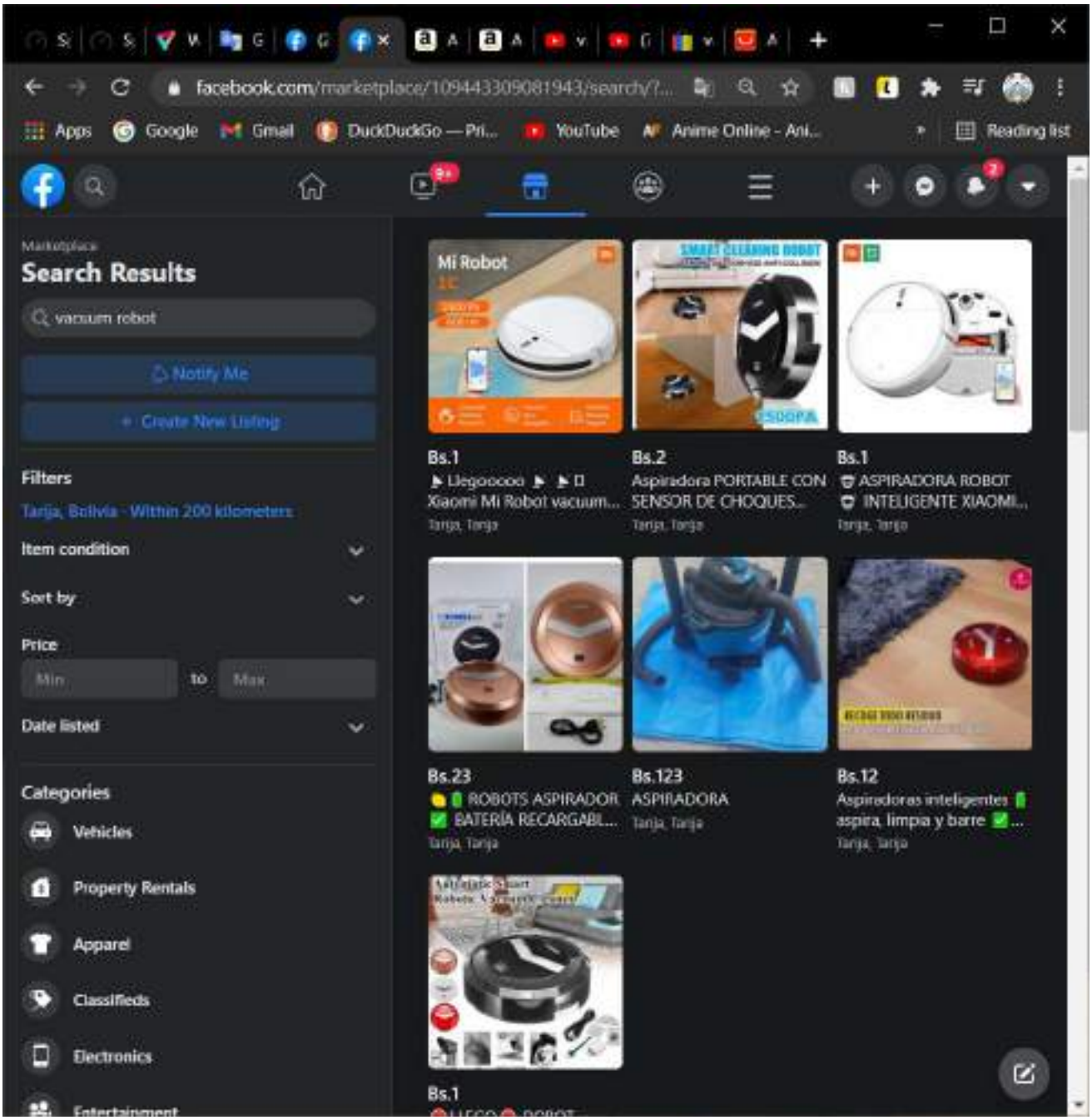


*Figura 2 – 63 Buscamos Aspiradoras Robot en Facebook*

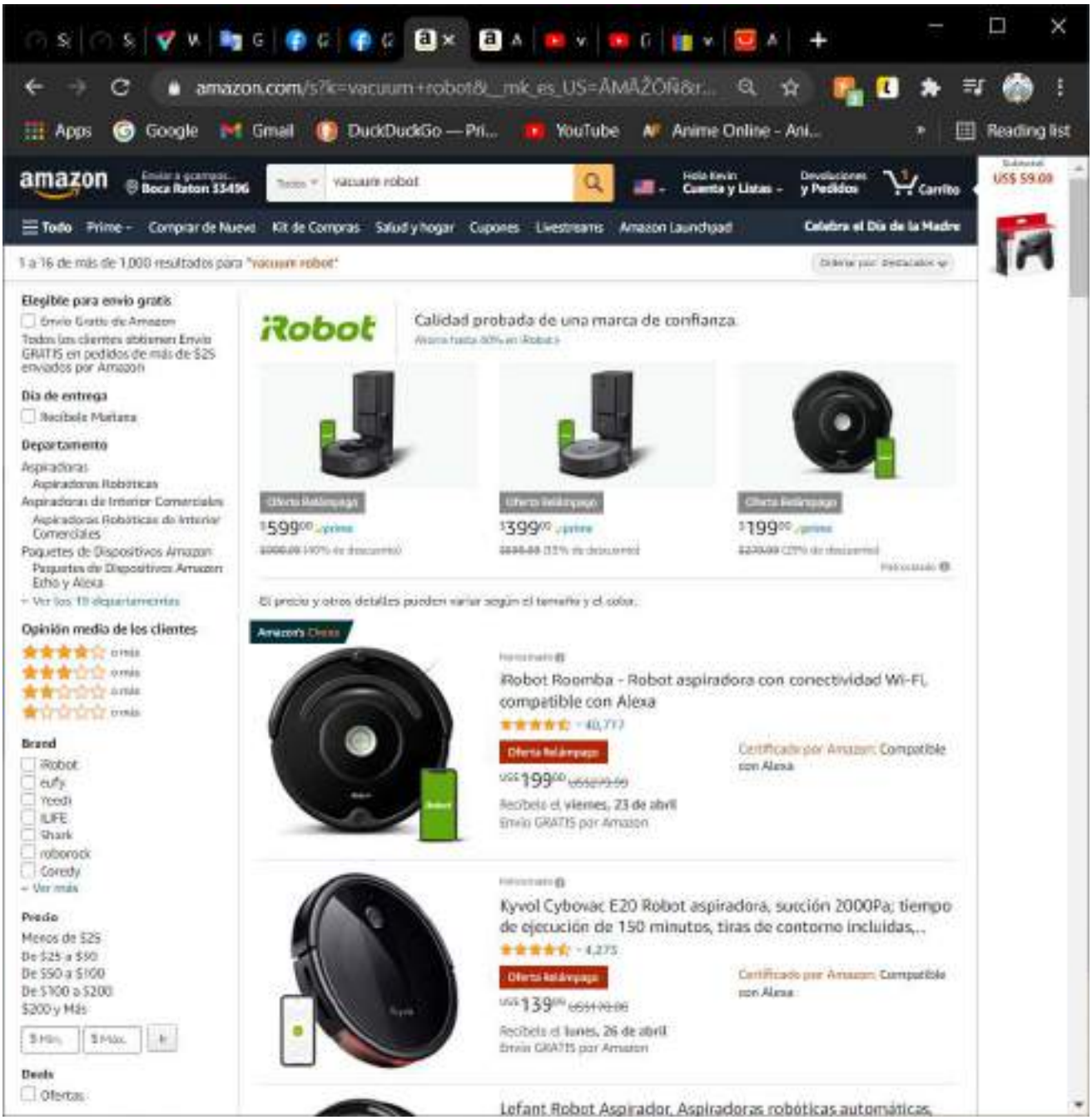


*Figura 2 – 64 Buscamos Aspiradoras Robot en Amazon*

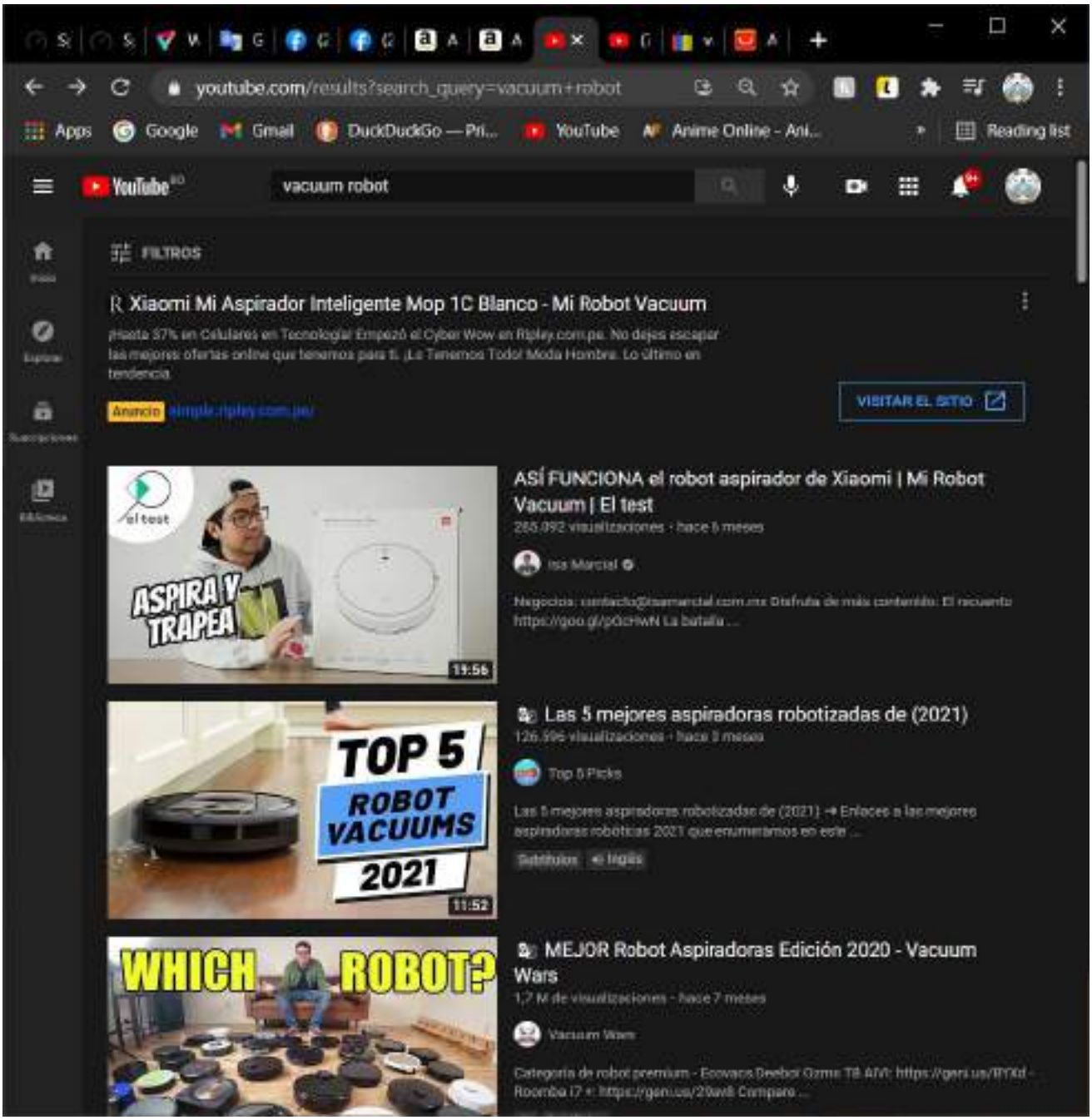


*Figura 2 – 65 Buscamos Aspiradoras Robot en YouTube*

Como podemos ver después de haber buscado un poco sobre aspiradora robot ahora podemos apreciar que en una página totalmente distinta de venta ya sabe que estamos buscando y nos la ofrece incluso usando el navegador en modo Incognito esto también se puede ver que ingresando a la misma página Aliexpress en un navegador totalmente distinto también nos está ofreciendo eso varias veces.


*Figura 2 – 66 Página de Inicio Aliexpress Navegador en modo Incognito Chrome*

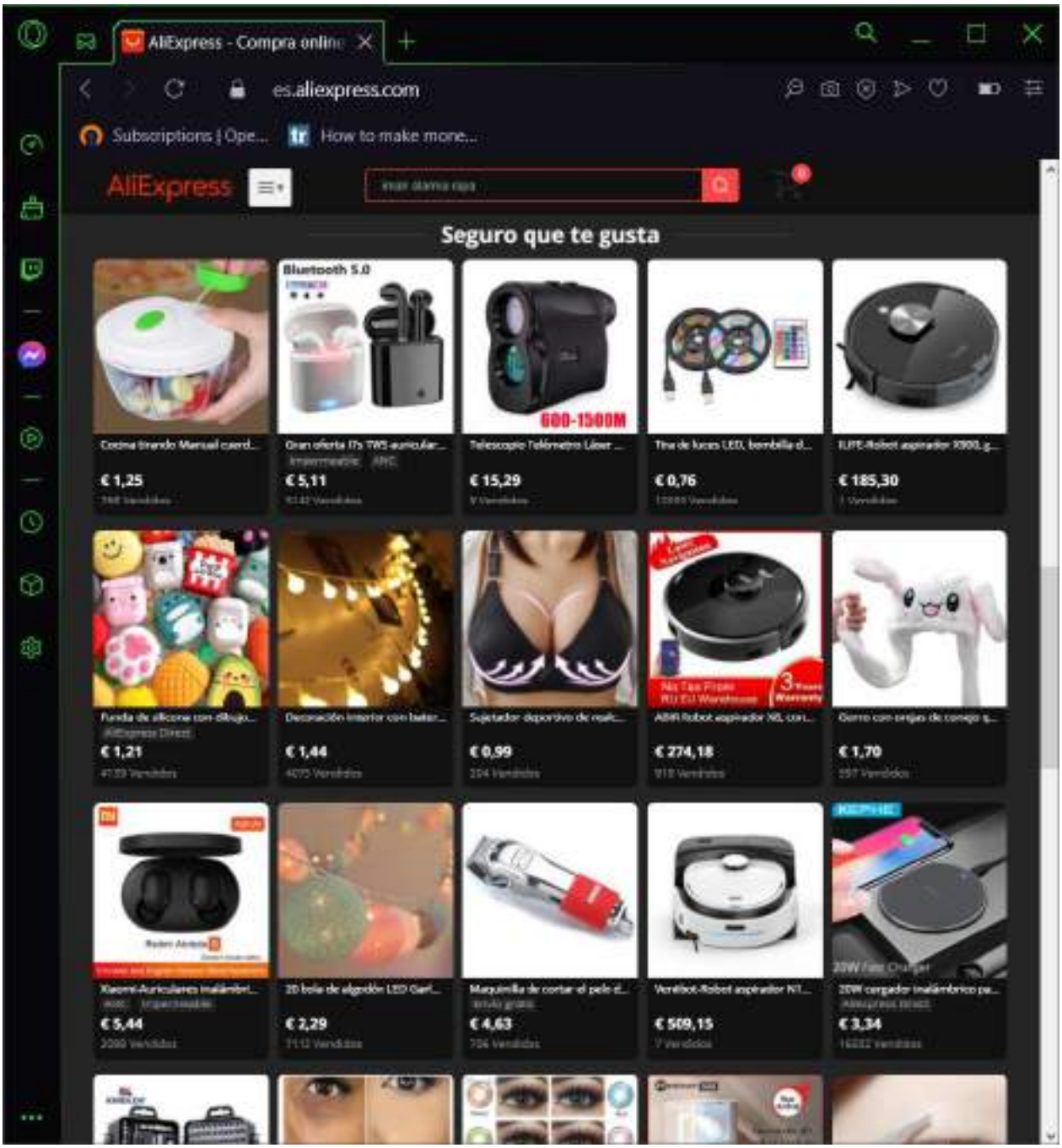


*Figura 2 – 67 Página de Inicio Aliexpress Navegador Opera GX*

En conclusión, podemos ver que la paginas casi todas registran y recolectan información sobre nosotros algunas que usamos mucho como redes sociales terminan por nuestro comportamiento en ella incluso creando perfiles sobre nosotros llegando a poder inferir nuestros gustos como así también preferencias y vendiendo esta información muy exacta y bastante aterradoras a las compañías que ofrezcan más por ellas.

Es por eso que gigantes de la tecnología estos últimos años han estado enfrentándose a demandas y regulación por los distintos gobiernos del mundo porque el tipo de recolección de información que hacen sobre sus usuarios explotándolo por ganancias muchas veces sin siquiera avisarles a sus usuarios que están haciendo eso aun peor pidiendo el consentimiento para ello. Uno de los casos mas aterradores de como este tipo de creación de perfiles detallados de usuarios se pudo ver cuando Facebook tuvo el escándalo de "Cambridge Analytica" donde Facebook vendió eses perfiles de sus usuarios hecho con la recolección de información de sus acciones y el trabajo de la misma por AI a la empresa "Cambridge Analytica" la cual la uso para servir propaganda muy específica a cada persona para cambiar la dirección de las elecciones de Estados Unidos de una manera significante.

#### II.1.5.4 Pruebas de Restricciones Geográficas

Una de las principales razones para usar un VPN aparte de la seguridad que brindan es poder modificar la localización geográfica de donde estamos solicitando servicios a paginas esto es algo muy bueno para cuando queremos acceder a contenido que por alguna extraña razón no está disponible para nosotros, esta situación es inaceptable cuando servicios de streaming ponen este tipo de restricciones porque los usuarios están pagando por un servicio y que este servicio quite o aumente contenido según nuestra localización no es algo aceptable.

Como en el siguiente caso, se puede apreciar que página de Prime Video no nos ofrece ninguna temporada de Pokémon cuando estamos en Bolivia si no que tengo que cambiar la localización para poder acceder a ellos en este caso estoy cambiándome al Reino Unido que es el servidor que se creó para las pruebas.

Esto es algo que se tiene que hacer para poder consumir contenido que se a pagado, pero por alguna razón no licenciaron el contenido para nuestro país, pero pagamos lo mismo que todos los demás países por un servicio peor.

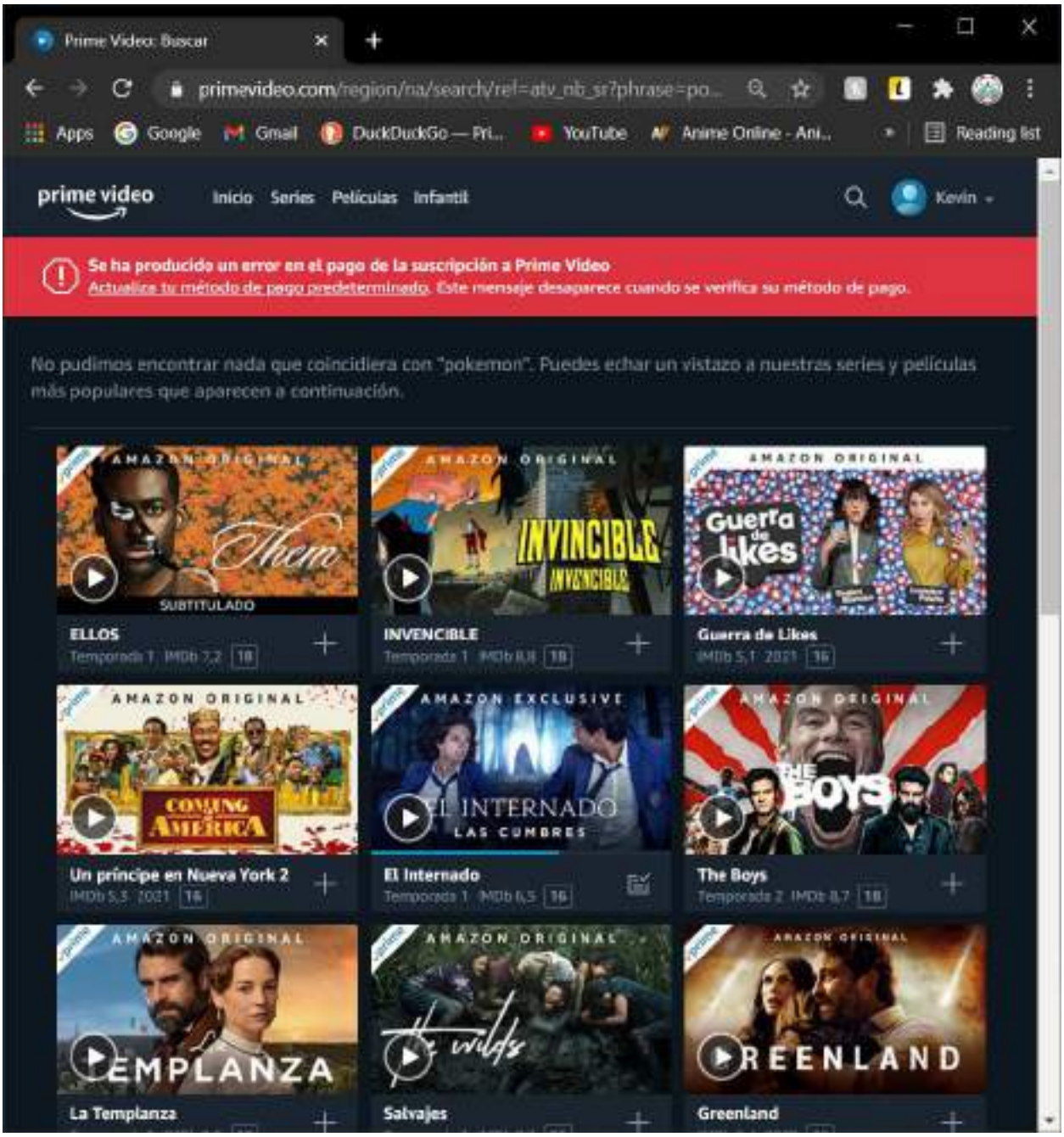


*Figura 2 – 68 Página Prime Video sin VPN*

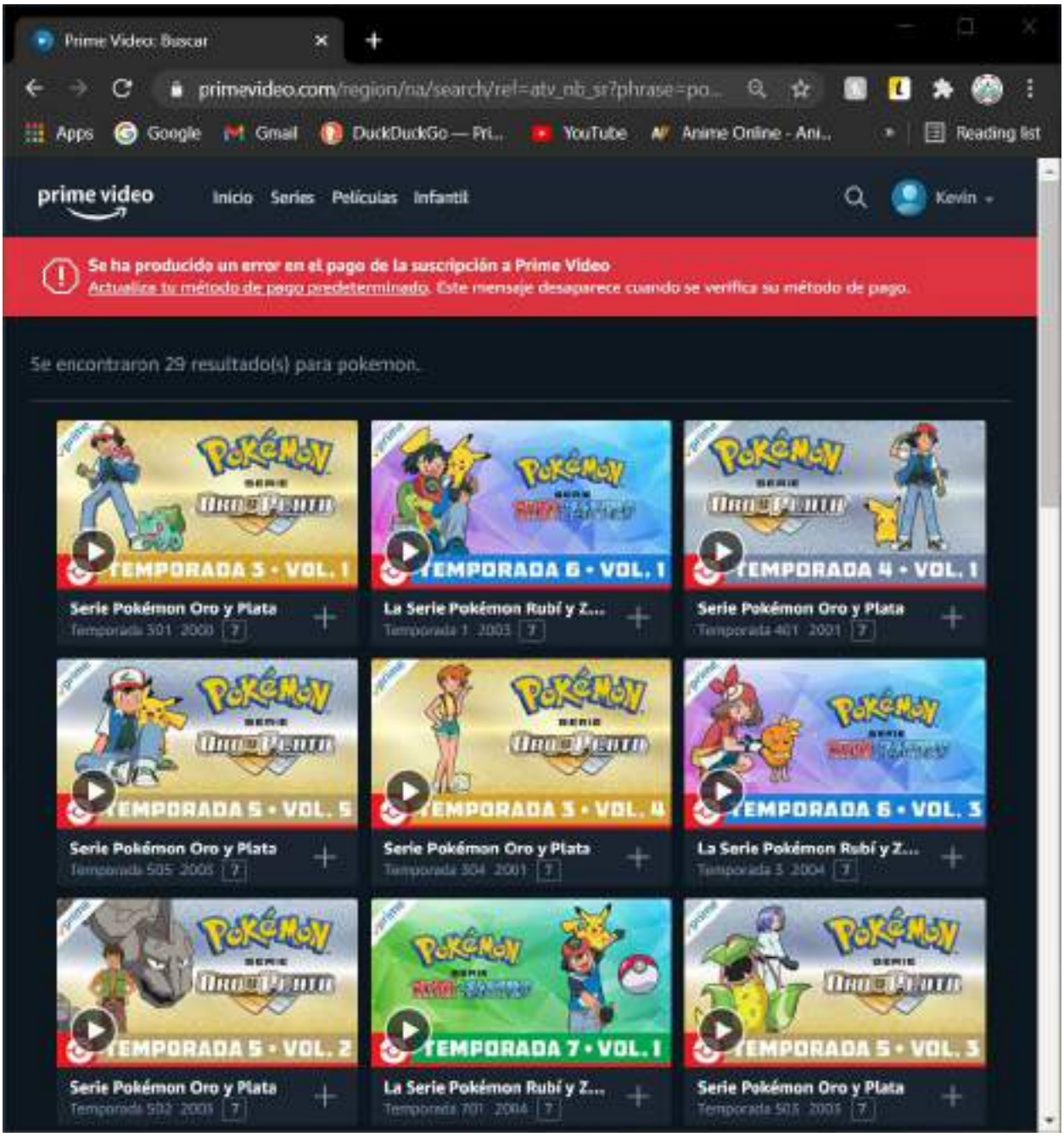


*Figura 2 – 69 Página Prime Video con VPN*

Lo mismo ocurre en muchos otros servicios y páginas que por la localización donde nos encontramos nos restringen el acceso a contenido tanto como el que es “gratis” y el pagado y esto es algo muy perjudicial para los usuarios, uno podría estar tratando de aprender algo nuevo o buscar guía para algo para sorprenderse que el video, guía, tutorial no esta disponible para su país lo que es algo frustrante.

## II.2 Componente 2: Sistema de Web

El sistema web de gestión de usuarios proveerá con una página para promocionar el VPN y la creación de las cuentas de los usuarios. Permitiendo después de un inicio de sesión poder manear su información básica y suscripción a los usuarios dado que la privacidad es prioridad solo se tomarán los datos más básicos de los usuarios.

### II.2.1 Marco Teórico

### II.2.2 Metodología de Desarrollo

#### II.2.2.1 Metodología RUP (Rational Unified Process)

El Proceso Racional Unificado o RUP (por sus siglas en inglés de Rational Unified Process) es un proceso de desarrollo de software desarrollado por la empresa Rational Software, actualmente propiedad de IBM.1 Junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, diseño, implementación y documentación de sistemas orientados a objetos.

Es un proceso de ingeniería de software que suministra un enfoque para asignar tareas y responsabilidades dentro de una organización de desarrollo. Su objetivo es asegurar la producción de software de alta y de mayor calidad para satisfacer las necesidades de los usuarios que tienen un cumplimiento al final dentro de un límite de tiempo y presupuesto previsible. Es una metodología de desarrollo iterativo que es enfocada hacia "diagramas de los casos de uso, y manejo de los riesgos y el manejo de la arquitectura" como tal.

**A. Principales características**

- Forma disciplinada de asignar tareas y responsabilidades (quién hace qué, cuándo y cómo).
- Pretende implementar las mejores prácticas en Ingeniería de Software.
- Desarrollo iterativo.
- Administración de requisitos.
- Uso de arquitectura basada en componentes.
- Control de cambios.

- Modelado visual del software.
- Verificación de la calidad del software.

**B. Ciclo de Vida**

El ciclo de vida RUP es una implementación del Desarrollo en espiral. Fue creado ensamblando los elementos en secuencias semi-ordenadas. El ciclo de vida organiza las tareas en fases e iteraciones.

RUP divide el proceso en cuatro fases, dentro de las cuales se realizan varias iteraciones en número variable según el proyecto y en las que se hace un mayor o menor hincapié en las distintas actividades. Fases del ciclo de vida del RUP:

1. **Fase de Inicio:**

   Esta fase tiene como propósito definir y acordar el alcance del proyecto con los patrocinadores, identificar los riesgos asociados al proyecto, proponer una visión muy general de la arquitectura de software y producir el plan de las fases y el de iteraciones posteriores.

2. **Fase de elaboración:**

   En la fase de elaboración se seleccionan los casos de uso que permiten definir la arquitectura base del sistema y se desarrollaran en esta fase, se realiza la especificación de los casos de uso seleccionados y el primer análisis del dominio del problema, se diseña la solución preliminar.

3. **Fase de Desarrollo o Construcción:**

   El propósito de esta fase es completar la funcionalidad del sistema, para ello se deben clarificar los requerimientos pendientes, administrar los cambios de acuerdo a las evaluaciones realizados por los usuarios y se realizan las mejoras para el proyecto.

4. **Fase de Transición:**

   El propósito de esta fase es asegurar que el software esté disponible para los usuarios finales, ajustar los errores y defectos encontrados en las pruebas de aceptación,

capacitar a los usuarios y proveer el soporte técnico necesario. Se debe verificar que el producto cumpla con las especificaciones entregadas por las personas involucradas en el proyecto.

**C. Elementos del RUP**

**Actividades:** Procesos que se han de realizar en cada etapa/iteración.

**Trabajadores:** Personas involucradas en cada actividad del proyecto.

**Artefactos:** Herramientas empleadas para el desarrollo del proyecto. Puede ser un documento, un modelo, un elemento del modelo. Estos artefactos (entre otros) son los siguientes:

**Inicio**

- Documento Visión
- Especificación de Requerimientos

**Elaboración**

- Diagramas de caso de uso

**Construcción**

- Documento Arquitectura que trabaja con las siguientes vistas:
    - **Vista lógica**
        - Diagrama de clases
        - Modelo E-R
    - **Vista de implementación**
        - Diagrama de Secuencia
        - Diagrama de estados
        - Diagrama de Colaboración
    - **Vista conceptual**
        - Modelo de dominio
    - **Vista física**
        - Mapa de comportamiento a nivel de hardware

(Booch, Ivar, & Rumbaugh, 1998)

Para el desarrollo del presente proyecto se utilizó la metodología RUP, al ser flexible y adaptable al proceso del proyecto, realizándose de manera iterativa en cada una de sus fases.

#### II.2.2.2 UML (Lenguaje Unificado de Modelado)

Lenguaje Unificado de Modelado (UML, por sus siglas en inglés, Unified Modeling Language) es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad; está respaldado por el OMG (Object Management Group). Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. UML ofrece un estándar para describir un "plano" del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio, funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y compuestos reciclados. Es importante remarcar que UML es un "lenguaje de modelado" para especificar o para describir métodos o procesos. Se utiliza para definir un sistema, para detallar los artefactos en el sistema y para documentar y construir. En otras palabras, es el lenguaje en el que está descrito el modelo (Booch, Ivar, & Rumbaugh, 1998).

En el presente proyecto se utilizó UML para el diseño y elaboración de diagramas de clases, casos de uso, actividades y de secuencias que reflejan los requerimientos y el funcionamiento del sistema.

#### II.2.2.3 Tipos de Diagrama Utilizados

##### II.2.2.3.1 Diagrama de Clases

El propósito de un diagrama de clase es describir las clases que conforman el modelo de un determinado sistema. Dado el carácter de refinamiento iterativo que caracteriza un desarrollo orientado a objetos, el diagrama de clase va a ser creado y refinado durante las fases de análisis y diseño, estando presente como guía en la implementación del sistema (Booch, Ivar, & Rumbaugh, 1998).

#### II.2.2.3.2 Diagrama de Actividades

Un Diagrama de Actividades representa un flujo de trabajo paso a paso de negocio y operacionales de los componentes en un sistema.

En UML 1, un diagrama de actividades es una variación del Diagrama de Estados UML donde los estados representan operaciones y las transiciones representan las actividades que ocurren cuando la operación es completa.

Los diagramas de actividades se utilizaron para definir el comportamiento interno de los procesos del presente Sistema (Booch, Ivar, & Rumbaugh, 1998).

#### II.2.2.3.3 Diagrama de Secuencia

Un Diagrama de Secuencias muestra una interacción ordenada según la secuencia temporal de eventos y el intercambio de mensajes. Los diagramas de secuencia ponen especial énfasis en el orden y el momento en el que se envían los mensajes a los objetos.

En los diagramas de Secuencias los elementos están representados por líneas intermitentes verticales, con el nombre del objeto en la parte más alta (Booch, Ivar, & Rumbaugh, 1998).

Los diagramas de Secuencias se utilizaron para reflejar cómo interactúan los componentes principales del presente sistema.

### II.2.2.4 Herramientas de Construcción de Software

#### II.2.2.4.1 Sublime Text

Sublime Text es un editor de desarrollo y texto súper rápido y lleno de funciones. Si vas a codificar regularmente, quieres probar este increíble editor (IDE). Siguiendo algunas de las excelentes características que hacen que Sublime Text se destaque de otros editores de código.

Características:

- Múltiples cursores: una vez que haya descubierto múltiples cursores, ya no querrá trabajar sin ellos. Como su nombre lo indica, le permiten escribir o editar en varios lugares de un documento al mismo tiempo.
- Rápido como el rayo: este es el editor de código más rápido que encontrarás en este momento.
- Paleta de comandos: una gran característica que le permite acceder a todas las funciones del editor a través del teclado. Difícilmente usará su mouse y, por lo tanto, codificará de manera más eficiente.
- Colección de complementos: una comunidad muy activa crea complementos para casi cualquier tarea en Sublime Text. Esto incluye resaltado de sintaxis y fragmentos de código para una gran cantidad de idiomas, por ejemplo, Javascript, PHP, CSS, HTML, Python, LESS, XML y C ++, por nombrar solo algunos.
- Control de paquetes: este complemento le permite instalar complementos en cuestión de segundos directamente desde el editor.

(Sublimetext, 2020)

#### II.2.2.4.2 Enterprise Architect

Enterprise Architect es una plataforma de alto desempeño para el modelado, visualización y diseño, basada en el estándar UML 2.4.1. Ofrece trazabilidad completa desde mapas mentales, pasando por los requerimientos y hasta el diseño y la distribución del software, con el nivel de eficiencia, robustez, herramientas de colaboración y seguridad requerida para sacar adelante proyectos altamente demandantes y cualquier tamaño.

Enterprise Architect es una aplicación completa para la elaboración de proyectos de Ingeniería. Está diseñado especialmente para el enfoque empresarial, y junto a ello, se especializa en la realización de diagramas UML de todo tipo: Componentes, Clases y Bases de Datos. Soporta el trabajo sobre varios lenguajes de programación como Java.

Características:

- Completa herramienta de análisis y diseño en UML
- Modelado avanzado para negocios, software y sistemas
- Completa trazabilidad desde los requerimientos hasta la distribución
- Ingeniería de código en más de 10 lenguajes
- Altamente escalable, repositorios basados en el equipo de trabajo
- Mapas mentales, BPMN, Arquitectura Empresarial, etc.

(Sparxsystems, 2020)

Se utilizó Enterprice Architect para la elaboración de los diagramas UML empleados en el presente proyecto.

#### II.2.2.4.3 MariaDB

MariaDB es un sistema de base de datos que proviene de MySQL, pero con licencia GPL, desarrollado por Michael Widenius, fundador de MySQL y la comunidad de desarrolladores de software libre.

Características:

- MariaDB maneja hasta 32 segmentos clave por clave
- Se agregó –abort-source-on-error al cliente mysql
- Precisión de microsegundos en la lista de procesos
- Pool de hilos de ejecución o procesos
- Eliminación de tablas
- Extensiones de prueba mysqltest
- Columnas virtuales
- Estadísticas extendidas para el usuario
- Caché de claves segmentadas
- Autenticación a través de plugins
- Especificación de motor de almacenamiento en CREATE TABLE
- Mejoras a la tabla INFORMATION SCHEMA.PLUGINS
- Se agregó –rewrite-db como opción en mysqlbinlog al cambiar de base de datos usada
- Reporte de Procesos para ALTER TABLE y LOAD DATA INFILE (Mariadb, 2020).

(Mariadb, 2020).

### II.2.2.5 Técnica

#### II.2.2.5.1 HTML (HyperText Markup Language)

HTML, que significa Lenguaje de Marcado para Hipertextos (HyperText Markup Language) es el elemento de construcción más básico de una página web y se usa para crear y representar visualmente una página web. Determina el contenido de la página web, pero no su funcionalidad.

HTML le añade "marcado" a un texto estándar en español. "Hiper Texto" se refiere a enlaces que conectan una página Web con otra, haciendo de la Telaraña Mundial (World Wide Web) lo que es hoy. Al crear y subir páginas Web a Internet, usted se hace un participante activo de esta Telaraña Mundial una vez su sitio está en línea. HTML soporta imágenes y también otro tipo de elementos multimedia. Con la ayuda de HTML todos pueden hacer sítios web estáticos y dinámicos. HTML es el lenguaje que describe la estructura y el contenido semántico de un documento web. El contenido dentro de una página web es etiquetado con elementos HTML como <img>, <title>, <p>, , y así sucesivamente. Estos elementos conforman los bloques de construcción de un sitio web (Mozilla, 2020).

Para el desarrollo del Sistema se utilizó html para el diseño de las páginas web que serán visualizadas por el usuario.

#### II.2.2.5.2 XML (Extensible Markup Languaje)

XML, siglas en inglés de Xtensible Markup Language ("lenguaje de marcas Extensible"), es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible. Proviene del lenguaje SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML) para estructurar documentos grandes. A diferencia de otros lenguajes, XML da soporte a bases de datos, siendo útil cuando varias aplicaciones deben comunicarse entre sí o integrar información.

XML no ha nacido sólo para su aplicación para Internet, sino que se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable.

Objetivos:

- XML debe ser directamente utilizable en Internet
- XML debe soportar una amplia variedad de aplicaciones
- XML debe ser compatible con SGML
- Debería se sencillo escribir programas que procesaran documentos XML
- El número de las características opcionales en XML debería ser el mínimo posible, a ser posible cero
- Los documentos XML deberían ser legibles por las personas y razonablemente claros
- El diseño de XML debe ser rápido
- XML debería ser simple, pero perfectamente normalizado
- Los documentos XML deben ser de fácil creación
- La concisión de las marcas XML tiene una importancia mínima

(Mozilla, 2020)

Se empleó XML en el desarrollo del presente Sistema para el intercambio de información entre los controladores modelo visto controlador.

#### II.2.2.5.3 CCS (cascading Style Sheets)

Hojas de Estilo en Cascada (del inglés Cascading Style Sheets) o CSS es el lenguaje de estilos utilizado para describir la presentación de documentos HTML o XML (incluyendo varios languages basados en XML como SVG, MathML o XHTML). CSS describe como debe ser renderizado el elemento estructurado en la pantalla, en papel, en el habla o en otros medios.

CSS es uno de los lenguajes base de la Open Web y posee una especificación estandarizada por parte del W3C. Anteriormente, el desarrollo de varias partes de las especificaciones de CSS era realizado de manera sincrónica, lo que permiía el versionado de las recomendaciones. Probablemente habrás escuchado acerca de CSS1, CSS2.1, CSS3. Sin embargo, CSS4 nunca se ha lanzado como una versión oficial (Mozilla, 2021).

#### II.2.2.5.4 JQuery

jQuery es una biblioteca de JavaScript, creada inicialmente por John Resig, que permite simplificar la manera de interactuar con los documentos HTML, manipular el árbol DOM, manejar eventos, desarrollar animaciones y agregar interacción con la técnica AJAX a páginas web. Fue presentada el 14 de enero de 2006 en el BarCamp NYC. jQuery es la biblioteca de JavaScript más utilizada. JQuery es software libre y de código abierto, posee un doble licenciamiento bajo la Licencia MIT y la Licencia Pública General de GNU v2, permitiendo su uso en proyectos libres y privados.2 jQuery, al igual que otras bibliotecas, ofrece una serie de funcionalidades basadas en JavaScript que de otra manera requerirían de mucho más código, es decir, con las funciones propias de esta biblioteca se logran grandes resultados en menos tiempo y espacio (Jquery, 2020).

JQuery se utilizó en el desarrollo del sistema para agregar efectos y funciones de validación en los campos de ingreso datos.

#### II.2.2.5.5 JavaScript

JavaScript es un lenguaje de programación que se utiliza principalmente para crear páginas web dinámicas. Una página web dinámica es aquella que incorpora efectos como texto que aparece y desaparece, animaciones, acciones que se activan al pulsar botones y ventanas con mensajes de aviso al usuario. Técnicamente, JavaScript es un lenguaje de programación interpretado, por

lo que no es necesario compilar los programas para ejecutarlos. En otras palabras, los programas escritos con JavaScript se pueden probar directamente en cualquier navegador sin necesidad de procesos intermedios. A pesar de su nombre, JavaScript no guarda ninguna relación directa con el lenguaje de programación Java. Legalmente, JavaScript es una marca registrada de la empresa Sun Microsystems (Mozilla, 2020).

Para un diseño dinámico y más amigable de las páginas web para el usuario se utilizó el lenguaje de programación JavaScript.

#### II.2.2.5.6 PHP (Hypertext Preprocessor)

PHP (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. PHP es un lenguaje de código abierto muy popular, adecuado para desarrollo web y que puede ser incrustado en HTML. Es popular porque un gran número de páginas y portales web están creadas con PHP. Código abierto significa que es de uso libre y gratuito para todos los programadores que quieran usarlo. Incrustado en HTML significa que en un mismo archivo vamos a poder combinar código PHP con código HTML, siguiendo unas reglas. PHP se utiliza para generar páginas web dinámicas. Recordar que llamamos página estática a aquella cuyos contenidos permanecen siempre igual, mientras que llamamos páginas dinámicas a aquellas cuyo contenido no es el mismo siempre. Por ejemplo, los contenidos pueden cambiar en base a los cambios que haya en una base de datos, de búsquedas o aportaciones de los usuarios, etc (PHP, 2020).

#### II.2.2.5.7 Laravel

Laravel es un framework de código abierto para desarrollar aplicaciones y servicios web con PHP 5 y PHP 7. Su filosofía es desarrollar código PHP de forma elegante y simple, evitando el "código espagueti". Fue creado en 2011 y tiene una gran influencia de frameworks como Ruby on Rails, Sinatra y ASP.NET MVC.

Características:

- Sistema de ruteo, también RESTful
- Blade, Motor de plantillas
- Peticiones Fluent
- Eloquent ORM
- Basado en Composer8
- Soporte para el caché
- Soporte para MVC
- Usa componentes de Symfony
- Adopta las especificaciones PSR-212 y PSR-4

(laravel, 2020)

La influencia de Laravel ha crecido rápidamente desde su lanzamiento. En la comunidad de desarrolladores es considerado como alternativa sencilla de usar pero que tiene todas las funcionalidades que debe tener un framework. Ha sido descargado más de 320.000 veces, y se espera que supere en popularidad a otros frameworks ya establecidos más antiguos.

#### II.2.2.6 Sistema de Información Automatizado

##### II.2.2.6.1 Internet

Internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP. Tuvo sus orígenes en 1969, cuando una agencia del Departamento de Defensa de los Estados Unidos comenzó a buscar alternativas ante una eventual guerra atómica que pudiera incomunicar a las personas. Tres años más tarde se realizó la primera demostración pública del sistema ideado, gracias a que tres universidades de California y una de Utah lograron establecer una conexión conocida como ARPANET (Advanced Research Projects Agency Network) (Nebreda , 2013).

##### II.2.2.6.2 Sistema de Información Vía Web

El incremento del ancho de banda disponible en las conexiones a Internet, así como la inclusión de nuevas tecnologías en los navegadores web, han permitido que se abandonen los sistemas de información tradicionales construidos con aplicaciones de escritorio para pasar a sistemas de información basados en aplicaciones web que se ejecutan y visualizan en un servidor web (Nebreda , 2013).

##### II.2.2.6.3 Modelo vista controlador (MVC)

El Modelo Vista Controlador es un patrón de arquitectura de software, que utilizando 3 componentes, separa la lógica de la aplicación de la lógica de la vista, es una arquitectura importante utilizada en sistemas gráficos básicos como en sistemas empresariales.

La lógica del negocio es un conjunto de reglas que se siguen en el software para reaccionar ante distintas situaciones. Cuando un usuario se comunica con el sistema por medio de la interfaz, que

a la vez realiza una serie de operaciones que se conocen como la lógica del negocio, esta lógica tiene normas sobre lo que se puede hacer y lo que no se puede hacer, a esto se conoce también como las reglas del negocio, entonces la lógica del negocio queda al lado de los modelos.

La razón de utilizar este modelo es que permite separar los componentes de nuestra aplicación dependiendo de la responsabilidad que tienen, esto significa que cuando hacemos un cambio en alguna parte de nuestro código, esto afecte otra parte del mismo. Esto respeta el principio de la responsabilidad única. Cuando el usuario manda una petición al navegador este se conecta con el controlador, una vez este que analiza la petición le pide al modelo que obtenga la información solicitada, el modelo se encarga se obtener los datos de la base de datos, lo devuelve al controlador y este se encarga de retornar la vista correspondiente a la petición.

### II.2.3 Plan de desarrollo de software RUP

#### II.2.3.1 Introducción

Este documento provee una visión general del enfoque de desarrollo propuesto. El proyecto fue desarrollado por el universitario KEVIN TAMBO SOSSA, Basado en la metodología de Rational Unified Process (RUP) en la que únicamente se procederá a cumplir con las tres primeras fases, las cuales marcan la metodología. Es importante destacar esto puesto que utilizaremos la terminología RUP en este documento. Se incluirá el detalle para las fases de Inicio, Elaboración y Construcción.

- **Inicio. -** En esta fase se establece los requisitos de negocio que cubrirá el sistema, se obtendrá la especificación de requerimientos. Mediante entrevistas para posteriormente especificar los requerimientos según la norma IEEE 830.
- **Elaboración. -** En esta fase el problema se analiza y comprende desde el punto de vista del equipo de desarrollo. Al final de la fase se tiene definida la arquitectura y el modelo de requisitos del sistema empleando los diagramas de casos de uso especificados en lenguaje UML.
- **Construcción. -** En esta fase se profundiza en el diseño de los componentes del sistema y de manera iterativa se van añadiendo las funcionalidades al software a medida que se construyen y prueban, permitiendo a la vez que se puedan ir incorporando cambios.

Al final de esta fase se obtiene un sistema completamente operativo y la documentación (diagrama de clases, de secuencia, modelo entidad-relación, modelo de dominio, manual de instalación, manual de usuario) para entregar a los usuarios. El enfoque de desarrollo propuesto constituye una configuración del proceso RUP de acuerdo a las características del proyecto, seleccionando los roles de los participantes, las actividades a realizar y los entregables que serán generados. Este documento es a su vez uno de los artefactos de RUP.

El registro de los vehículos y sus custodias en la actualidad son manuales esto genera perdida de información y tiempo al realizar los reportes y consultas respectivas, el presente proyecto contribuirá a mejorar estos procesos permitiendo una administración optima de la gestión de los vehículos, se pretende desarrollar un sistema informático para automatizar la mayoría de los procesos inherentes en la gestión de vehículos y sus custodias

### II.2.3.2 Propósito

El propósito del Plan de Desarrollo de Software es proporcionar la información necesaria para controlar el proyecto. En él que se describe el enfoque de desarrollo del software.

El Plan de Desarrollo del Software se utilizará:

- Para organizar la agenda y necesidades de recursos, y para realizar su seguimiento.
- Para entender lo qué deben hacer, cuándo deben hacerlo y qué otras actividades dependen de ello.
- Elaborar los diagramas de UML de acuerdo a los requerimientos del proyecto.
- Desarrollar el código del proyecto de acuerdo a la documentación del proyecto.
- Llevar una correcta planificación del cronograma del proyecto y el cálculo de métricas.

### II.2.3.3 Alcance

Este documento proporcionará una idea del software a desarrollar exponiendo a la vez su estructura hasta una visión terminada.

El Plan de Desarrollo del Proyecto describe el plan global usado para el desarrollo en el proyecto con nombre “Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual.”. Durante el proceso de desarrollo en el artefacto “Visión” se definen las características del producto a desarrollar, lo cual constituye la base para la planificación de las iteraciones. Para la versión preliminar del Plan de Desarrollo del Software.

#### II.2.3.4 Resumen

Después de esta introducción, el resto del documento está organizado en las siguientes secciones:

- Vista General del Proyecto — proporciona una descripción del propósito, alcance y objetivos del proyecto, estableciendo los artefactos que serán producidos y utilizados durante el proyecto.
- Organización del Proyecto — describe la estructura organizacional del equipo de desarrollo.
- Gestión del Proceso — explica los costos y planificación estimada, define las fases e hitos del proyecto y describe cómo se realizará su seguimiento.
- Planes y Guías de aplicación — proporciona una vista global del proceso de desarrollo de software, incluyendo métodos, herramientas y técnicas que serán utilizadas.

#### II.2.3.5 Vista General de Proyecto

##### II.2.3.5.1 Propósito

El sistema Web contribuirá en el proyecto a poder hacer publicidad sobre el servicio de VPN que ofrecerá el proyecto también informando sobre los peligros presentes al momento de conectarse al internet y sobre todo manejará la creación de usuarios y suscripciones al servicio a los usuarios para poder obtener una conexión más directa y siendo priorizado.

##### II.2.3.5.2 Alcances

- Informar sobre los peligros que podrían ser evitados al usar los servicios de un VPN como así también explicar el servicio mismo e informar sobre las plataformas en las que estamos presentes.

- Manejar la creación de los usuarios dentro del sistema informático permitiendo a los mismo el control respectivo de sus suscripciones y usuarios y contraseñas.
- Permitir el acceso a la aplicación sin la necesidad de un log in
- Nombre del sistema “Fast Tunnel VPN”
- El sistema WEB incluye los siguientes módulos:
    - Modulo Gestión de Usuarios
    - Modulo Gestión de Roles
    - Modulo Gestión de Suscripciones

#### II.2.3.5.3 Limitaciones

- El sistema web no cuenta con un módulo de Contabilidad
- El sistema web para creación de usuarios solo pide la información mínima necesaria
- El sistema web no tendrá reportes de actividad de usuarios por motivos de privacidad
- El sistema web no manejara directamente los pagos en línea usados un motor para ellos

#### II.2.3.5.4 Objetivos

##### II.2.3.5.4.1 Objetivo General

Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual.

##### II.2.3.5.4.2 Objetivo Específicos

- Desarrollar un sistema web para el VPN “Fast Tunnel VPN” para la gestión de usuarios del mismo.
- El desarrollo del sistema con el uso de las siguientes tecnologías:
    - Bootstrap (CSS Framework)
    - Jquery (Biblioteca multiplataforma de JavaScript)
    - PHP (Lenguaje de programación)
    - Laravel (Framework de código abierto para desarrollar con PHP)
    - MariaDB (Gestión de bases de datos derivado de MySQL con licencia GPL.)
- Aplicar la metodología de desarrollo RUP (Proceso Unificado Racional).

- Diseñar una Interfaz fácil de usar, amigable para que el usuario tenga facilidad en la operación de Sistema.
- Proveer de seguridad adicional al acceso del tipo de usuario mediante el tipo de rol correspondiente así protegiendo información que solo puede ser vista por un usuario de alto nivel en este caso un administrador.

### II.2.3.6 Entregables del proyecto

A continuación, se indican y describen cada uno de los artefactos que serán generados y utilizados por el proyecto y que constituyen los entregables. Esta lista constituye la configuración de RUP desde la perspectiva de artefactos, y que proponemos para este proyecto.

Es preciso destacar que de acuerdo a la filosofía de RUP, todos los artefactos son objeto de modificaciones a lo largo del proceso de desarrollo, con lo cual, sólo al término del proceso podríamos tener una versión definitiva y completa de cada uno de ellos. Sin embargo, el resultado de cada iteración y los hitos del proyecto están enfocados a conseguir un cierto grado de completitud y estabilidad de los artefactos. Esto será indicado más adelante cuando se presenten los objetivos de cada iteración.

Los Artefactos (Entregables) Son los siguientes:

- Plan de desarrollo del software.
- Visión.
- Modelos de casos de uso del negocio.
- Modelo de objetos del negocio
- Glosario.
- Modelos de casos de uso.
- Especificación de los Casos de Uso.
- Prototipo Interfaces de Usuario.
- Modelos de análisis y diseño.
- Modelo de Datos.
- Modelo de Implementación.
- Modelo de despliegue.

- Casos de Prueba.
- Manual de usuario e Instalación.
- Material de apoyo al usuario Final.
- Diagrama de Actividades.
- Diagrama de Secuencia.
- Diagrama de componentes
- Producto

#### II.2.3.6.1 Plan de desarrollo de software

El presente documento describe paso a paso los puntos del proyecto según la metodología.

#### II.2.3.6.2 Visión

##### II.2.3.6.2.1 Introducción

Este documento define la visión del producto desde la perspectiva del cliente, especificando las necesidades y características del producto. Constituye una base de acuerdo en cuanto a los requerimientos del sistema.

##### II.2.3.6.2.2 Limitación

Entre las limitantes del producto, señalamos que el sistema no contara con módulos de contabilidad y no se registra más información de la necesaria.

##### II.2.3.6.2.3 Oportunidad del Negocio

El proyecto viene a ofrecer un servicio de seguridad para todas las personas que se conectan al internet y desean hacerlo de la manera más segura posible no solo para ellos mismo que si no también para su familia y para las empresas y sus trabajadores.

### II.2.3.6.2.3.1 Sentencias que define el Proyecto

| | |
|---|---|
| El problema de | La inseguridad presente en el internet sobre nuestra información e identidad. |
| Afecta a | Todas las personas que se conecta al internet para su uso diario y cotidiano. |
| El impacto asociado es | Mejorar la seguridad al momento de conectarse al internet.<br><br>Mejorar la velocidad de conexión en algunos casos bien específicos.<br><br>Desbloquear contenido para los usuarios que están restringidos por regiones |
| Una solución adecuada seria | Conectarse a el internet atreves de un VPN el cual permitirá navegar de una manera mas segura y sin restricciones. |

*Tabla 2 – 2 Sentencias que define el Proyecto*

### II.2.3.6.2.3.2 Sentencia que define la Posición del Proyecto.

| | |
|---|---|
| Para | Internautas |
| Quienes | Interactuaran de manera directa e indirecta con el sistema. |
| El nombre del producto | “Fast Tunnel VPN” |
| Que | Mejorar la conexión al internet.<br><br>Mejorar la seguridad de los internautas al navegar en ella.<br><br>Desbloquear contenido bloqueo en el internet.<br><br>Proteger la información de los internautas. |
| No como | |

| | |
|---|---|
| | La manera en la que se conectamos ahora nos pone en riesgo a muchas cosas ya que no |
| Nuestro producto | Asegura una mejor conexión al internet<br>Desbloquea el contenido que lo estaba regionalmente permitiendo cambiar tu localización<br>Protege tu información y anonimidad |

*Tabla 2 – 3 Sentencias que define el Proyecto*

#### II.2.3.6.2.3.3 Descripción de los participantes en el desarrollo del sistema y usuarios

### II.2.3.6.2.4 Descripción Global del Sistema

#### II.2.3.6.2.4.1 Perspectiva del producto

El producto a desarrollar es un sistema web para el "Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual: Rapid Tunnel VPN" con la intención de agilizar su funcionamiento y brindar información actualizada para lo que se desarrolló el sistema.

El producto contará con las siguientes gestiones:

- Modulo Gestión de Usuarios
- Modulo Gestión de Roles
- Modulo Gestión de Suscripciones

#### II.2.3.6.2.4.2 Resumen de Características

A continuación, se mostrará un listado con los beneficios que obtendrá el cliente a partir del producto:

| **Beneficio del cliente** | **Características que lo apoyan** |
|---|---|
| Gestión de Usuarios del servicio | Sistema permitirá al administrador y a los usuarios el controlar sus suscripciones al servicio VPN como así también su información. |

| | |
|---|---|
| Publicidad del servicio e Información | El sistema web permitirá promocionar el servicio y educar a los posibles usuarios sobre el mismo y sus beneficios |

*Tabla 2 – 4 Resumen de Características*

#### II.2.3.6.2.4.3 Supuestos y Dependencias

Las suposiciones y restricciones están mencionadas en la Matriz de Marco Lógico del proyecto.

### II.2.3.6.3 Glosario

#### II.2.3.6.3.1 Introducción

Este documento recoge términos manejados durante la elaboración del proyecto de desarrollo de un sistema web de gestión, se trata de un diccionario informal de datos y de definiciones de la nomenclatura que se maneja, de tal modo que se crea un estándar para el proyecto.

#### II.2.3.6.3.2 Propósito

Comprender la Es definir con exactitud y sin ambigüedad la tecnología manejada en el proyecto en desarrollo. También sirve como guía de consulta para la aclaración de los puntos conflictivos o poco esclarecedores.

#### II.2.3.6.3.3 Alcance

El alcance del presente entregable se extiende a todo el sistema.

#### II.2.3.6.3.4 Organización del proyecto

El presente documento está organizado por definiciones de términos ordenados en forma ascendente según el alfabeto.

**VPN:** Virtual Private Network.

**UML:** Lenguaje Unificado de Modelos.

**USUARIOS:** Administrador, personas que usaran el servicio.

### II.2.3.6.3.5 Glosario de los Diagramas

| | |
|---|---|
| Actor del Negocio |  |
| Casos de Uso Negocio |  |
| Comunicación |  |
| Relación |  |
| Actor |  |
| Casos de Uso |  |
| Relación de Inclusión |  |
| Relación de Extensión |  |

*Tabla 2 – 5 Glosario de los Diagramas*

### II.2.3.6.4 Modelo de casos de uso del negocio

#### II.2.3.6.4.1 Introducción

Es un modelo de las funciones del negocio vista desde la perspectiva de los actores externos (Agentes de registro, solicitantes finales, otros sistemas etc.) permite situar al sistema en el contexto organizacional haciendo énfasis en los objetivos en este ámbito. Este modelo se representa con un Diagrama de Casos de Uso usando estereotipos específicos para este modelo. La definición del conjunto de procesos del negocio es una tarea crucial, ya que define los límites del proceso de modelado posterior, consideramos los objetivos estratégicos de la organización, teniendo en cuenta que esos objetivos serán descompuestos en un conjunto de sub objetivos más concretos, para la identificación de procesos de negocio. Se presentan los modelos definidos en RUP como modelo del negocio (modelo de casos de uso del negocio y de objetos del negocio).

#### II.2.3.6.4.2 Propósito

- Comprender la Estructura y la Dinámica de los procesos que se realizan entre los usuarios del servicio del VPN "Fast Tunnel VPN" y el VPN.
- Capturar los requerimientos de los usuarios.
- Comprender los problemas de los internautas.

#### II.2.3.6.4.3 Alcance

- Describe el comportamiento de los procesos de negocio.
- Identificar y definir los casos de uso del negocio.

#### II.2.3.6.4.4 Matriz de Roles

| ACTORES | ROLES | FUNCIONES |
|---|---|---|
| Administrador | Administración del servicio | Administrar Usuarios<br>Administrar Roles<br>Administrar Suscripciones |
| Usuario | Usuario del servicio | Gestionar su cuenta<br>Gestionar su suscripción |

*Tabla 2 – 6 Matriz de Roles*

### II.2.3.6.4.5 Diagrama de Caso de Uso General del Negocio

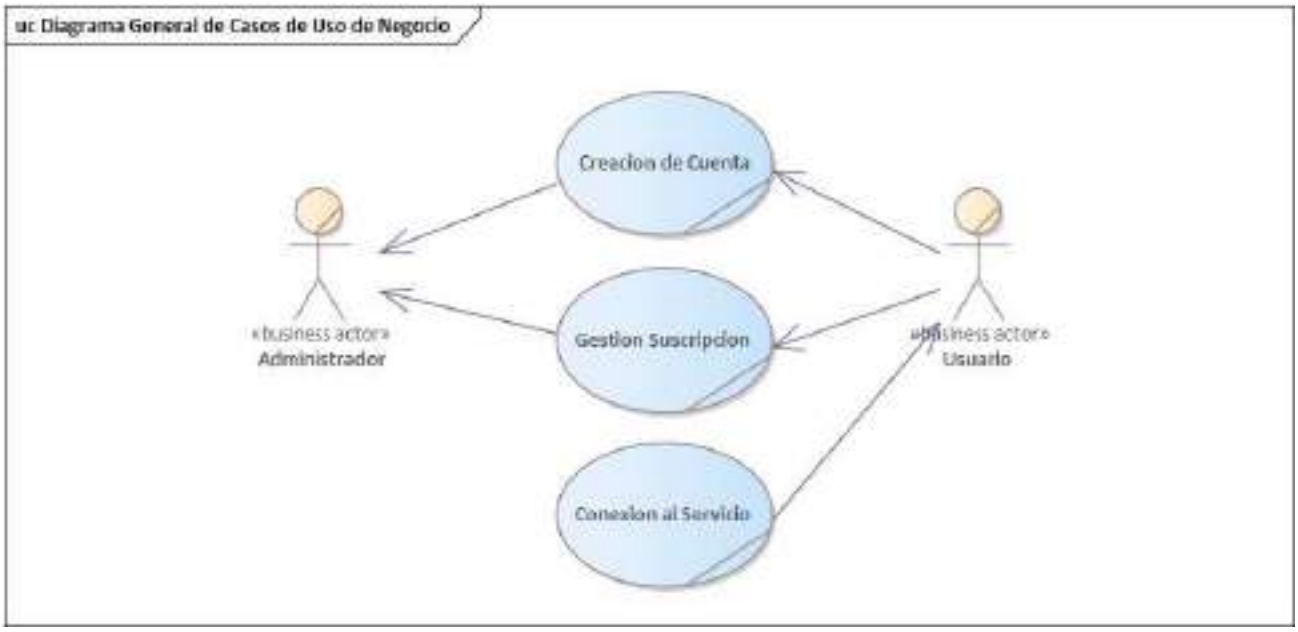


*Figura 2 – 70* Diagrama de Caso de Uso General del Negocio

### II.2.3.6.5 Modelo de casos de uso

#### II.2.3.6.5.1 Introducción

El modelo de Casos de Uso es un modelo del Sistema que contiene actores, casos de uso y sus relaciones, describe lo que hace el sistema para cada tipo de usuario, es decir cada forma en que los actores usan el sistema se representa con un caso de uso, los mismos que son fragmentos de funcionalidad, especifican una secuencia de acciones que el sistema puede llevar a cabo interactuando con sus actores.

#### II.2.3.6.5.2 Propósito

- Comprender la estructura y la dinámica del sistema deseado para la organización
- Identificar posibles mejoras

#### II.2.3.6.5.3 Alcance

- Describe los procesos del sistema.
- Identificar y definir los procesos del sistema según los objetivos de la organización
- Definir un caso de uso para cada proceso del sistema (el diagrama de casos de uso puede mostrar el contexto y los límites del Sistema).

### II.2.3.6.5.4 Actores del Sistema

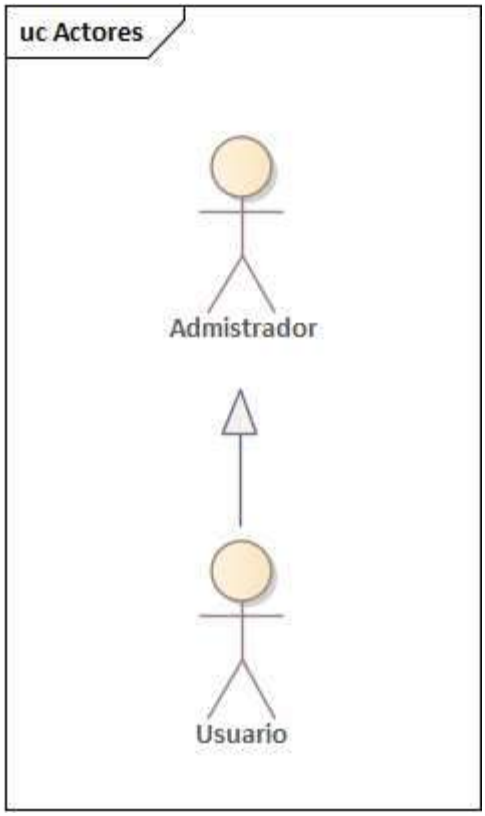


*Figura 2 – 71* Actores del Sistema

### II.2.3.6.5.5 Diagrama de caso de uso General

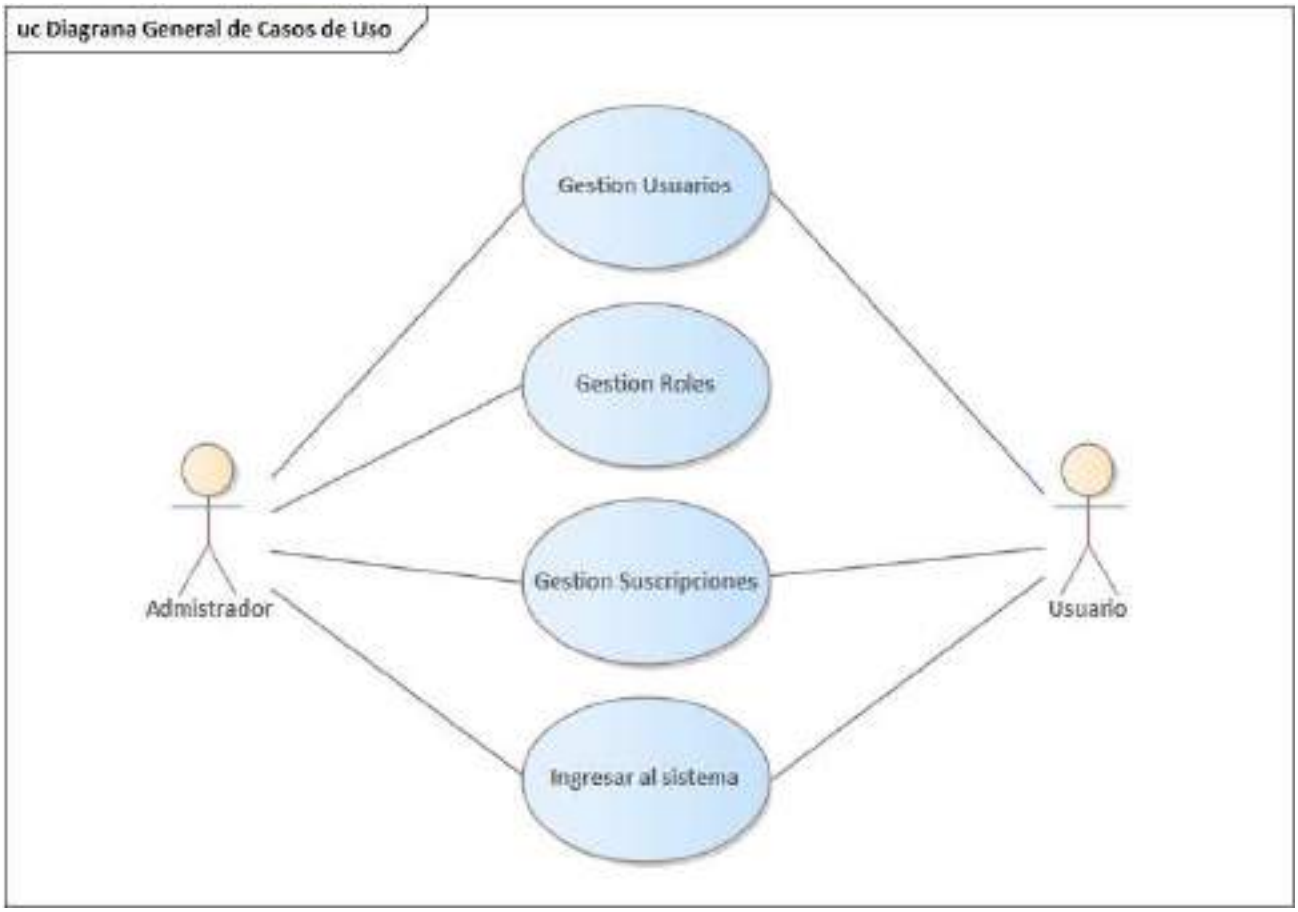


*Figura 2 –72 Diagrama de caso de uso General*

### II.2.3.6.6 Diagramas de Casos de Uso Específicos

#### II.2.3.6.6.1 Diagrama de Caso de Uso: Ingreso al Sistema

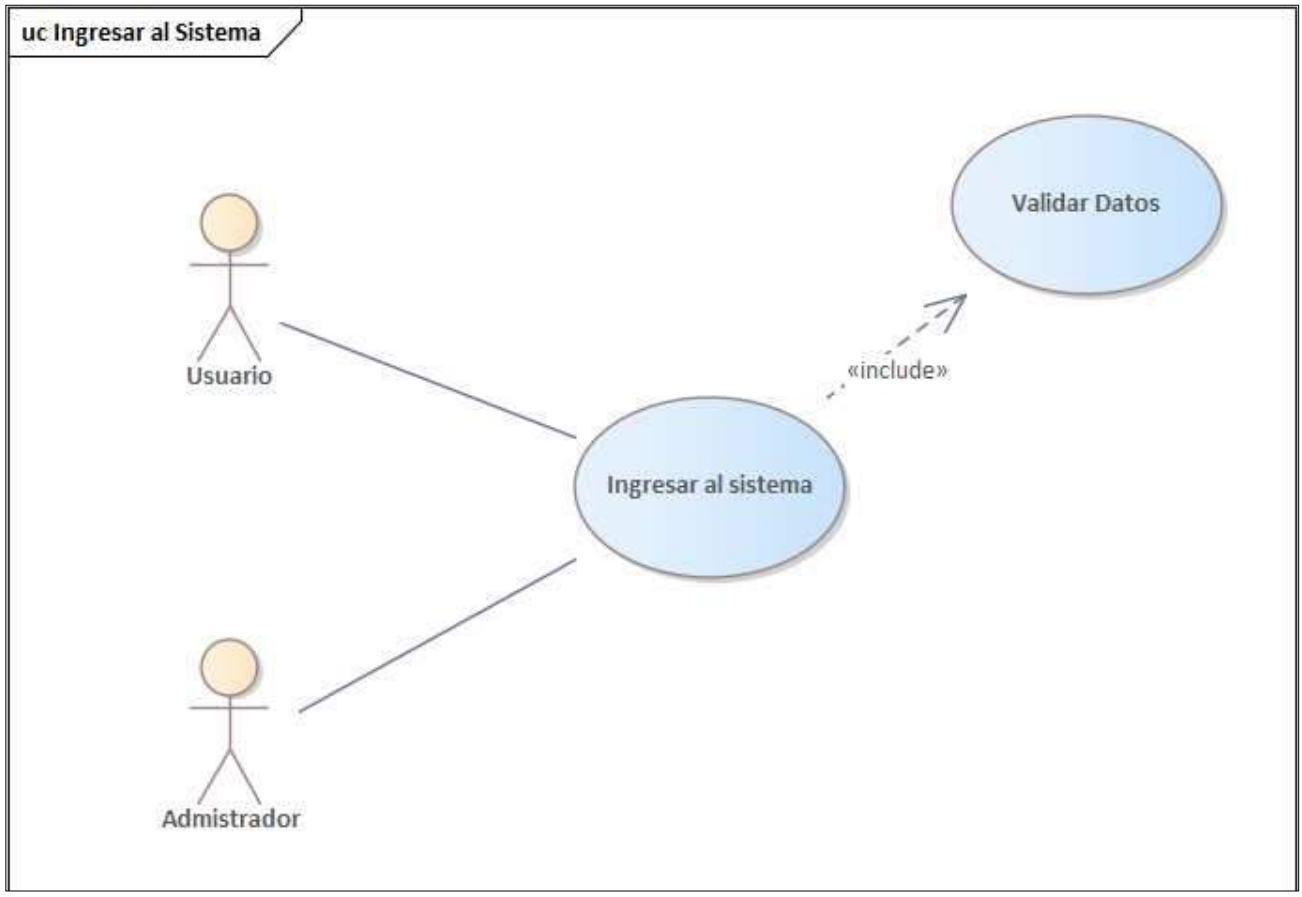


*Figura 2 – 73 Diagrama de Caso de Uso: Ingreso al Sistema*

### II.2.3.6.6.2 Diagrama de Caso de Uso: Gestión Usuarios

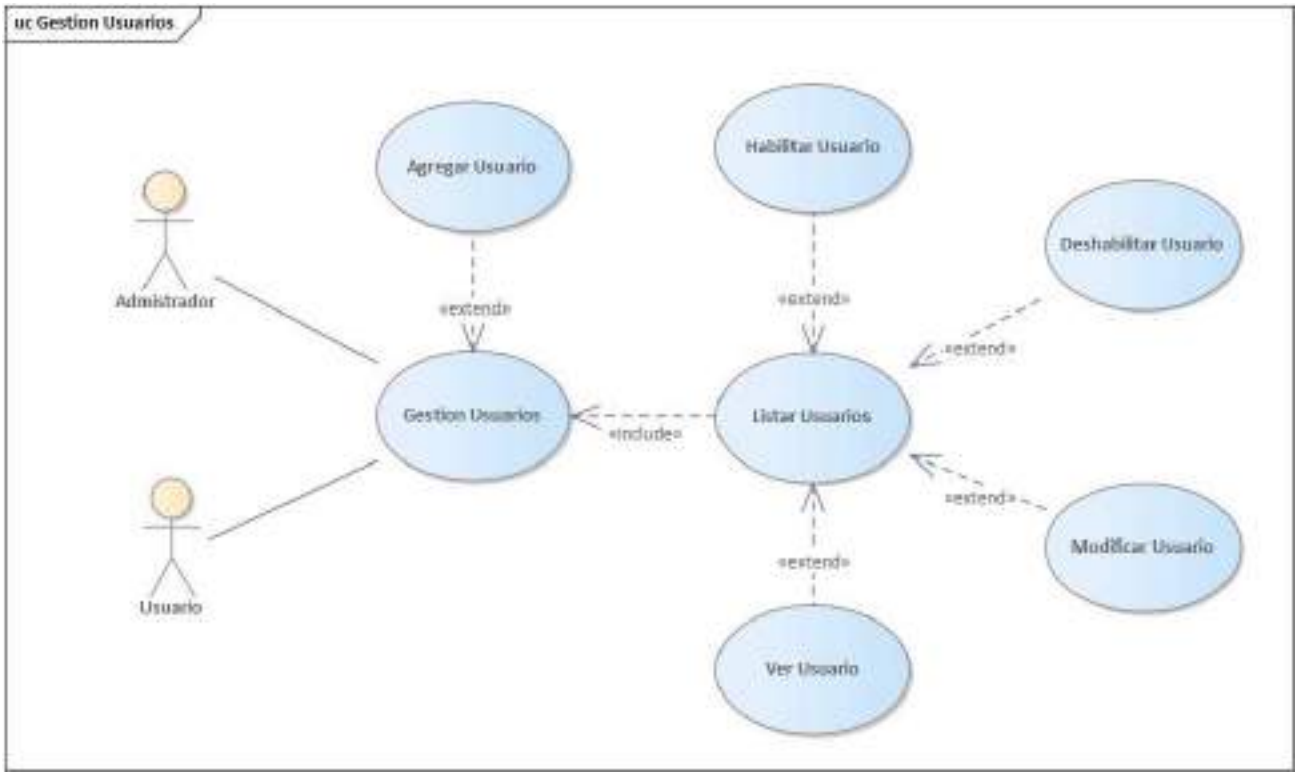


*Figura 2 – 74 Diagrama de Caso de Uso: Gestión Usuarios*

### II.2.3.6.6.3 Diagrama de Caso de Uso: Gestión Roles

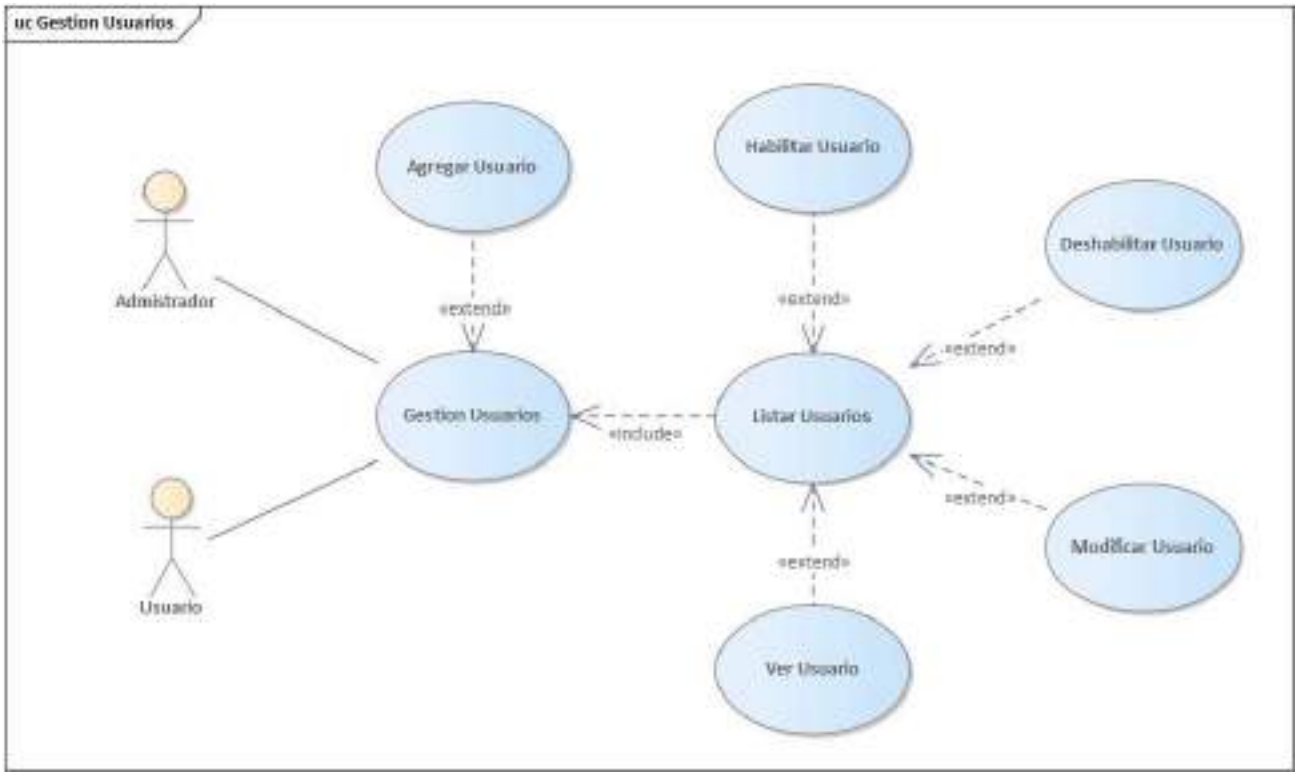


*Figura 2 – 75 Diagrama de Caso de Uso: Gestión Roles*

### II.2.3.6.6.4 Diagrama de Caso de Uso: Gestión Suscripciones

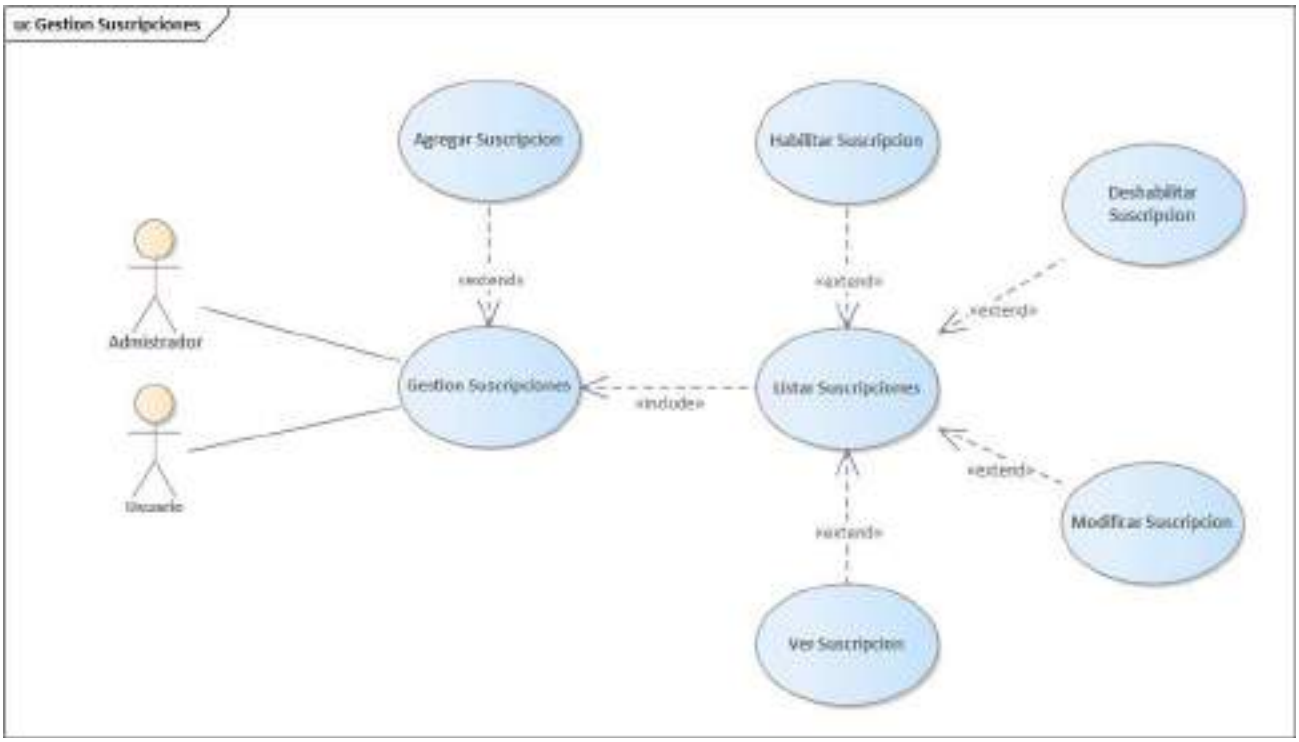


*Figura 2 – 76 Diagrama de Caso de Uso: Gestión Suscripciones*

### II.2.3.6.7 Especificación de casos de uso

#### II.2.3.6.7.1 Introducción

La Especificación de Casos de Uso es una descripción detallada de los casos de uso del sistema

#### II.2.3.6.7.2 Propósito

- Comprender los casos de Uso del Sistema
- Describir específicamente cada caso de uso

#### II.2.3.6.7.3 Alcance

- Describir los procesos internos de los casos de uso
- Describir los flujos de cada caso de uso según lo establecido por la organización.

### II.2.3.6.7.4 Especificación de Casos de Uso General

| | |
|---|---|
| **ACTOR:** | Administrador/usuario |
| **CASO DE USO:** | Ingreso al Sistema<br>Gestión de Roles<br>Gestión de Usuarios<br>Gestión de Suscripciones |
| **TIPO** | Prioritario |
| **DESCRIPCION** | Son las Gestiones totales del sistema |

*Tabla 2 – 7 Especificación de Casos de Uso General*

### II.2.3.6.7.5 Especificación de Casos de Uso: Ingreso al Sistema

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Ingreso al Sistema** |
| **Actores** | Administrador |
| **Tipo** | Básico |
| **Propósito** | Ingresar al sistema web. |
| **Resumen** | El usuario debe introducir sus datos para iniciar una sesión dentro del sistema. |
| **Flujo Principal** | 1 El usuario accede al sistema.<br>2 El sistema desplegara la pantalla (Inicio).<br>3 El usuario selecciona “Ingresar al sistema”.<br>4 El sistema desplegara la pantalla (Ingreso)<br>5 El usuario ingresara los datos de ‘Login’ y ‘Password’.<br>6 El usuario selecciona “Acceder”, los datos se envían al sistema.<br>7 El sistema verifica los datos de inicio de sesión del usuario, si los datos son incorrectos se genera la excepción (E-1), si los datos de usuario son correctos el sistema despliega la pantalla (Menú) |
| **Sub Flujo** | |
| **Excepción** | E-1.- Se mostrará un mensaje de advertencia especificando que campos son los incorrectos. |

*Tabla 2 – 8 Especificación de Casos de Uso: Ingreso al Sistema*

### II.2.3.6.7.6 Especificación de Casos de Uso: Gestión Usuarios

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Ingreso al Sistema** |
| **Actores** | Administrador, Usuario |
| **Tipo** | Básico |
| **Propósito** | Gestionar los Usuarios del sistema, listar, agregar, modificar, eliminar y ver sus datos |
| **Resumen** | Este caso de uso hace referencia a la gestión de los usuarios, permitiendo visualizar una lista completa de los usuarios del sistema dando la posibilidad de agregar, ver, modificar, deshabilitar y habilitar |
| **Precondición** | El administrador y el Usuario se debe haber logeado previamente al sistema. |
| **Flujo Principal** | 1. El usuario selecciona “Usuarios” en la pantalla (Menú).<br>2. El sistema desplegara la pantalla (Gestión usuarios) con una lista de todos usuarios registrados en el sistema, la lista de los usuarios es mostrada en una tabla con filtros y opciones, dependiendo de las opciones seleccionadas por el administrador, se continuará con los diversos sub flujos de este caso de uso. |

| | |
|---|---|
| **Sub Flujo** | El administrador puede seleccionar entre las siguientes opciones:<br>1. Si selecciona la opción “Agregar usuario” se ejecuta el sub flujo adicionar usuario (S-1).<br>2. Si selecciona la opción “Ver” se ejecuta el sub flujo ver usuario (S-2).<br>3. Si selecciona la opción “Modificar” se ejecuta el sub flujo modificar usuario (S-3)<br>4. Si selecciona la opción “Deshabilitar” se ejecuta el sub flujo deshabilitar usuario (S-4).<br>5. Si selecciona la opción “Habilitar” se ejecuta el sub flujo deshabilitar usuario (S-5).<br><br>El usuario puede seleccionar entre las siguientes opciones:<br><br>6. Si selecciona la opción “Modificar” su Usuario se ejecuta el sub flujo modificar usuario (S-1).<br>7. Si selecciona la opción “Ver” se ejecuta el sub flujo ver usuario (S-2). |
| **Excepción** | E-1.- Se mostrará un mensaje de advertencia especificando que campos son los incorrectos. |

*Tabla 2 – 9 Especificación de Casos de Uso: Gestión Usuarios*

### II.2.3.6.7.7 Especificación de Casos de Uso: Listar Usuarios

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Listar Usuarios** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Listar los usuarios del sistema. |
| **Resumen** | Este caso de uso hace referencia a la posibilidad de listar todos usuarios registrados en el sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú “Usuarios” asignado en su rol. |

| | |
|---|---|
| **Flujo Principal** | 1. El usuario selecciona “Usuarios” en la pantalla (Menú).<br>2. El sistema desplegara la pantalla (Gestión usuarios) con una lista de todos los usuarios registrados en el sistema, la lista de usuarios es mostrada en una tabla con filtros y opciones. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 10 Especificación de Casos de Uso: Listar Usuarios*

### II.2.3.6.7.8 Especificación de Casos de Uso: Agregar Usuario

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Agregar Usuario** |
| **Actores** | Administrador, Usuario |
| **Tipo** | Extensión |
| **Propósito** | Añadir nuevos usuarios al sistema. |
| **Resumen** | Permite el registro de un nuevo usuario al sistema |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú “Usuarios” asignado en su rol.<br>3. Debe haber escogido la opción “Agregar usuario” de la tabla de datos de usuarios en la pantalla (Gestión usuarios). |

| | |
|---|---|
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario (Agregar usuario)<br>2. El administrador deberá llenar los siguientes campos:<br>2.1. '**Imagen o foto del usuario**' que es requerido, este campo hace referencia a la imagen del usuario en el sistema más conocida como avatar.<br>2.3. '**Que rol tendrá el usuario en el sistema'** este campo es requerido y hace referencia al rol que el usuario tendrá en el sistema.<br>2.4. **'Nombre'** este campo es requerido y hace referencia al nombre de usuario.<br>2.5. **'Apellidos'** este campo es requerido y hace referencia a los apellidos paterno y materno del usuario.<br>2.8. **'Login'** este campo es requerido y hace referencia al login que el usuario deberá utilizar para ingresar al sistema.<br>2.9. **'Password'** este campo es requerido y hace referencia al password o clave que el usuario requiere para el ingreso al sistema.<br>3. El administrador tiene dos opciones:<br>3.1. "Guardar" con la cual se enviarán los datos al sistema para ser verificados, si los datos son incorrectos se genera la excepción (E-1), si el 'ci' ya se encuentra registrado genera la excepción (E-2), si el 'login' ya se encuentra registrado se genera la excepción (E-3), si los datos son correctos se procede a registrar el nuevo usuario en el sistema, posterior mente el sistema despliega la pantalla (Gestión usuarios) con un mensaje de éxito.<br>3.2. "Cancelar" con la cual los datos no se envían y el sistema despliega la pantalla (Gestión usuarios)<br>4. El Usuario deberá llenar los siguientes campos:<br>2.1. '**Imagen o foto del usuario**' que es requerido, este campo hace referencia a la imagen del usuario en el sistema más conocida como avatar.<br>2.4. **'Nombre'** este campo es requerido y hace referencia al nombre de usuario.<br>2.5. **'Apellidos'** este campo es requerido y hace referencia a los apellidos paterno y materno del usuario.<br>2.8. **'Login'** este campo es requerido y hace referencia al login que el usuario deberá utilizar para ingresar al sistema.<br>2.9. **'Password'** este campo es requerido y hace referencia al password o clave que el usuario requiere para el ingreso al sistema. |

| | |
|---|---|
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 11 Especificación de Casos de Uso: Agregar Usuario*

### II.2.3.6.7.9 Especificación de Casos de Uso: Modificar Usuario

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Modificar Usuario** |
| **Actores** | Administrador, Usuario |
| **Tipo** | Extensión |
| **Propósito** | Modificar datos de un usuario del sistema |
| **Resumen** | Permite modificar el registro de un usuario en el sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú “Usuarios” asignado en su rol.<br>3. Debe haber escogido la opción “Modificar” escogiendo en específico el usuario a modificar de la tabla de datos de los usuarios en la pantalla (Gestión usuarios). |

| | |
|---|---|
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario (Modificar usuario).<br>2. El administrador podrá modificar los siguientes campos:<br>2.1. 'Imagen o foto del usuario' que es requerido, este campo hace referencia a la imagen del usuario en el sistema más conocida como avatar.<br>2.2. 'Que rol tendrá el usuario en el sistema' este campo es requerido y hace referencia al rol que el usuario tendrá en el sistema.<br>2.3. 'Nombre' este campo es requerido y hace referencia al nombre de usuario.<br>2.4. 'Apellidos' este campo es requerido y hace referencia a los apellidos paterno y materno del usuario.<br>2.5. 'Password' este campo es requerido y hace referencia al password o clave que el usuario requiere para el ingreso al sistema.<br>3. El administrador tiene dos opciones:<br>3.1. "Modificar" con la cual se enviarán los datos al sistema para ser verificados, si los datos son incorrectos se genera la excepción (E-1), si los datos son correctos se procede a modificar el registro del usuario en el sistema, posteriormente el sistema despliega la pantalla (Gestión usuarios) con un mensaje de éxito.<br>3.2. "Cancelar" con la cual los datos no se envían y el sistema despliega la pantalla (Gestión usuarios).<br>4. El Usuario podrá modificar los siguientes campos sobre su Usuario:<br>4.1. 'Imagen o foto del usuario' que es requerido, este campo hace referencia a la imagen del usuario en el sistema más conocida como avatar.<br>4.2. 'Nombre' este campo es requerido y hace referencia al nombre de usuario.<br>4.3. 'Apellidos' este campo es requerido y hace referencia a los apellidos paterno y materno del usuario.<br>4.4. 'Password' este campo es requerido y hace referencia al password o clave que el usuario requiere para el ingreso al sistema. |
| **Sub Flujo** | Ninguno |
| **Excepción** | E-1.- Se mostrará un mensaje de advertencia especificando que campos son los incorrectos. |

*Tabla 2 – 12 Especificación de Casos de Uso: Modificar Usuario*

### II.2.3.6.7.10 Especificación de Casos de Uso: Ver Usuario

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Ver Usuario** |
| **Actores** | Administrador, Usuario |
| **Tipo** | Extensión |
| **Propósito** | Ver datos de un usuario del sistema. |
| **Resumen** | Permite ver datos del registro de un usuario del sistema. |
| **Precondicion** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Usuarios" asignado en su rol.<br>3. Debe haber escogido la opción "Ver" escogiendo en específico el usuario que desea ver de la tabla de datos de usuarios en la pantalla (Gestión usuarios). |
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario (Modificar usuario).<br>2. Los Actores podrá modificar los siguientes campos:<br>2.1. 'Imagen o foto del usuario' que es requerido, este campo hace referencia a la imagen del usuario en el sistema más conocida como avatar.<br>2.2. 'Que rol tendrá el usuario en el sistema' este campo es requerido y hace referencia al rol que el usuario tendrá en el sistema.<br>2.3. 'Nombre' este campo es requerido y hace referencia al nombre de usuario.<br>2.4. 'Apellidos' este campo es requerido y hace referencia a los apellidos paterno y materno del usuario.<br>2.5. 'Password' este campo es requerido y hace referencia al password o clave que el usuario requiere para el ingreso al sistema.<br>3. Los Actores tiene la opción de seleccionar "Cancelar" con la cual y el sistema despliega la pantalla (Gestión usuarios) |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 13 Especificación de Casos de Uso: Ver Usuario*

### II.2.3.6.7.11 Especificación de Casos de Uso: Deshabilitar Usuario

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Deshabilitar Usuario** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Deshabilitar un usuario del sistema. |
| **Resumen** | Permite deshabilitar un usuario del sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Usuarios" asignado en su rol.<br>3. Debe haber escogido la opción "Deshabilitar" escogiendo en específico el usuario que desea deshabilitar de la tabla de datos de usuarios en la pantalla (Gestión usuarios). |
| **Flujo Principal** | 1. El sistema deshabilitara el usuario del sistema.<br>2. El sistema despliega la pantalla (Gestión usuarios) con un mensaje de que el usuario fue deshabilitado con éxito. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 14 Especificación de Casos de Uso: Deshabilitar Usuario*

### II.2.3.6.7.12 Especificación de Casos de Uso: Habilitar Usuario

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Habilitar Usuario** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Habilitar un usuario del sistema. |
| **Resumen** | Permite habilitar un usuario del sistema. |

| | |
|---|---|
| **Precondición** | 4. El administrador se debe haber logeado previamente al sistema.<br>5. Tener el menú "Usuarios" asignado en su rol.<br>6. Debe haber escogido la opción "Habilitar" escogiendo en específico el usuario que desea deshabilitar de la tabla de datos de usuarios en la pantalla (Gestión usuarios). |
| **Flujo Principal** | 3. El sistema deshabilitara el usuario del sistema.<br>4. El sistema despliega la pantalla (Gestión usuarios) con un mensaje de que el usuario fue deshabilitado con éxito. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 15 Especificación de Casos de Uso: Habilitar Usuario*

#### II.2.3.6.7.13 Especificación de Casos de Uso: Gestión Roles

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Gestión de Roles** |
| **Actores** | Administrador |
| **Tipo** | Básico |
| **Propósito** | Gestionar los **Roles** del sistema, listar, agregar, modificar, funciones, eliminar y ver sus datos |
| **Resumen** | Este caso de uso hace referencia a la gestión de los roles, permitiendo visualizar una lista completa de los roles del sistema dando la posibilidad de agregar, ver, modificar, modificar sus funciones, deshabilitar y habilitar |
| **Precondición** | El administrador se debe haber logeado previamente al sistema. |

| | |
|---|---|
| **Flujo Principal** | 1. El usuario selecciona “Roles” en la pantalla (Menú).<br>2. El sistema desplegara la pantalla (Gestión roles) con una lista de todos roles registrados en el sistema, la lista de los roles es mostrada en una tabla con filtros y opciones, dependiendo de las opciones seleccionadas por el administrador, se continuará con los diversos sub flujos de este caso de uso. |
| **Sub flujos** | El administrador puede seleccionar entre las siguientes opciones:<br>1. Si selecciona la opción “Agregar rol” se ejecuta el sub flujo adicionar rol (S-1).<br>2. Si selecciona la opción “Funciones” se ejecuta el sub flujo modificar funciones del rol (S-2).<br>3. Si selecciona la opción “Ver” se ejecuta el sub flujo ver rol (S-3).<br>4. Si selecciona la opción “Modificar” se ejecuta el sub flujo modificar rol (S-4).<br>5. Si selecciona la opción “Deshabilitar” se ejecuta el sub flujo deshabilitar rol (S-5).<br>6. Si selecciona la opción “Habilitar” se ejecuta el sub flujo deshabilitar rol (S-6). |
| **Sub flujos** | Ninguno. |

*Tabla 2 – 16 Especificación de Casos de Uso: Gestión Roles*

#### II.2.3.6.7.14 Especificación de Casos de Uso: Listar Roles

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Listar Roles** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Listar los roles del sistema. |
| **Resumen** | Este caso de uso hace referencia a la posibilidad de listar todos roles registrados en el sistema. |

| | |
|---|---|
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú “Roles” asignado en su rol. |
| **Flujo Principal** | 1. El usuario selecciona “Roles” en la pantalla (Menú).<br>2. El sistema desplegara la pantalla (Gestión roles) con una lista de todos los roles registrados en el sistema, la lista de roles es mostrada en una tabla con filtros y opciones |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 16 Especificación de Casos de Uso: Listar Roles*

#### II.2.3.6.7.15 Especificación de Casos de Uso: Agregar Rol

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Agregar Rol** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Añadir nuevos roles para usuarios al sistema. |
| **Resumen** | Permite el registro de un nuevo rol para usuarios del sistema |
| **Precondición** | Permite el registro de un nuevo rol para usuarios del sistema<br><br>1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú “Roles” asignado en su rol.<br>3. Debe haber escogido la opción “Agregar rol” de la tabla de datos de roles en la pantalla (Gestión roles). |

| | |
|---|---|
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario (Agregar rol)<br>2. El administrador deberá llenar los siguientes campos:<br>2.1. '**Nombre**' que es requerido, este campo hace referencia al nombre del rol.<br>2.2. '**Descripción**' este campo no es requerido y hace referencia a una pequeña descripción del rol que se quiere agregar.<br>3. El administrador tiene dos opciones:<br>3.1. "Guardar" con la cual se enviarán los datos al sistema para ser verificados, si los datos son incorrectos se genera la excepción (E-1), si los datos son correctos se procede a registrar el nuevo rol en el sistema, posterior mente el sistema despliega la pantalla (Gestión roles) con un mensaje de éxito.<br>3.2. "Cancelar" con la cual los datos no se envían y el sistema despliega la pantalla (Gestión roles) |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 18 Especificación de Casos de Uso: Agregar Roles*

### II.2.3.6.7.16 Especificación de Casos de Uso: Modificar Rol

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Modificar Rol** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Modificar datos de un rol del sistema |
| **Resumen** | Permite el cambio de un registro de un rol del sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Roles" asignado en su rol.<br>3. Debe haber escogido la opción "Modificar" escogiendo en específico el rol a modificar de la tabla de datos de los roles en la pantalla (Gestión roles). |

| | |
|---|---|
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario (Modificar rol)<br>2. El administrador podrá modificar los siguientes campos:<br>2.1. '**Descripción**' este campo no es requerido y hace referencia a una pequeña descripción del rol que se quiere agregar.<br>3. El administrador tiene dos opciones:<br>3.1. "Modificar" con la cual se enviarán los datos al sistema para ser verificados, si los datos son incorrectos se genera la excepción (E-1), si los datos son correctos se procede a modificar el registro del rol en el sistema, posteriormente el sistema despliega la pantalla (Gestión roles) con un mensaje de éxito.<br>3.2. "Cancelar" con la cual los datos no se envían y el sistema despliega la pantalla (Gestión roles) |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 19 Especificación de Casos de Uso: Modificar Roles*

### II.2.3.6.7.17 Especificación de Casos de Uso: Ver Rol

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Ver Rol** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Ver datos de un rol del sistema. |
| **Resumen** | Permite ver datos del registro de un rol del sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Roles" asignado en su rol.<br>3. Debe haber escogido la opción "Ver" escogiendo en específico el rol que desea ver de la tabla de datos de roles en la pantalla (Gestión roles). |

| | |
|---|---|
| **Flujo Principal** | 1. El sistema despliega la pantalla con formulario de solo lectura (Ver unidad)<br>2. El administrador podrá visualizar los siguientes campos:<br>2.1. '**Nombre'**, este campo hace referencia al nombre del rol.<br>2.2. '**Descripción**', este campo hace referencia a una pequeña descripción del rol.<br>3. El administrador tiene la opción de seleccionar "Cancelar" con la cual y el sistema despliega la pantalla (Gestión roles) |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 20 Especificación de Casos de Uso: Ver Roles*

#### II.2.3.6.7.18 Especificación de Casos de Uso: Deshabilitar Rol

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Deshabilitar Rol** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Deshabilitar un rol del sistema. |
| **Resumen** | Permite deshabilitar un rol del sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Roles" asignado en su rol.<br>3. Debe haber escogido la opción "Deshabilitar" escogiendo en específico el rol que desea deshabilitar de la tabla de datos de roles en la pantalla (Gestión roles). |
| **Flujo Principal** | 1. El sistema deshabilitara el rol del sistema.<br>2. El sistema despliega la pantalla (Gestión roles) con un mensaje de que el rol fue deshabilitado con éxito. |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 21 Especificación de Casos de Uso: Deshabilitar Roles*

### II.2.3.6.7.19 Especificación de Casos de Uso: Habilitar Rol

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Habilitar Rol** |
| **Actores** | Administrador |
| **Tipo** | Extensión |
| **Propósito** | Habilitar un rol del sistema. |
| **Resumen** | Permite habilitar un rol del sistema. |
| **Precondición** | 1. El administrador se debe haber logeado previamente al sistema.<br>2. Tener el menú "Roles" asignado en su rol.<br>3. Debe haber escogido la opción "Habilitar" escogiendo en específico el rol que desea habilitar de la tabla de datos de roles en la pantalla (Gestión roles). |
| **Flujo Principal** | 1. El sistema habilitara el rol en el sistema.<br>2. El sistema despliega la pantalla (Gestión roles) con un mensaje de que el rol fue habilitado con éxito. |
| **Sub flujos** | Ninguno. |
| **Excepción** | Ninguno. |

*Tabla 2 – 22 Especificación de Casos de Uso: Habilitar Roles*

### II.2.3.6.7.20 Especificación de Casos de Uso: Gestión Suscripciones

### II.2.3.6.8 Diagramas de actividades

#### II.2.3.6.8.1 Introducción

En un diagrama de actividades muestra la iteración de un conjunto de objetos en una aplicación a través del tiempo, nos permite mostrar el flujo de los datos que pasan de una acción a otra, en estos diagramas no se muestra ni se describe la estructura de los datos

#### II.2.3.6.8.2 Propósito

Comprende la estructura y la dinámica del sistema deseado para la organización.

### II.2.3.6.8.3 Alcance

- Describe los procesos del sistema
- Identificar y definir los procesos del sistema según los objetivos de la organización.
- Definir un diagrama de actividades para cada proceso del sistema.

### II.2.3.6.8.4 Diagrama de Actividades: Ingreso al sistema

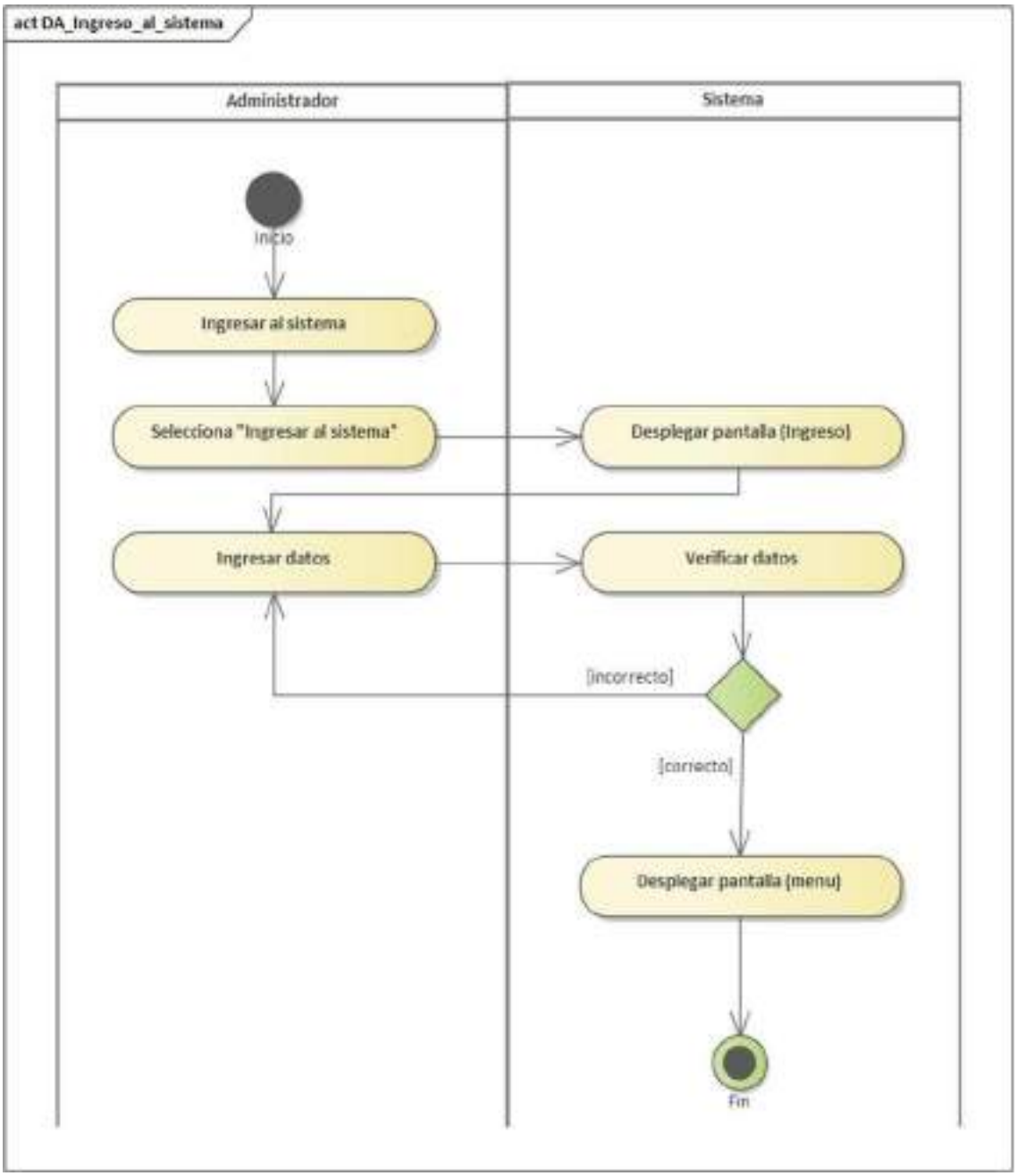


*Figura 2 – 77 Diagrama de Actividades: Ingreso al sistema*

### II.2.3.6.8.5 Diagrama de Actividades: Modificar Perfil

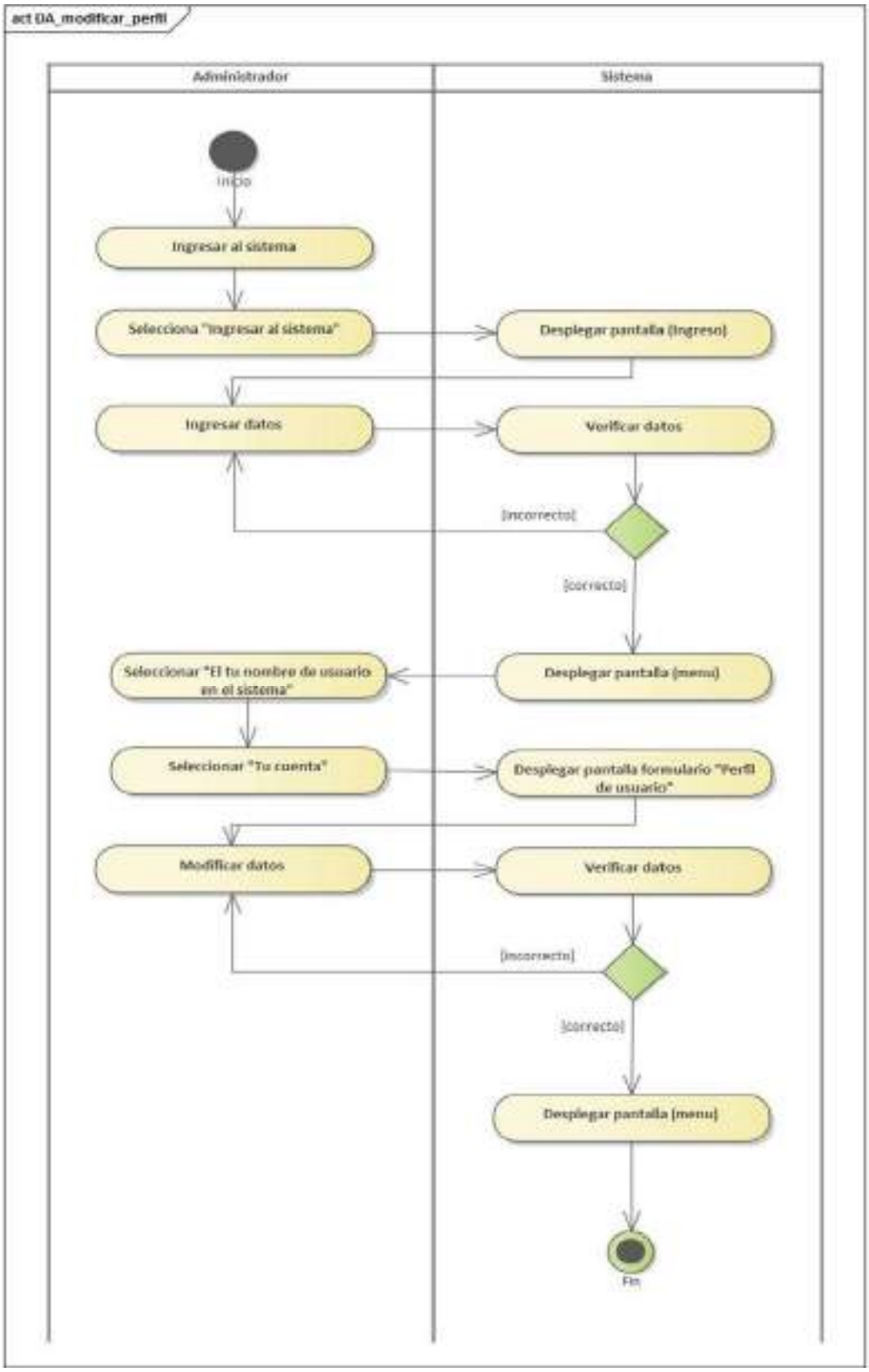


*Figura 2 – 78 Diagrama de Actividades: Modificar Perfil*

### II.2.3.6.8.6 Diagrama de Actividades: Gestión de Roles

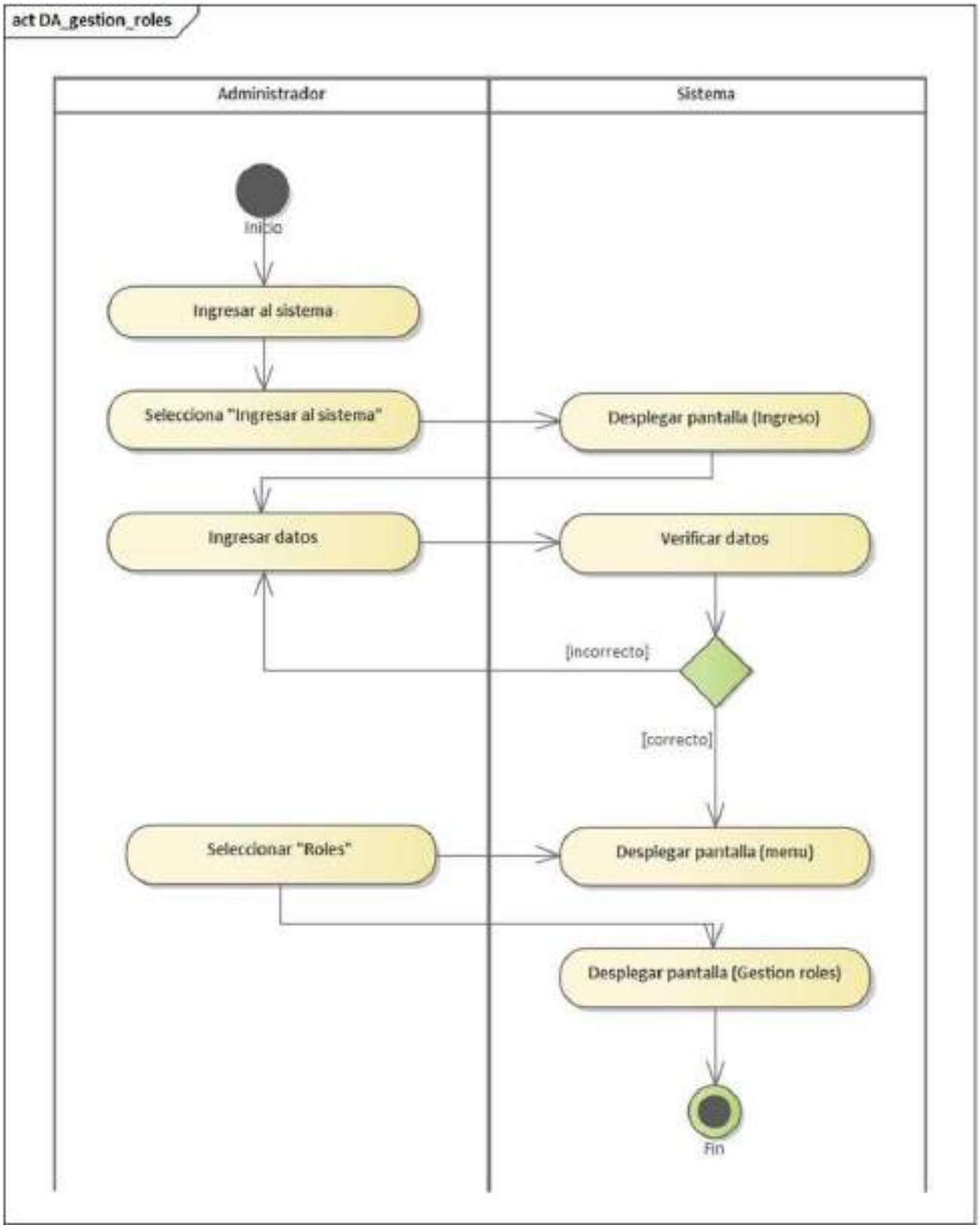


*Figura 2 – 79 Diagrama de Actividades: Gestión de Roles*

### II.2.3.6.8.7 Diagrama de Acti75idades: Listar Roles

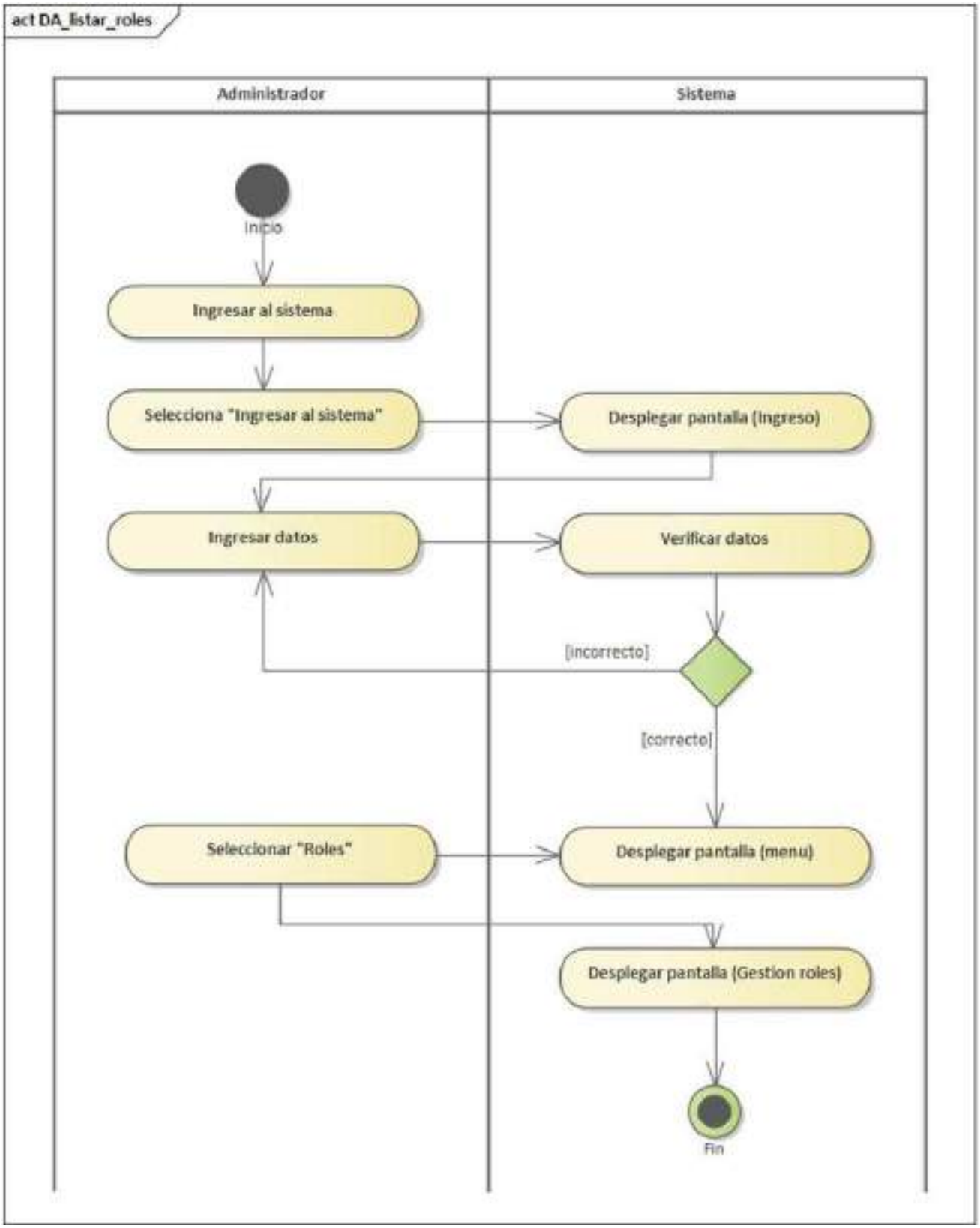


*Figura 2 – 80 Diagrama de Actividades: Listar Roles*

### II.2.3.6.8.8 Diagrama de Actividades: Agregar Rol

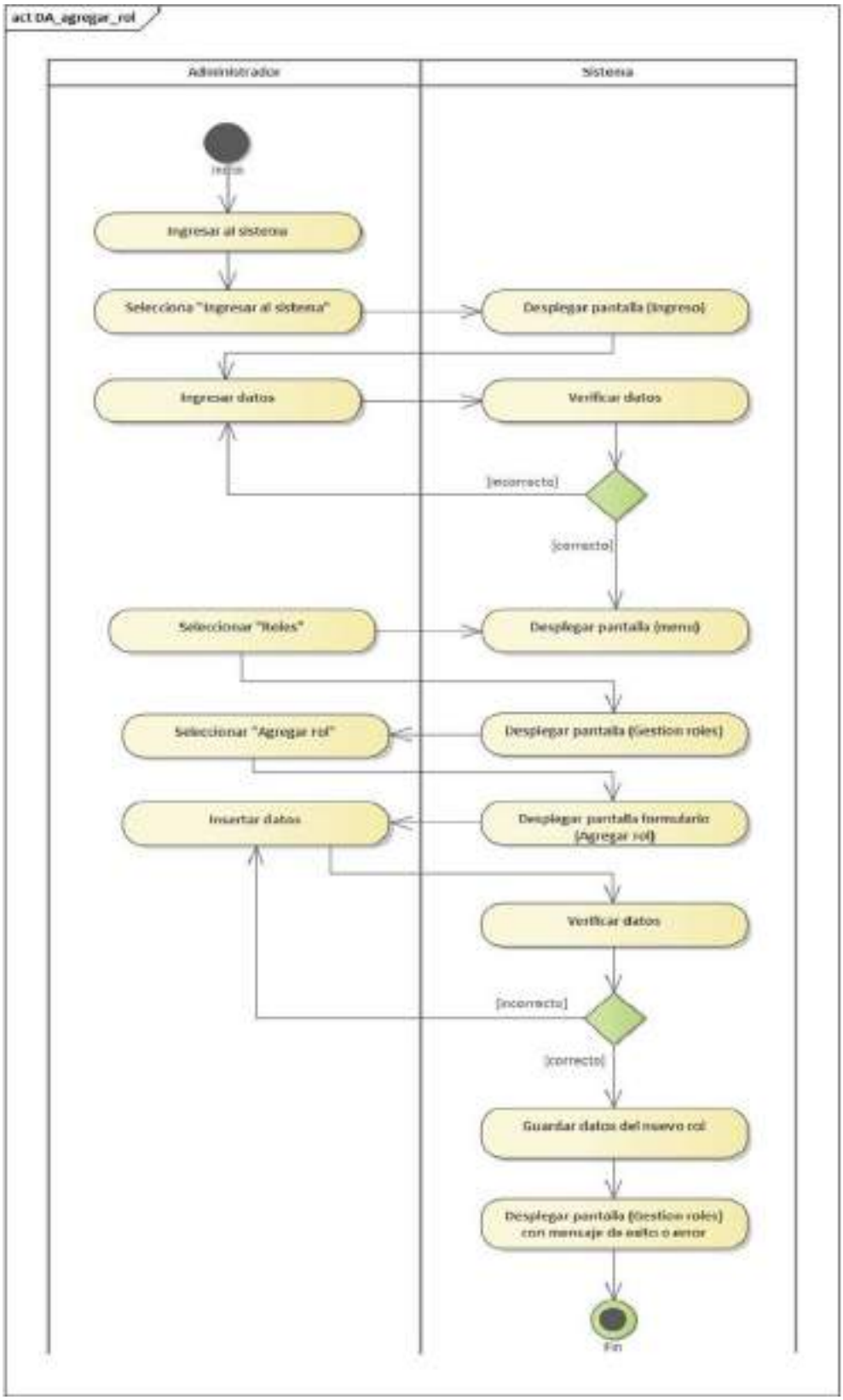


*Figura 2 – 81 Diagrama de Actividades: Agregar Rol*

### II.2.3.6.8.9 Diagrama de Actividades: Modificar Rol

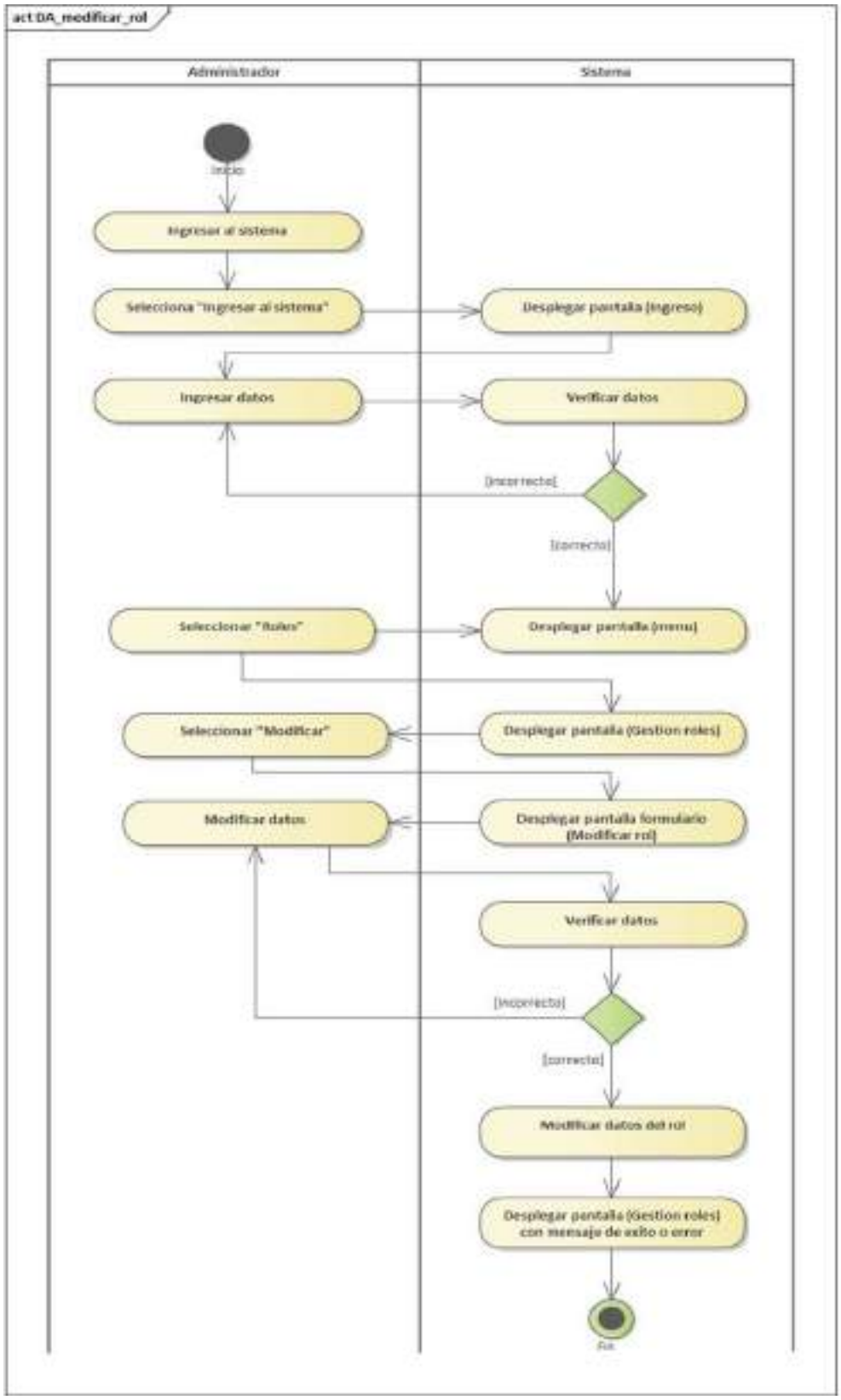


*Figura 2 – 82 Diagrama de Actividades: Modificar Rol*

### II.2.3.6.8.10 Diagrama de Actividades: Ver Rol

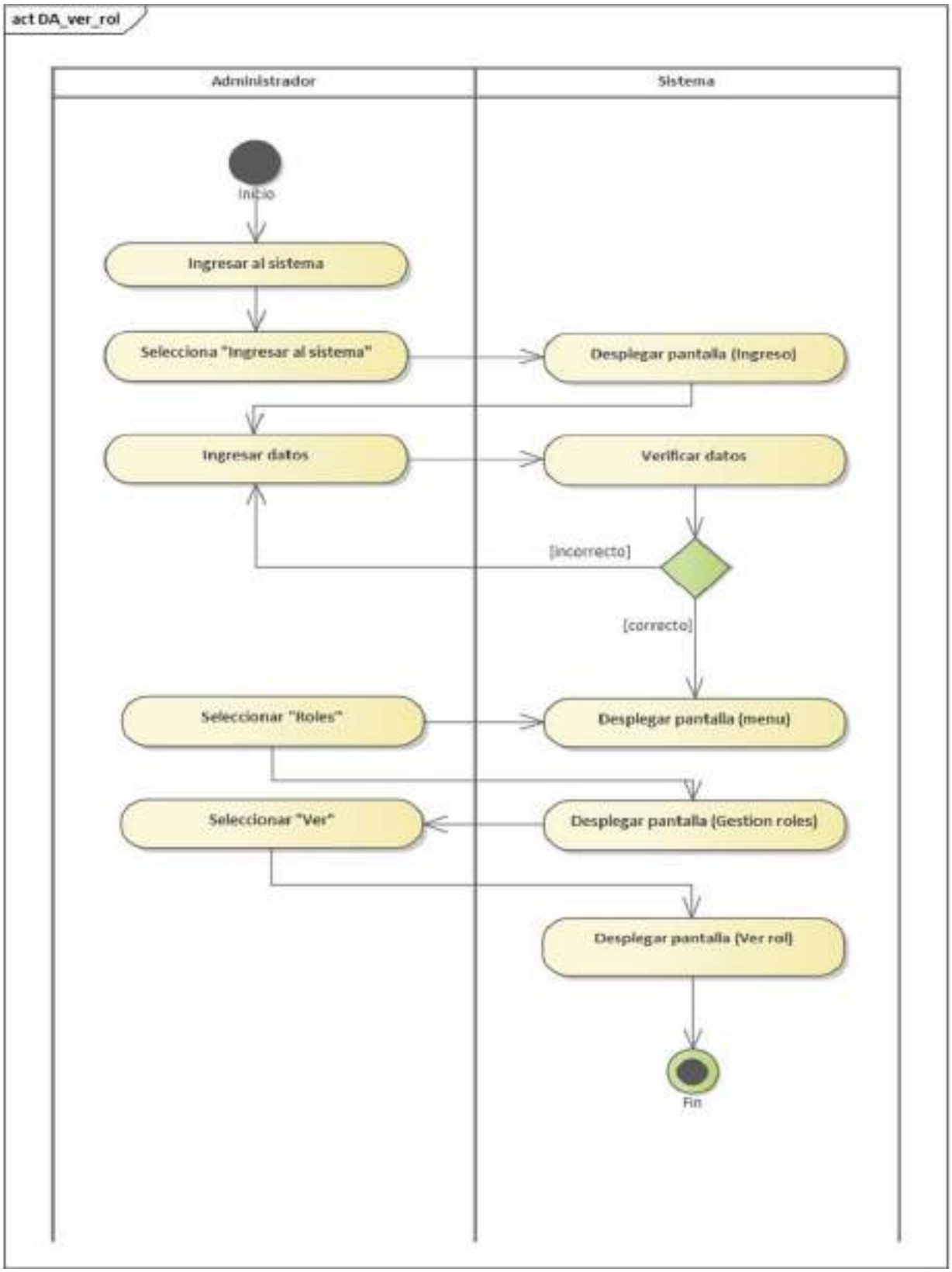


*Figura 2 – 83 Diagrama de Actividades: Ver Rol*

### II.2.3.6.8.11 Diagrama de Actividades: Deshabilitar Rol

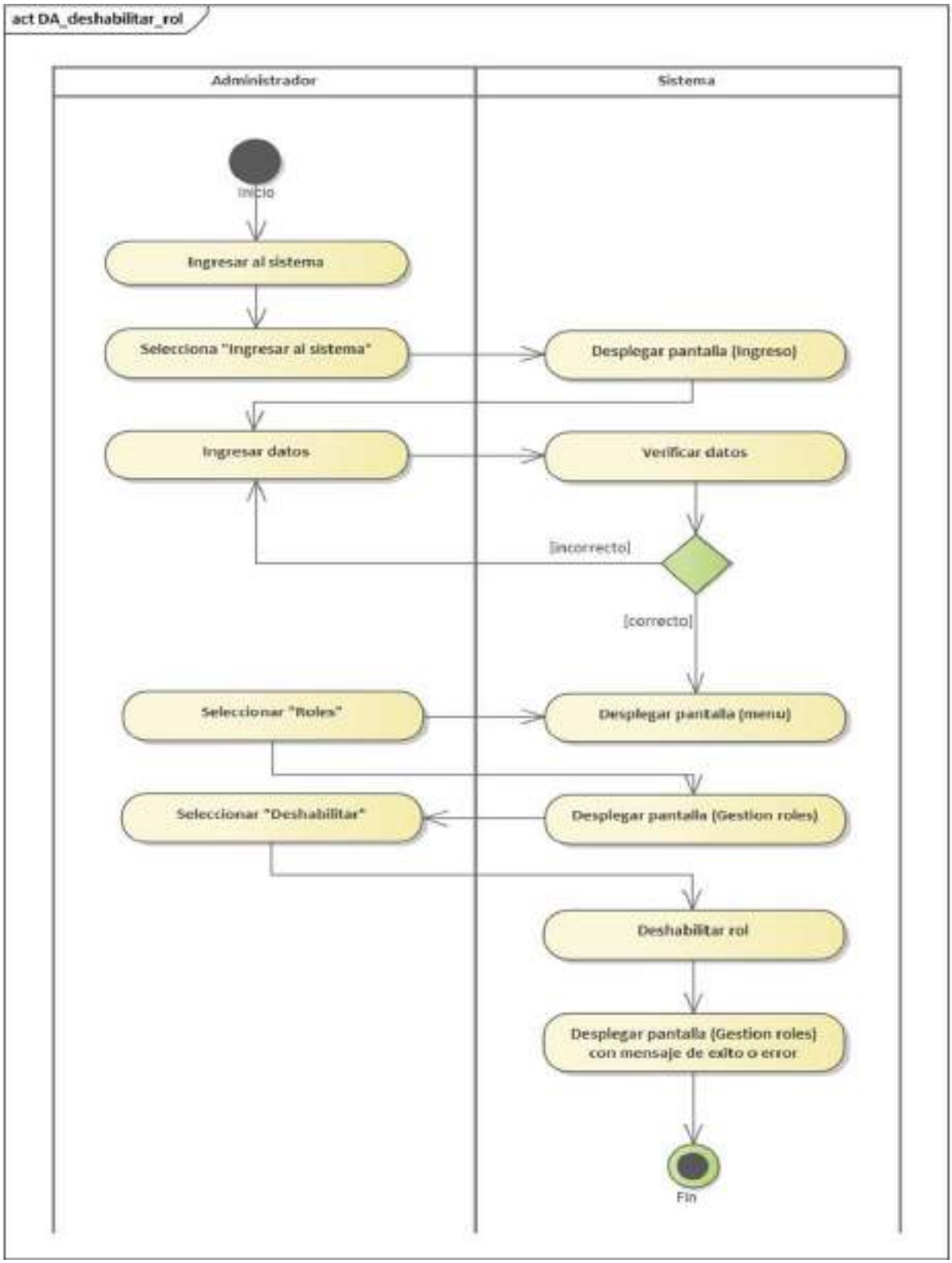


*Figura 2 – 84 Diagrama de Actividades: Deshabilitar Rol*

### II.2.3.6.8.12 Diagrama de Actividades: Habilitar Rol

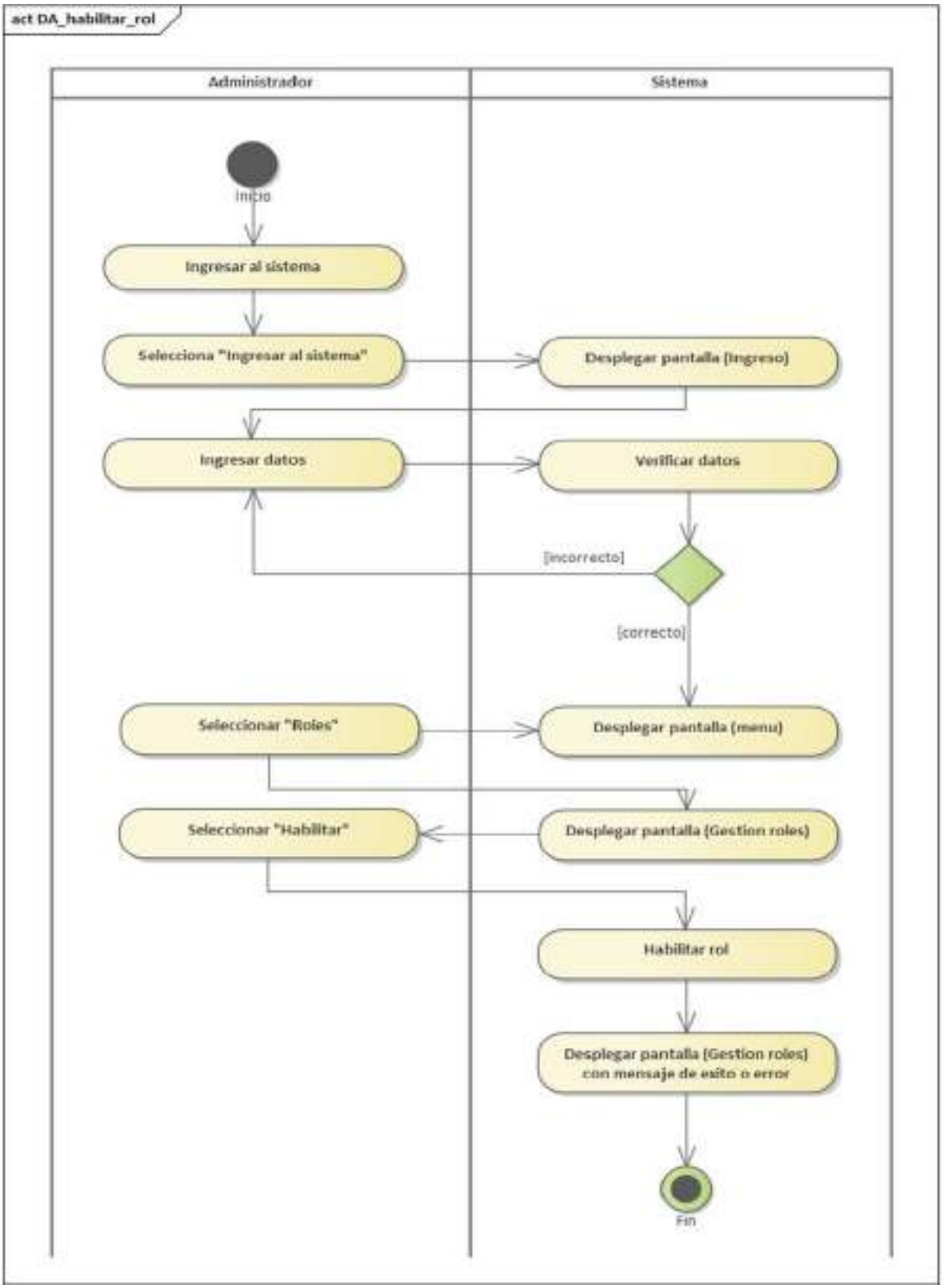


*Figura 2 – 85 Diagrama de Actividades: Habilitar Rol*

### II.2.3.6.8.13 Diagrama de Actividades: Gestión de Usuarios

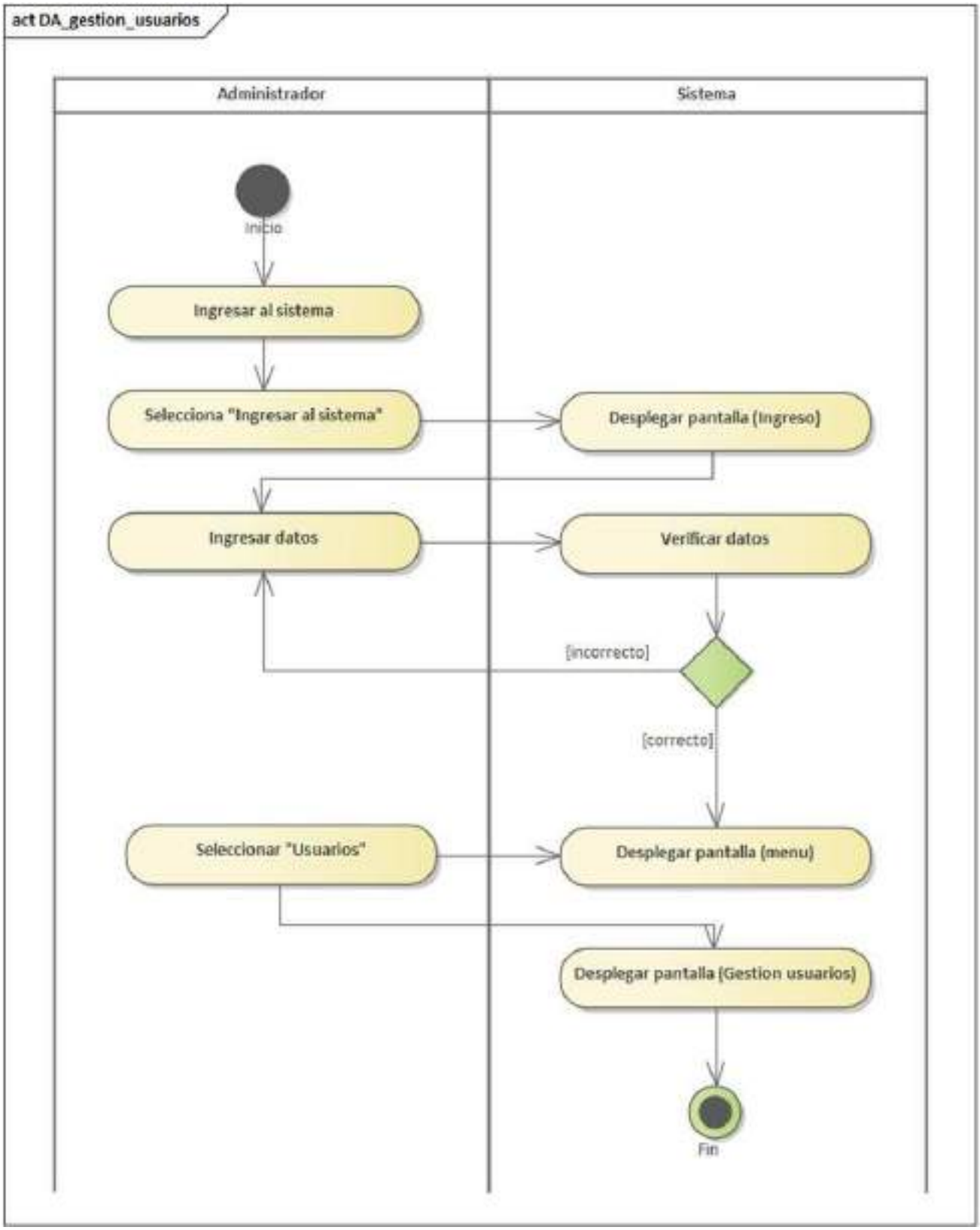


*Figura 2 – 86 Diagrama de Actividades: Gestión de Usuarios*

### II.2.3.6.8.14 Diagrama de Actividades: Listar Usuarios

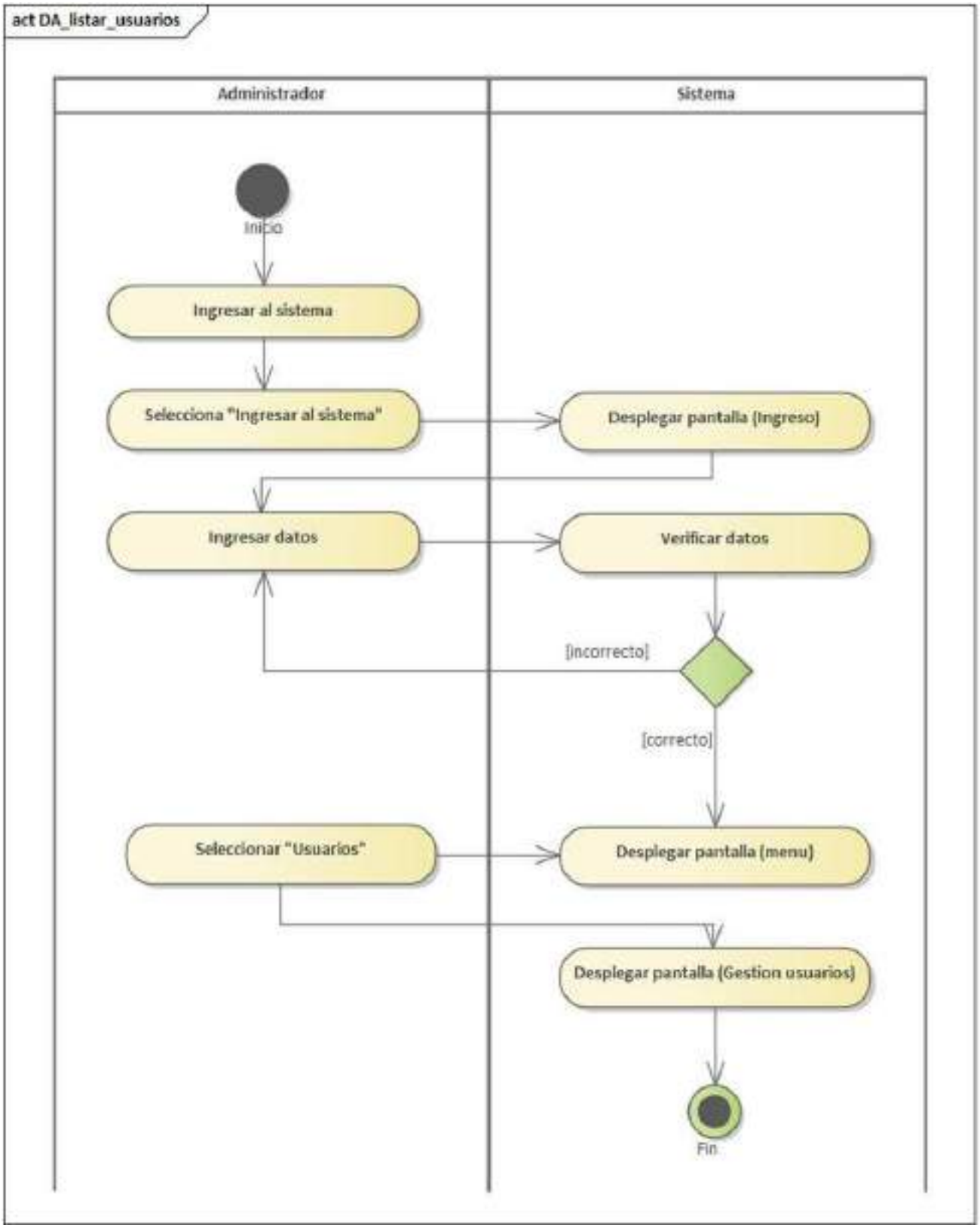


*Figura 2 – 87 Diagrama de Actividades: Listar Usuarios*

### II.2.3.6.8.15 Diagrama de Actividades: Agregar Usuario

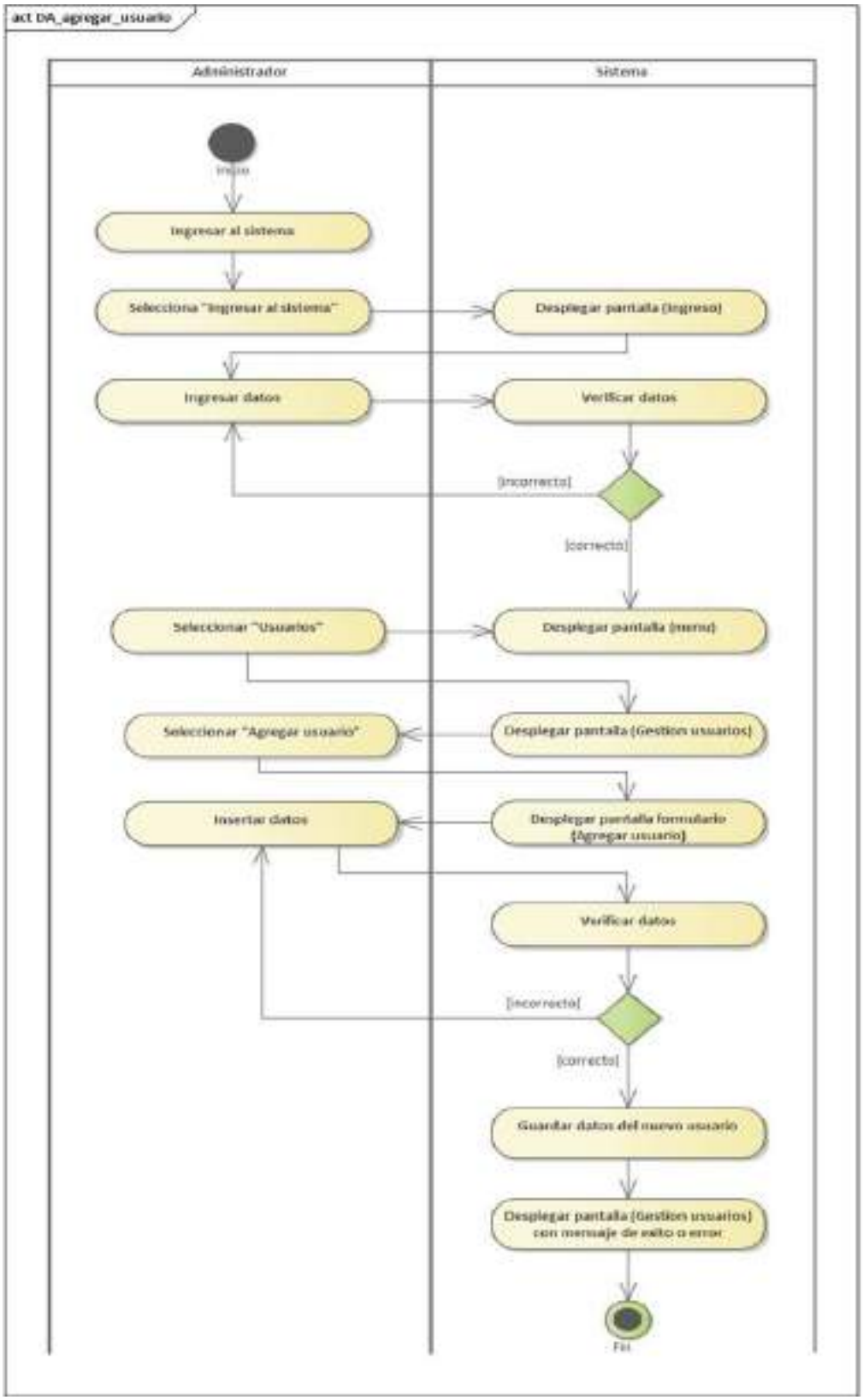


*Figura 2 – 88 Diagrama de Actividades: Agregar Usuario*

### II.2.3.6.8.16 Diagrama de Actividades: Modificar Usuario

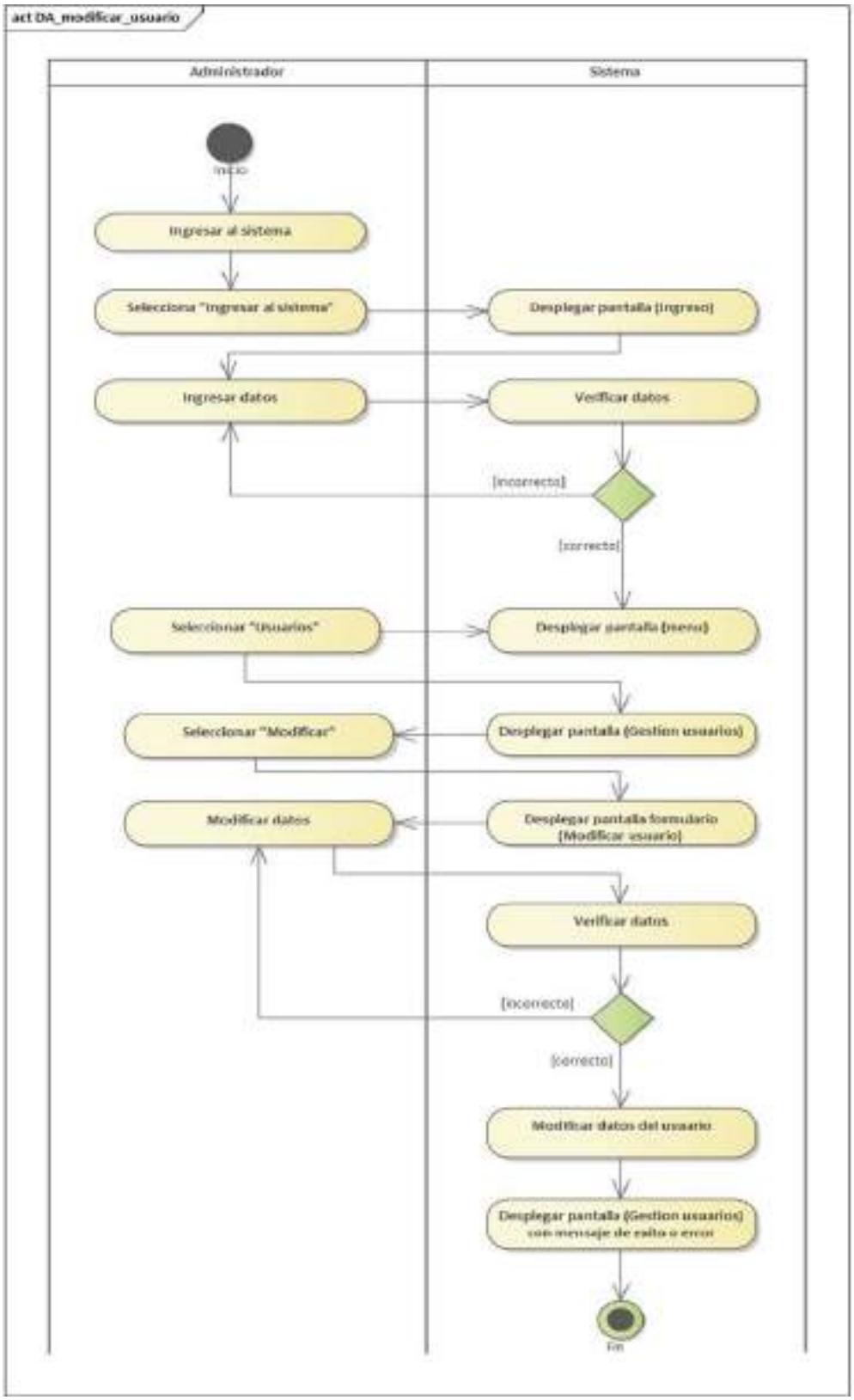


*Figura 2 – 89 Diagrama de Actividades: Modificar Usuario*

### II.2.3.6.8.17 Diagrama de Actividades: Ver Usuario

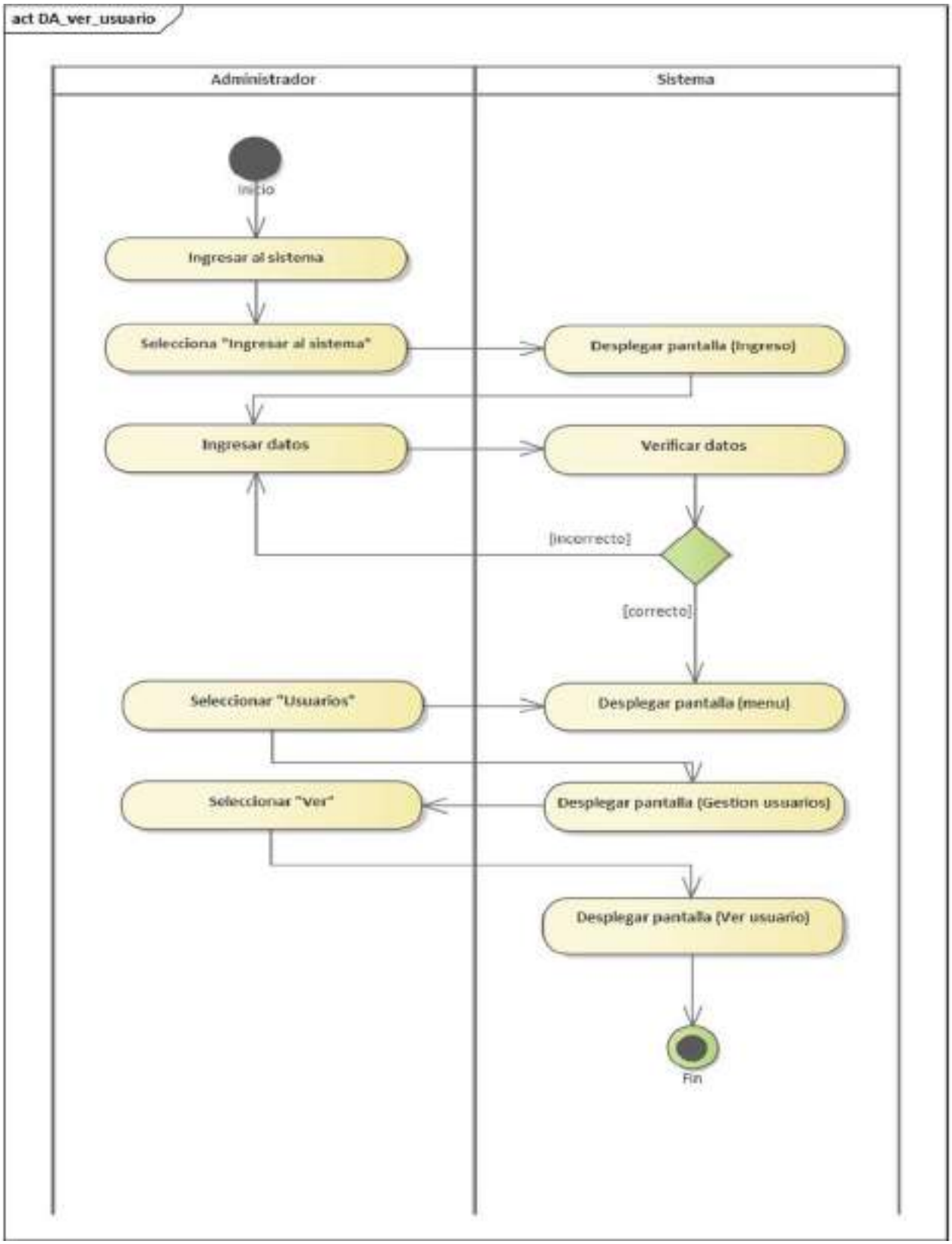


*Figura 2 – 90 Diagrama de Actividades: Ver Usuario*

### II.2.3.6.8.18 Diagrama de Actividades: Deshabilitar Usuario

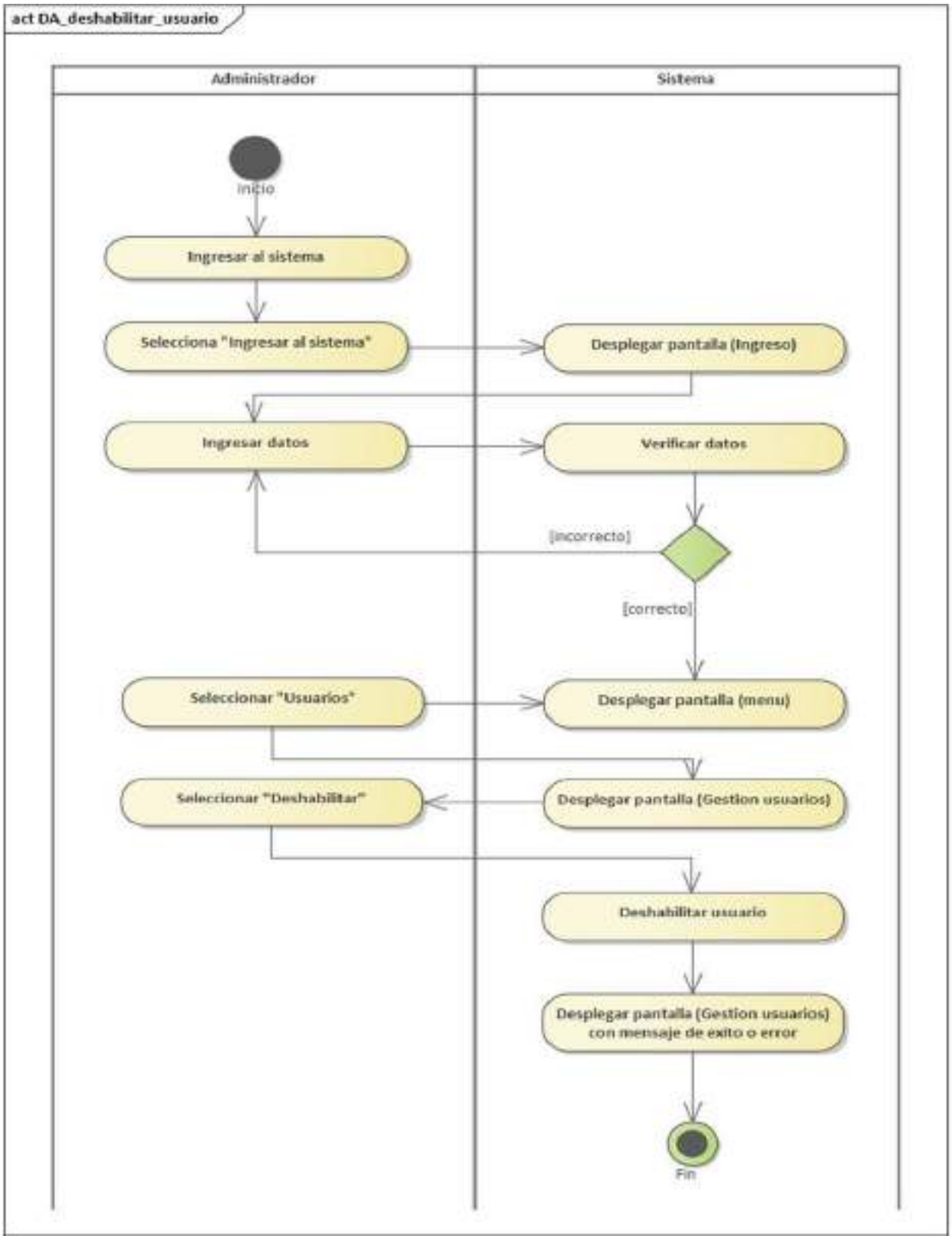


*Figura 2 – 91 Diagrama de Actividades: Deshabilitar Usuario*

### II.2.3.6.8.19 Diagrama de Actividades: Habilitar Usuario

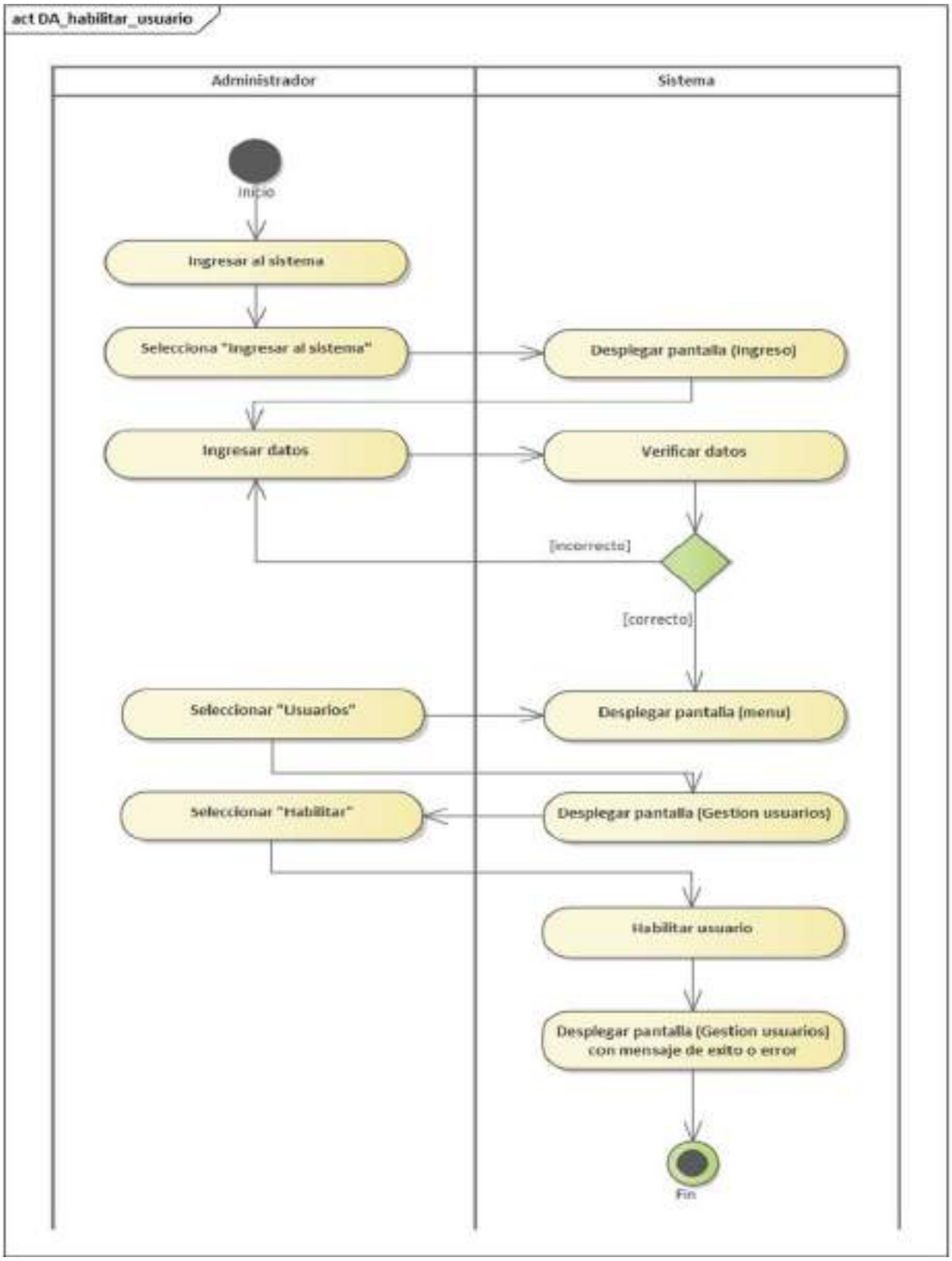


*Figura 2 – 92 Diagrama de Actividades: Habilitar Usuario*

### II.2.3.6.8.20 Diagrama de Actividades: Gestión Suscripciones

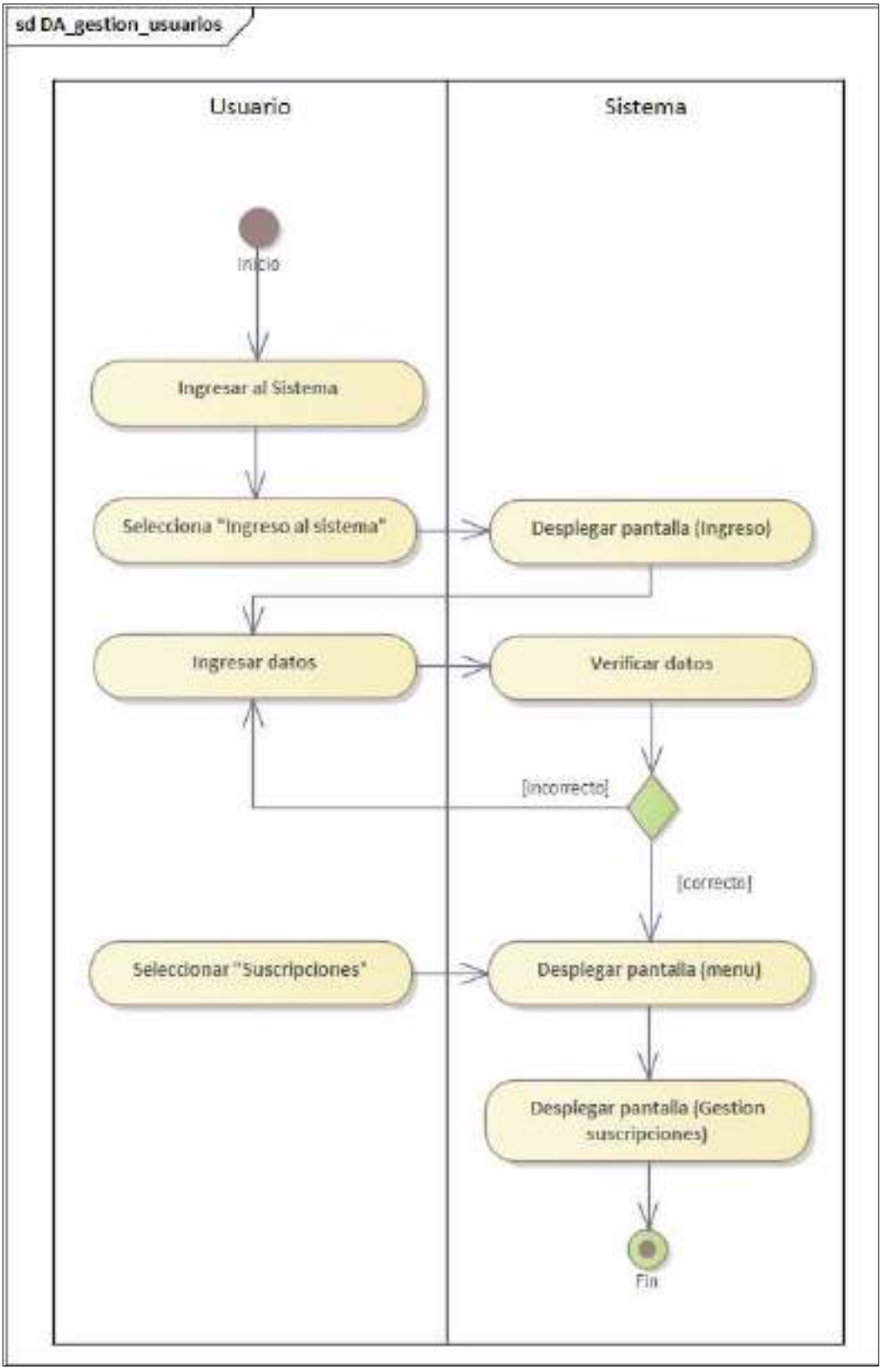


*Figura 2 – 93 Diagrama de Actividades: Gestión Suscripciones*

### II.2.3.6.8.21 Diagrama de Actividades: Agregar Suscripción

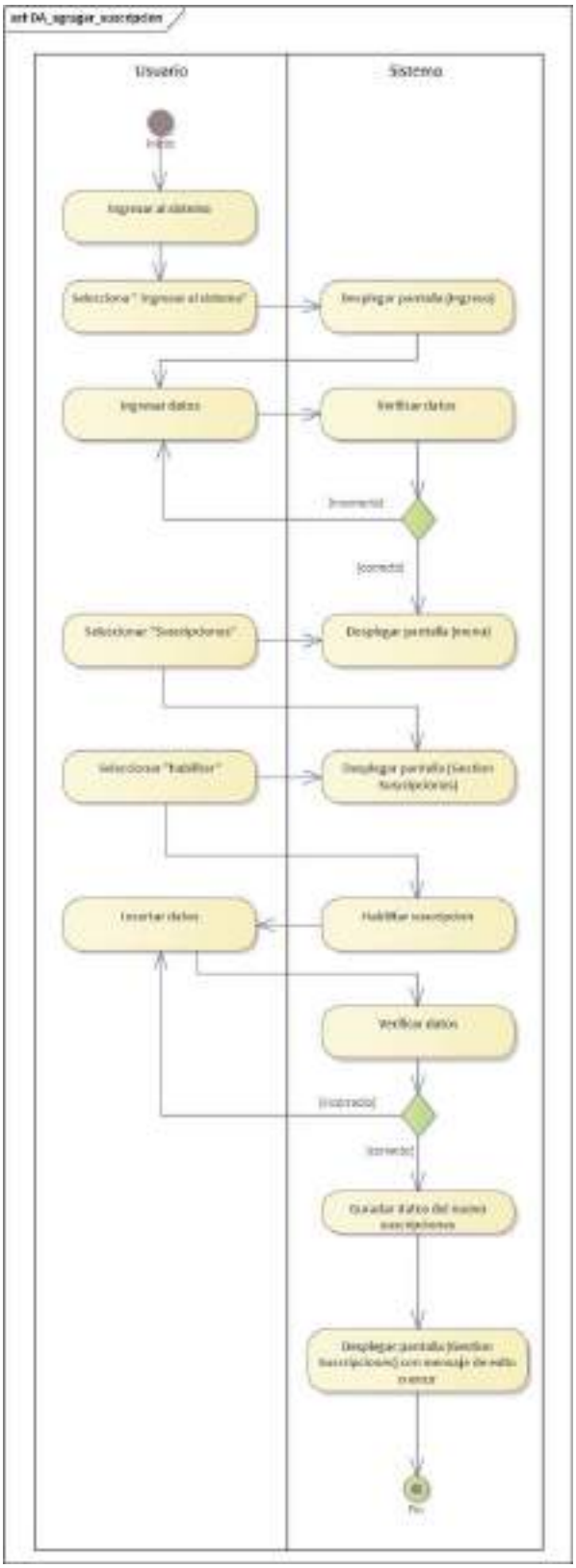


*Figura 2 – 94 Diagrama de Actividades: Agregar Suscripción*

### II.2.3.6.8.22 Diagrama de Actividades: Deshabilitar Suscripción

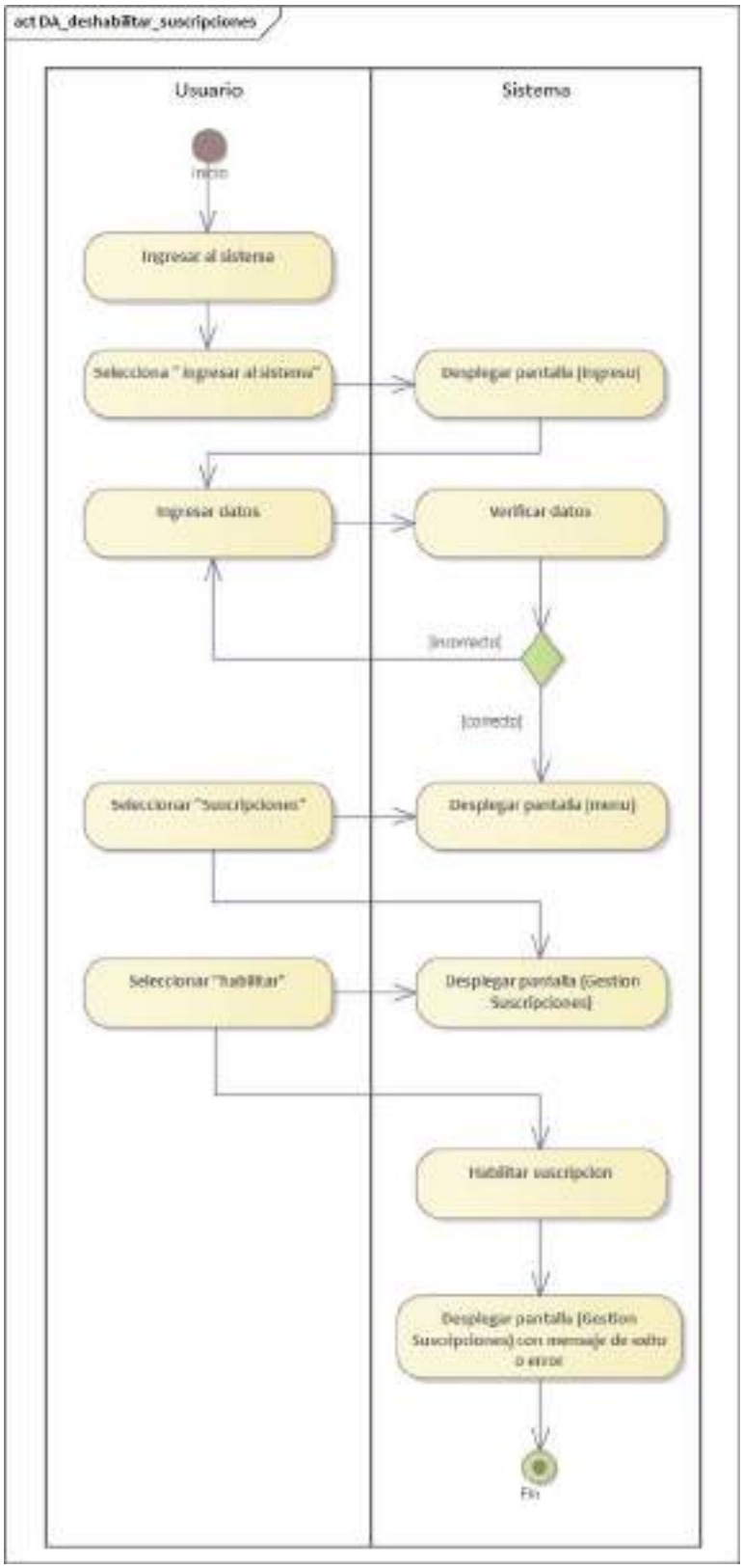


*Figura 2 – 95 Diagrama de Actividades: Deshabilitar Suscripción*

### II.2.3.6.8.23 Diagrama de Actividades: Habilitar Suscripción

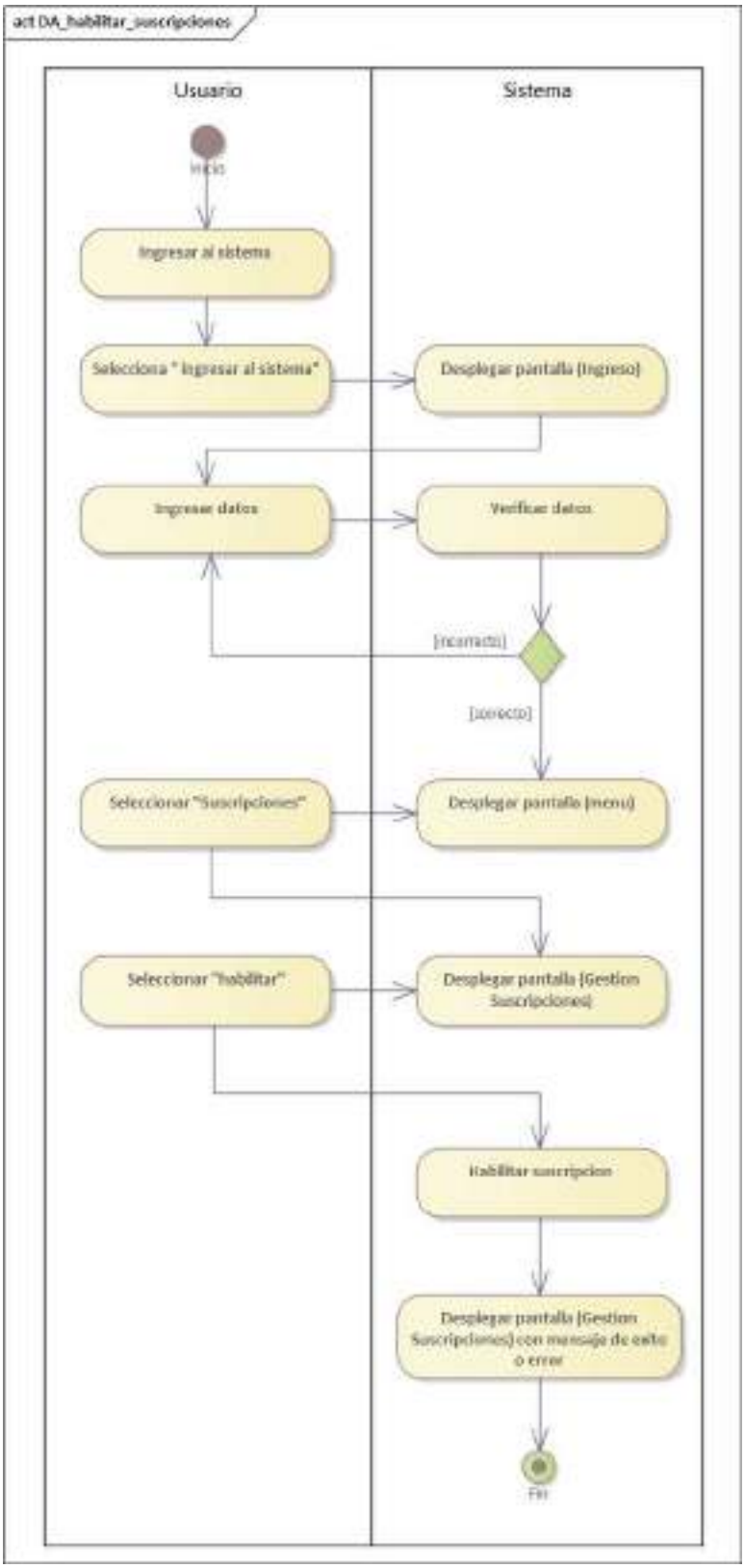


*Figura 2 – 96 Diagrama de Actividades: Habilitar Suscripción*

### II.2.3.6.8.24 Diagrama de Actividades: Listar Suscripción

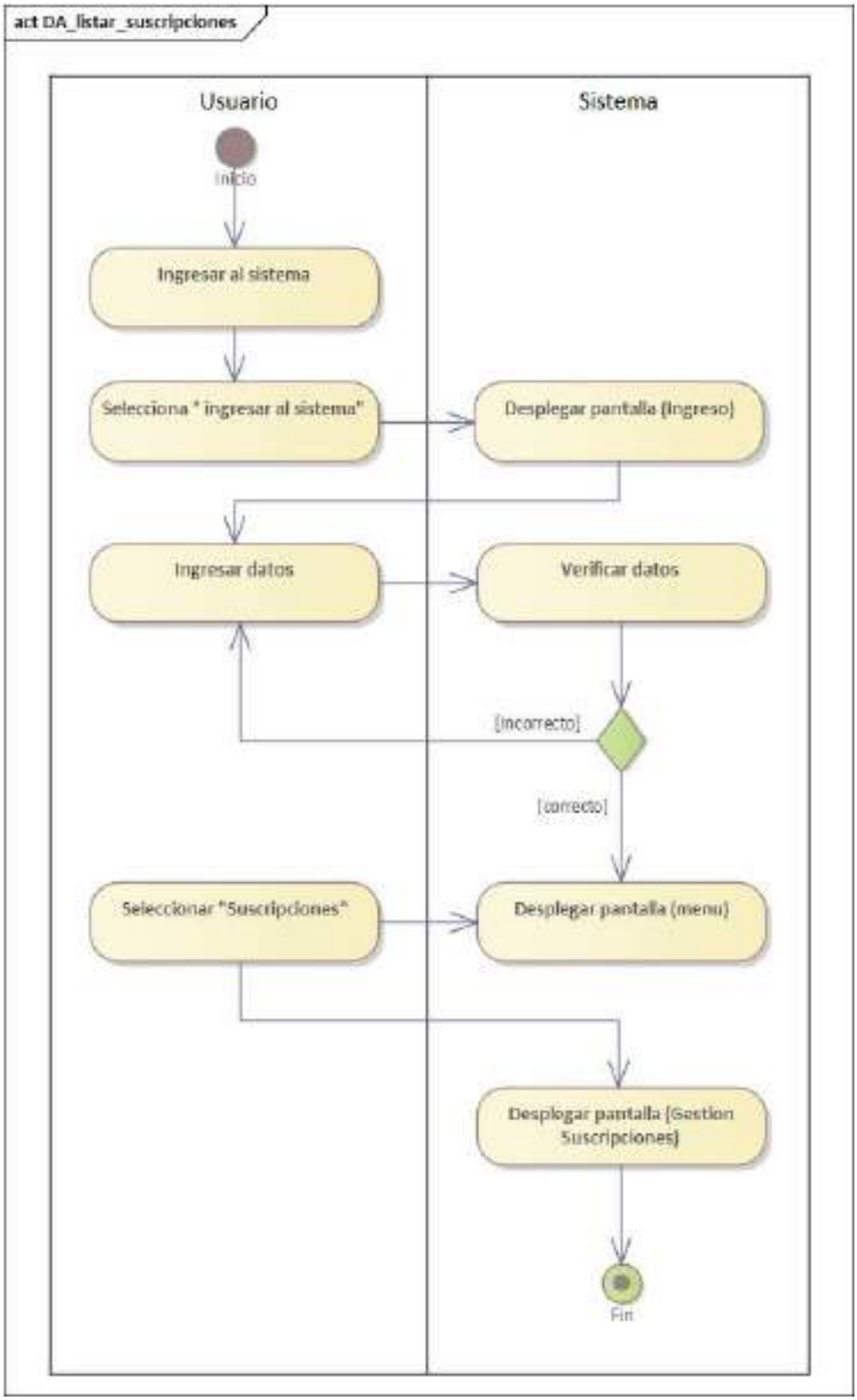


*Figura 2 – 97 Diagrama de Actividades: Listar Suscripción*

### II.2.3.6.8.25 Diagrama de Actividades: Modificar Suscripción

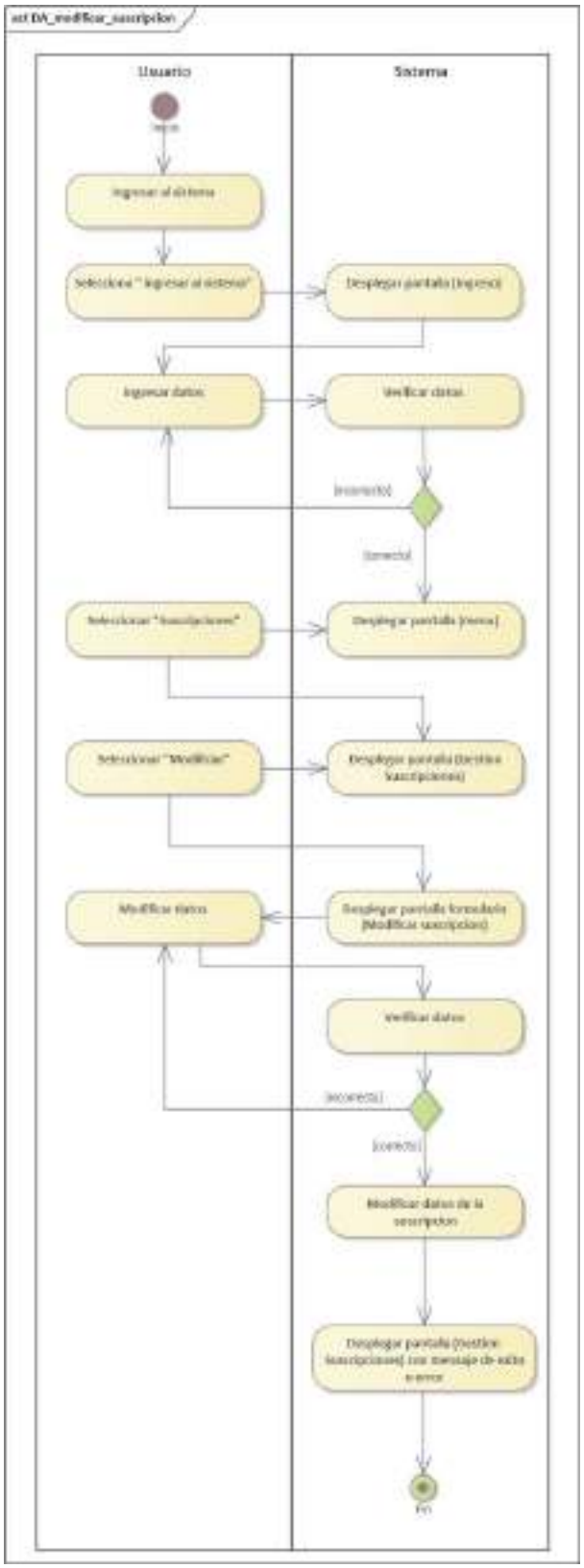


*Figura 2 – 98 Diagrama de Actividades: Modificar Suscripción*

### II.2.3.6.8.26 Diagrama de Actividades: Ver Suscripción

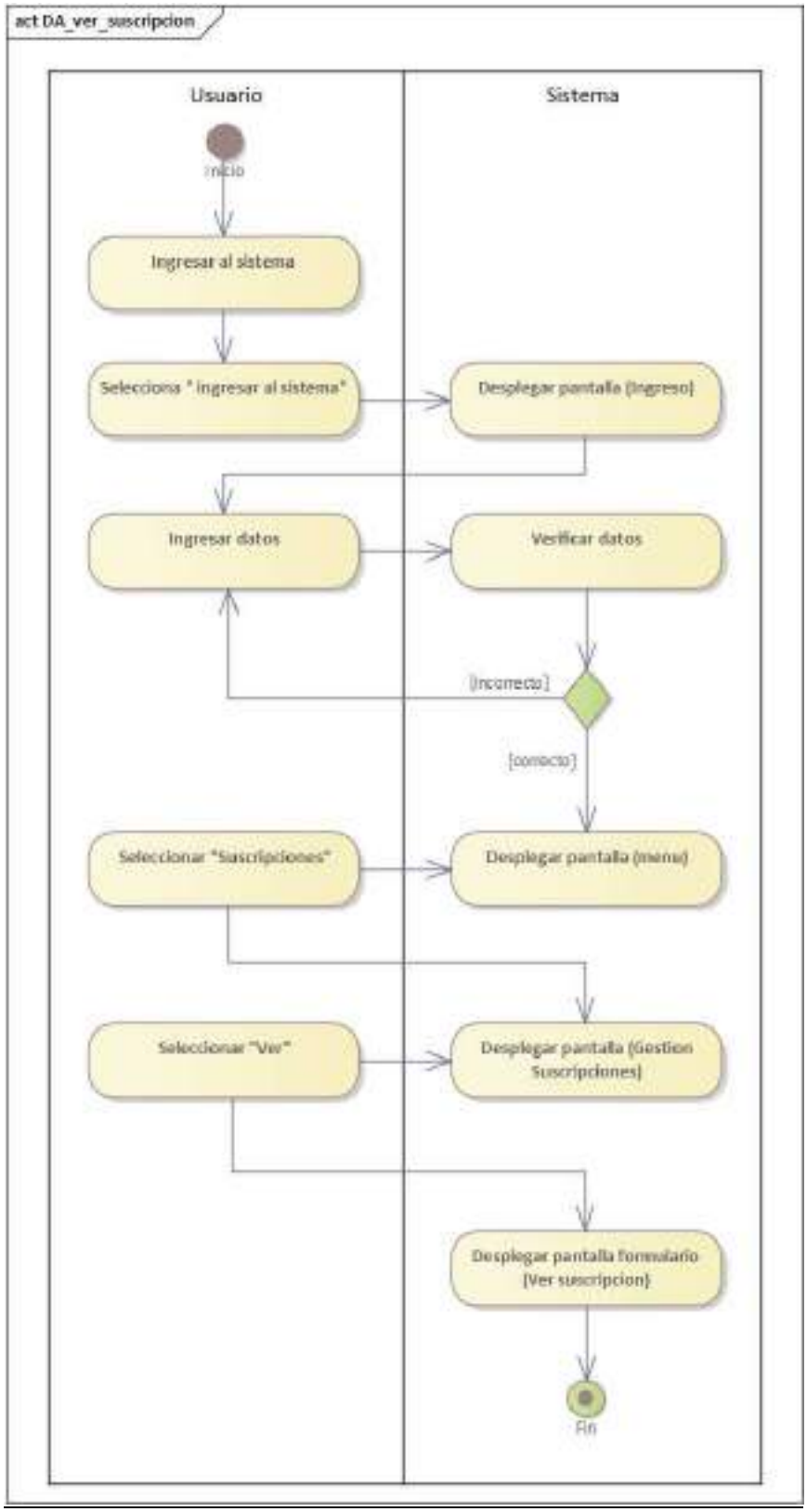


*Figura 2 – 99 Diagrama de Actividades: Ver Suscripción*

### II.2.3.6.8.27 Diagrama de Actividades: Habilitar Suscripción

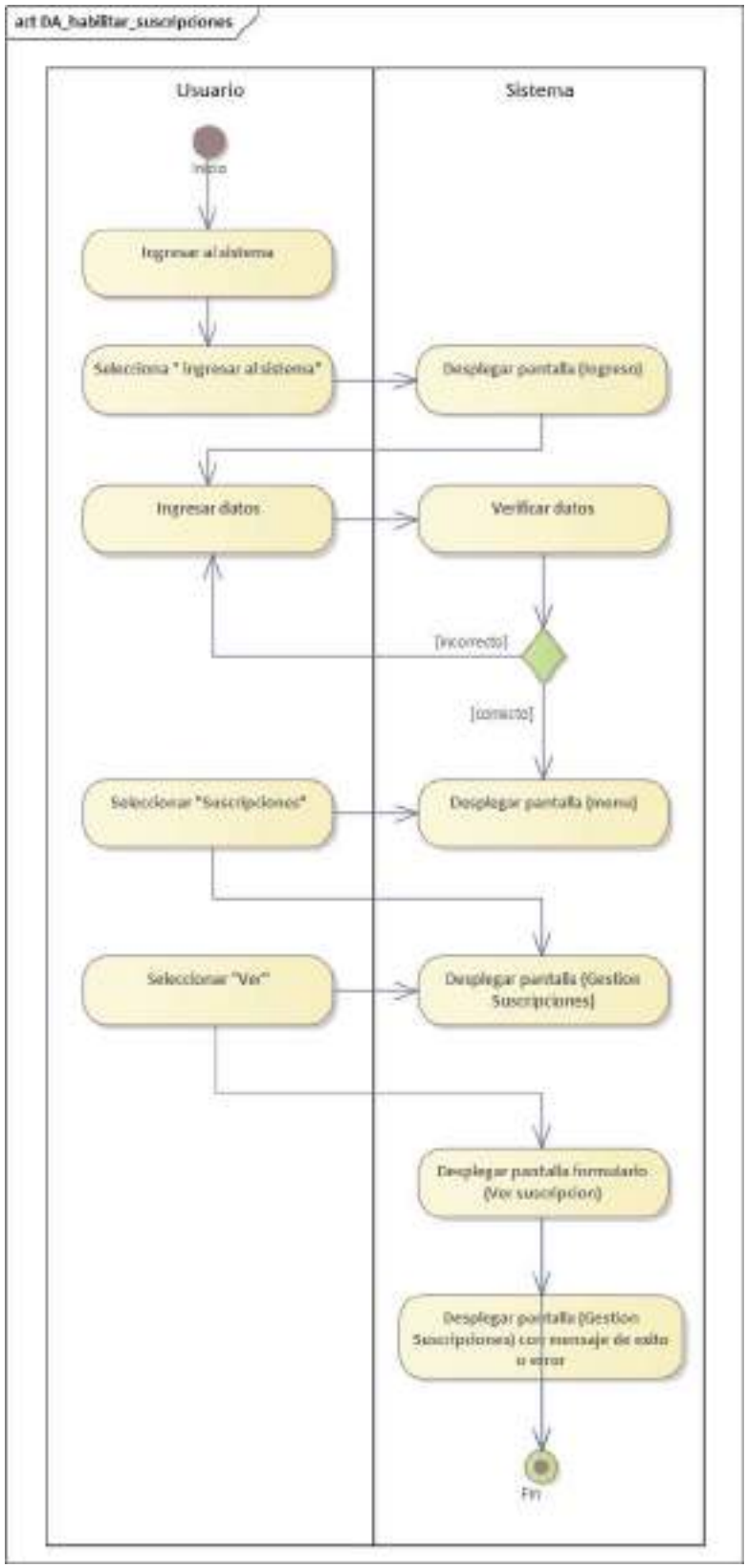


*Figura 2 – 100 Diagrama de Actividades: Habilitar Suscripción*

### II.2.3.6.9 Diagramas de secuencia

#### II.2.3.6.9.1 Introducción

En un diagrama de secuencias muestra una iteración ordenada según la secuencia temporal de eventos en particular muestra los objetos participantes en la iteración y los mensajes (llamadas a métodos) que intercambian según su secuencia en el tiempo.

Frecuentemente estos diagramas se ubican bajo los casos de uso o componentes en el modelo para ilustrar un escenario, un conjunto de pasos comunes que siguen en respuesta a un evento externo y que generalmente un resultado.

El modelo incluye, que inicia la actividad en el sistema, que procesamientos y cambias ocurren internamente y que salidas se generan.

Muchas veces las instancias de los objetos se representan usando iconos especialmente estereotipo; existen iconos para objetos de interfaz, controladores, entidades persistentes, etc.

#### II.2.3.6.9.2 Propósito

Los diagramas de secuencia se usan para mostrar las iteraciones entre los usuarios, las pantallas y las instancias de los objetos en el sistema. Proveen una secuencia de pasos y de los mensajes entre los objetos a lo largo del tiempo.

#### II.2.3.6.9.3 Alcance

- Muestran gráficamente las iteraciones del actor y de las operaciones a las que dan origen.
- Muestran un determinado escenario de un caso de uso, los eventos generados por actores externos, su orden y sus eventos internos.

### II.2.3.6.9.4 Diagrama de Secuencia: Ingreso al sistema

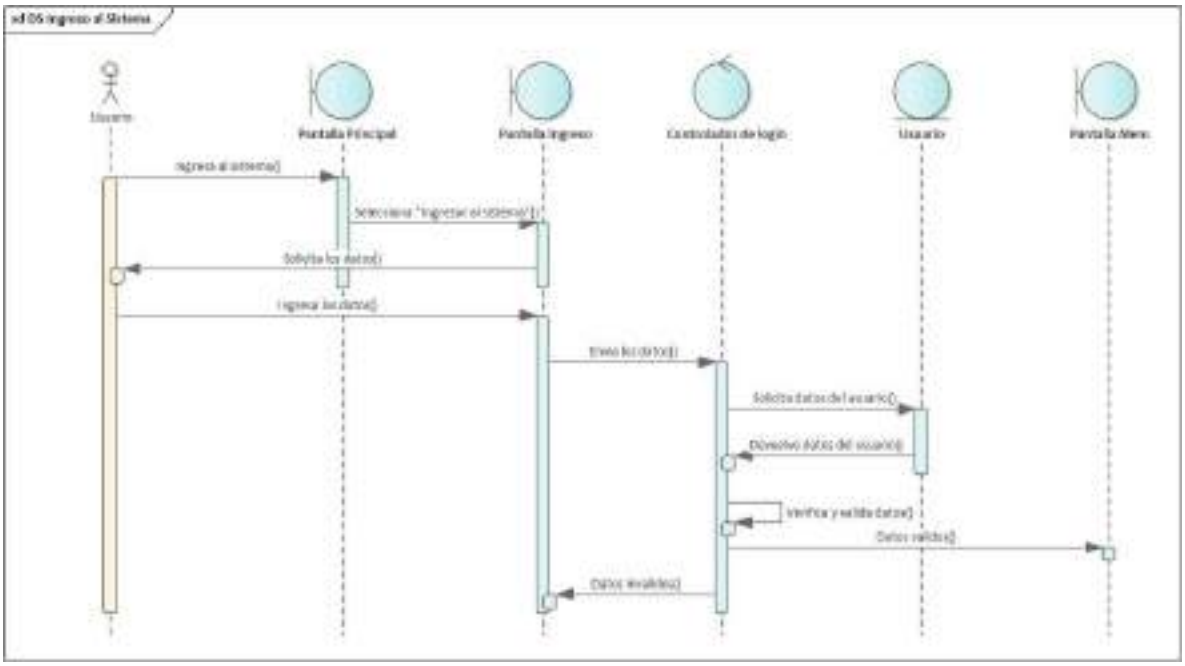


*Figura 2 – 101 Diagrama de Secuencia: Ingreso al sistema*

### II.2.3.6.9.5 Diagrama de Secuencia: Modificar Perfil

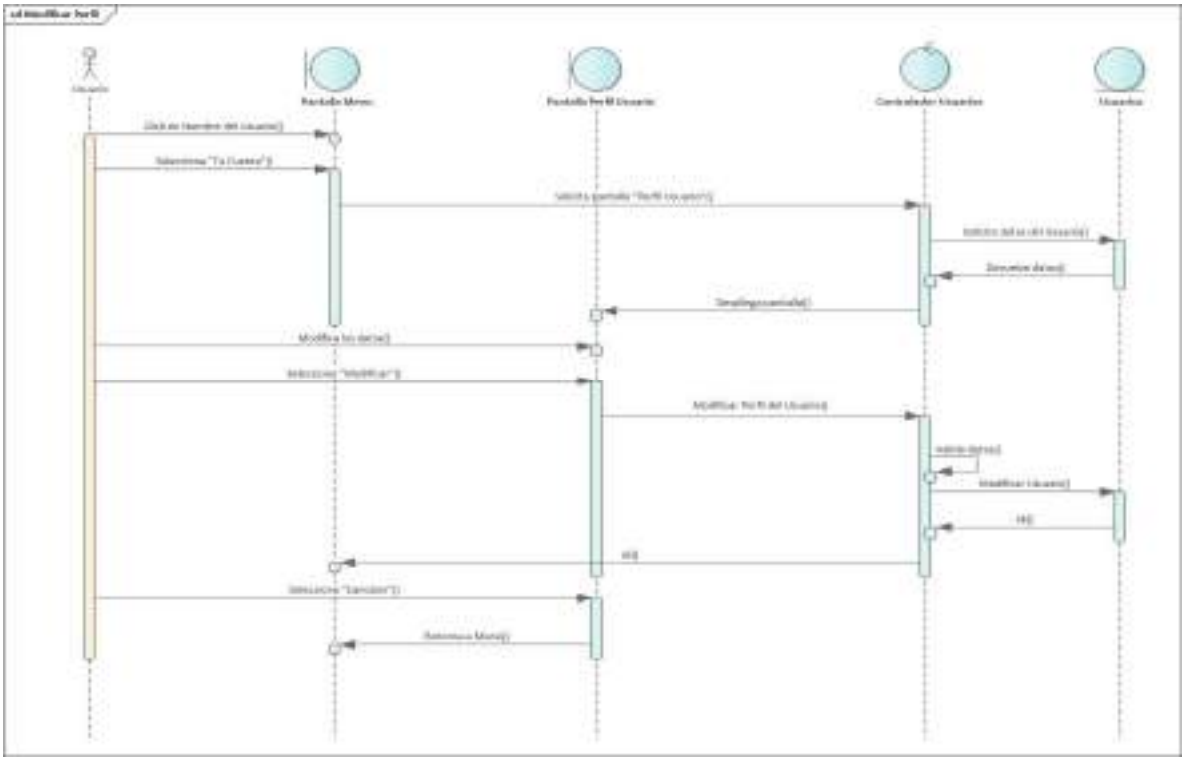

*Figura 2 – 102 Diagrama de Secuencia: Modificar Perfil*

### II.2.3.6.9.6 Diagrama de Secuencia: Gestión de Roles

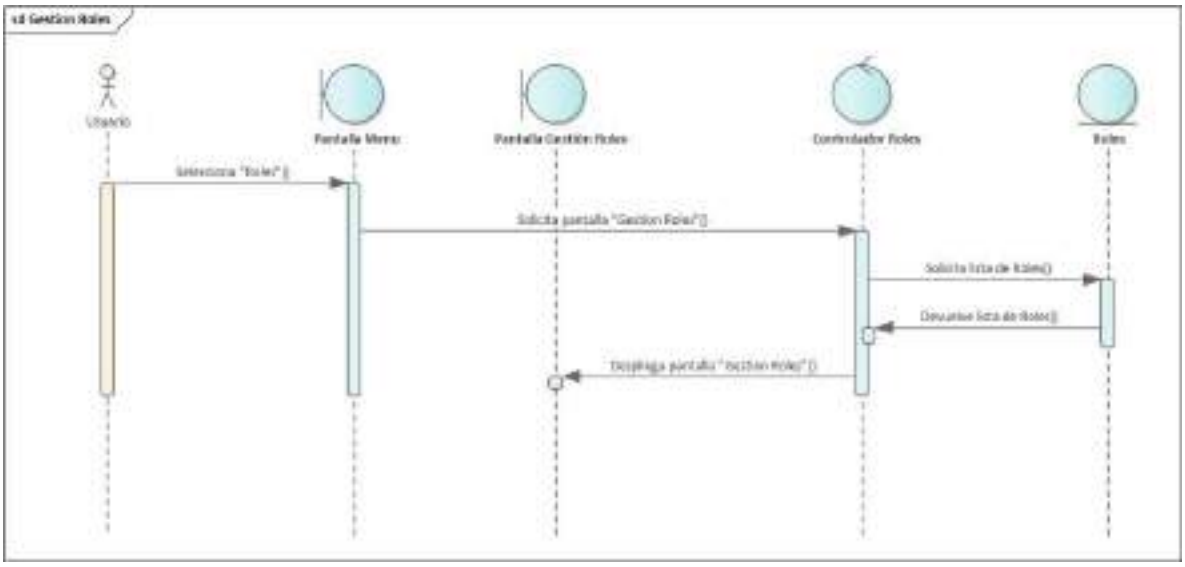

*Figura 2 – 103 Diagrama de Secuencia: Gestión de Roles*

### II.2.3.6.9.7 Diagrama de Secuencia: Agregar Rol

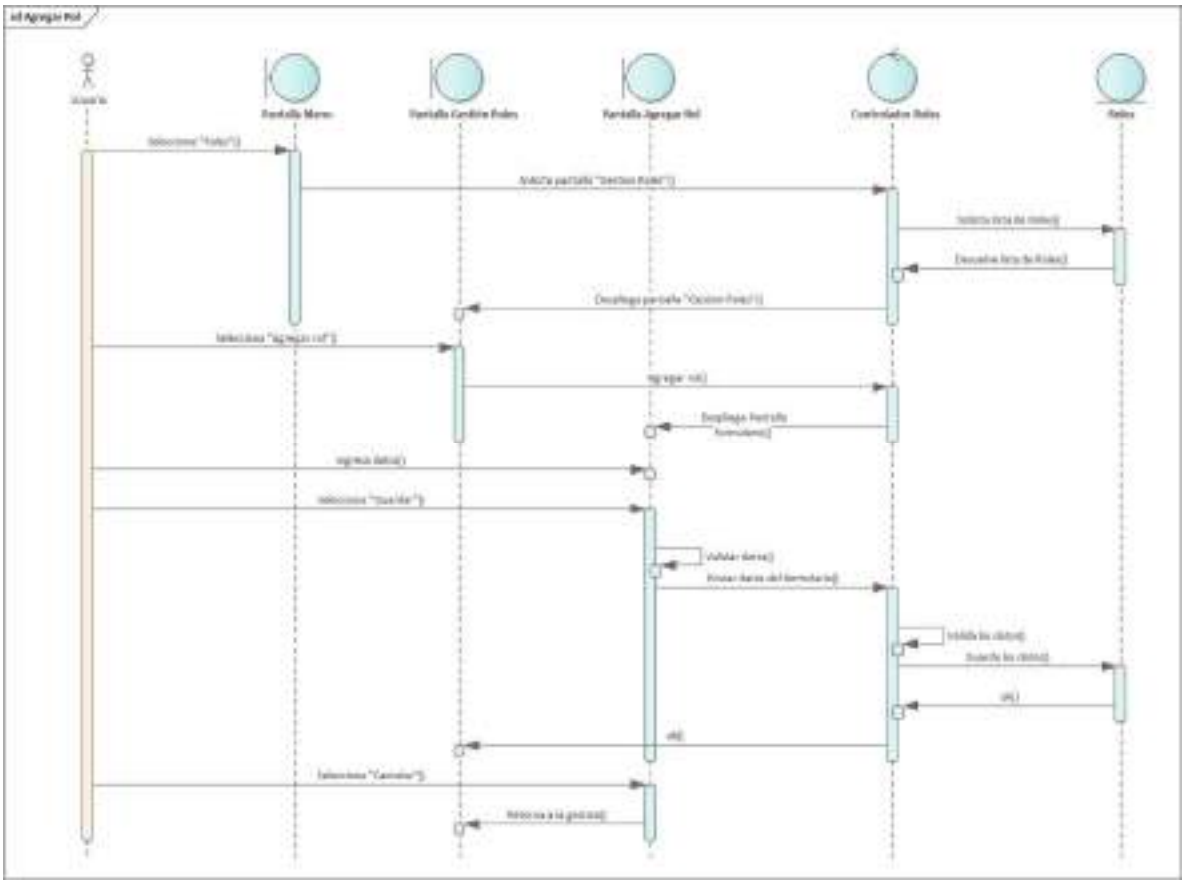

*Figura 2 – 104 Diagrama de Secuencia: Agregar Rol*

## II.2.3.6.9.8 Diagrama de Secuencia: Modificar Rol

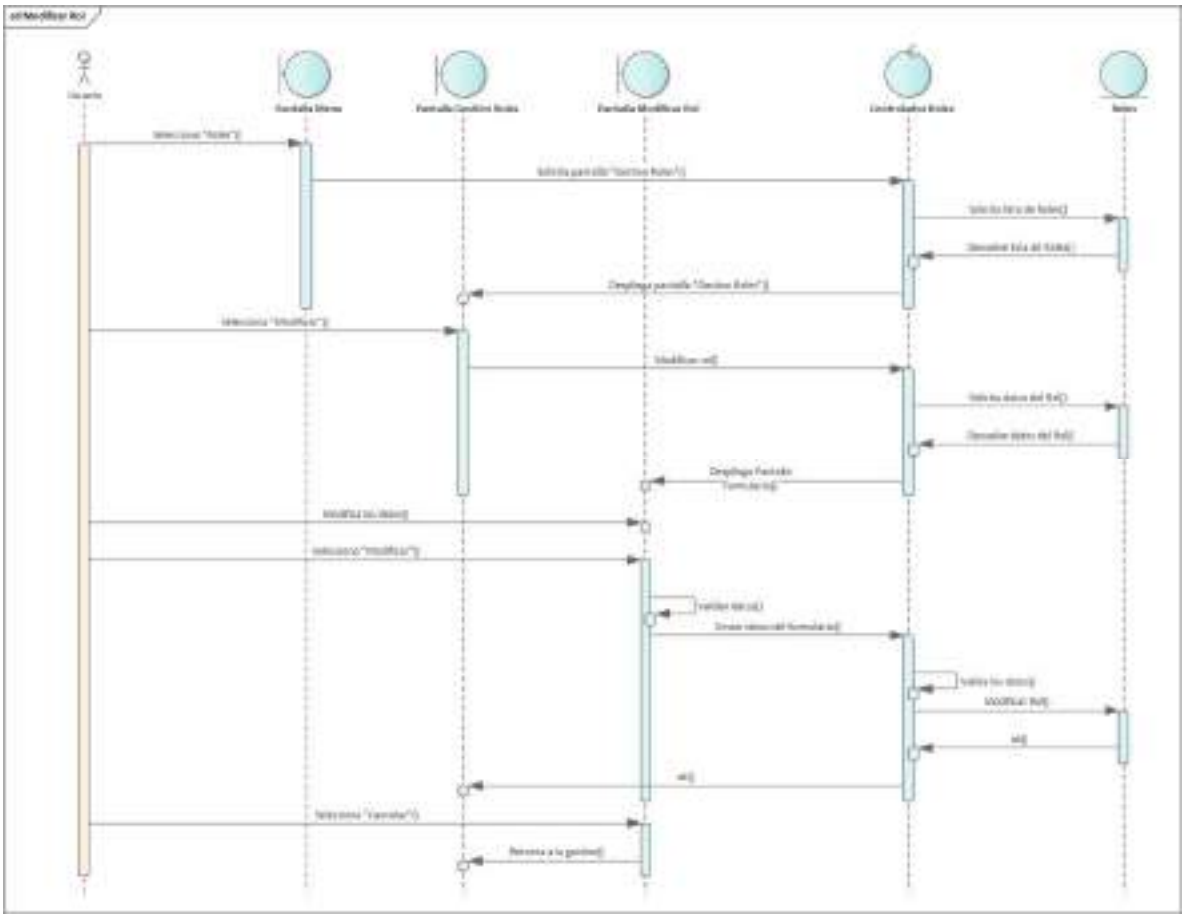

*Figura 2 – 105 Diagrama de Secuencia: Modificar Rol*

### II.2.3.6.9.9 Diagrama de Secuencia: Modificar Rol

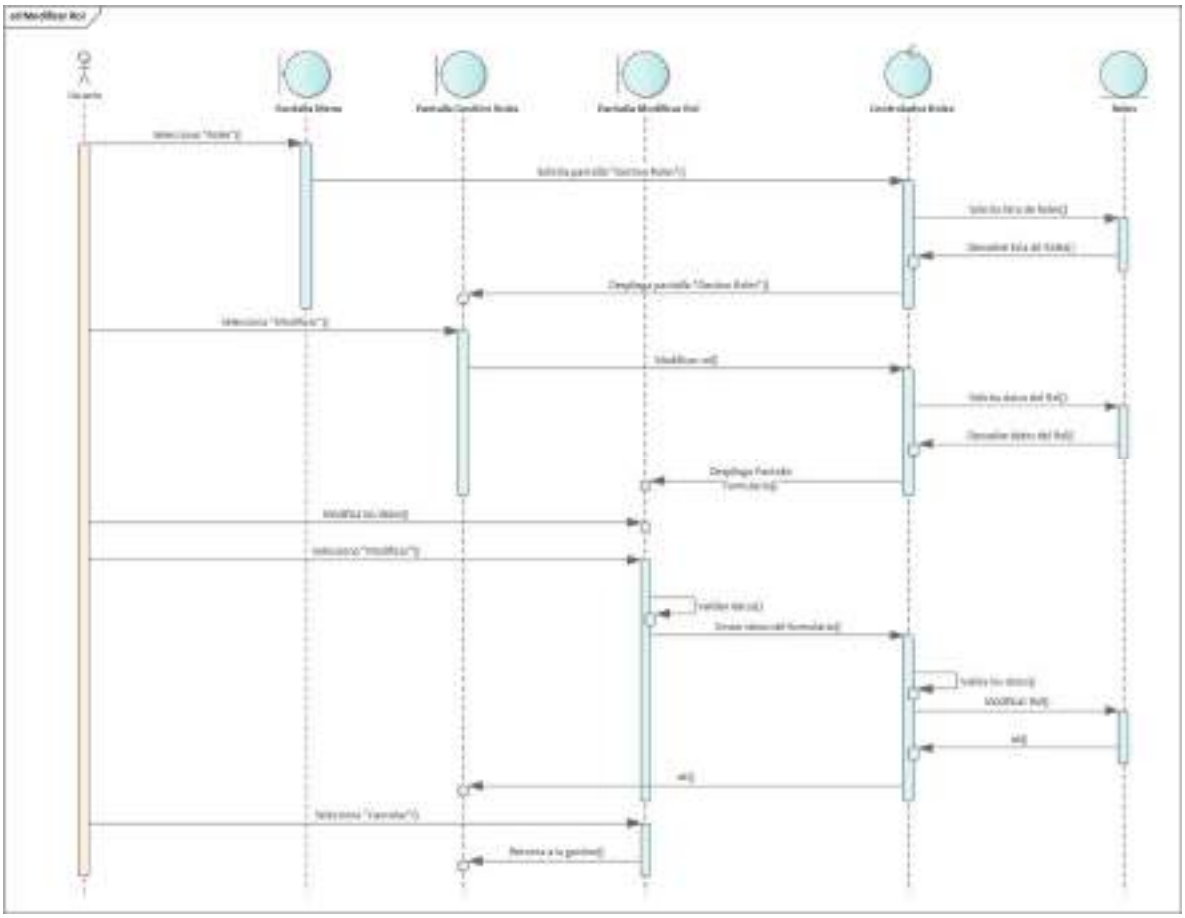

*Figura 2 – 106 Diagrama de Secuencia: Modificar Rol*

### II.2.3.6.9.10 Diagrama de Secuencia: Ver Rol

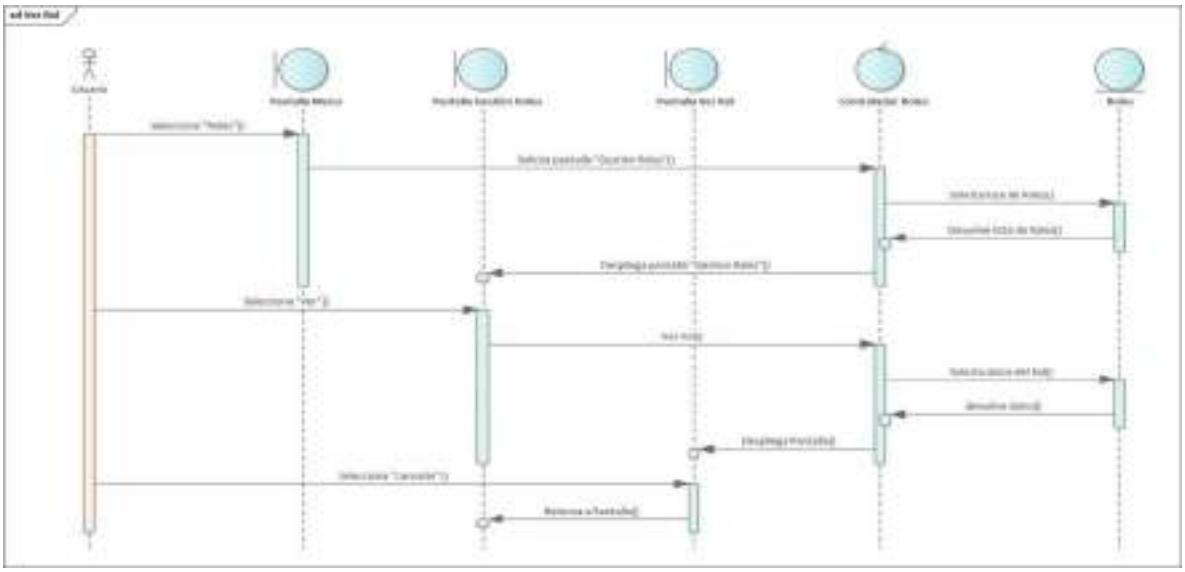

*Figura 2 – 107 Diagrama de Secuencia: Ver Rol*

### II.2.3.6.9.11 Diagrama de Secuencia: Deshabilitar Rol

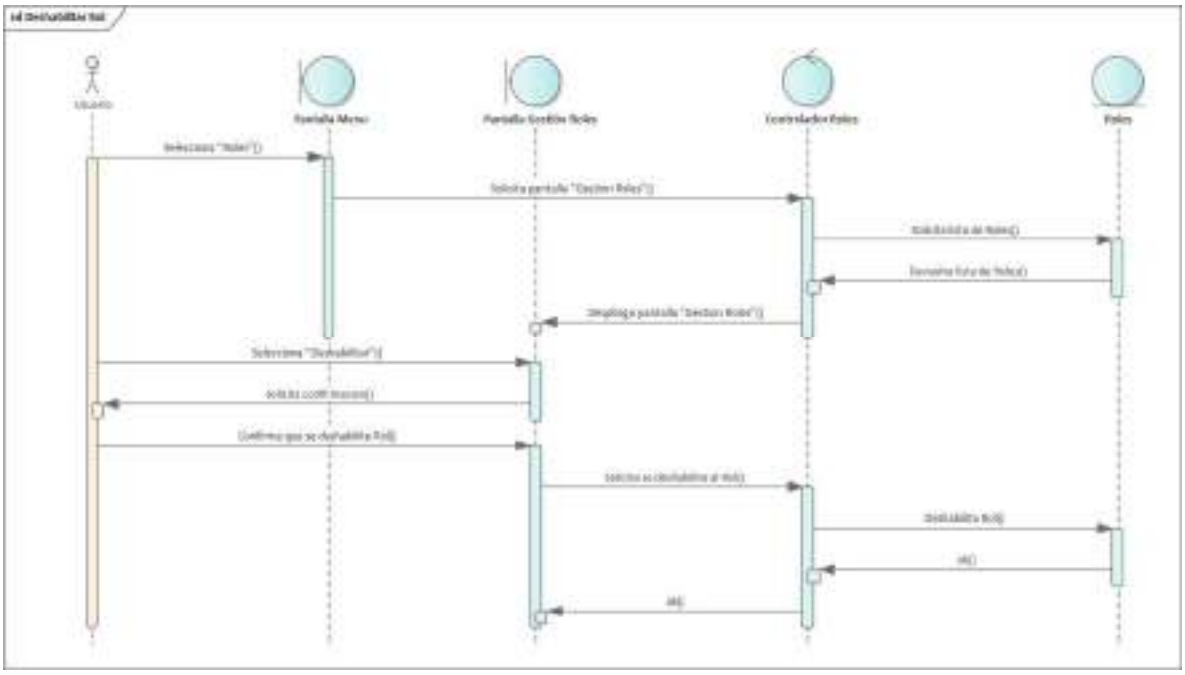

*Figura 2 – 108 Diagrama de Secuencia: Deshabilitar Rol*

### II.2.3.6.9.12 Diagrama de Secuencia: Habilitar Rol

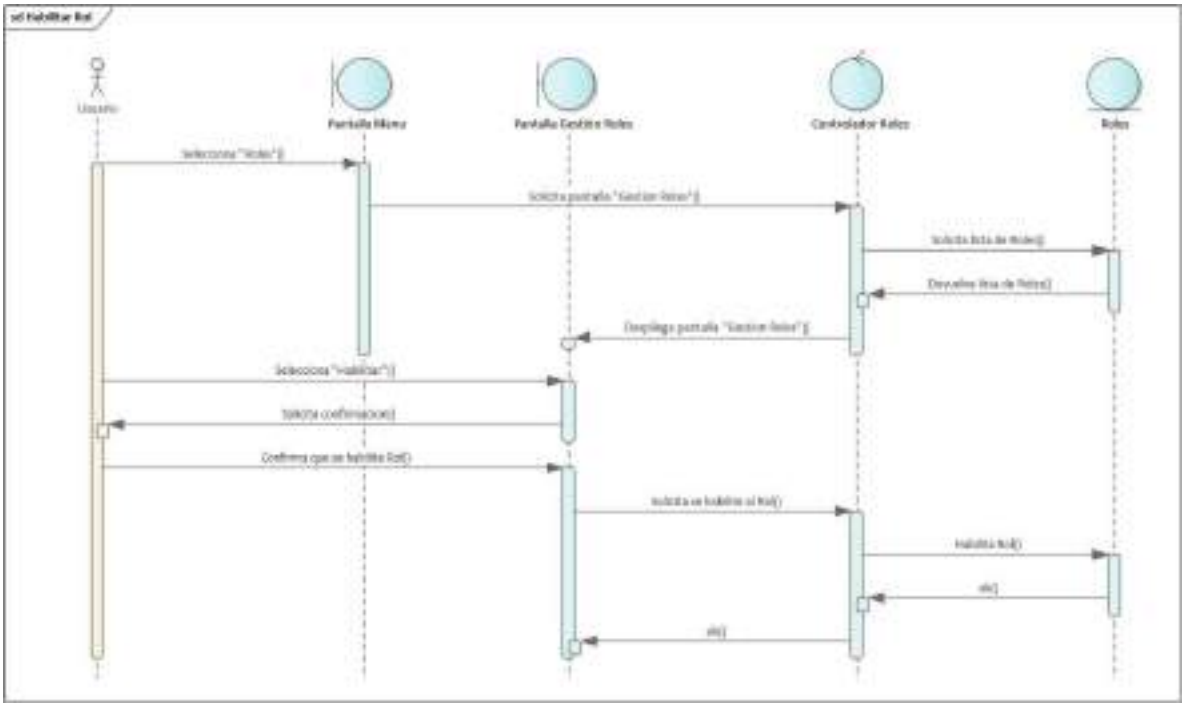

*Figura 2 – 109 Diagrama de Secuencia: Habilitar Rol*

### II.2.3.6.9.13 Diagrama de Secuencia: Gestión de Usuarios

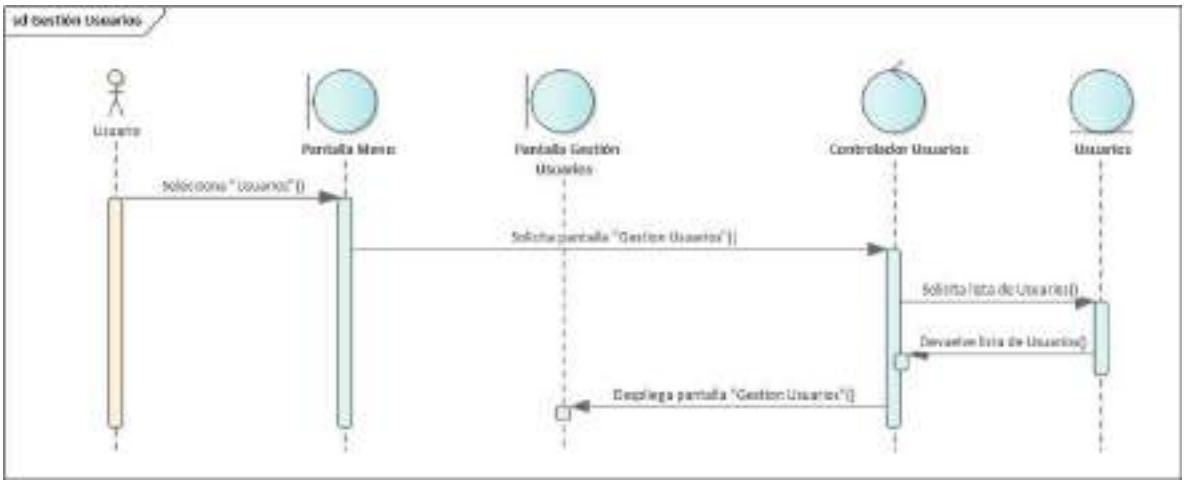


*Figura 2 – 110 Diagrama de Secuencia: Gestión de Usuarios*

### II.2.3.6.9.14 Diagrama de Secuencia: Agregar Usuario

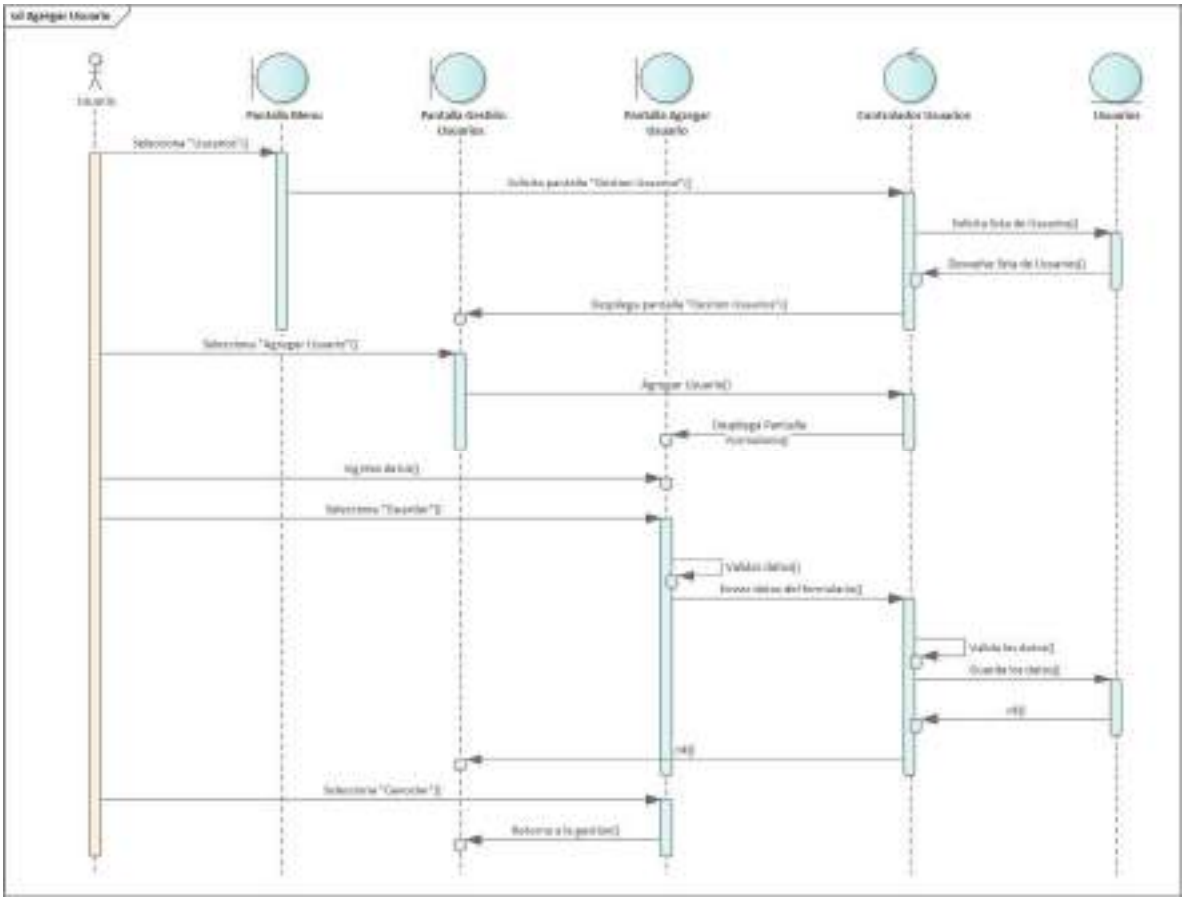

*Figura 2 – 111 Diagrama de Secuencia: Agregar Usuario*

### II.2.3.6.9.15 Diagrama de Secuencia: Modificar Usuario

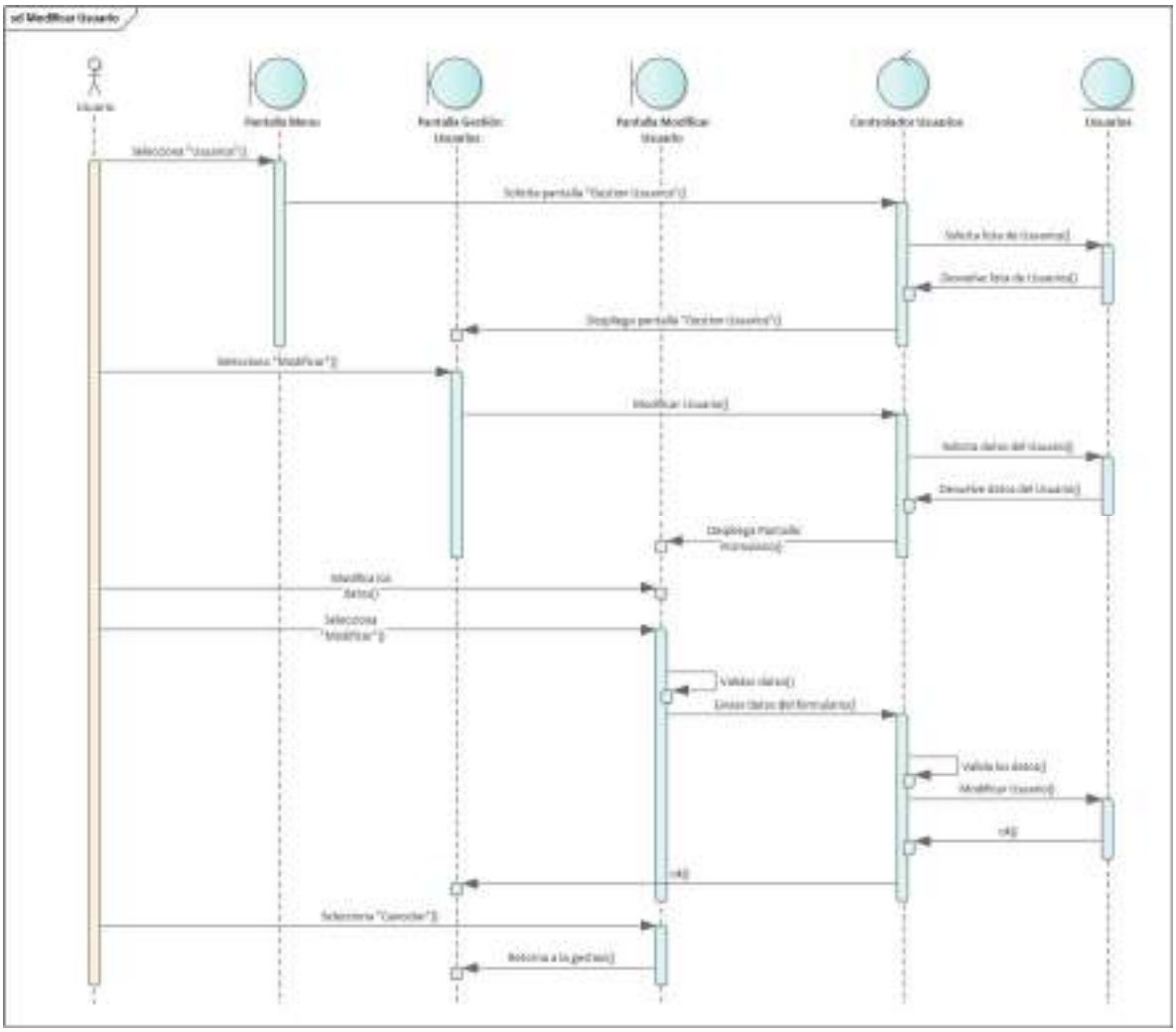

*Figura 2 – 112 Diagrama de Secuencia: Modificar Usuario*

### II.2.3.6.9.16 Diagrama de Secuencia: Ver Usuario

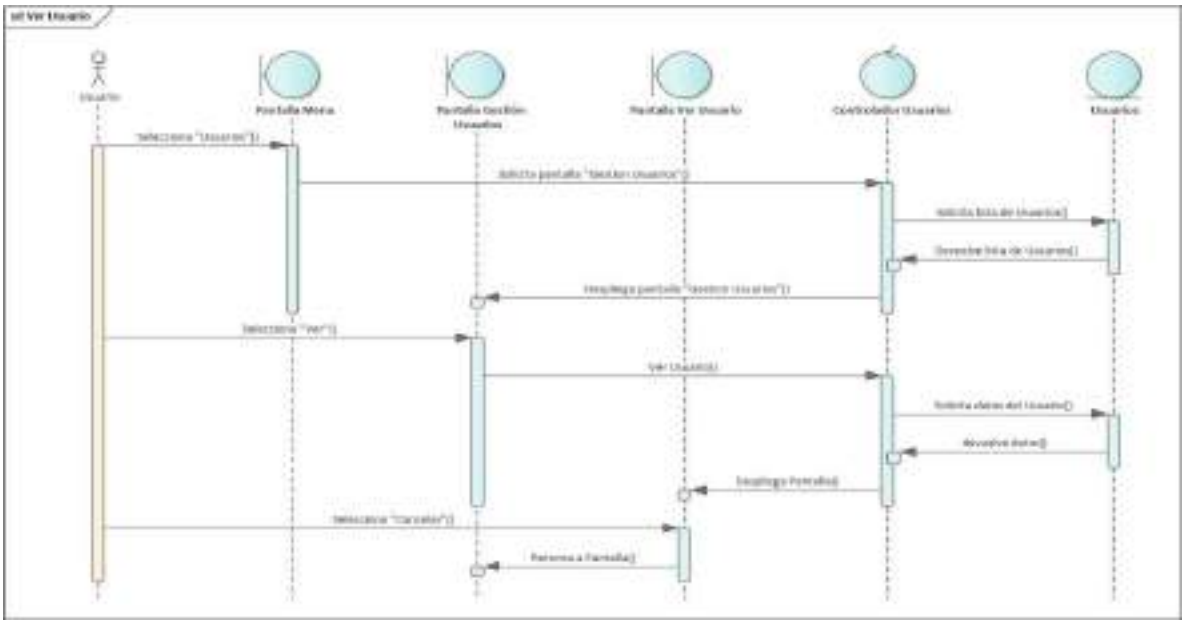

*Figura 2 – 113 Diagrama de Secuencia: Ver Usuario*

### II.2.3.6.9.17 Diagrama de Secuencia: Deshabilitar Usuario

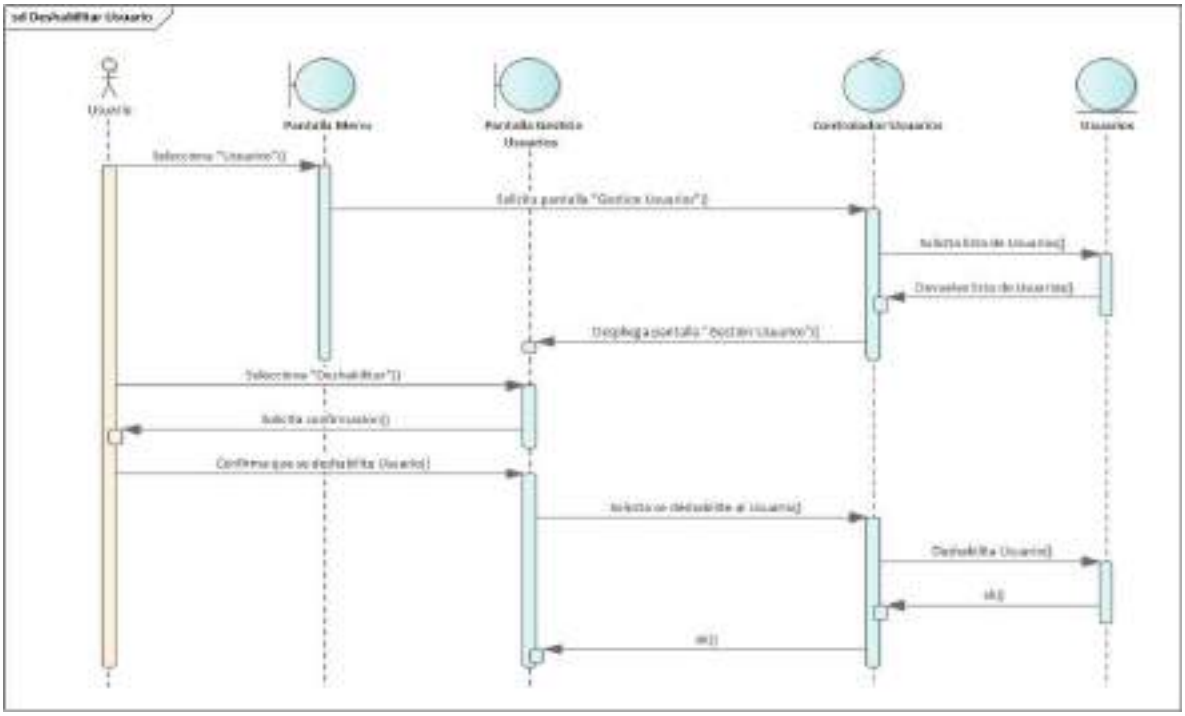

*Figura 2 – 114 Diagrama de Secuencia: Deshabilitar Usuario*

### II.2.3.6.9.18 Diagrama de Secuencia: Habilitar Usuario

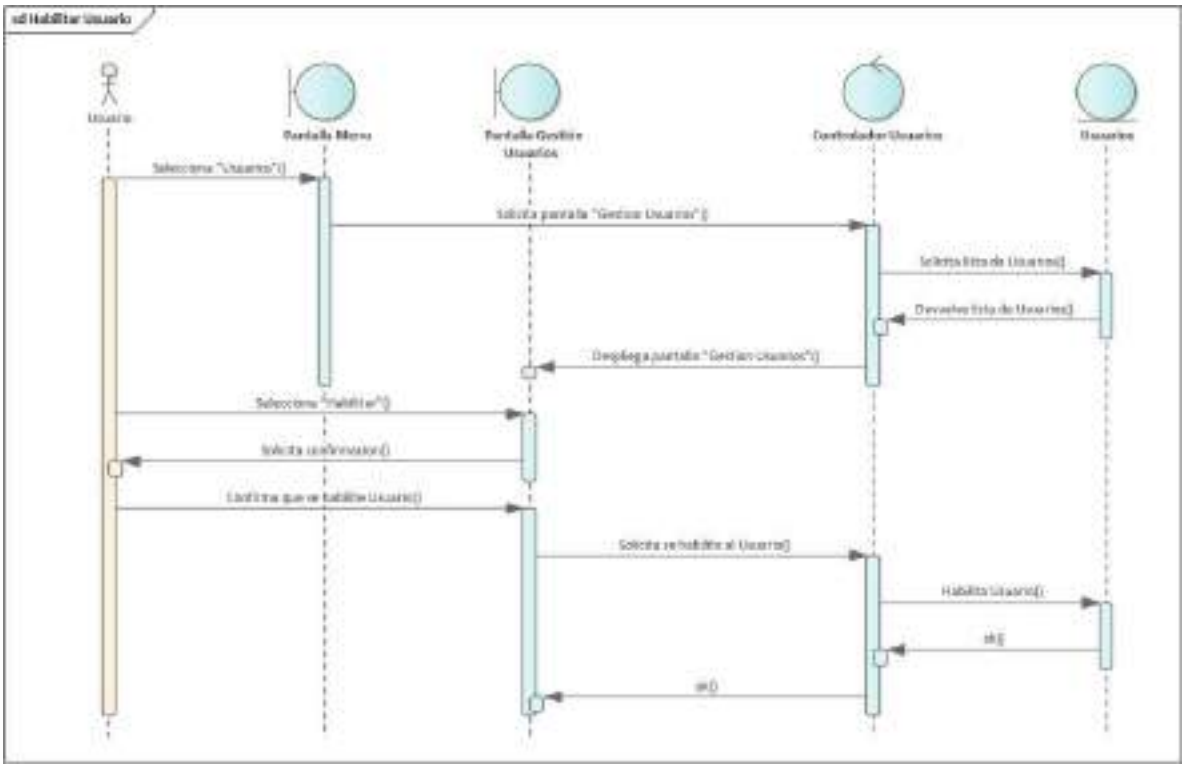

*Figura 2 – 115 Diagrama de Secuencia: Habilitar Usuario*

### II.2.3.6.9.19 Diagrama de Secuencia: Gestión de Suscripciones

## II.2.3.6.10 Modelo de datos

### II.2.3.6.10.1 Introducción

Previendo que la persistencia de la información del sistema será soportada por una base de datos relacional, este modelo describe la representación lógica de los datos persistentes, de acuerdo con el enfoque para modelado relacional de datos. Para expresar este modelo se utiliza un Diagrama de Clases (donde se utiliza un modelo UML para Modelado de Datos, para conseguir la representación de tablas, claves, etc.).

Los Diagramas de Clases son diagramas de estructura estática que muestra las clases del sistema y sus interrelaciones (incluye herencia, agregación, asociación, etc.).

Los diagramas de Clases son el pilar fundamental del modelo con UML, siendo utilizados tanto para mostrar lo que el sistema puede hacer (análisis), como para mostrar cómo puede ser construido (diseño).

#### II.2.3.6.10.2 Propósito

Comprende la estructura del sistema deseado para la Organización e identificar posibles mejoras.

#### II.2.3.6.10.3 Alcance

- Describir las tablas de diseño del sistema en su segunda iteración.
- Identificar y definir las relaciones entre tablas según los objetivos del sistema deseado aprobado por la Organización.

#### II.2.3.6.10.4 Diagrama de Clases

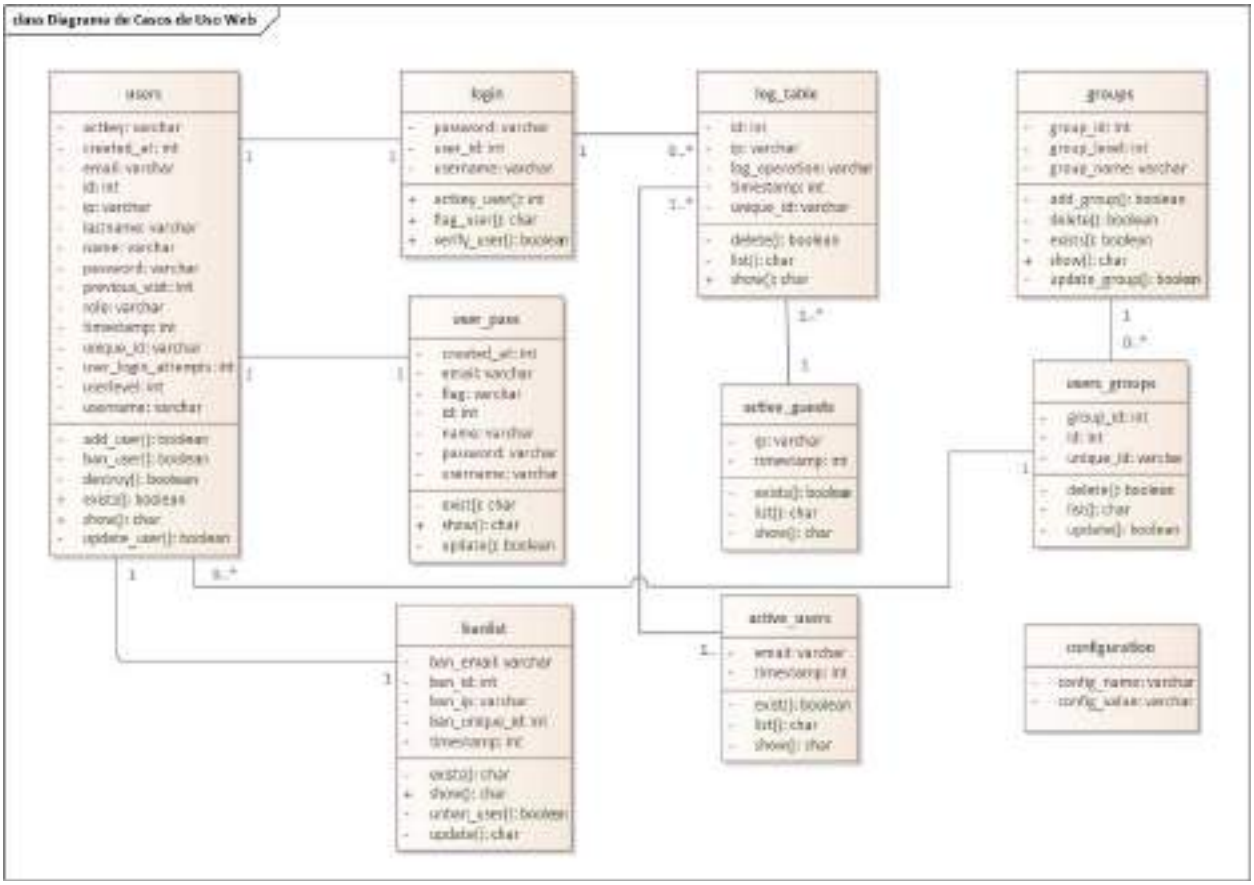


*Figura 2 – 116 Diagrama de Clases*

#### II.2.3.6.10.5 Diccionario de datos

##### II.2.3.6.10.5.1 Tabla: active_guests

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| ip | varchar(200) | NO | | SI | | IPs de los usuarios del servicio. |
| timestamp | int(11) | NO | | | | Tiempo de conexión. |

*Tabla 2 – 23 Diccionario de datos tabla: active_guests*

##### II.2.3.6.10.5.2 Tabla: active_users

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| email | varchar(30) | NO | | SI | | Correos de los usuarios del servicio. |
| timestamp | int(11) | NO | | | | Tiempo de conexión. |

*Tabla 2 – 24 Diccionario de datos tabla: active_users*

##### II.2.3.6.10.5.3 Tabla: banlist

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| ban_id | mediumint(8) | NO | SI | | auto_increment | Identificador ban |
| ban_email | varchar(255) | NO | | | | Correo baneado |
| ban_unique_id | varchar (32) | NO | | | | Identificador unico ban |
| ban_ip | varchar(200) | NO | | | | IPs baneadas |
| timestamp | int (11) | NO | | | | Tiempo de conexión. |

*Tabla 2 – 25 Diccionario de datos tabla: banlist*

#### II.2.3.6.10.5.4 Tabla: configuration

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| config_name | varchar(20) | NO | | | | Nombre de la configuración. |
| config_value | varchar(64) | NO | | | | Valor de la configuración. |

*Tabla 2 – 26 Diccionario de datos tabla: configuration*

#### II.2.3.6.10.5.5 Tabla: groups

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| group_id | smallint(5) | NO | SI | | auto_increment | Identificador ban. |
| group_name | varchar(50) | NO | | | | Correo baneado. |
| group_level | tinyint (3) | NO | | | | Identificador unico ban. |

*Tabla 2 – 27 Diccionario de datos tabla: groups*

#### II.2.3.6.10.5.6 Tabla: login

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| user_id | int(11) | NO | SI | | auto_increment | Identificador usuario. |
| username | varchar(30) | NO | | | | Nombre de usuario para inicio de sesión. |
| password | varchar(200 | NO | | | | Contraseña del usuario para el inicio de sesión. |

*Tabla 2 – 28 Diccionario de datos tabla: login*

#### II.2.3.6.10.5.7 Tabla: log_table

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| id | int(10) | NO | SI | | auto_increment | Identificador de los registros. |
| unique_id | varchar (32) | NO | | | | Identificador único de los registros. |
| timestamp | int(11) | NO | | | | Tiempo de conexión. |
| ip | varchar(200) | SI | | | | IPs de los usuarios del servicio. |
| log_operation | varchar(255) | SI | | | | Registros de operaciones de los usuarios. |

*Tabla 2 – 29 Diccionario de datos tabla: log_table*

#### II.2.3.6.10.5.8 Tabla: users

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| id | int(11) | NO | SI | | auto_increment | Identificador de los usuarios. |
| unique_id | varchar (32) | NO | | | | Identificador único de los usuarios. |
| name | varchar(50) | NO | | | | Nombre del Usuario. |
| email | varchar(100 | NO | | | | Correo del Usuario. |
| password | varchar(80) | NO | | | | Contraseña de Usuarios para inicio de sesión. |
| username | varchar(200) | NO | | | | Nombre de Usuarios. |
| role | varchar(200) | NO | | | | Rol de Usuarios. |
| lastname | varchar(200) | SI | | | | Apellidos de Usuarios. |

| | | | | | | |
|---|---|---|---|---|---|---|
| userlevel | tinyint(4) | SI | | | | Nivel de Usuarios |
| previous_visit | int(11) | SI | | | | Inicio de sesión previa. |
| timestamp | int(11) | SI | | | | Tiempo de Conexión. |
| actkey | varchar(200) | SI | | | | Código de autentificación inicio de sesión. |
| ip | varchar(200) | SI | | | | IPs de los usuarios. |
| user_login_attempts | tinyint(4) | SI | | | | Intento de inicio de sesión los Usuarios |
| created_at | int(11) | SI | | | | Fecha de Creación de Usuario. |

*Tabla 2 – 30 Diccionario de datos tabla: users*

### II.2.3.6.10.5.9 Tabla: users_groups

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| id | smallint(5) | NO | SI | | auto_increment | Identificador Usuario Grupo. |
| unique_id | varchar (32) | NO | | SI | | Identificador único Usuario. |
| group_id | smallint(6) | NO | | SI | | Identificador único Grupo. |

*Tabla 2 – 31 Diccionario de datos tabla: users_groups*

### II.2.3.6.10.5.10 Tabla: user_pass.

| Nombre | Tipo | Nulo | PK | FK | Extra | Descripción |
|---|---|---|---|---|---|---|
| id | int(11) | NO | SI | | auto_increment | Identificador usuarios contraseñas. |
| username | varchar (32) | NO | | | | Nombre de Usuario inicio de sesión. |
| password | varchar (32) | NO | | | | Contraseña Usuario para inicio de session. |
| flag | varchar (32) | SI | | | | Mensajes de consideración. |
| name | varchar(50) | SI | | | | Nombre de Usuario. |
| email | varchar(255) | NO | | | | Correo de Usuario. |
| created_at | timestamp | NO | | | | Tiempo de creación. |

*Tabla 2 – 32 Diccionario de datos tabla: users_groups*

### II.2.3.6.11 Prototipo de interfaces de pantalla

#### II.2.3.6.11.1 Introducción

Se trata de prototipos que permiten al usuario hacerse una idea más o menos precisa de las interfaces que proveerá el sistema y así, conseguir retroalimentación de su parte respecto a los requisitos del sistema.

Estos prototipos se realizarán como: dibujos a mano en papel dibujos con alguna herramienta grafica o prototipos ejecutables interactivos, siguiendo ese orden de acuerdo al avance del proyecto. Solo los de este último tipo serán entregados al final de la fase de Elaboración, los otros serán desechados en la fase de Construcción en la medida que el resultado de las iteraciones vaya desarrollando el producto final.

#### II.2.3.6.11.2 Propósito

- Comprender la idea de cómo será el sistema más adelante.
- Identificar posibles mejoras.

#### II.2.3.6.11.3 Alcance

- Describir las pantallas para conocer su navegación.
- Identificar y definir las Pantallas del sistema según los objetivos del sistema deseado y aprobado por la organización.

### II.2.3.6.11.4 Pantalla (Ingreso)

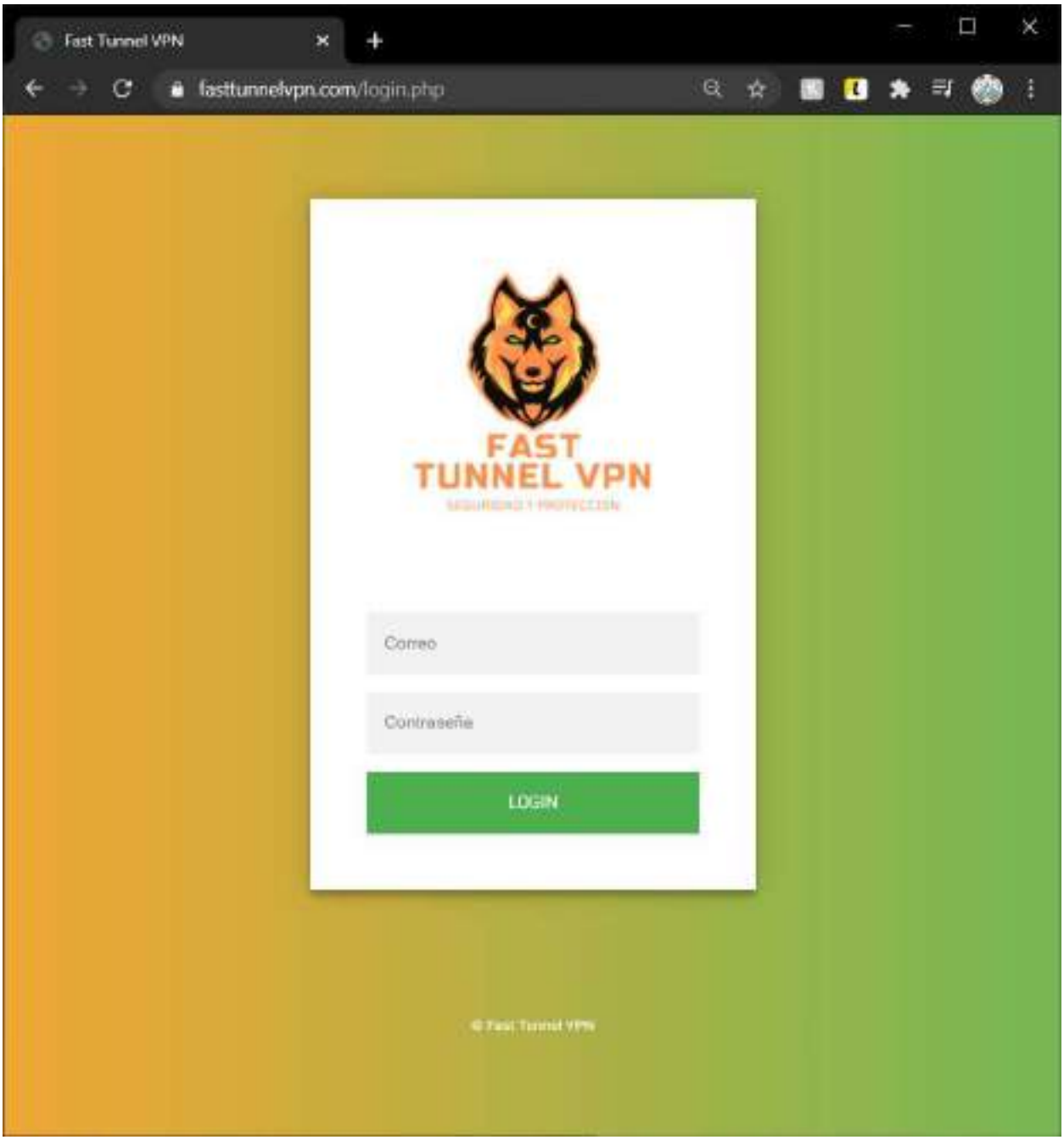


*Figura 2 – 118 Pantalla de Inicio*

### II.2.3.6.11.5 Pantalla (Panel de Control)

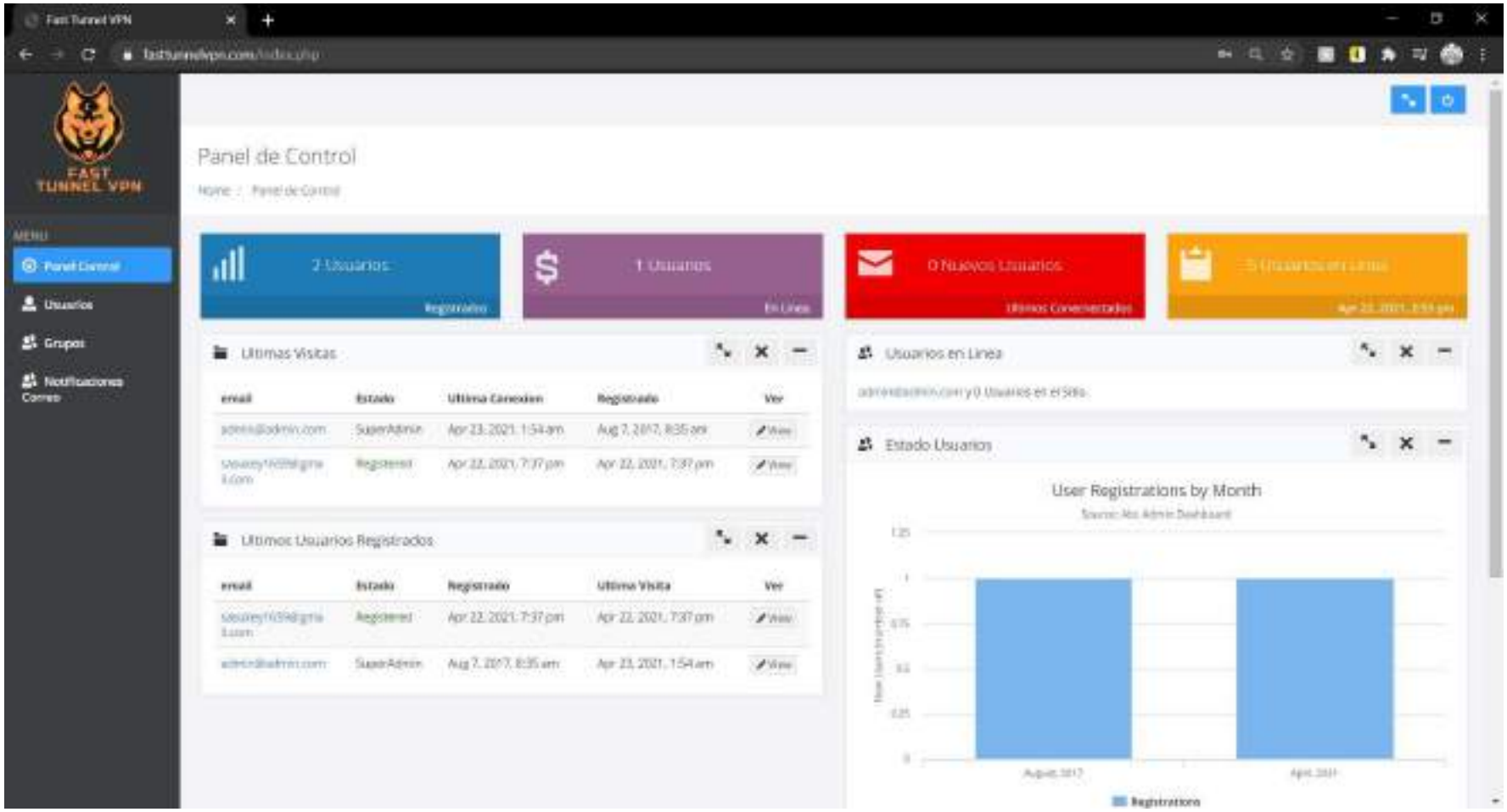


*Figura 2 – 119 Pantalla Panel de Control*

### II.2.3.6.11.6 Pantalla (Usuarios)

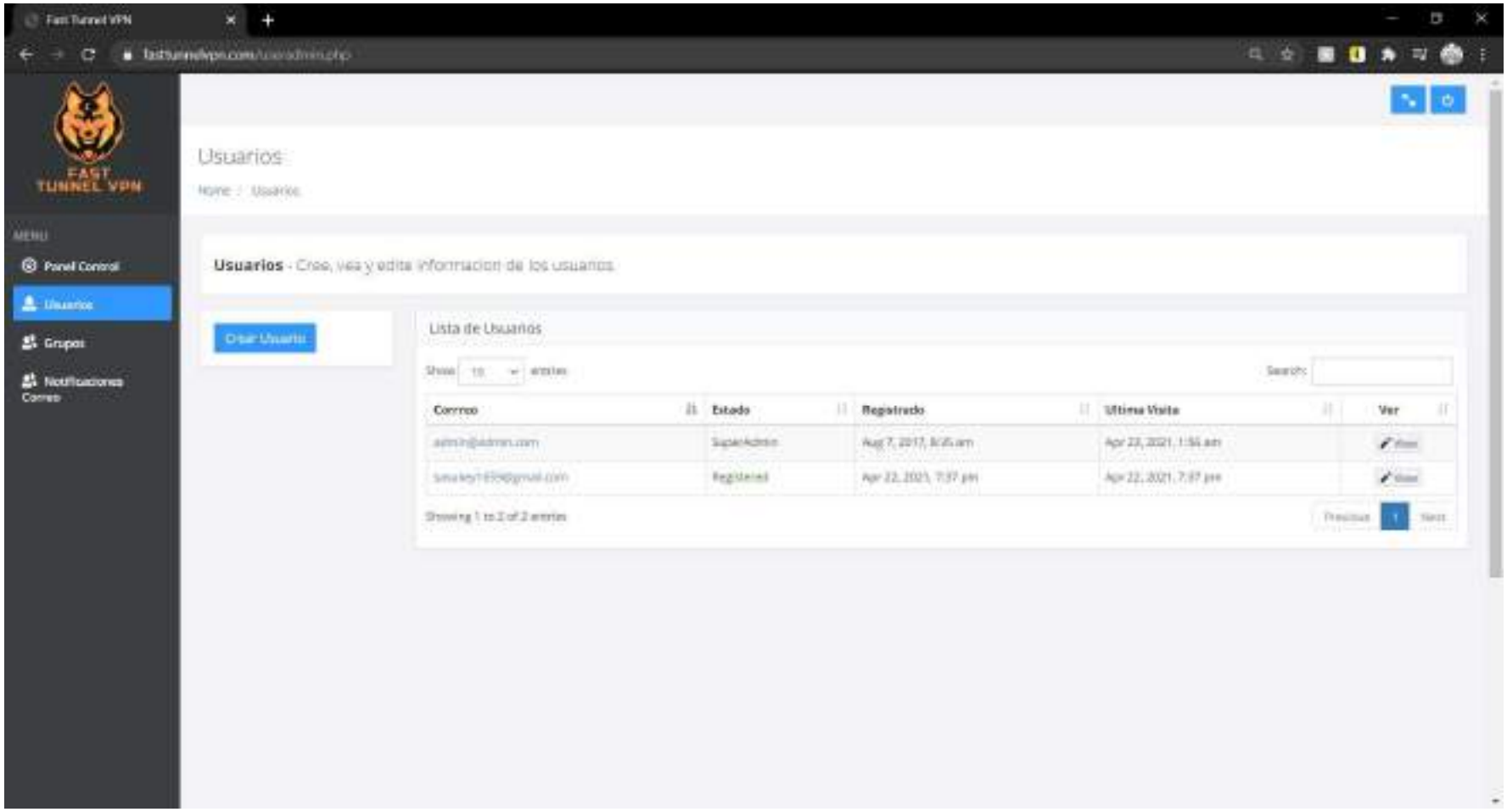


*Figura 2 – 120 Pantalla Usuarios*

### II.2.3.6.11.7 Pantalla (Crear Usuario)

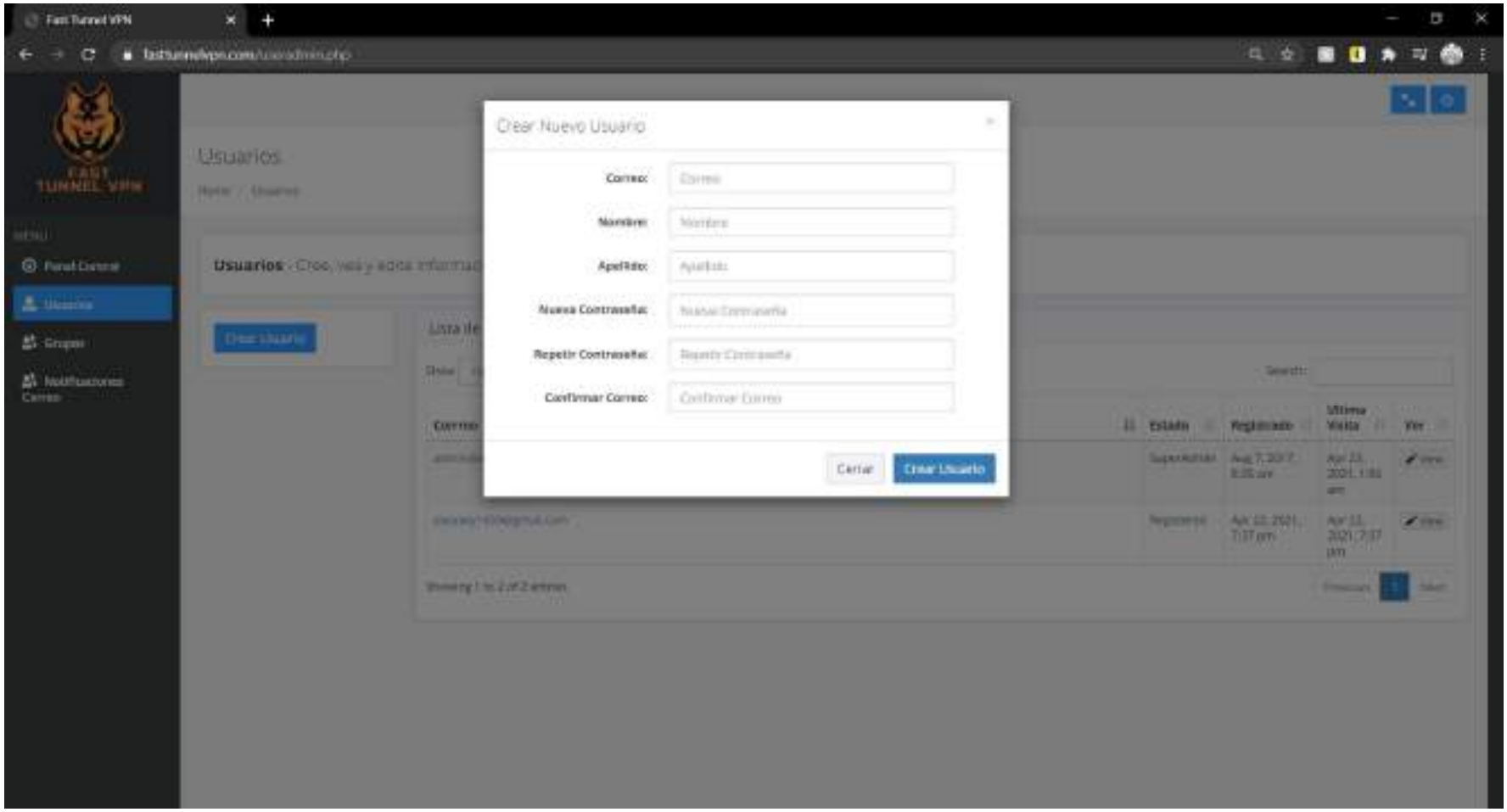


*Figura 2 – 121 Pantalla Crear Usuario*

### II.2.3.6.11.8 Pantalla (Usuario Información)

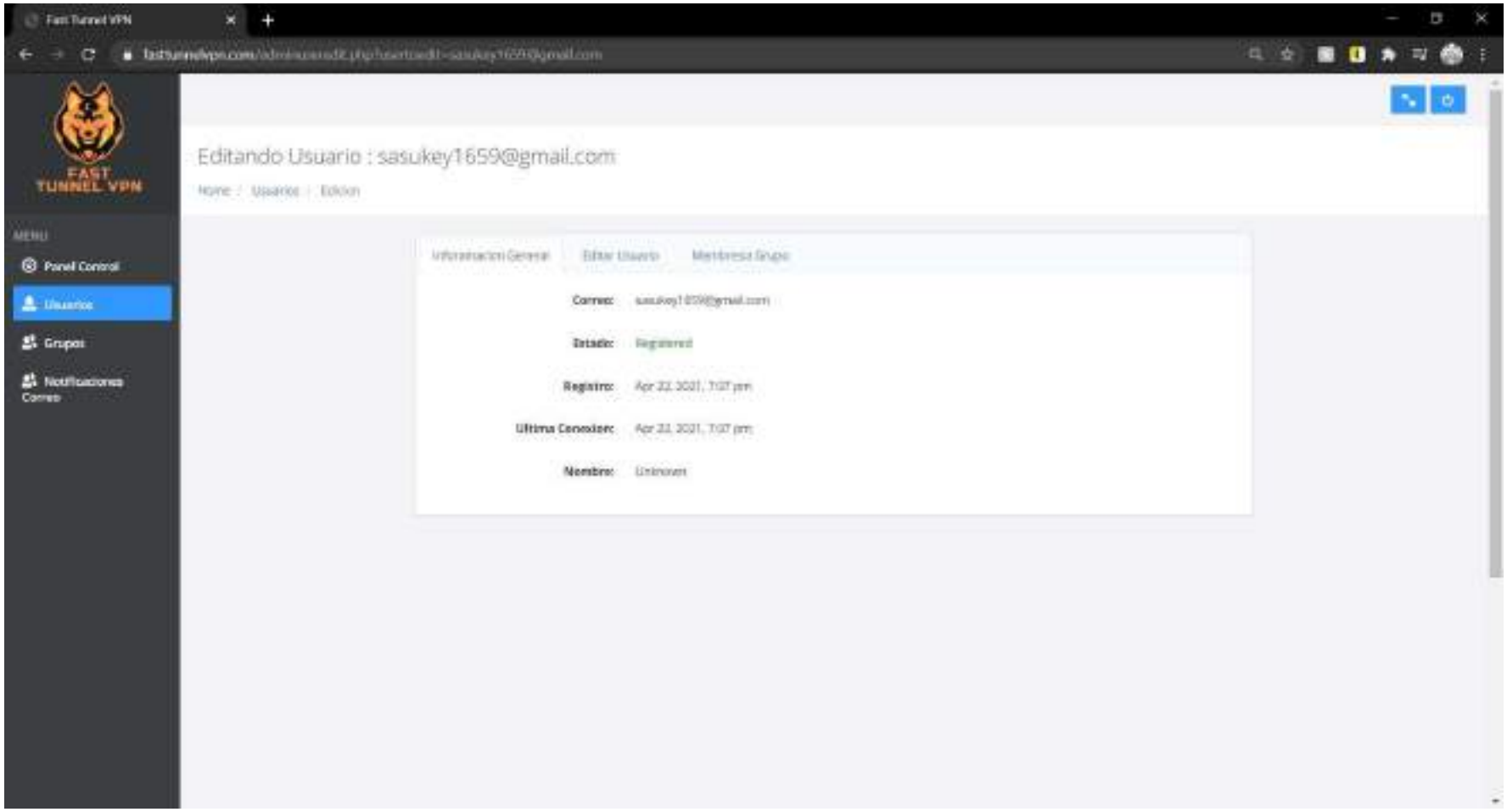


*Figura 2 – 122 Pantalla Usuario Información*

### II.2.3.6.11.9 Pantalla (Modificar Usuario)

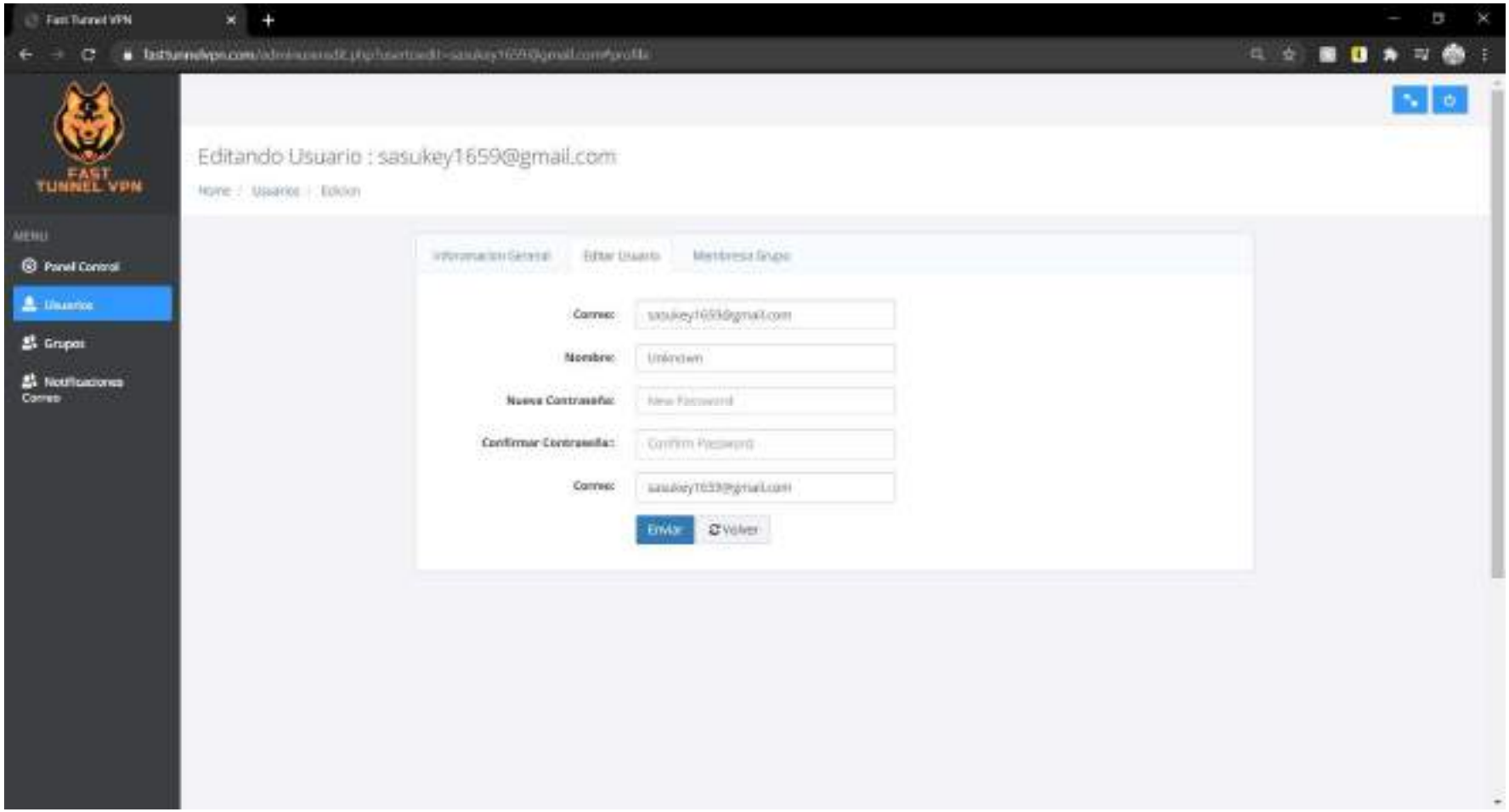


*Figura 2 – 123 Pantalla Modificar Usuario*

### II.2.3.6.11.10 Pantalla (Modificar Usuario Membresía)

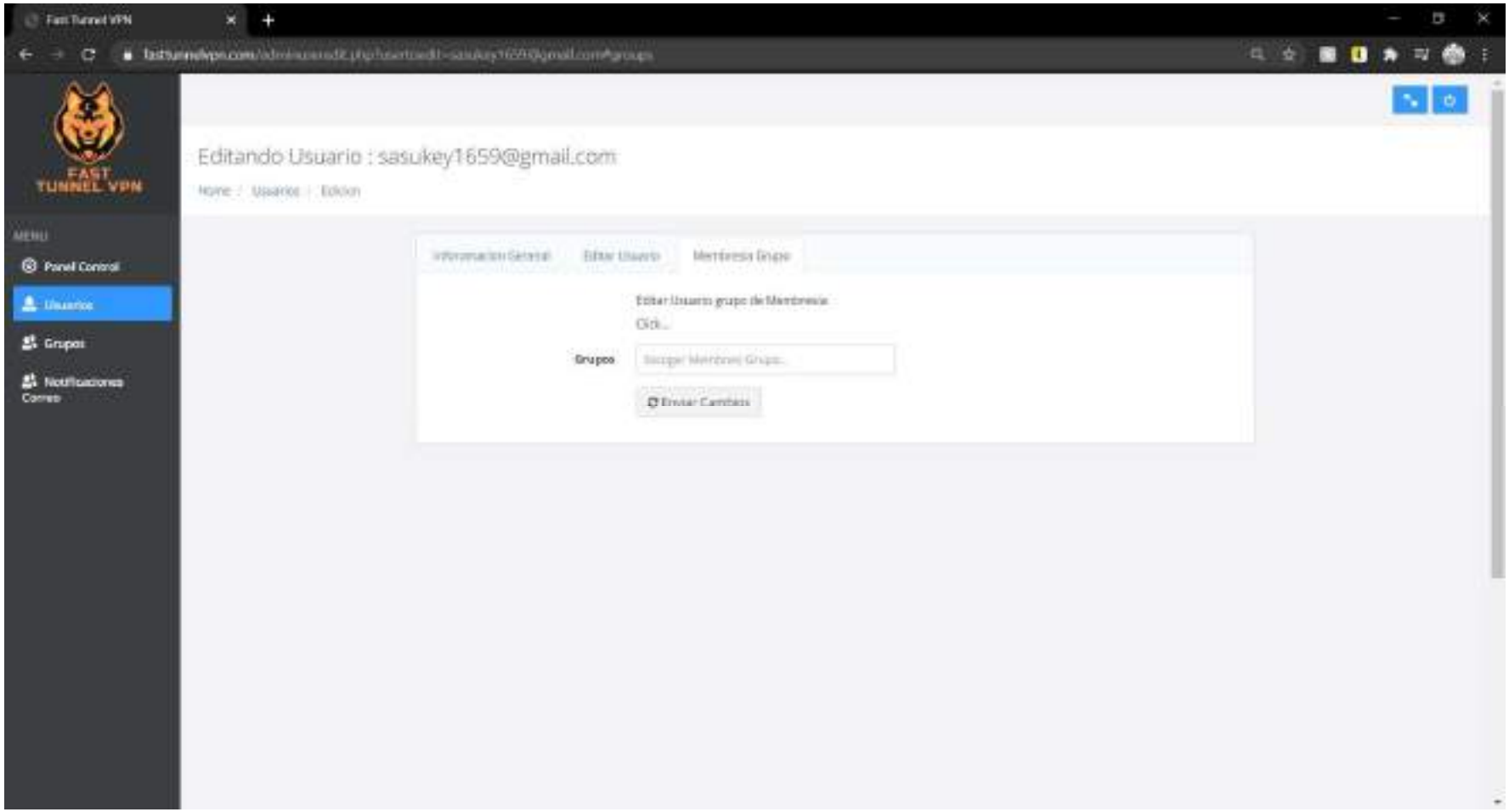


*Figura 2 – 124 Pantalla Modificar Usuario Membresía*

### II.2.3.6.11.11 Pantalla (Grupos)

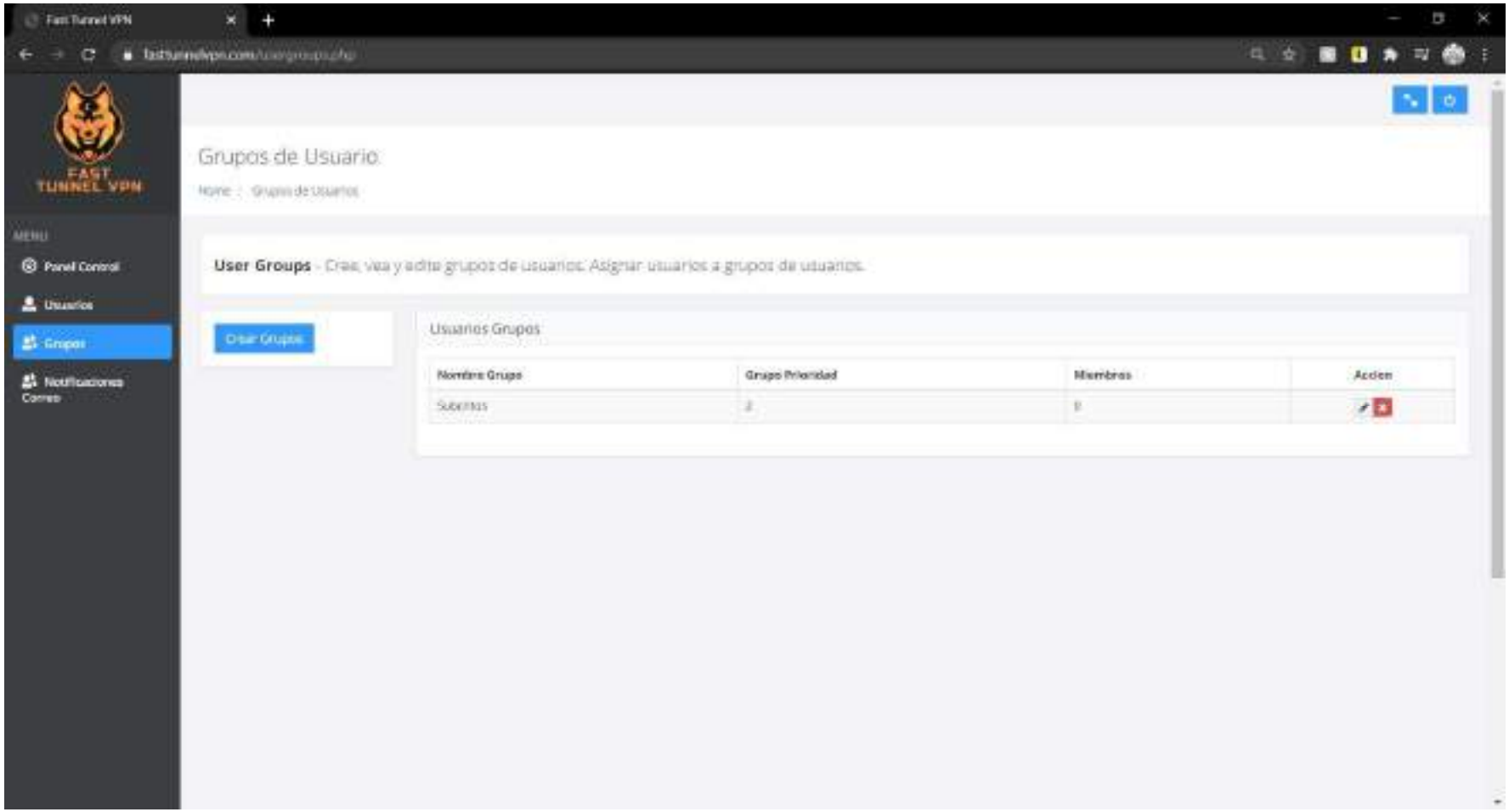


*Figura 2 – 125 Pantalla Grupos*

### II.2.3.6.11.12 Pantalla (Crear Grupo)

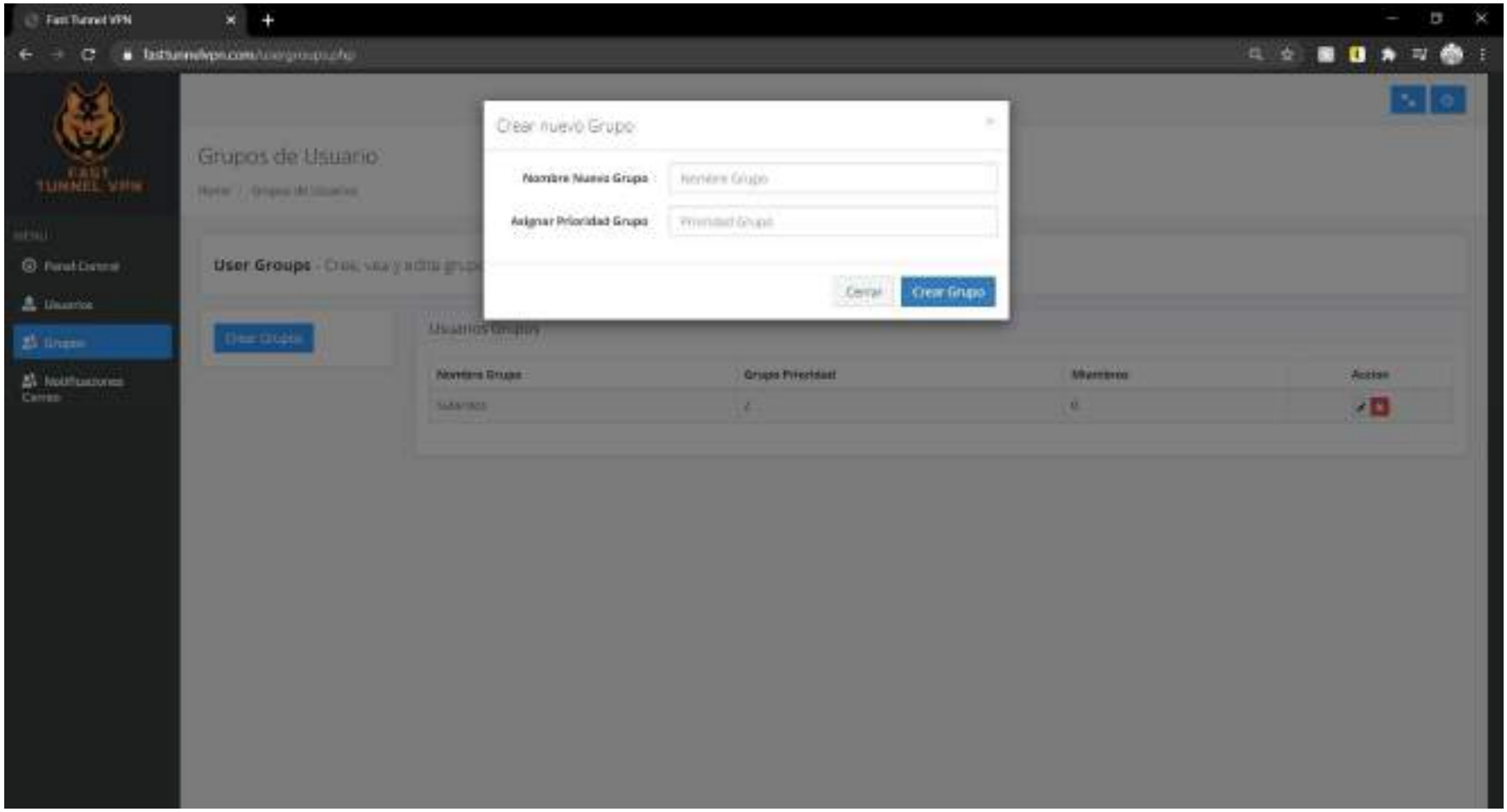


*Figura 2 – 126 Pantalla Crear Grupo*

### II.2.3.6.11.13 Pantalla (Modificar Grupo)

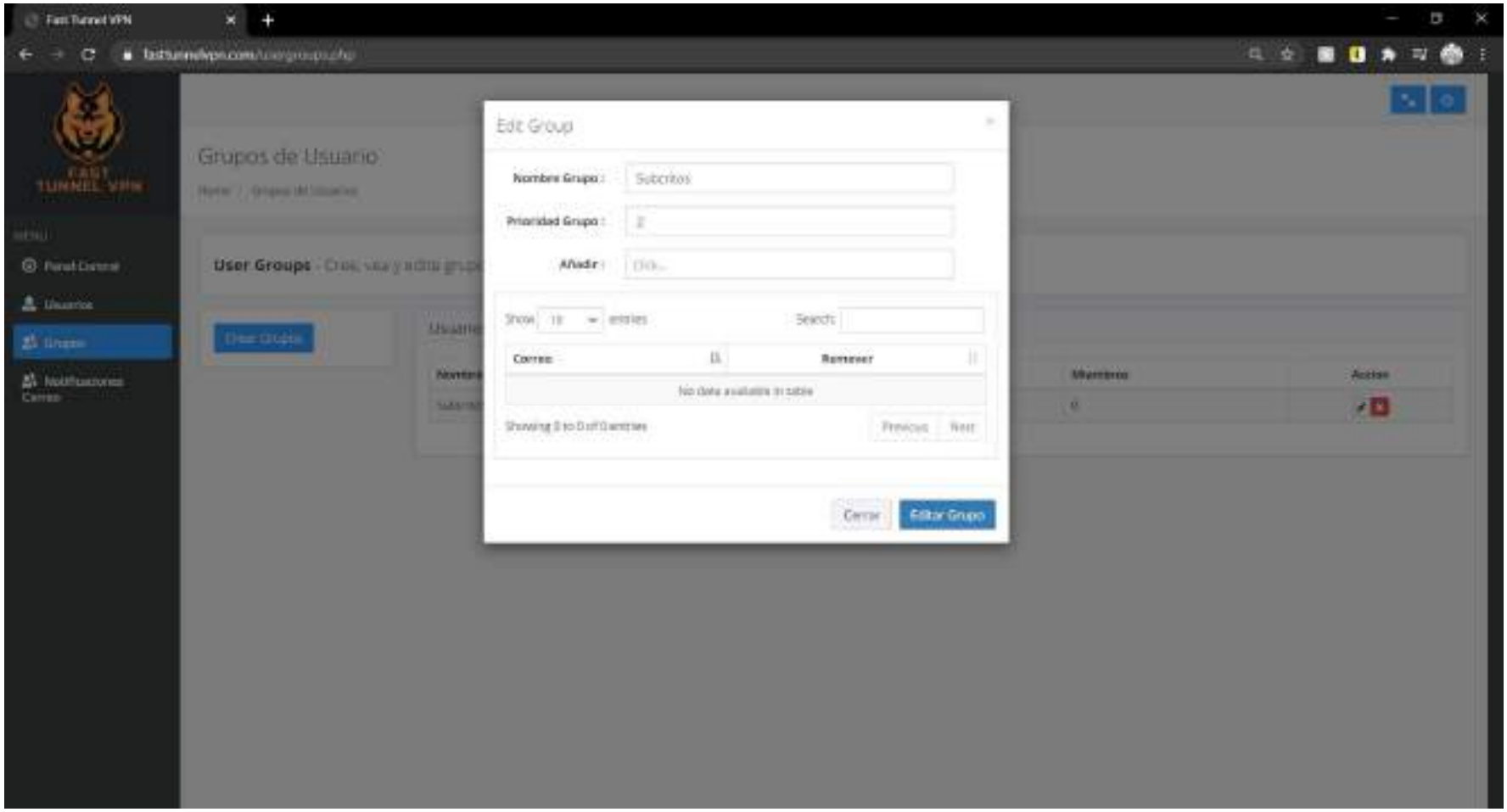


*Figura 2 – 127 Pantalla Modificar Grupo*

### II.2.3.6.11.14 Pantalla (Notificaciones)

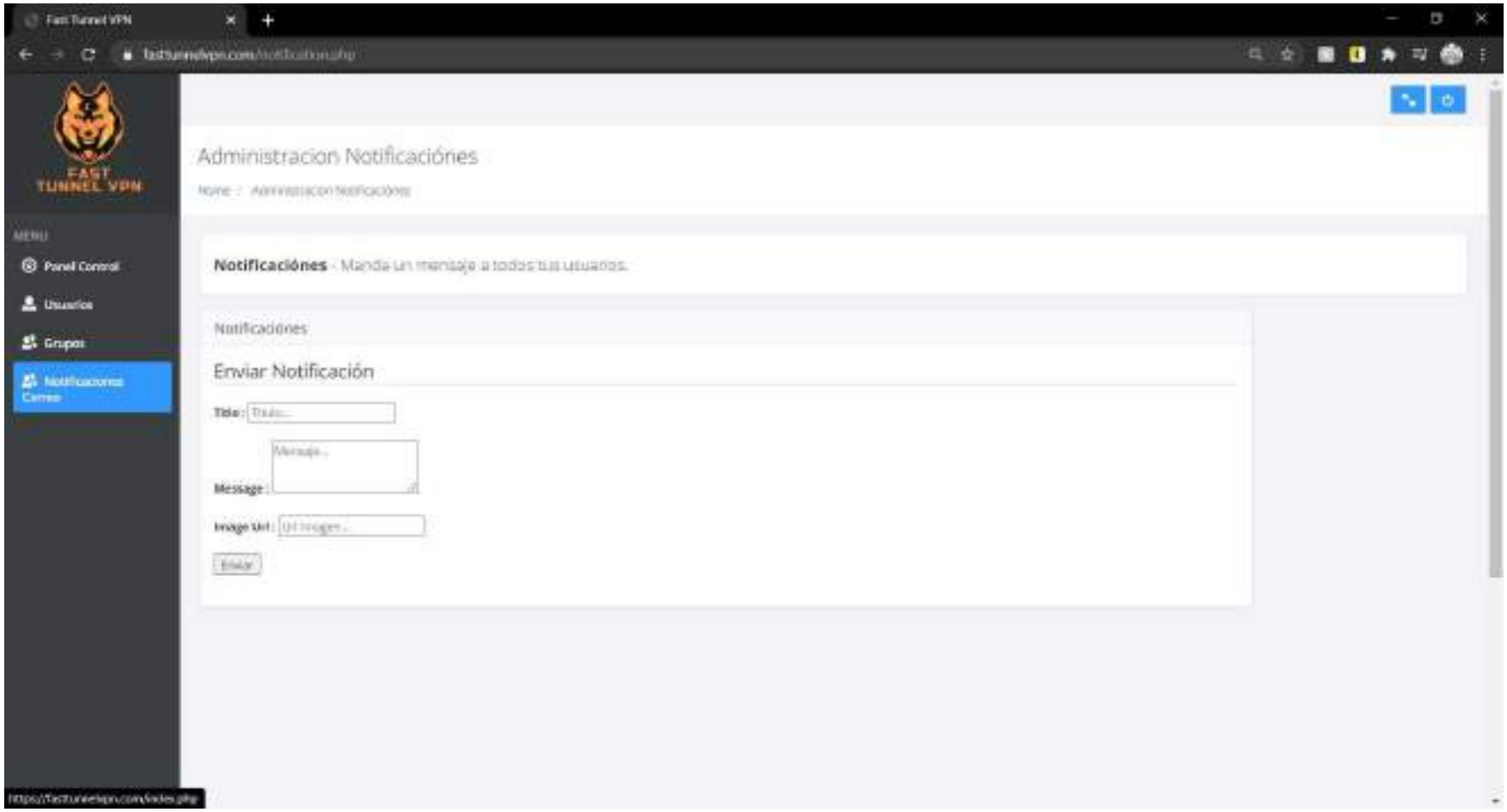


*Figura 2 – 128 Pantalla Notificaciones*

### II.2.3.6.11.15 Pantalla (Solicitudes Mensaje)

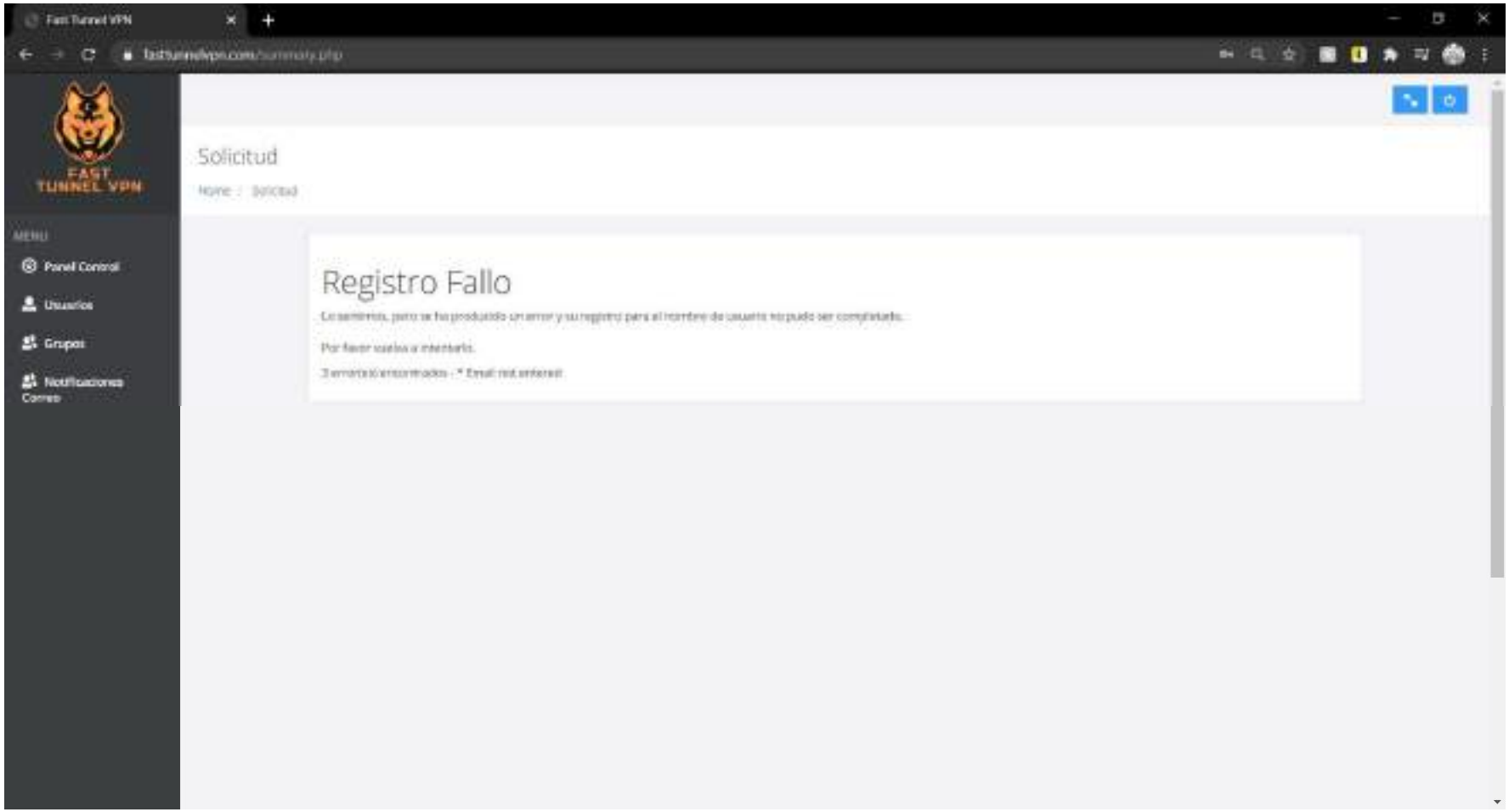


*Figura 2 – 129 Pantalla Solicitudes Mensaje*

### II.2.4 Medios de verificación (Componente 2)

#### II.2.4.1 Seguridad Web

#### II.2.4.2 Certificación SSL

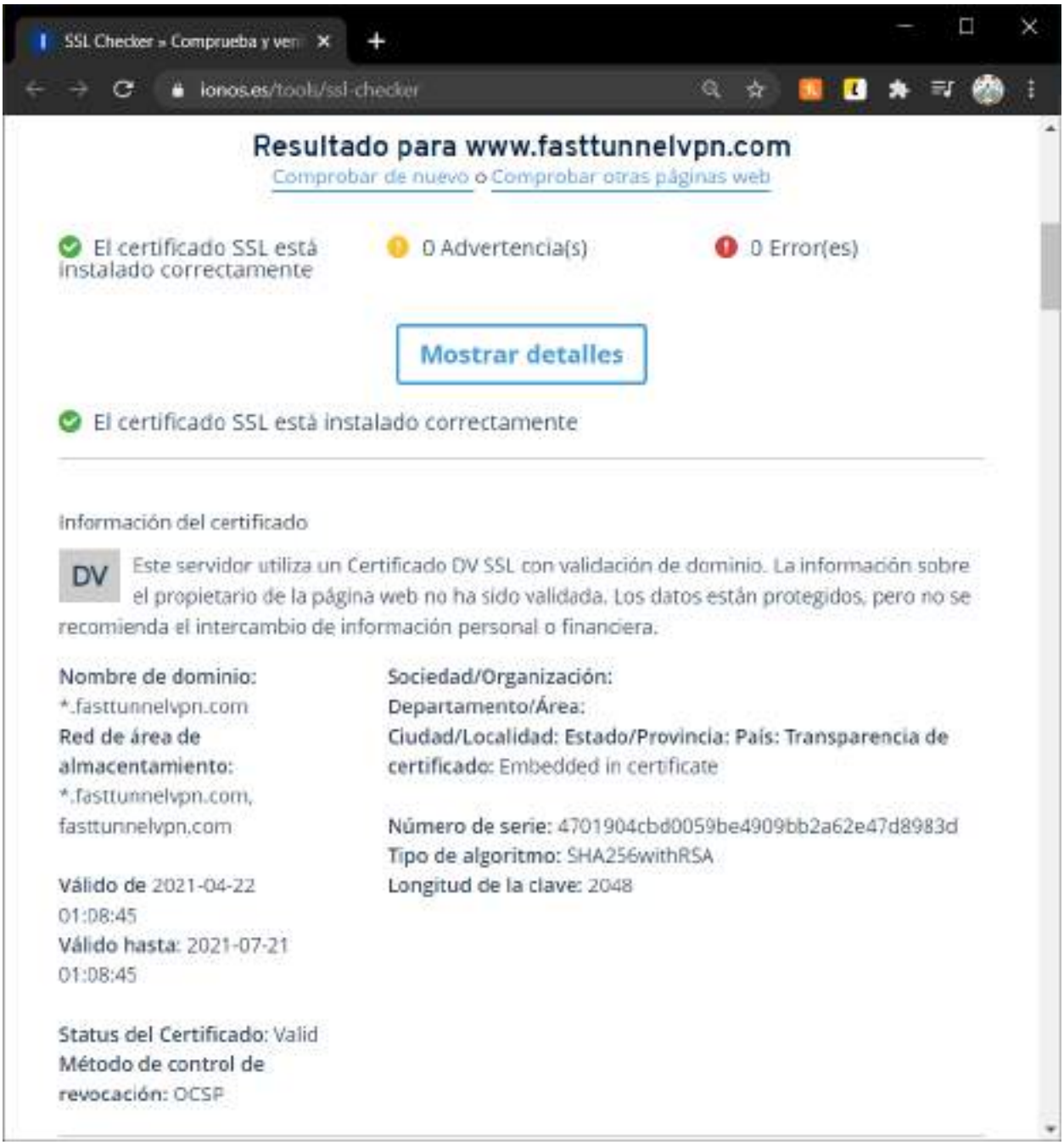


*Figura 2 – 130 Verificación Certificado SSL ionos.es certificado*

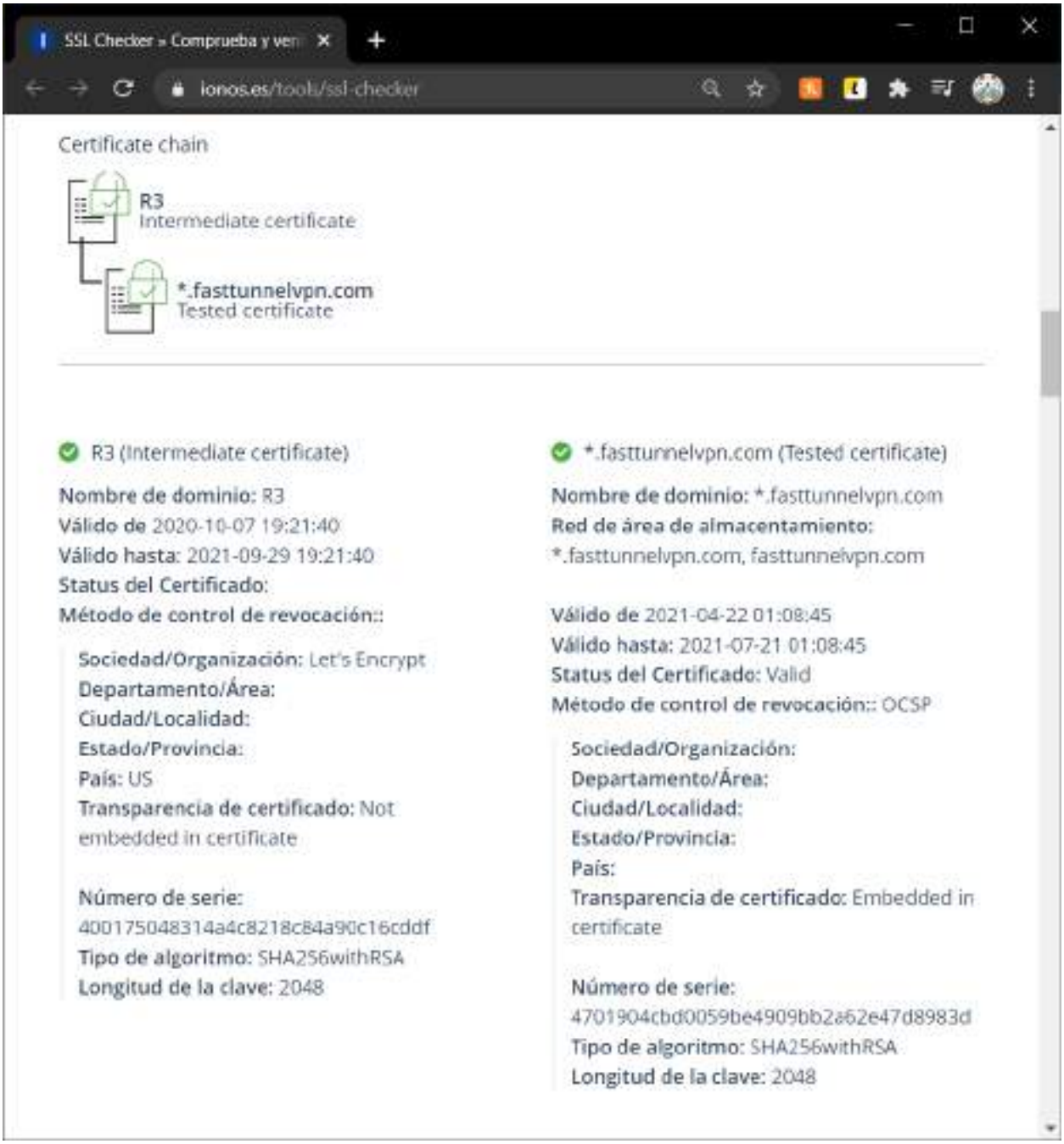


*Figura 2 – 131 Verificación Certificado SSL ionos.es credenciales*

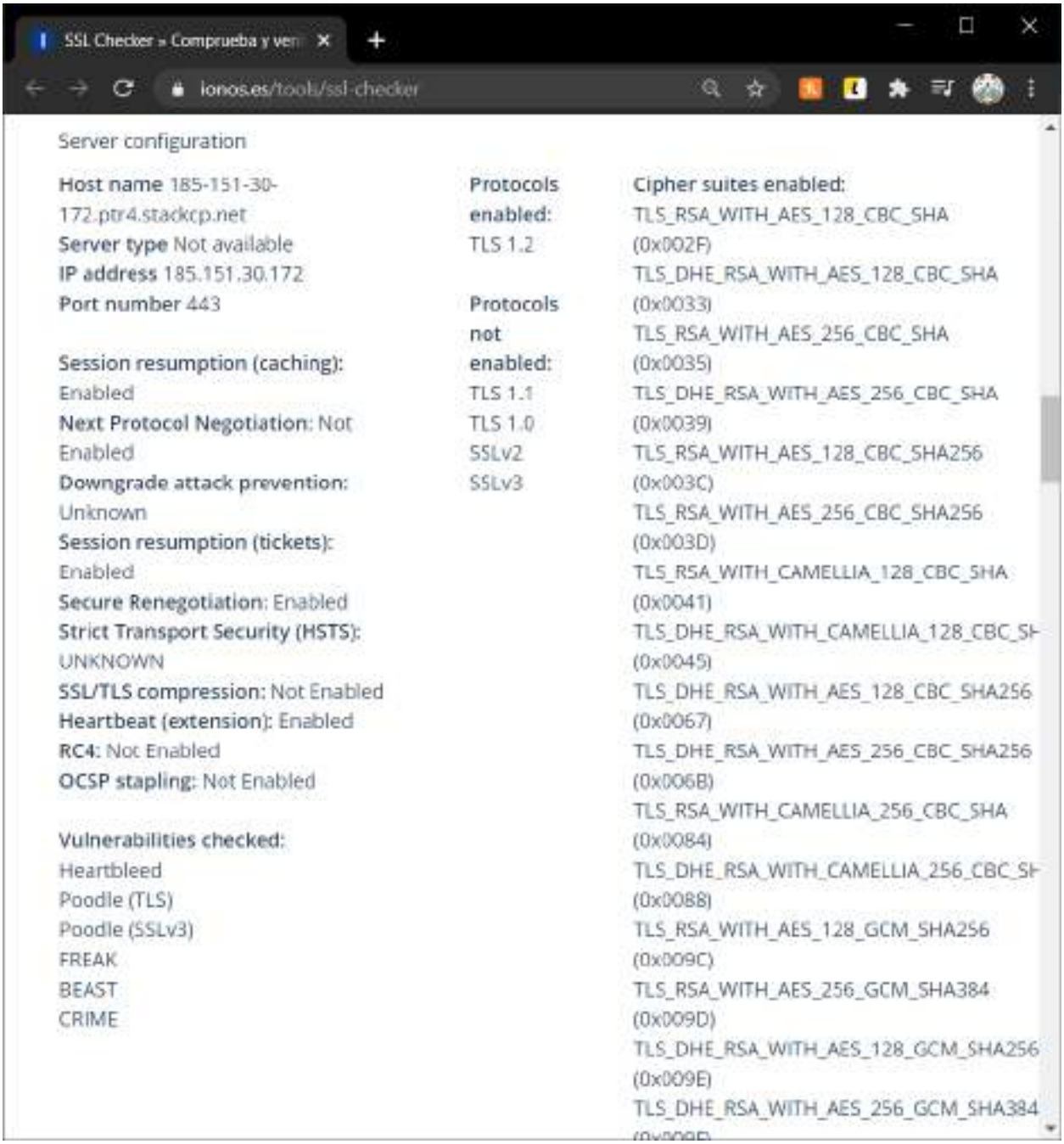


*Figura 2 – 132 Verificación Certificado SSL ionos.es servidor*

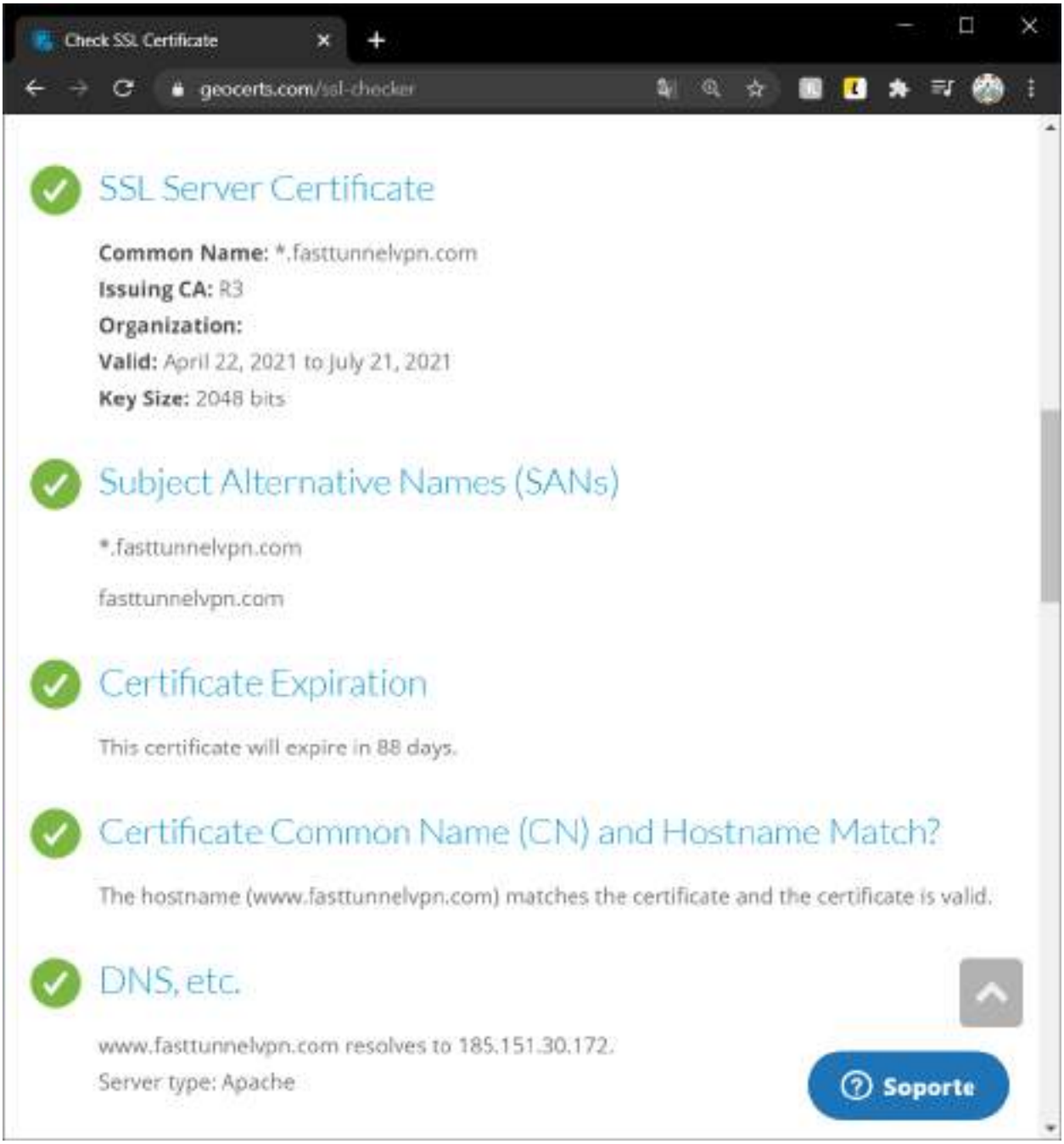


*Figura 2 – 133 Verificación Certificado SSL geocerts.com servidor*

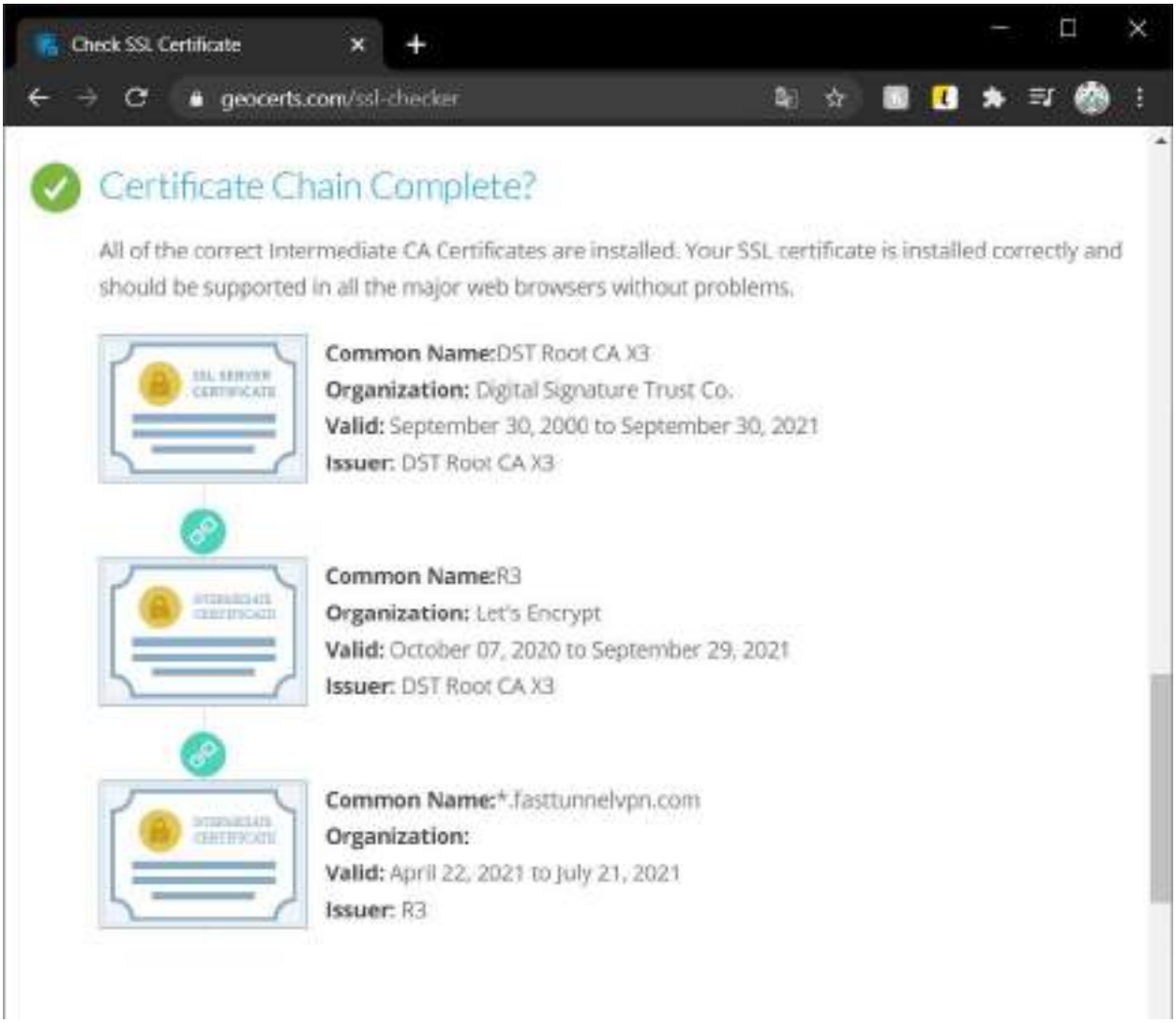


*Figura 2 – 134 Verificación Certificado SSL geocerts.com certificados*

### II.2.4.3 Sistema Web Vulnerabilidades

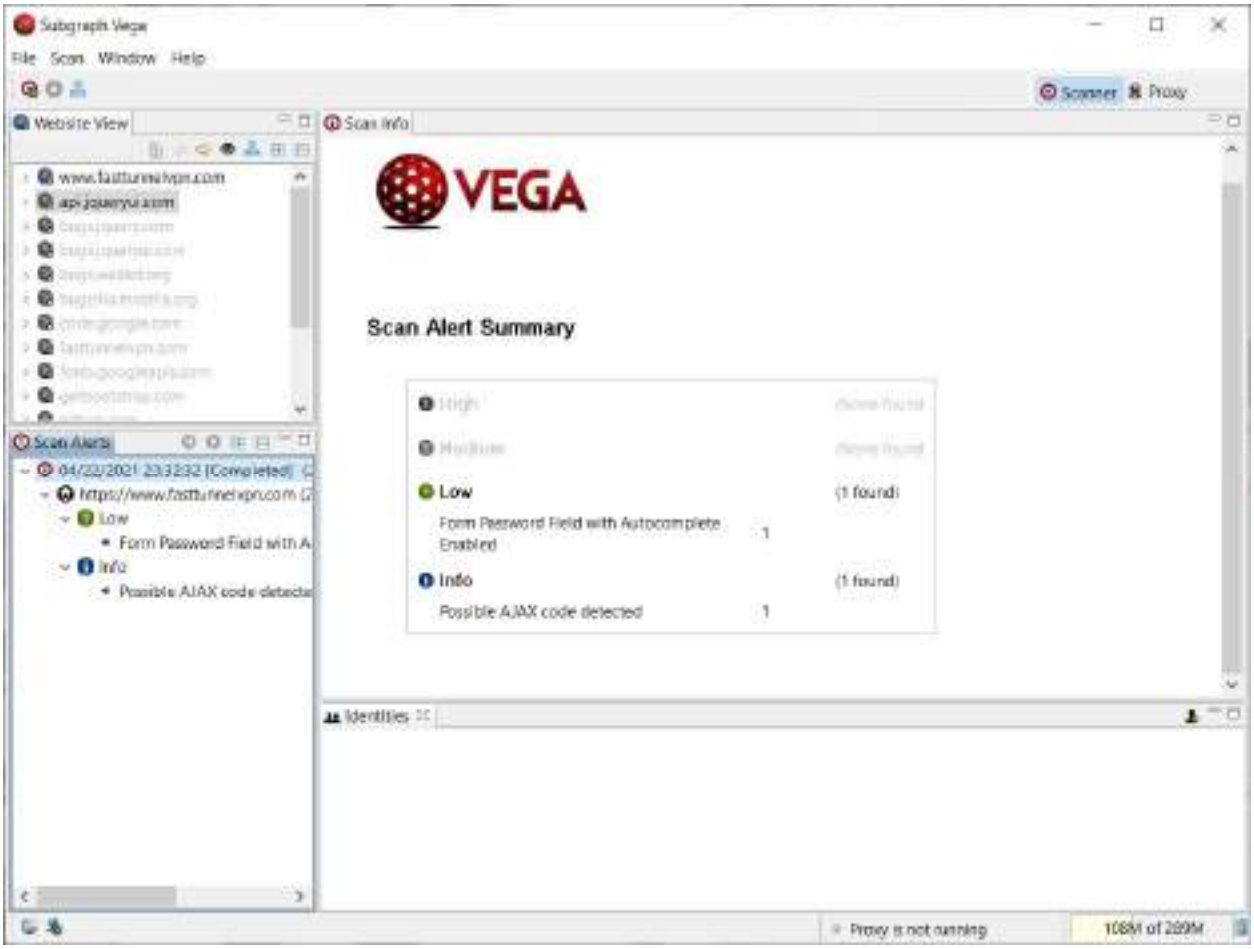


*Figura 2 – 135 Verificación Vulnerabilidades Sistema Web Vega Resumen*

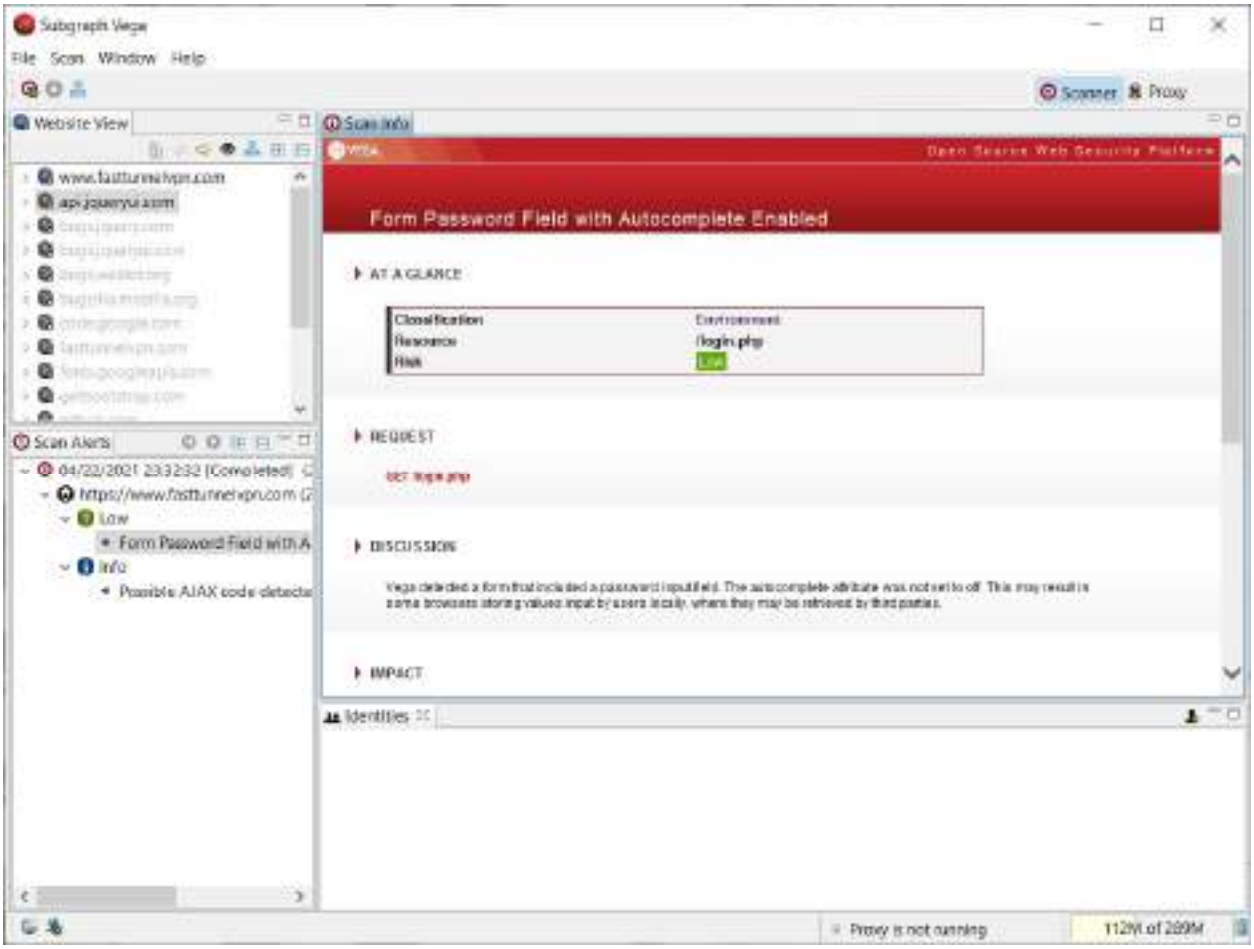


*Figura 2 – 136 Verificación Vulnerabilidades Sistema Web Vega low*

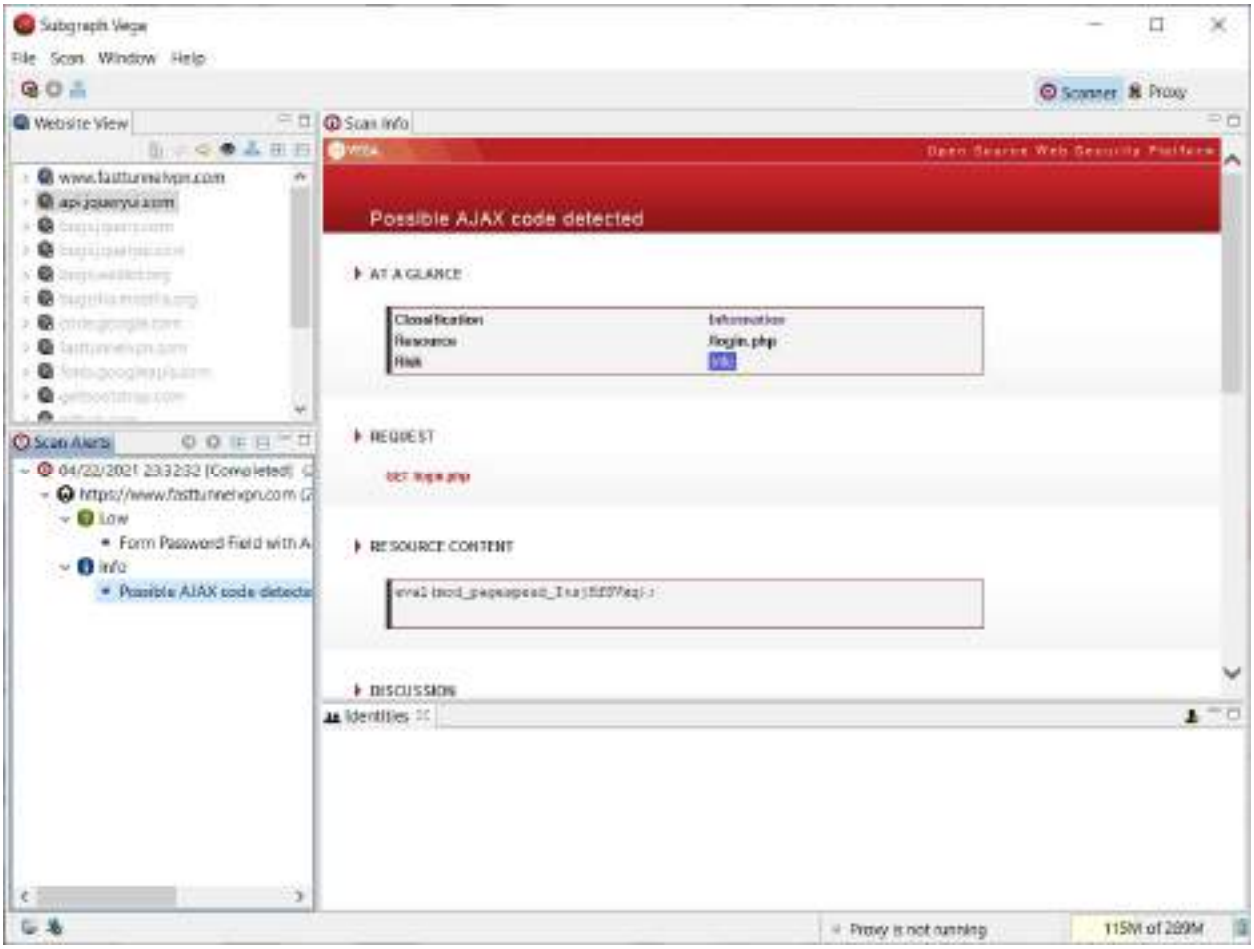


*Figura 2 – 137 Verificación Vulnerabilidades Sistema Web Vega Info*

## II.3 Componente 3: Aplicación móvil Android

Aplicación que gestionará la conexión a la red privada virtual y permitirá a los usuarios escoger el servidor en el país de su preferencia previo inicio de sesión dentro de la aplicación. Esta estará construida en la versión más usada de Android por temas de compatibilidad.

### II.3.1 Marco Teórico

#### II.3.1.1 Aplicaciones móviles

Una aplicación móvil es un software desarrollado con características diferentes que cumplen con los objetivos por los que fueron creados y éstas son específicamente para dispositivos móviles, por ejemplo: smartphone, Tablet, mp3, etc.

##### II.3.1.1.1 Tipos de aplicación móvil

###### II.3.1.1.1.1 Aplicaciones Nativas

Una aplicación nativa es aquella que se puede descargar desde la tienda de acuerdo al sistema operativo, por lo que de inmediato se lo podrá utilizar sin la necesidad de tener acceso a internet porque ya se encuentra instalado en el dispositivo móvil. Es por eso que cuando exista una nueva versión de dicha aplicación nuevamente tendrá que descargarla e instalarla en el dispositivo.

La ventaja de este tipo de aplicaciones es que sin necesidad de internet se obtendrán notificaciones que emitan las aplicaciones y tiene la posibilidad de acceder a todos las opciones que le ofrece el dispositivo como, por ejemplo: la cámara, GPS, etc.

###### II.3.1.1.1.2 Aplicaciones Web

Una aplicación web es aquella que se la desarrolla utilizando código HTML, JavaScript y CSS, por lo que éstas pueden ser utilizadas en varias plataformas. Para tener el acceso a este tipo de aplicación se debe ingresar por medio de un navegador web y no necesita ser instalada, para lo cual necesita de que siempre esté conectado a internet.

La ventaja principal de las aplicaciones Web es que el usuario final siempre contará con la última versión.

#### II.3.1.1.1.3 Aplicaciones Híbridas

Este tipo de aplicación combina tanto el tipo de aplicación nativa como la aplicación web, que a la vez se la puede utilizar como una aplicación nativa, con la ventaja de que con el mismo código se obtenga aplicaciones en diferentes plataformas. Para su desarrollo se puede utilizar Apache Cordova, Icenium, PhoneGap, etc.

La ventaja de utilizar una aplicación híbrida es que se la puede publicar tanto en la tienda de Android como en la de iOS.

| | **Aplicación Nativa** | **Aplicación Web** | **Aplicación Híbrida** |
|---|---|---|---|
| **Uso de internet** | No | Si | Si |
| **Actualización** | Necesita actualizarse | Actualización Automática | Actualización Automática |
| **Manera de utilización** | Se debe descargar desde la tienda. | Necesitan de un navegador web. | Es una combinación de la aplicación nativa y aplicación web. |
| **Ventaja principal** | Se puede descargar fácilmente y utilizarlo sin necesidad de internet. | El código de una aplicación puede ser implementada en otras plataformas. | Permite la distribución a través de las tiendas de su respectiva plataforma. |
| **Desventaja** | Una misma aplicación no puede ser utilizada en todas las plataformas. Necesitar ser desarrollada una por cada plataforma | Requiere siempre la conexión a internet. | El diseño visual de la aplicación no se lo representa con la de su sistema operativo. |

*Tabla 2 – 33 Tipos de Aplicaciones*

### II.3.1.2 Tecnologías y plataformas

#### II.3.1.2.1 Android Studio

Es un IDE (Integrated Development Environment) que se basa en IntelliJ, con su nuevo sistema de construcción basado en Gradle, el mismo que es una interfaz de usuario gráfica y de texto para diseñar el entorno gráfico de la aplicación.

#### II.3.1.2.2 SDK Android

Es un paquete el cual contiene todas las herramientas necesarias para la creación de una aplicación en Android, este paquete está disponible para Windows, Mac OS y Linux. Además, permite crear y gestionar los emuladores.

Características:

- Ofrece un sistema de compilación basado en Gradle flexible.
- Presenta un emulador gráfico con todas las características a un dispositivo móvil real.
- Muestra un entorno consolidado en el que se puede desarrollar código para todos los dispositivos Android.
- Tiene un Instant Run que sirve para aplicar cambios mientras la aplicación se está ejecutando y no existiría la necesidad de compilar nuevamente un APK.
- Integra plantillas de código y GitHub para ayudar a compilar funciones comunes de las apps e importar ejemplos de código.
- Ofrece una gran cantidad de herramientas y frameworks de prueba.
- Utiliza herramientas Lint para detectar problemas de rendimiento, usabilidad, compatibilidad de versión, etc.
- Es compatible con C++ y NDK
- Viene con soporte incorporado para Google Cloud Platform, lo que facilita la integración de Google Cloud Messaging y App Engine.

#### II.3.1.2.3 Estructura de un proyecto

Los proyectos en Android Studio contienen uno o más módulos con archivos de código fuente y archivos de recursos, el número de módulos dependerán de acuerdo a como se vaya creciendo el proyecto desarrollado. Entre los tipos de módulos se incluyen los siguientes:

- Módulos de apps para Android
- Módulos de bibliotecas
- Módulos de Google App Engine

Por cada módulo que se vaya añadiendo en la aplicación contiene las siguientes carpetas:

- manifest: Contiene el archivo AndroidManifest.xml.
- java: Contiene los archivos de código fuente Java.
- res: Contiene todos los recursos, como diseños XML, cadenas de IU e imágenes de mapa de bits.

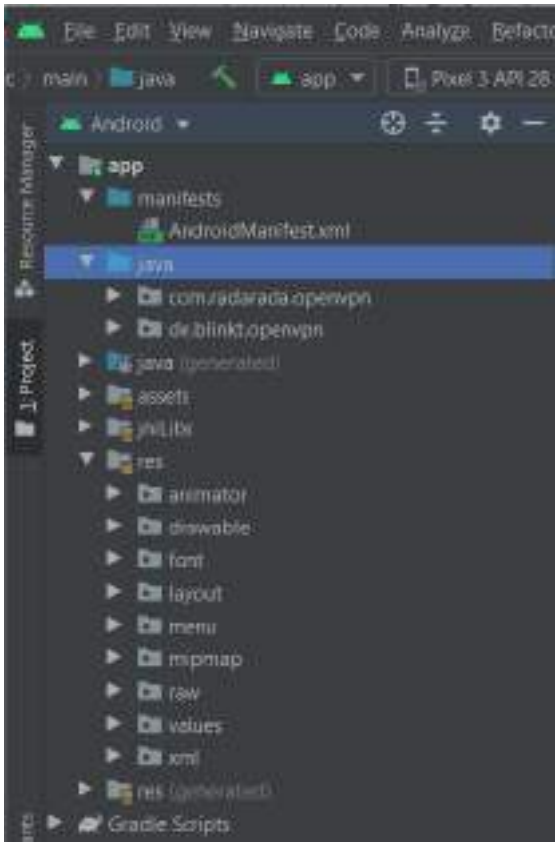


*Figura 2 – 138 Estructura de una aplicación*

#### II.3.1.2.4 Emulador

El emulador dentro de Android Studio es una herramienta que simula el funcionamiento con todas las características de un teléfono o Tablet con sistema operativo Android. No solo se puede simular un tipo de emulador, sino que también puede simular varios teléfonos a la vez con características diferentes ya sea tanto de acuerdo a la resolución de la pantalla, tamaño de la memoria y entre otros.

#### II.3.1.2.5 Arquitectura Android

La arquitectura tiene como objetivo controlar los recursos y el consumo de las aplicaciones, y consta de las siguientes partes:

- **Aplicación:** Representa el conjunto de aplicaciones proporcionadas con Android.
- **Framework Android:** Representa el framework que permite a los desarrolladores crear aplicaciones accediendo al conjunto de API y funcionalidades disponibles en el dispositivo móvil.

- **Librerías:** Android dispone de un conjunto de librerías que utilizan los distintos componentes del sistema.
- **Android Runtime:** contiene entro otros, la máquina virtual ART.

#### II.3.1.3 Componentes Android

Dentro del framework de Android se encuentra con los siguientes elementos principales para la creación de una aplicación: Actividad, fragmento, servicio, receptor de eventos y proveedor de contenido.

##### II.3.1.3.1 Actividad (Activity)

Una actividad está enfocada en interactuar directamente con el usuario. Es el lugar en donde se puede crear la interfaz de usuario.

##### II.3.1.3.2 Fragmento (Fragment)

Permite crear interfaces de usuario más sofisticadas para pantallas grandes y ayuda a escalar su aplicación entre pantallas pequeñas y grandes.

##### II.3.1.3.3 Servicio (Service)

Un servicio permite la ejecución de un tratamiento en segundo plano, teniendo en cuenta que no tiene interfaz. Y para que se detenga un servicio se debe interrumpir o enviar alguna instrucción para que termine.

##### II.3.1.3.4 Receptor de eventos (Broadcast receiver)

Es otro componente que no tiene interfaz de usuario y reacciona con un evento de sistema. Puesto que no trabaja con interfaces solo permite mostrar una notificación, iniciar una actividad o servicio.

##### II.3.1.3.5 Proveedor de contenido (content provider)

Este tipo de componente permite compartir los datos de una aplicación. Y Android ofrece proveedores de contenido disponibles por defecto tales como: Contactos, agenda, multimedia, etc.

##### II.3.1.3.6 Ciclo de Vida de Android

Las actividades del sistema en Android se gestionan como una pila de actividades. Cuando se inicia una nueva actividad, se coloca en la parte superior de la pila y se convierte en la actividad en ejecución y la actividad anterior permanece siempre debajo de la actividad que se encuentra en la parte superior de la pila y no volverá a primer plano hasta que se cierre la nueva actividad.

### II.3.1.3.6.1 Estados de una actividad

De acuerdo al Institut Puig Castellar una actividad cuenta con los siguientes estados:

Si una actividad está en el primer plano de la pantalla (en la parte superior de la pila), está activa o en ejecución.

Si una actividad ha perdido el enfoque, pero sigue siendo visible (es decir, una actividad nueva o no transparente se centra en la parte superior de su actividad), se detiene. Una actividad en pausa está completamente viva (mantiene toda la información de estado y de miembro y permanece unida al administrador de ventanas), pero puede ser eliminada por el sistema en situaciones de baja memoria extrema.

Si una actividad es completamente oscurecida por otra actividad, se detiene. Todavía conserva toda la información de estado y miembro, sin embargo, ya no es visible para el usuario por lo que su ventana está oculta y que a menudo será asesinado por el sistema cuando la memoria se necesita en otra parte.

Si una actividad se detiene o se detiene, el sistema puede dejar caer la actividad de la memoria ya sea pidiéndole que finalice o simplemente mate su proceso. Cuando se vuelve a mostrar al usuario, debe reiniciarse completamente y volver a su estado anterior.

En la siguiente Figura muestra las rutas de estado importantes de una actividad. Los rectángulos cuadrados representan métodos de devolución de llamada que puede implementar para realizar operaciones cuando la actividad se mueve entre estados. Los óvalos coloreados son estados importantes en los que puede estar la actividad.

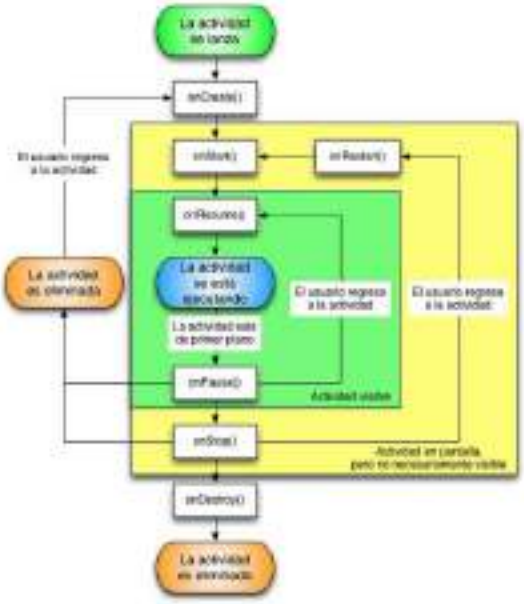


*Figura 2 – 139 Ciclo de vida aplicación Android*

El sistema puede terminar una Activity en cualquier momento, por medio del método finish() o a su vez matando el proceso. Otra manera en la que se pueden dar por finalizadas las actividades es que cuando escasee los recursos, terminará primero con las actividades que están paradas, luego con las pausadas y, ya en una situación crítica, con aquellas activas.

En cada caso cuando una Activity termina debe guardar su estado para que cuando sea lanzada lo pueda recuperar. Cuando se realizan cambios de estado la plataforma invoca determinados métodos de la actividad para que esta pueda realizar las operaciones oportunas.

La vida entera de una actividad ocurre entre la primera llamada a onCreate (Bundle) hasta una sola llamada final a onDestroy (). Una actividad realizará toda la configuración del estado "global" en onCreate () y liberará todos los recursos restantes en onDestroy ().

La vida útil visible de una actividad ocurre entre una llamada a onStart () hasta una llamada correspondiente a onStop (). Durante este tiempo, el usuario puede ver la actividad en pantalla, aunque puede que no esté en primer plano e interactúe con el usuario. Entre estos dos métodos puede mantener los recursos necesarios para mostrar la actividad al usuario.

La vida de primer plano de una actividad ocurre entre una llamada a onResume() hasta una llamada correspondiente a onPause (). Durante este tiempo la actividad se encuentra frente a todas las demás actividades e interactuando con el usuario. Una actividad puede ir frecuentemente entre los estados reanudados y pausados, por ejemplo, cuando el dispositivo se duerme, cuando se entrega un resultado de actividad, cuando se entrega una nueva intención, por lo que el código en estos métodos debe ser bastante ligero. El ciclo de vida completo de una actividad se lo puede manifestar en los siguientes métodos de actividad.

- **void onCreate(Bundle savedInstanceState)** : Este método es el primero que se crea, en este método se debe realizar toda la configuración de la pantalla principal, como declaración de botones, listas, etc. Por defecto viene incluido el parámetro Bundle , el cual es un diccionario en donde se almacena y transmite información de estado y de los objetos entre las actividades.
- **void onStart():** Se llama cuando la actividad es visible para el usuario.
- **void onPause():** Se ejecuta cuando el sistema comienza a reanudar una actividad anterior. Y todas las implementaciones que se hayan realizado dentro de este método deben finalizarse lo más pronto posible ya que ninguna Actividad sucesiva se reanudará hasta que este método devuelve un valor.

- **void onResume():** Empieza a ejecutarse cuando la actividad va a empezar a interactuar con el usuario.
- **void onStop():** Se llama cuando la actividad ya no es visible para el usuario, ya que otra actividad se ha reanudado y está cubriendo esta.
- **void onDestroy():** Este método se lo realiza luego de que todos los métodos anteriores ya se hayan ejecutado. Y permite terminar con todas las actividades.

#### II.3.1.3.7 Mysql

Mysql es un sistema gestor de base de datos, puesto que no cuenta con las mejores características es muy fácil de utilizar y su instalación también lo es, a su vez es de distribución libre. Algo importante de mysql es que además de almacenar información, es que todas las operaciones se realizan a través del lenguaje S.Q.L (Structured Query Language) "lenguaje de consultas estructuradas".

Características:

- Se lo puede utilizar en multiplataforma.
- Puede funcionar como cliente-servidor
- Se puede trabajar localmente o con un servidor remoto
- El tiempo de respuesta es muy rápido.
- Cuenta con un campo amplio en cuanto a sus tipos de datos.
- Brinda la posibilidad de administrar cuenta de usuarios y a su vez brindarles privilegios.
- Se tiene constancia de casos en los que maneja cincuenta millones de registros, sesenta mil tablas y cinco millones de columnas.
- Sus opciones de conectividad abarcan TCP/IP, sockets UNIX y sockets NT, además de soportar completamente ODBC.
- Los mensajes de error pueden estar en español y hacer ordenaciones correctas con palabras acentuadas o con la letra 'ñ'.
- Es altamente confiable en cuanto a estabilidad se refiere.
- No soporta procedimientos almacenados, disparadores ni vistas.
- No incluye características de objetos como tipos de datos estructurados definidos por el usuario, herencia etc.

#### II.3.1.3.8 Java

Java es un tipo de lenguaje de programación y una plataforma informática, creada y comercializada por Sun Microsystems en el año 1995. Se constituye como un lenguaje orientado a objetos, su intención es permitir que los desarrolladores de aplicaciones escriban el programa una sola vez y lo ejecuten en cualquier dispositivo.

Características:

- **Es simple. -** Java ofrece la funcionalidad de un lenguaje potente, derivado de C y C++, pero sin las características menos usadas y más confusas de estos, haciéndolo más sencillo.
- **Orientado a objetos. -** El enfoque orientado a objetos (OO) es uno de los estilos de programación más populares. Permite diseñar el software de forma que los distintos tipos de datos que se usen estén unidos a sus operaciones.
- **Es distribuido. -** Java proporciona una gran biblioteca estándar y herramientas para que los programas puedan ser distribuidos.
- **Independiente a la plataforma. -** Esto significa que programas escritos en el lenguaje Java pueden ejecutarse en cualquier tipo de hardware, lo que lo hace portable.
- **Recolector de basura. -** Cuando no hay referencias localizadas a un objeto, el recolector de basura de Java borra dicho objeto, liberando así la memoria que ocupaba. Esto previene posibles fugas de memoria.
- **Es seguro y sólido. -** Proporcionando una plataforma segura para desarrollar y ejecutar aplicaciones que, administra automáticamente la memoria, provee canales de comunicación segura protegiendo la privacidad de los datos y, al tener una sintaxis rigurosa evita que se quiebre el código, es decir, no permite la corrupción del mismo.
- **Es multihilo. -** Java logra llevar a cabo varias tareas simultáneamente dentro del mismo programa. Esto permite mejorar el rendimiento y la velocidad de ejecución.

### II.3.2 Metodología de Desarrollo

#### II.3.2.1 Metodología RUP (Rational Unified Process)

El Proceso Racional Unificado o RUP (por sus siglas en inglés de Rational Unified Process) es un proceso de desarrollo de software desarrollado por la empresa Rational Software, actualmente propiedad de IBM.1 Junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, diseño, implementación y documentación de sistemas orientados a objetos.

Es un proceso de ingeniería de software que suministra un enfoque para asignar tareas y responsabilidades dentro de una organización de desarrollo. Su objetivo es asegurar la producción de software de alta y de mayor calidad para satisfacer las necesidades de los usuarios que tienen un cumplimiento al final dentro de un límite de tiempo y presupuesto previsible. Es una metodología de desarrollo iterativo que es enfocada hacia "diagramas de los casos de uso, y manejo de los riesgos y el manejo de la arquitectura" como tal.

**D. Principales características**

- Forma disciplinada de asignar tareas y responsabilidades (quién hace qué, cuándo y cómo).
- Pretende implementar las mejores prácticas en Ingeniería de Software.
- Desarrollo iterativo.
- Administración de requisitos.
- Uso de arquitectura basada en componentes.
- Control de cambios.
- Modelado visual del software.
- Verificación de la calidad del software.

**E. Ciclo de Vida**

El ciclo de vida RUP es una implementación del Desarrollo en espiral. Fue creado ensamblando los elementos en secuencias semi-ordenadas. El ciclo de vida organiza las tareas en fases e iteraciones.

RUP divide el proceso en cuatro fases, dentro de las cuales se realizan varias iteraciones en número variable según el proyecto y en las que se hace un mayor o menor hincapié en las distintas actividades. Fases del ciclo de vida del RUP:

5. **Fase de Inicio:**

   Esta fase tiene como propósito definir y acordar el alcance del proyecto con los patrocinadores, identificar los riesgos asociados al proyecto, proponer una visión muy general de la arquitectura de software y producir el plan de las fases y el de iteraciones posteriores.

6. **Fase de elaboración:**

   En la fase de elaboración se seleccionan los casos de uso que permiten definir la arquitectura base del sistema y se desarrollaran en esta fase, se realiza la especificación de los casos de uso seleccionados y el primer análisis del dominio del problema, se diseña la solución preliminar.

7. **Fase de Desarrollo o Construcción:**

   El propósito de esta fase es completar la funcionalidad del sistema, para ello se deben clarificar los requerimientos pendientes, administrar los cambios de acuerdo a las evaluaciones realizados por los usuarios y se realizan las mejoras para el proyecto.

8. **Fase de Transición:**

   El propósito de esta fase es asegurar que el software esté disponible para los usuarios finales, ajustar los errores y defectos encontrados en las pruebas de aceptación, capacitar a los usuarios y proveer el soporte técnico necesario. Se debe verificar que el producto cumpla con las especificaciones entregadas por las personas involucradas en el proyecto.

## F. Elementos del RUP

**Actividades:** Procesos que se han de realizar en cada etapa/iteración.

**Trabajadores:** Personas involucradas en cada actividad del proyecto.

**Artefactos:** Herramientas empleadas para el desarrollo del proyecto. Puede ser un documento, un modelo, un elemento del modelo. Estos artefactos (entre otros) son los siguientes:

**Inicio**

- Documento Visión
- Especificación de Requerimientos

**Elaboración**

- Diagramas de caso de uso

**Construcción**

- Documento Arquitectura que trabaja con las siguientes vistas:
    - **Vista lógica**
        - Diagrama de clases
        - Modelo E-R
    - **Vista de implementación**
        - Diagrama de Secuencia
        - Diagrama de estados
        - Diagrama de Colaboración
    - **Vista conceptual**
        - Modelo de dominio
    - **Vista física**
        - Mapa de comportamiento a nivel de hardware

(Booch, Ivar, & Rumbaugh, 1998)
Para el desarrollo del presente proyecto se utilizó la metodología RUP, al ser flexible y adaptable al proceso del proyecto, realizándose de manera iterativa en cada una de sus fases.

### II.3.2.2 UML (Lenguaje Unificado de Modelado)

Lenguaje Unificado de Modelado (UML, por sus siglas en inglés, Unified Modeling Language) es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad; está respaldado por el OMG (Object Management Group). Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. UML ofrece un estándar para describir un "plano" del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio, funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y compuestos reciclados. Es importante remarcar que UML es un "lenguaje de modelado" para especificar o para describir métodos o procesos. Se utiliza para definir un sistema, para detallar los artefactos en el sistema y para documentar y construir. En otras palabras, es el lenguaje en el que está descrito el modelo (Booch, Ivar, & Rumbaugh, 1998).

En el presente proyecto se utilizó UML para el diseño y elaboración de diagramas de clases, casos de uso, actividades y de secuencias que reflejan los requerimientos y el funcionamiento del sistema.

### II.3.2.3 Tipos de Diagrama Utilizados

#### II.3.2.3.1 Diagrama de Clases

El propósito de un diagrama de clase es describir las clases que conforman el modelo de un determinado sistema. Dado el carácter de refinamiento iterativo que caracteriza un desarrollo orientado a objetos, el diagrama de clase va a ser creado y refinado durante las fases de análisis y diseño, estando presente como guía en la implementación del sistema (Booch, Ivar, & Rumbaugh, 1998).

#### II.3.2.3.2 Diagrama de Actividades

Un Diagrama de Actividades representa un flujo de trabajo paso a paso de negocio y operacionales de los componentes en un sistema.

En UML 1, un diagrama de actividades es una variación del Diagrama de Estados UML donde los estados representan operaciones y las transiciones representan las actividades que ocurren cuando la operación es completa.

Los diagramas de actividades se utilizaron para definir el comportamiento interno de los procesos del presente Sistema (Booch, Ivar, & Rumbaugh, 1998).

#### II.3.2.3.3 Diagrama de Secuencia

Un Diagrama de Secuencias muestra una interacción ordenada según la secuencia temporal de eventos y el intercambio de mensajes. Los diagramas de secuencia ponen especial énfasis en el orden y el momento en el que se envían los mensajes a los objetos.

En los diagramas de Secuencias los elementos están representados por líneas intermitentes verticales, con el nombre del objeto en la parte más alta (Booch, Ivar, & Rumbaugh, 1998).

Los diagramas de Secuencias se utilizaron para reflejar cómo interactúan los componentes principales del presente sistema.

### II.3.2.4 Herramientas de Construcción de Software.

#### II.3.2.4.1 Android Studio

Está basado en el software IntelliJ IDEA de JetBrains y ha sido publicado de forma gratuita a través de la Licencia Apache 2.0. Está disponible para las plataformas Microsoft Windows, macOS y GNU/Linux. Ha sido diseñado específicamente para el desarrollo de Android.

Estuvo en etapa de vista previa de acceso temprano a partir de la versión 0.1, en mayo de 2013, y luego entró en etapa beta a partir de la versión 0.8, lanzada en junio de 2014. Android Studio está disponible para Windows 2003, Vista, 7, 8, y 10 tanto plataformas de 32 como de 64 bits, GNU/Linux, Linux con GNOME o KDE y 2 GB de memoria RAM mínimo y macOS, desde 10.8.5 en adelante.

Características:

- Integración de ProGuard y funciones de firma de aplicaciones.
- Renderizado en tiempo real
- Consola de desarrollador: consejos de optimización, ayuda para la traducción, estadísticas de uso.
- Soporte para construcción basada en Gradle.
- Refactorización específica de Android y arreglos rápidos.
- Un editor de diseño enriquecido que permite a los usuarios arrastrar y soltar componentes de la interfaz de usuario
- Herramientas Lint para detectar problemas de rendimiento, usabilidad, compatibilidad de versiones, y otros problemas.
- Plantillas para crear diseños comunes de Android y otros componentes.
- Soporte para programar aplicaciones para Android Wear.
- Soporte integrado para Google Cloud Platform, que permite la integración con Google Cloud Messaging y App Engine.
- Un dispositivo virtual de Android que se utiliza para ejecutar y probar aplicaciones

(Sparxsystems, 2020)

Se utilizó Android Studio para la elaboración de la aplicación del proyecto para la conexión de los usuarios a la Red Privada Virtual.

#### II.3.2.4.2 Firebase

Firebase se trata de una plataforma móvil creada por Google, cuya principal función es desarrollar y facilitar la creación de apps de elevada calidad de una forma rápida, con el fin de que se pueda aumentar la base de usuarios y ganar más dinero. La plataforma está subida en la nube y está disponible para diferentes plataformas como iOS, Android y web. Contiene diversas funciones para que cualquier desarrollador pueda combinar y adaptar la plataforma a medida de sus necesidades.

Característica:

- Desarrollo: Firebase permite la creación de mejores apps, minimizando el tiempo de optimización y desarrollo, mediante diferentes funciones, entre las que destacan la detección de errores y de testeo, que supone poder dar un salto de calidad a la app. Poder almacenar todo en la nube, testear la app o poder configurarla de manera remota, son características destacables de la plataforma.
- Analitica: Tener un control máximo del rendimiento de la app mediante métricas analíticas, todo desde un único panel y de forma gratuita. Los datos analíticos que facilita Firebase, facilita la toma de decisiones basadas y fundamentadas en datos reales.
- Poder de crecimiento: Permite gestionar de manera fácil todos los usuarios de las aplicaciones, con el añadido de que se pueden captar nuevos usuarios, mediante invitaciones o notificaciones.
- Monetización: Mediante AdMob, Firebase permite que puedas ganar dinero.
- Rapidez: Implementar Firebase puede ser fácil y rápido, gracias a su API que es muy intuitiva, sostenida en un solo SDK. Con Firebase puedes centrar tus esfuerzos en resolver los problemas de tus clientes y así poder evitar la pérdida de tiempo en la creación de una infraestructura compleja.
- Agilidad: Firebase ofrece apps multiplataforma con una APIs integradas a SDK individuales para iOS, Android y Javascript, de tal forma que se puede gestionar diferentes apps sin necesidad de salir de la propia plataforma.

(Firabase, 2021)

Se utilizó Android Studio para la elaboración de la aplicación del proyecto para la conexión de los usuarios a la Red Privada Virtual.

#### II.3.2.4.3 Enterprise Architect

Enterprise Architect es una plataforma de alto desempeño para el modelado, visualización y diseño, basada en el estándar UML 2.4.1. Ofrece trazabilidad completa desde mapas mentales, pasando por los requerimientos y hasta el diseño y la distribución del software, con el nivel de eficiencia, robustez, herramientas de colaboración y seguridad requerida para sacar adelante proyectos altamente demandantes y cualquier tamaño.

Enterprise Architect es una aplicación completa para la elaboración de proyectos de Ingeniería. Está diseñado especialmente para el enfoque empresarial, y junto a ello, se especializa en la realización de diagramas UML de todo tipo: Componentes, Clases y Bases de Datos. Soporta el trabajo sobre varios lenguajes de programación como Java.
Características:

- Completa herramienta de análisis y diseño en UML
- Modelado avanzado para negocios, software y sistemas
- Completa trazabilidad desde los requerimientos hasta la distribución
- Ingeniería de código en más de 10 lenguajes
- Altamente escalable, repositorios basados en el equipo de trabajo
- Mapas mentales, BPMN, Arquitectura Empresarial, etc.

(Sparxsystems, 2020)

Se utilizó Enterprice Architect para la elaboración de los diagramas UML empleados en el presente proyecto.

### II.3.2.5 Técnica

#### II.3.2.5.1 XML (Extensible Markup Languaje)

XML, siglas en inglés de Xtensible Markup Language ("lenguaje de marcas Extensible"), es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible. Proviene del lenguaje SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML) para estructurar documentos grandes. A diferencia de otros lenguajes, XML da soporte a bases de datos, siendo útil cuando varias aplicaciones deben comunicarse entre sí o integrar información.

XML no ha nacido sólo para su aplicación para Internet, sino que se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable.
Objetivos:

- XML debe ser directamente utilizable en Internet
- XML debe soportar una amplia variedad de aplicaciones
- XML debe ser compatible con SGML
- Debería se sencillo escribir programas que procesaran documentos XML
- El número de las características opcionales en XML debería ser el mínimo posible, a ser posible cero
- Los documentos XML deberían ser legibles por las personas y razonablemente claros
- El diseño de XML debe ser rápido
- XML debería ser simple, pero perfectamente normalizado
- Los documentos XML deben ser de fácil creación
- La concisión de las marcas XML tiene una importancia mínima

(Mozilla, 2020)

Se empleó XML en el desarrollo del presente Sistema para el intercambio de información entre los controladores modelo visto controlador.

#### II.3.2.5.2 JavaScript

JavaScript es un lenguaje de programación que se utiliza principalmente para crear páginas web dinámicas. Una página web dinámica es aquella que incorpora efectos como texto que aparece y desaparece, animaciones, acciones que se activan al pulsar botones y ventanas con mensajes de aviso al usuario. Técnicamente, JavaScript es un lenguaje de programación interpretado, por lo que no es necesario compilar los programas para ejecutarlos. En otras palabras, los programas escritos con JavaScript se pueden probar directamente en cualquier navegador sin necesidad de procesos intermedios. A pesar de su nombre, JavaScript no guarda ninguna relación directa con el lenguaje de programación Java. Legalmente, JavaScript es una marca registrada de la empresa Sun Microsystems (Mozilla, 2020).
Para un diseño dinámico y más amigable de las páginas web para el usuario se utilizó el lenguaje de programación JavaScript.

#### II.3.2.5.3 Java

Java es un tipo de lenguaje de programación y una plataforma informática, creada y comercializada por Sun Microsystems en el año 1995.

Se constituye como un lenguaje orientado a objetos, su intención es permitir que los desarrolladores de aplicaciones escriban el programa una sola vez y lo ejecuten en cualquier dispositivo.

Características:

- **Es simple.**
- **Orientado a objetos.**
- **Es distribuido.**
- **Independiente a la plataforma.**
- **Recolector de basura.**
- **Es seguro y sólido.**
- **Es multihilo.**

### II.3.3 Plan de desarrollo de software RUP

#### II.3.3.1 Introducción

Este documento provee una visión general del enfoque de desarrollo propuesto. El proyecto fue desarrollado por el universitario KEVIN TAMBO SOSSA, Basado en la metodología de Rational Unified Process (RUP) en la que únicamente se procederá a cumplir con las tres primeras fases, las cuales marcan la metodología. Es importante destacar esto puesto que utilizaremos la terminología RUP en este documento. Se incluirá el detalle para las fases de Inicio, Elaboración y Construcción.

- **Inicio. -** En esta fase se establece los requisitos de negocio que cubrirá el sistema, se obtendrá la especificación de requerimientos. Mediante entrevistas para posteriormente especificar los requerimientos según la norma IEEE 830.
- **Elaboración. -** En esta fase el problema se analiza y comprende desde el punto de vista del equipo de desarrollo. Al final de la fase se tiene definida la arquitectura y el modelo de requisitos del sistema empleando los diagramas de casos de uso especificados en lenguaje UML.

- **Construcción. -** En esta fase se profundiza en el diseño de los componentes del sistema y de manera iterativa se van añadiendo las funcionalidades al software a medida que se construyen y prueban, permitiendo a la vez que se puedan ir incorporando cambios.

Al final de esta fase se obtiene un sistema completamente operativo y la documentación (diagrama de clases, de secuencia, modelo entidad-relación, modelo de dominio, manual de instalación, manual de usuario) para entregar a los usuarios. El enfoque de desarrollo propuesto constituye una configuración del proceso RUP de acuerdo a las características del proyecto, seleccionando los roles de los participantes, las actividades a realizar y los entregables que serán generados. Este documento es a su vez uno de los artefactos de RUP.

El registro de los vehículos y sus custodias en la actualidad son manuales esto genera perdida de información y tiempo al realizar los reportes y consultas respectivas, el presente proyecto contribuirá a mejorar estos procesos permitiendo una administración optima de la gestión de los vehículos, se pretende desarrollar un sistema informático para automatizar la mayoría de los procesos inherentes en la gestión de vehículos y sus custodias

### II.3.3.2 Propósito

El propósito del Plan de Desarrollo de Software es proporcionar la información necesaria para controlar el proyecto. En él que se describe el enfoque de desarrollo del software.

El Plan de Desarrollo del Software se utilizará:

- Para organizar la agenda y necesidades de recursos, y para realizar su seguimiento.
- Para entender lo qué deben hacer, cuándo deben hacerlo y qué otras actividades dependen de ello.
- Elaborar los diagramas de UML de acuerdo a los requerimientos del proyecto.
- Desarrollar el código del proyecto de acuerdo a la documentación del proyecto.
- Llevar una correcta planificación del cronograma del proyecto y el cálculo de métricas.

#### II.3.3.3 Alcance

Este documento proporcionará una idea del software a desarrollar exponiendo a la vez su estructura hasta una visión terminada.

El Plan de Desarrollo del Proyecto describe el plan global usado para el desarrollo en el proyecto con nombre "Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual.". Durante el proceso de desarrollo en el artefacto "Visión" se definen las características del producto a desarrollar, lo cual constituye la base para la planificación de las iteraciones. Para la versión preliminar del Plan de Desarrollo del Software.

#### II.3.3.4 Resumen

Después de esta introducción, el resto del documento está organizado en las siguientes secciones:

- Vista General del Proyecto — proporciona una descripción del propósito, alcance y objetivos del proyecto, estableciendo los artefactos que serán producidos y utilizados durante el proyecto.
- Organización del Proyecto — describe la estructura organizacional del equipo de desarrollo.
- Gestión del Proceso — explica los costos y planificación estimada, define las fases e hitos del proyecto y describe cómo se realizará su seguimiento.
- Planes y Guías de aplicación — proporciona una vista global del proceso de desarrollo de software, incluyendo métodos, herramientas y técnicas que serán utilizadas.

#### II.3.3.5 Vista General de Proyecto

##### II.3.3.5.1 Propósito

La aplicación de Android permitirá que los usuarios del servicio que brindara el proyecto Rapid Tunnel VPN pueden conectarse a la red privada virtual permitiendo que los mismo puedan escoger entre varios servidores en distintos países para su comodidad.

#### II.3.3.5.2 Alcances

- Permitir que los usuarios con cuentas y suscripciones pueden acceder al servicio con mayores beneficios.
- Permitir que los usuarios pueden escoger el servidor en la localización de su preferencia.
- Encriptar todas las comunicaciones del dispositivo con la VPN y la VPN con el Internet.
- Nombre de la aplicación “Fast Tunnel VPN”

#### II.3.3.5.3 Limitaciones

- La aplicación no contará con la posibilidad de gestionar los usuarios, se redirigirá al sistema web para ello.

#### II.3.3.5.4 Objetivos

##### II.3.3.5.4.1 Objetivo General

Mejorar la Seguridad y Acceso al Internet de los Usuarios de la Red Privada Virtual.

##### II.3.3.5.4.2 Objetivo Específicos

- Desarrollar una aplicación en Android para el VPN “Fast Tunnel VPN” y la conexión de sus usuarios.
- El desarrollo de la aplicación con el uso de las siguientes tecnologías:
    - Java
    - XML
    - Firebase
- Aplicar la metodología de desarrollo RUP (Proceso Unificado Racional).
- Diseñar una Interfaz fácil de usar, amigable para que el usuario tenga facilidad en la operación de Sistema.

### II.3.3.6 Entregables del proyect

A continuación, se indican y describen cada uno de los artefactos que serán generados y utilizados por el proyecto y que constituyen los entregables. Esta lista constituye la configuración de RUP desde la perspectiva de artefactos, y que proponemos para este proyecto.

Es preciso destacar que de acuerdo a la filosofía de RUP, todos los artefactos son objeto de modificaciones a lo largo del proceso de desarrollo, con lo cual, sólo al término del proceso podríamos tener una versión definitiva y completa de cada uno de ellos. Sin embargo, el resultado de cada iteración y los hitos del proyecto están enfocados a conseguir un cierto grado de completitud y estabilidad de los artefactos. Esto será indicado más adelante cuando se presenten los objetivos de cada iteración.

Los Artefactos (Entregables) Son los siguientes:

- Plan de desarrollo del software.
- Visión.
- Modelos de casos de uso del negocio.
- Modelo de objetos del negocio
- Glosario.
- Modelos de casos de uso.
- Especificación de los Casos de Uso.
- Prototipo Interfaces de Usuario.
- Modelos de análisis y diseño.
- Modelo de Datos.
- Modelo de Implementación.
- Modelo de despliegue.
- Casos de Prueba.
- Manual de usuario e Instalación.
- Material de apoyo al usuario Final.
- Diagrama de Actividades.
- Diagrama de Secuencia.
- Diagrama de componentes
- Producto

#### II.3.3.6.1 Plan de desarrollo de software

El presente documento describe paso a paso los puntos del proyecto según la metodología.

#### II.3.3.6.2 Visión

##### II.3.3.6.2.1 Introducción

Este documento define la visión del producto desde la perspectiva del cliente, especificando las necesidades y características del producto. Constituye una base de acuerdo en cuanto a los requerimientos del sistema.

##### II.3.3.6.2.2 Limitación

Entre las limitantes del producto, señalamos que el sistema no contara con módulos de contabilidad y no se registra más información de la necesaria.

##### II.3.3.6.2.3 Oportunidad del Negocio

El proyecto viene a ofrecer un servicio de seguridad para todas las personas que se conectan al internet y desean hacerlo de la manera más segura posible no solo para ellos mismo que si no también para su familia y para las empresas y sus trabajadores.

###### II.3.3.6.2.3.1 Sentencias que define el Proyecto.

| | |
|---|---|
| El problema de | La inseguridad presente en el internet sobre nuestra información e identidad. |
| Afecta a | Todas las personas que se conecta al internet para su uso diario y cotidiano. |
| El impacto asociado es | Mejorar la seguridad al momento de conectarse al internet.<br><br>Mejorar la velocidad de conexión en algunos casos bien específicos.<br><br>Desbloquear contenido para los usuarios que están restringidos por regiones |
| Una solución adecuada seria | |

| | |
|---|---|
| | Conectarse a la internet atreves de un VPN el cual permitirá navegar de una manera más segura y sin restricciones. |

*Tabla 2 – 34 Sentencias que define el Proyecto*

#### II.3.3.6.2.3.2 Sentencia que define la Posición del Proyecto.

| | |
|---|---|
| Para | Internautas |
| Quienes | Interactuaran de manera directa e indirecta con el sistema. |
| El nombre del producto | "Fast Tunnel VPN" |
| Que | Mejorar la conexión al internet.<br><br>Mejorar la seguridad de los internautas al navegar en ella.<br><br>Desbloquear contenido bloqueo en el internet.<br><br>Proteger la información de los internautas. |
| No como | La manera en la que se conectamos ahora nos pone en riesgo a muchas cosas ya que no contamos con una encriptación para nada. |
| Nuestro producto | Asegura una mejor conexión al internet<br>Desbloquea el contenido que lo estaba regionalmente permitiendo cambiar tu localización<br>Protege tu información y anonimidad |

*Tabla 2 – 35 Sentencia que define la Posición del Proyecto*

#### II.3.3.6.2.3.3 Descripción de los participantes en el desarrollo del sistema y usuarios

### II.3.3.6.2.4 Descripción Global del Sistema

#### II.3.3.6.2.4.1 Perspectiva del producto

El producto a desarrollar es una aplicación para los usuarios del VPN “Fast Tunnel VPN” con la intención de proteger a los mismo al conectarse a la internet entre varias toras cosas las cuales permitirán mejoran la interacción de los usuarios con la internet manteniendo los protegidos.

#### II.3.3.6.2.4.2 Resumen de Características

A continuación, se mostrará un listado con los beneficios que obtendrá el cliente a partir del producto:

| Beneficio del cliente | Características que lo apoyan |
|---|---|
| Conexión más segura y libre al internet | ;a aplicación permitirá que los usuarios se conecten a la red privada virtual encriptando todas sus solicitudes y cambiando su localización. |
| Escoger la localización por la cual sus solicitudes será pasadas | La aplicación permitirá que estos usuarios sean capaces de escoger donde serán sus solicitudes enviadas (País). |

*Tabla 2 – 36 Resumen de Características*

#### II.3.3.6.2.4.3 Supuestos y Dependencias

Las suposiciones y restricciones están mencionadas en la Matriz de Marco Lógico del proyecto.

### II.3.3.6.3 Glosario

#### II.3.3.6.3.1 Introducción

Este documento recoge términos manejados durante la elaboración del proyecto de desarrollo de un sistema web de gestión, se trata de un diccionario informal de datos y de definiciones de la nomenclatura que se maneja, de tal modo que se crea un estándar para el proyecto.

#### II.3.3.6.3.2 Propósito

Comprender la Es definir con exactitud y sin ambigüedad la tecnología manejada en el proyecto en desarrollo. También sirve como guía de consulta para la aclaración de los puntos conflictivos o poco esclarecedores.

#### II.3.3.6.3.3 Alcance

El alcance del presente entregable se extiende a todo el sistema.

#### II.3.3.6.3.4 Organización del proyecto

El presente documento está organizado por definiciones de términos ordenados en forma ascendente según el alfabeto.

**VPN:** Virtual Private Network.

**UML:** Lenguaje Unificado de Modelos.

**USUARIOS:** Administrador, personas que usaran el servicio.

#### II.3.3.6.3.5 Glosario de los Diagramas

| | |
|---|---|
| Actor del Negocio |  |
| Casos de Uso Negocio |  |
| Comunicación |  |
| Relación |  |
| Actor |  |
| Casos de Uso |  |

| | |
|---|---|
| Relación de Inclusión |  |
| Relación de Extensión |  |

*Tabla 2 – 37 Glosario de los Diagramas*

#### II.3.3.6.4 Modelo de casos de uso

##### II.3.3.6.4.1 Introducción

El modelo de Casos de Uso es un modelo del Sistema que contiene actores, casos de uso y sus relaciones, describe lo que hace el sistema para cada tipo de usuario, es decir cada forma en que los actores usan el sistema se representa con un caso de uso, los mismos que son fragmentos de funcionalidad, especifican una secuencia de acciones que el sistema puede llevar a cabo interactuando con sus actores.

##### II.3.3.6.4.2 Propósito

- Comprender la estructura y la dinámica del sistema deseado para la organización
- Identificar posibles mejoras

##### II.3.3.6.4.3 Alcance

- Describe los procesos del sistema.
- Identificar y definir los procesos del sistema según los objetivos de la organización
- Definir un caso de uso para cada proceso del sistema (el diagrama de casos de uso puede mostrar el contexto y los límites del Sistema).

### II.3.3.6.4.4 Actores del Sistema

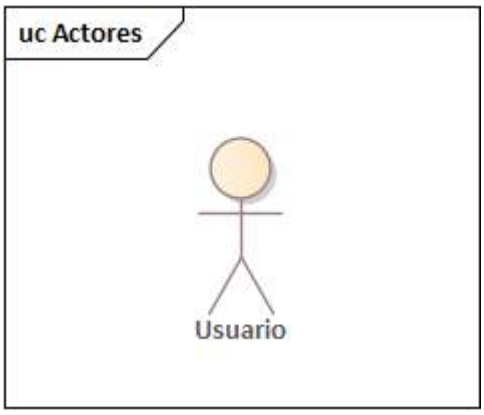


*Figura 2 – 140 Actores de la Aplicación*

### II.3.3.6.4.5 Diagrama de caso de uso General

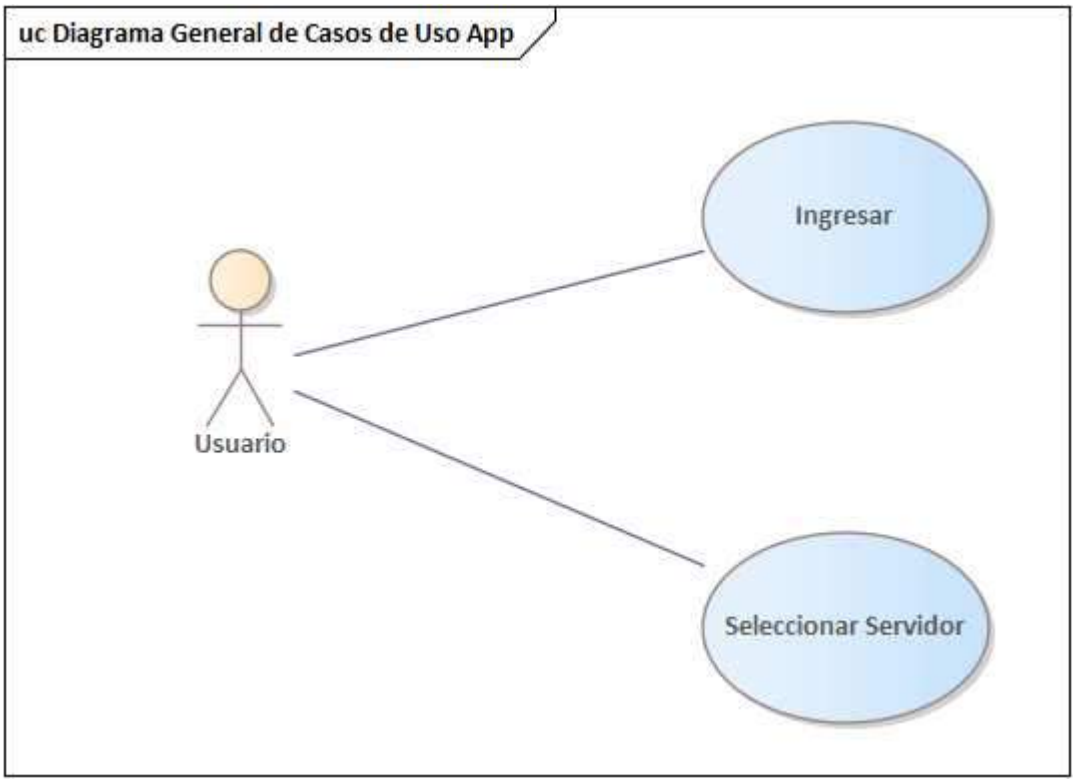


*Figura 2 – 141 Diagrama de caso de uso General*

### II.3.3.6.5 Diagramas de Casos de Uso Específicos

#### II.3.3.6.5.1 Diagrama de Caso de Uso: Ingresar

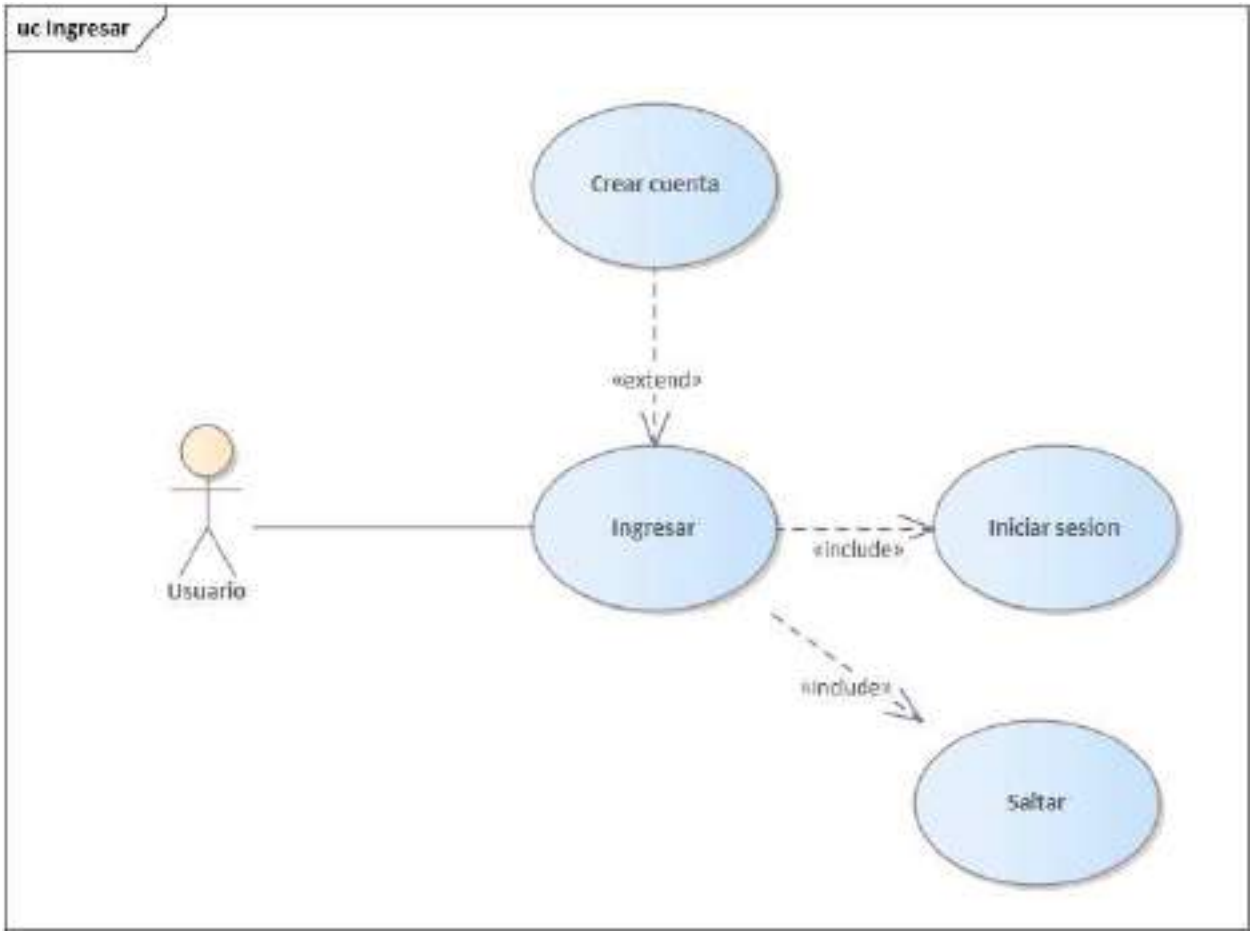


*Figura 2 – 142 Diagrama de Caso de Uso: Ingresar*

#### II.3.3.6.5.2 Diagrama de Caso de Uso: Seleccionar Servidor

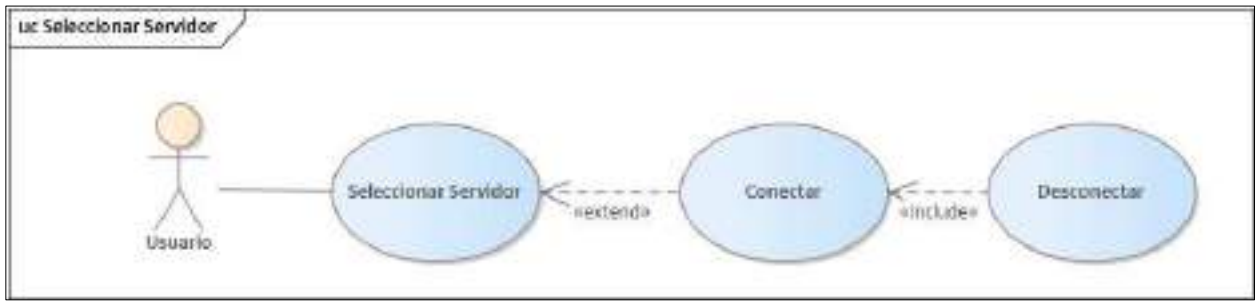


*Figura 2 – 143 Diagrama de Caso de Uso: Seleccionar Servidor*

### II.3.3.6.6 Especificación de casos de uso

#### II.3.3.6.6.1 Introducción

La Especificación de Casos de Uso es una descripción detallada de los casos de uso del sistema.

#### II.3.3.6.6.2 Propósito

- Comprender los casos de Uso del Sistema
- Describir específicamente cada caso de uso

#### II.3.3.6.6.3 Alcance

- Describir los procesos internos de los casos de uso
- Describir los flujos de cada caso de uso según lo establecido por la organización.

#### II.3.3.6.6.4 Especificación de Casos de Uso General

| | |
|---|---|
| **ACTOR:** | Usuario |
| **CASO DE USO:** | Ingresar<br>Seleccionar servidor |
| **TIPO** | Prioritario |
| **DESCRIPCION** | Son las Gestiones totales del sistema |

*Tabla 2 – 38 Especificación de Casos de Uso General*

#### II.3.3.6.6.5 Especificación de Casos de Uso: Ingresar

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Ingresar** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Usar la aplicación |
| **Resumen** | El usuario tiene 3 opciones para ingresar la aplicación:<br>1. Log In.<br>2. Sign In.<br>3. Saltar. |

| | |
|---|---|
| **Flujo Principal** | 1. Login<br>• El usuario selecciona “Login” en la pantalla de Ingreso.<br>• El usuario ingresara los datos de ‘Login’ y ‘Password’1 El usuario accede al sistema.<br>• El usuario selecciona “Acceder”, los datos se envían al sistema.<br>• El sistema verifica los datos.<br>• El usuario accede a la pantalla principal de la aplicación.<br>2. Sign In<br>• El usuario selecciona “Sign” In en la pantalla de Ingreso.<br>• La aplicación redirigirá al usuario a la pagina web para que pueda crearse una cuenta.<br>3. Saltar<br>• El usuario selecciona “Saltar” In en la pantalla de Ingreso.<br>• El usuario accede a la pantalla principal de la aplicación. |
| **Sub Flujo** | Ninguno |
| **Excepción** | E-1.- Se mostrará un mensaje de advertencia especificando que campos son los incorrectos. |

*Tabla 2 – 39 Especificación de Casos de Uso: Ingresar*

### II.3.3.6.6.6 Especificación de Casos de Uso: Iniciar Sesión

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Iniciar Sesión** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Ingresar a la aplicación con una cuenta de usuario. |
| **Resumen** | Los Usuarios de la aplicación que tengan una cuenta podrán iniciar sesión en la aplicación para poder acceder a sus beneficios. |

| | |
|---|---|
| **Precondición** | El usuario debe tener una cuenta. |
| **Flujo Principal** | 1. El usuario selecciona “Login” en la pantalla de Ingreso.<br>2. El usuario ingresara los datos de ‘Login’ y ‘Password’1 El usuario accede al sistema.<br>3. El usuario selecciona “Acceder”, los datos se envían al sistema.<br>4. El sistema verifica los datos.<br>5. El usuario accede a la pantalla principal de la aplicación. |
| **Sub Flujo** | Ninguno |
| **Excepción** | E-1.- Se mostrará un mensaje de advertencia especificando que campos son los incorrectos. |

*Tabla 2 – 40 Especificación de Casos de Uso: Iniciar Sesión*

### II.3.3.6.6.7 Especificación de Casos de Uso: Crear Cuenta

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Crear Cuenta** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Crear un Usuario para ingresar iniciando una sesión. |
| **Resumen** | Los usuarios de la ampliación que quieran poder crearse una cuenta lo podrán hacer afuera de la aplicación. |
| **Precondición** | Ninguna. |
| **Flujo Principal** | 1. El usuario selecciona “Sign In” en la pantalla de Ingreso.<br>2. La aplicación redirigirá al usuario a la página web para que pueda crearse una cuenta. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 41 Especificación de Casos de Uso: Crear Cuenta*

### II.3.3.6.6.8 Especificación de Casos de Uso: Desconectar

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Desconectar** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Detener la conexión con el servidor y volver a una normal y directa al internet. |
| **Resumen** | Ya no se pasarán las solicitudes del dispositivo atreves del servidor de preferencia si no que volverá una conexión directa al internet, pero no protegida. |
| **Precondición** | Estar conectado a un servidor. |
| **Flujo Principal** | 1. El usuario selecciona “Desconectar” en la pantalla de Principal.<br>2. La aplicación detendrá la conexión con el servidor.<br>3. La pantalla principal se refrescará a la inicial. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 42 Especificación de Casos de Uso: Desconectar*

### II.3.3.6.6.9 Especificación de Casos de Uso: Conectar

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Conectar** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Establecer la conexión con el servidor Cortando la conexión directa al internet del dispositivo y pasándola atreves del servidor de preferencia. |
| **Resumen** | Ya no se pasarán las solicitudes del dispositivo de manera directa por el internet si no que atreves del servidor de preferencia. |

| | |
|---|---|
| **Precondición** | Ninguna |
| **Flujo Principal** | 1. El usuario selecciona “Conectar” en la localización del servidor de preferencia, en la pantalla de Principal.<br>2. La aplicación establecerá la conexión con el servidor.<br>3. La pantalla principal se refrescará a la apareciendo la opción de “Desconectar”. |
| **Sub Flujo** | SU1: Estando conectado el usuario puede seleccionar otro servidor sin la necesidad de desconectarse. |
| **Excepción** | Ninguno |

*Tabla 2 – 43 Especificación de Casos de Uso: Conectar*

#### II.3.3.6.6.10 Especificación de Casos de Uso: Saltar

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Saltar** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Evitar la necesidad de iniciar sesión para poder usar la aplicación. |
| **Resumen** | La aplicación está diseñada para que no sea necesario el tener una cuenta para poder usar el servicio que ofrece de VPN. |
| **Precondición** | Ninguna |
| **Flujo Principal** | 1. El usuario selecciona “Saltar” en la localización del servidor de preferencia, en la pantalla de Principal.<br>2. El usuario accede a la pantalla principal de la aplicación. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 44 Especificación de Casos de Uso: Saltar*

#### II.3.3.6.6.11 Especificación de Casos de Uso: Seleccionar Servidor

| **Descripción de Casos de Uso** | |
|---|---|
| **Caso de Uso** | **Seleccionar Servidor** |
| **Actores** | Usuario |
| **Tipo** | Básico |
| **Propósito** | Escoger el servidor al que se desea conectar basado en la localización principalmente. |
| **Resumen** | Una de las cualidades más importantes que tiene servicio de VPN es de ofrecer muchas opciones de localizaciones en sus servidores para que los usuarios decidan el que prefieran. |
| **Precondición** | Ninguna |
| **Flujo Principal** | 1. El usuario accede a la pantalla principal de la aplicación.<br>2. La aplicación cargar la lista de servidores y sus localizaciones. |
| **Sub Flujo** | Ninguno |
| **Excepción** | Ninguno |

*Tabla 2 – 45 Especificación de Casos de Uso: Seleccionar Servidor*

### II.3.3.6.7 Diagramas de actividades

#### II.3.3.6.7.1 Introducción

En un diagrama de actividades muestra la iteración de un conjunto de objetos en una aplicación a través del tiempo, nos permite mostrar el flujo de los datos que pasan de una acción a otra, en estos diagramas no se muestra ni se describe la estructura de los datos

#### II.3.3.6.7.2 Propósito

Comprende la estructura y la dinámica del sistema deseado para la organización.

### II.3.3.6.7.3 Alcance

- Describe los procesos del sistema
- Identificar y definir los procesos del sistema según los objetivos de la organización.
- Definir un diagrama de actividades para cada proceso del sistema.

### II.3.3.6.7.4 Diagrama de Actividades: Ingreso a la Aplicación

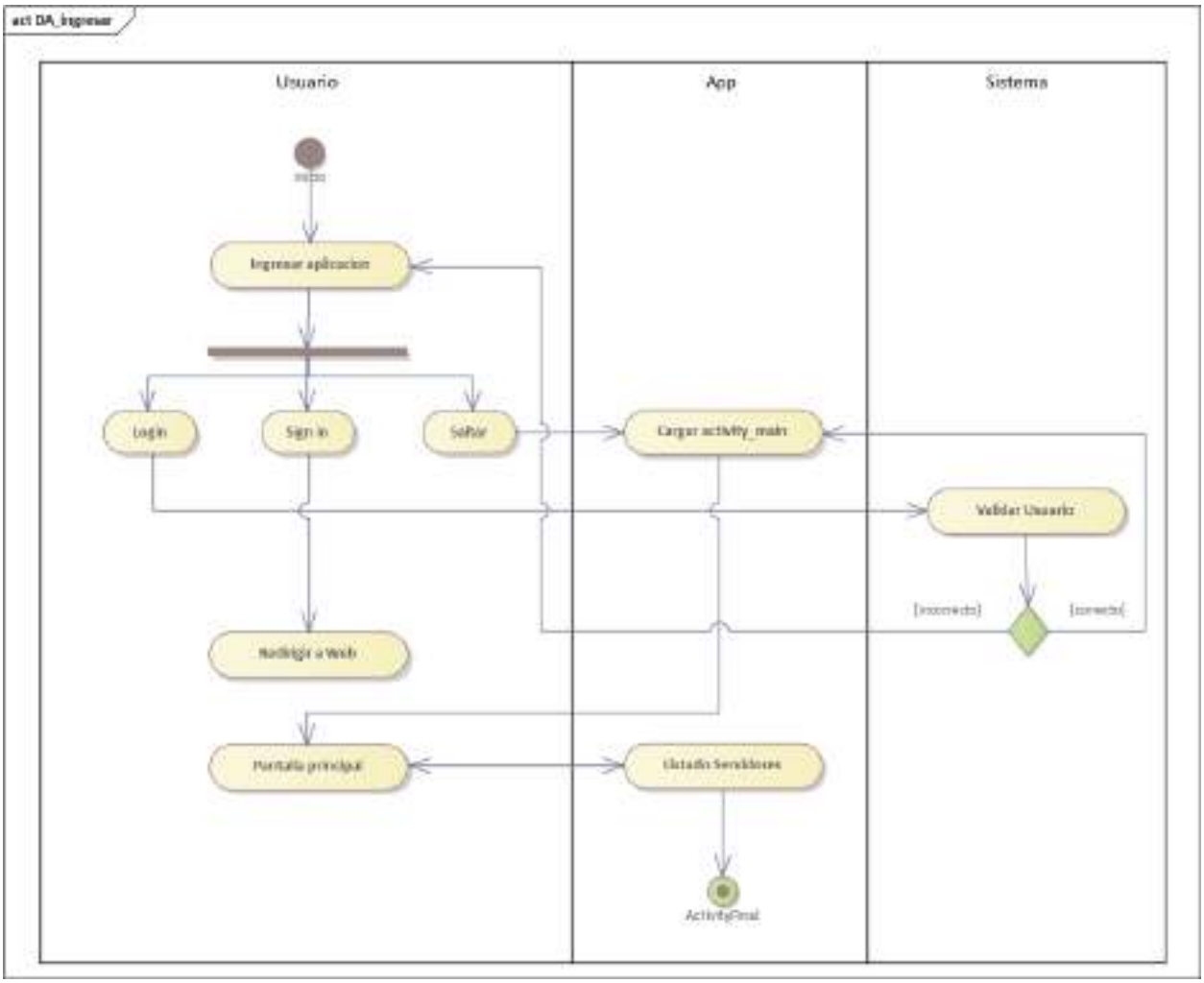


*Figura 2 – 144 Diagrama de Caso de Uso: Ingreso a la Aplicación*

### II.3.3.6.7.5 Diagrama de Actividades: Seleccionar servidor

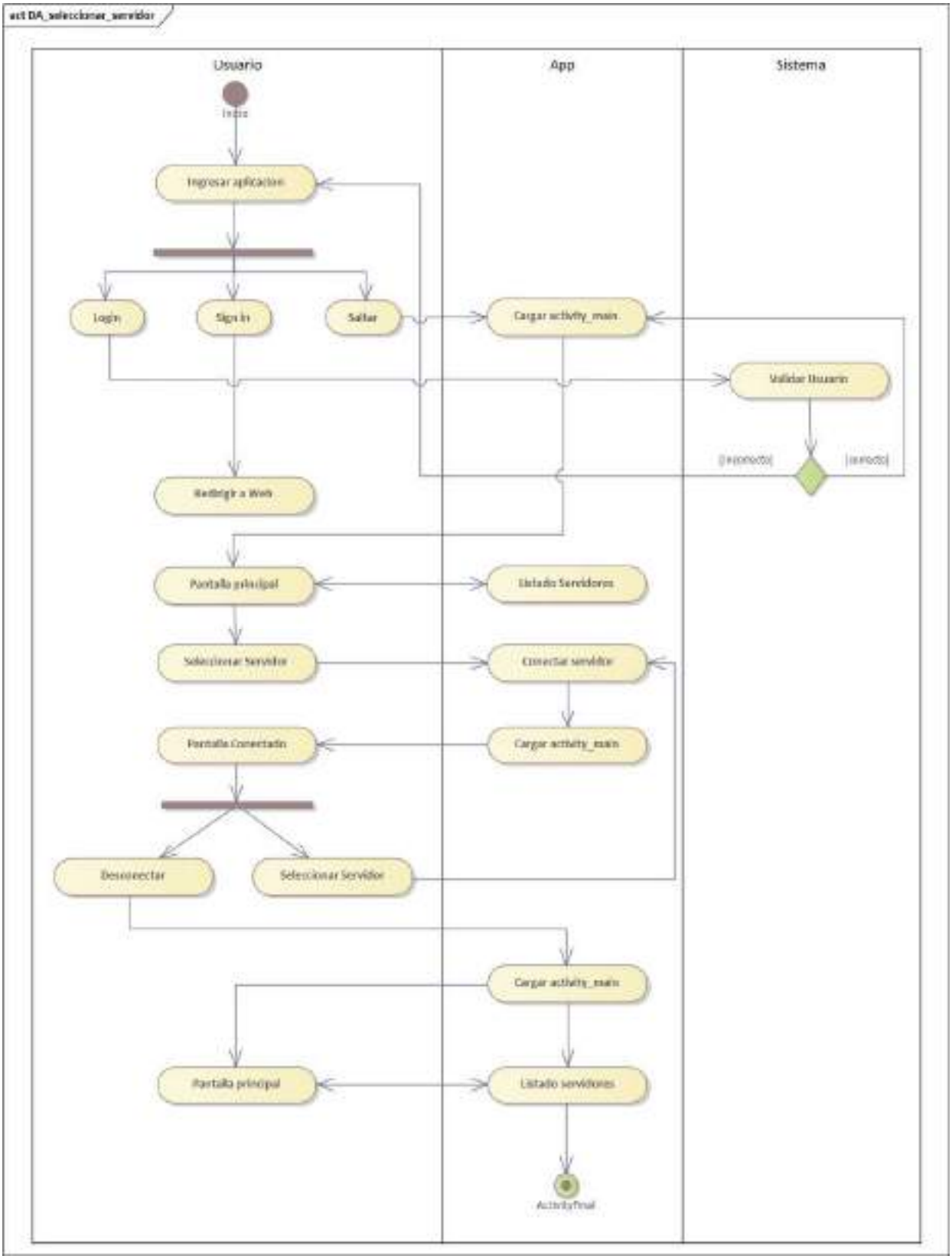


*Figura 2 – 145 Diagrama de Caso de Uso: Seleccionar servidor*

### II.3.3.6.7.6 Diagrama de Actividades: Conectar

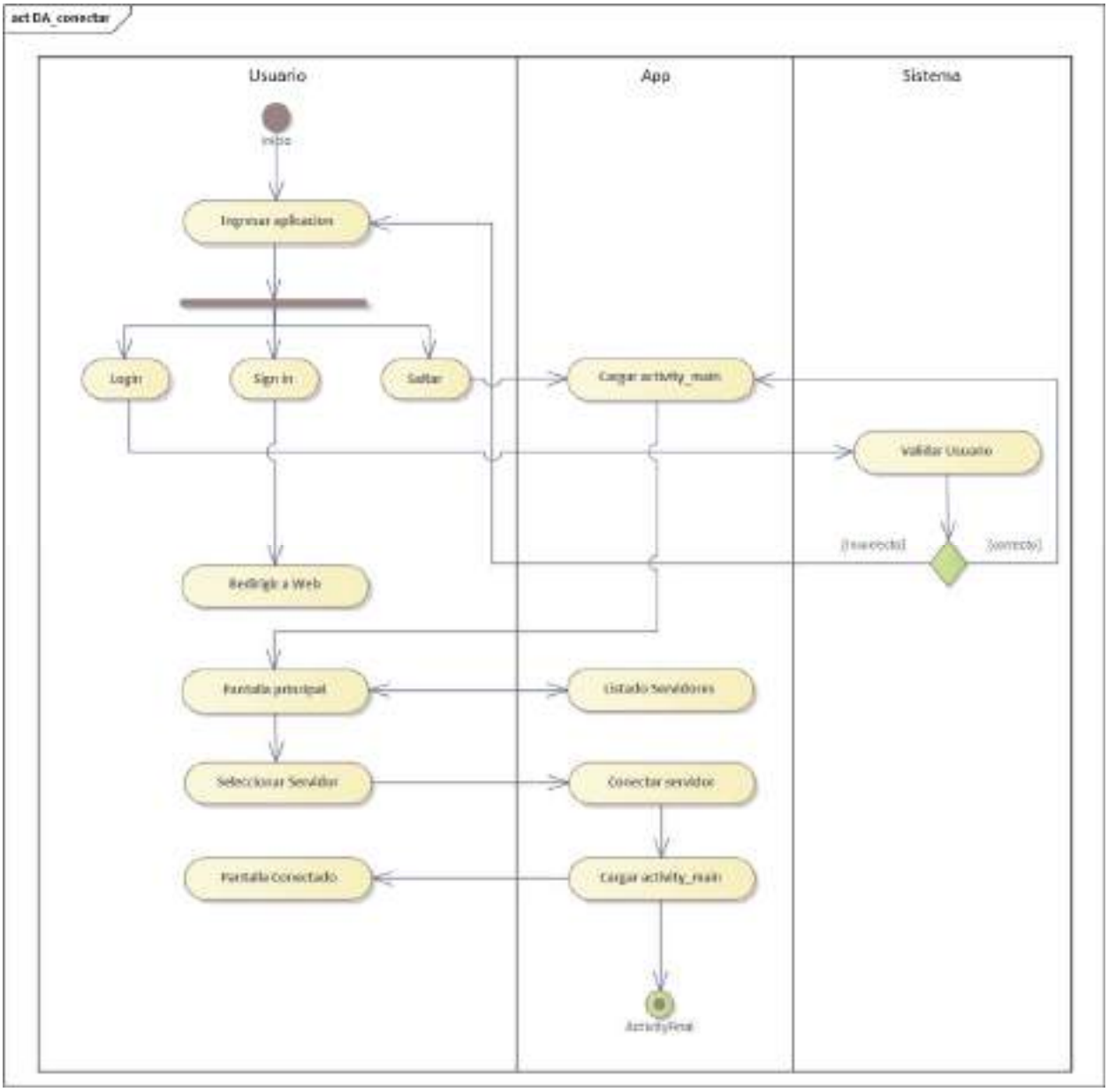


*Figura 2 – 146 Diagrama de Caso de Uso: Conectar*

### II.3.3.6.7.7 Diagrama de Actividades: Desconectar

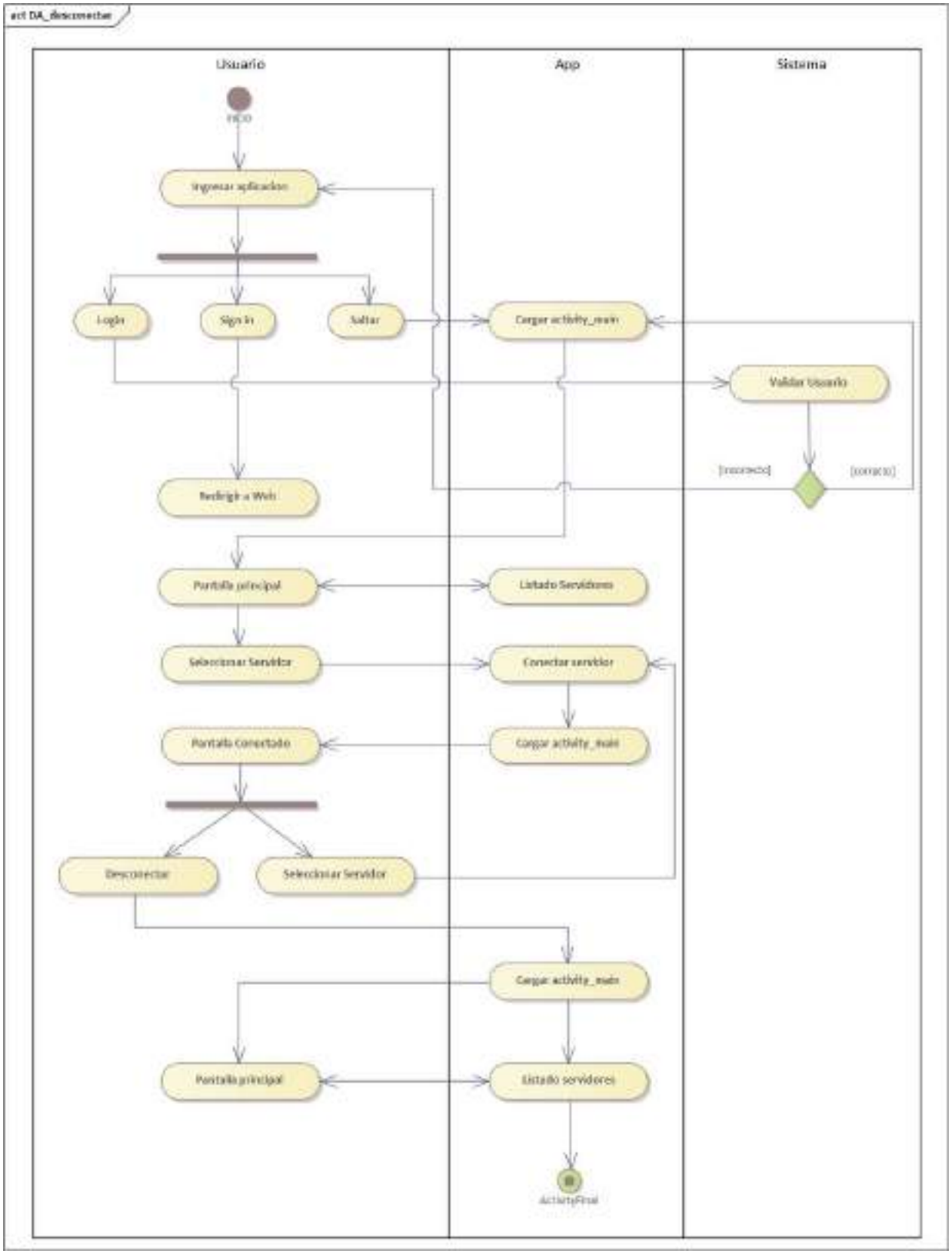


*Figura 2 – 147 Diagrama de Caso de Uso: Desconectar*

### II.3.3.6.7.8 Diagrama de Actividades: Crear Cuenta

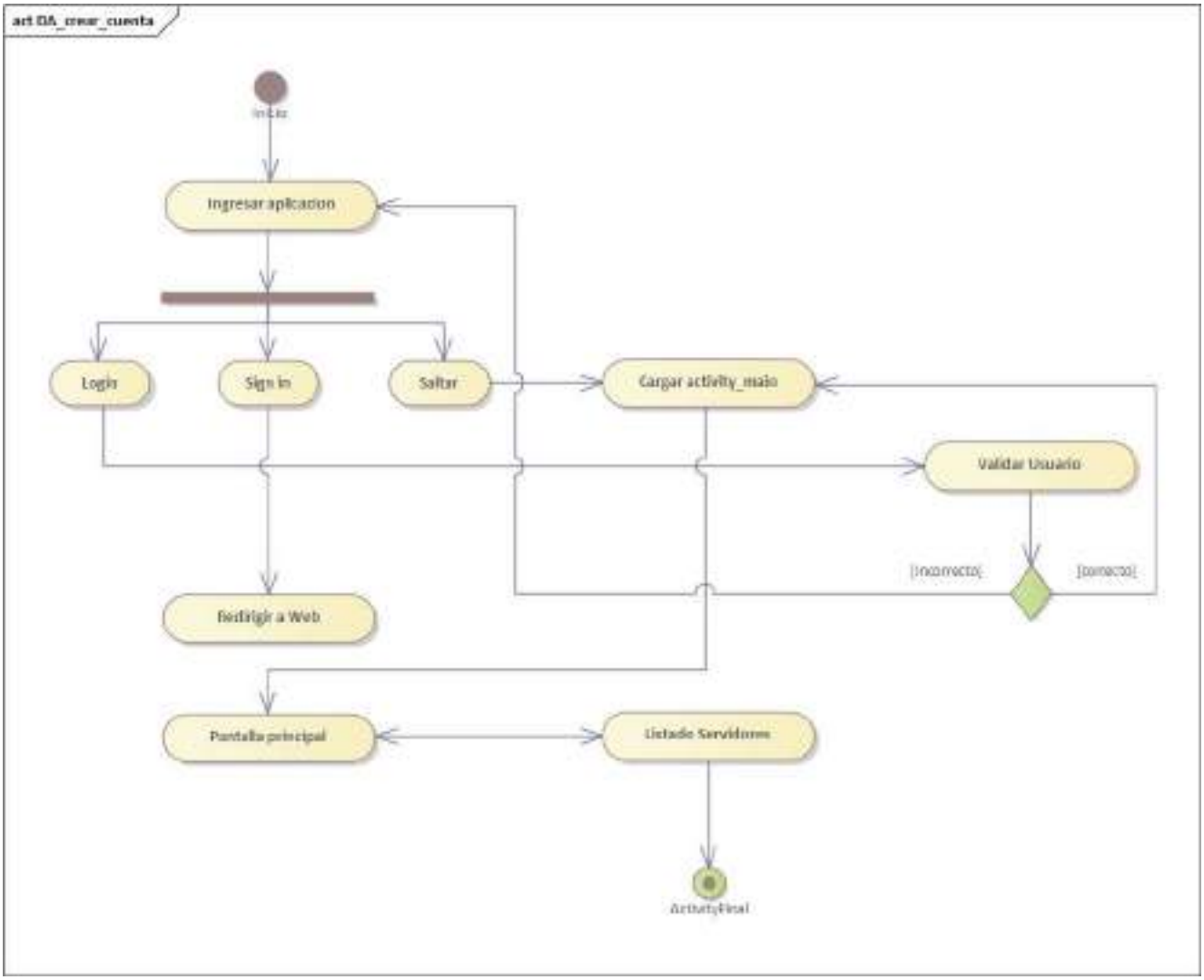


*Figura 2 – 148 Diagrama de Caso de Uso: Crear Cuenta*

### II.3.3.6.7.9 Diagrama de Actividades: Iniciar sesión

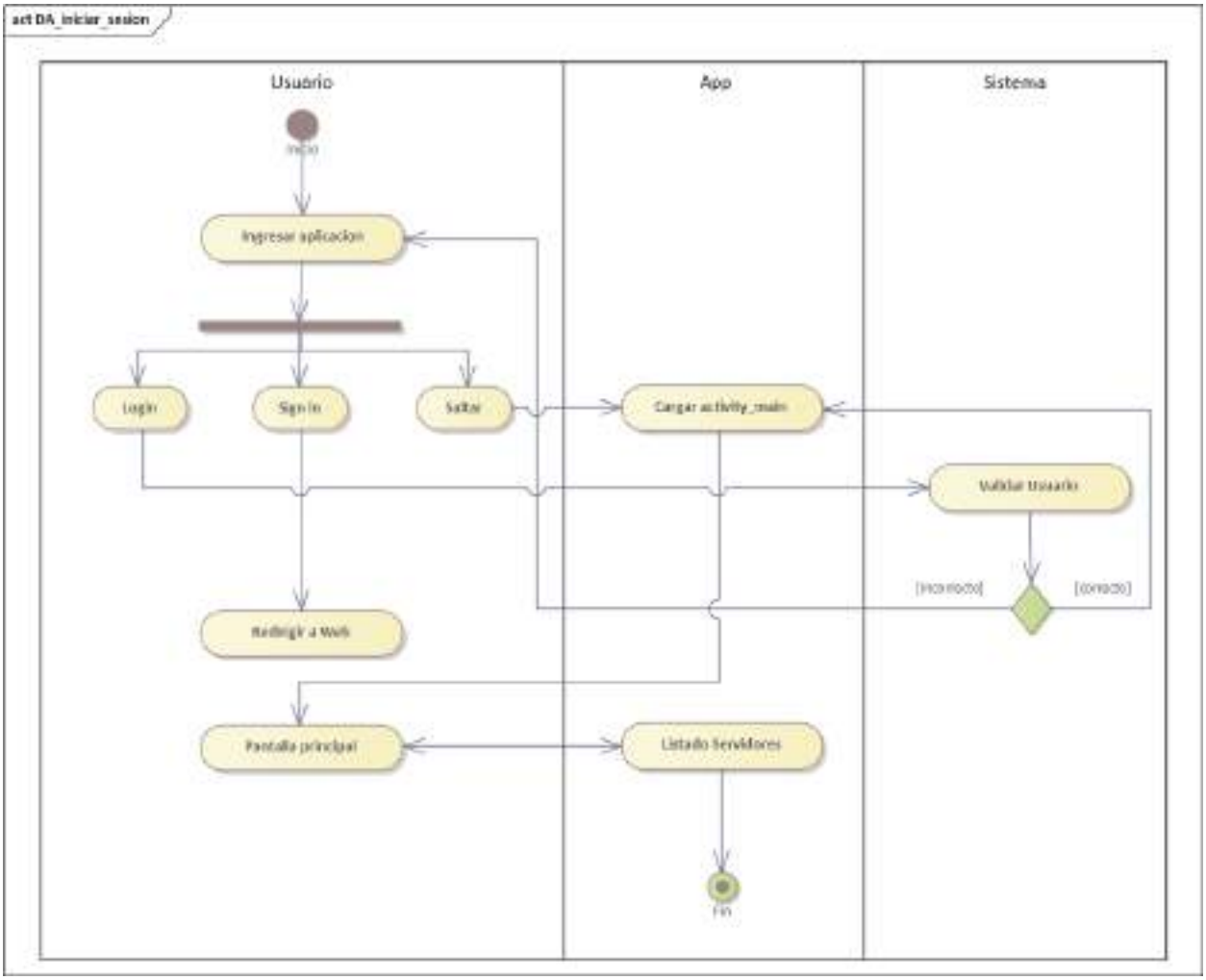


*Figura 2 – 149 Diagrama de Caso de Uso: Iniciar sesión*

### II.3.3.6.7.10 Diagrama de Actividades: Saltar

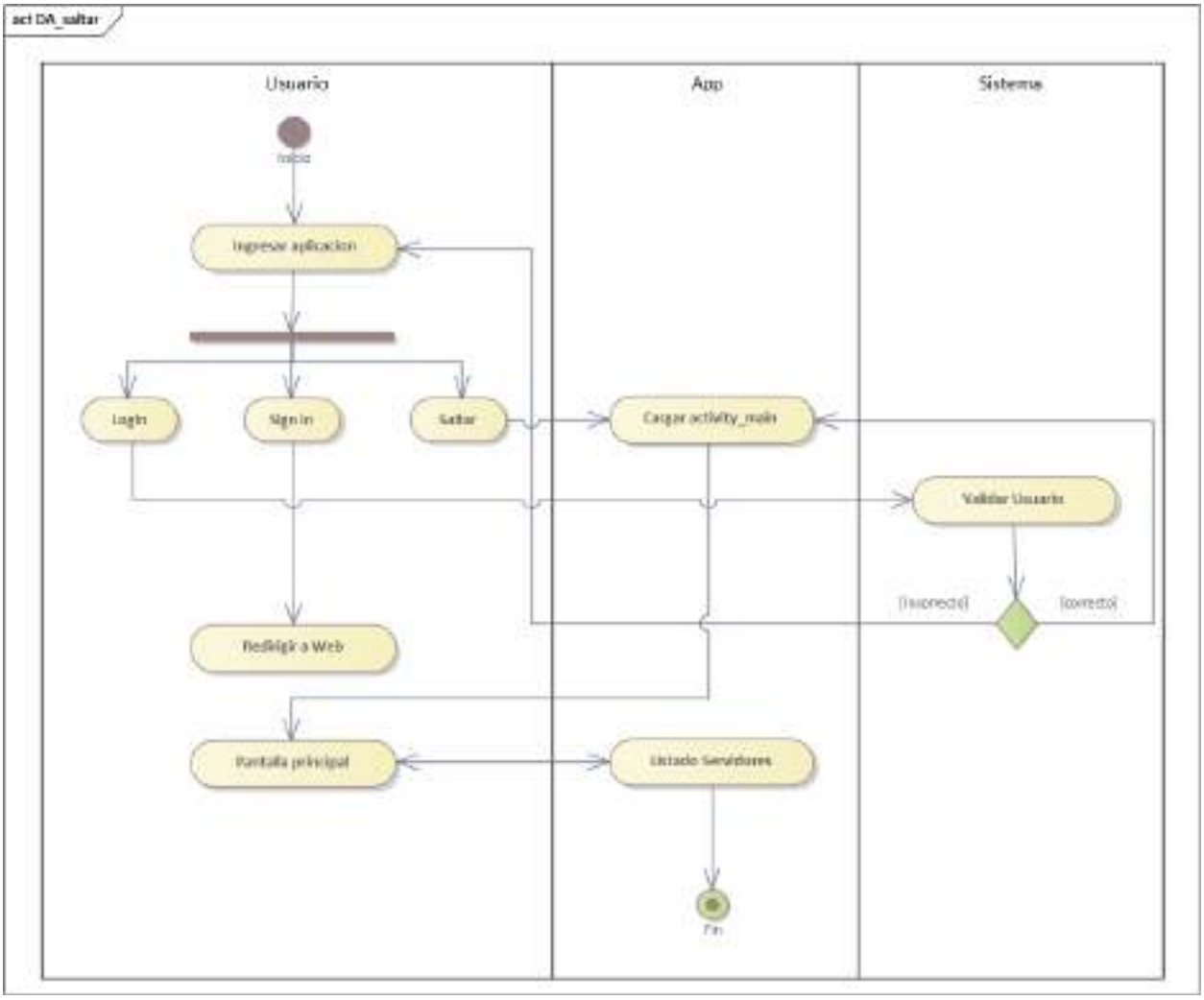


*Figura 2 – 150 Diagrama de Caso de Uso: Saltar*

### II.3.3.6.8 Diagramas de secuencia

#### II.3.3.6.8.1 Introducción

En un diagrama de secuencias muestra una iteración ordenada según la secuencia temporal de eventos en particular muestra los objetos participantes en la iteración y los mensajes (llamadas a métodos) que intercambian según su secuencia en el tiempo.

Frecuentemente estos diagramas se ubican bajo los casos de uso o componentes en el modelo para ilustrar un escenario, un conjunto de pasos comunes que siguen en respuesta a un evento externo y que generalmente un resultado.

El modelo incluye, que inicia la actividad en el sistema, que procesamientos y cambias ocurren internamente y que salidas se generan.

Muchas veces las instancias de los objetos se representan usando iconos especialmente estereotipo; existen iconos para objetos de interfaz, controladores, entidades persistentes, etc.

#### II.3.3.6.8.2 Propósito

Los diagramas de secuencia se usan para mostrar las iteraciones entre los usuarios, las pantallas y las instancias de los objetos en el sistema. Proveen una secuencia de pasos y de los mensajes entre los objetos a lo largo del tiempo

#### II.3.3.6.8.3 Alcance

- Muestran gráficamente las iteraciones del actor y de las operaciones a las que dan origen.
- Muestran un determinado escenario de un caso de uso, los eventos generados por actores externos, su orden y sus eventos internos.

## II.3.3.6.8.4 Diagrama de Secuencia: Conectar

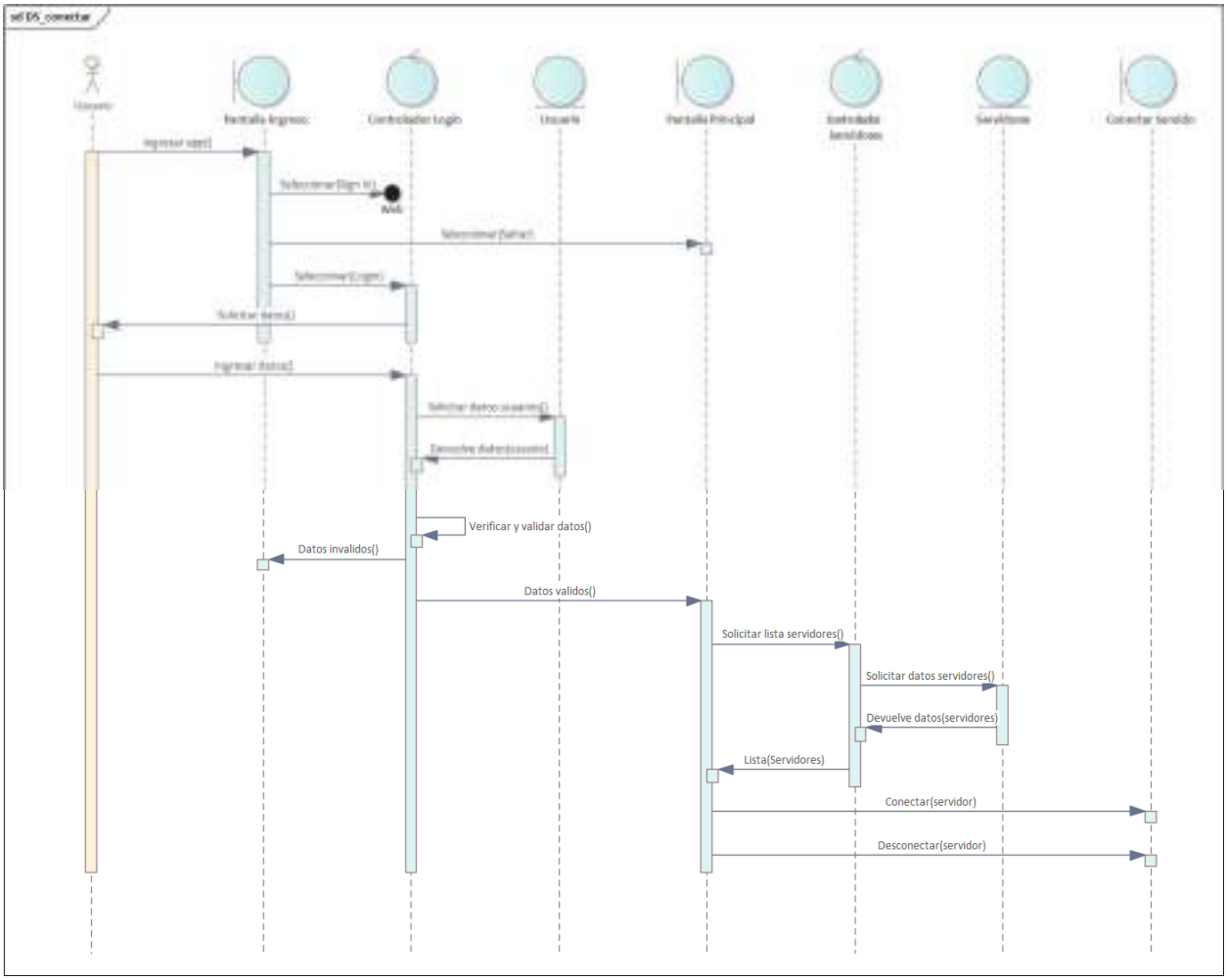


*Figura 2 – 151 Diagrama de Secuencia: Conectar*

### II.3.3.6.8.5 Diagrama de Secuencia: Crear Cuenta

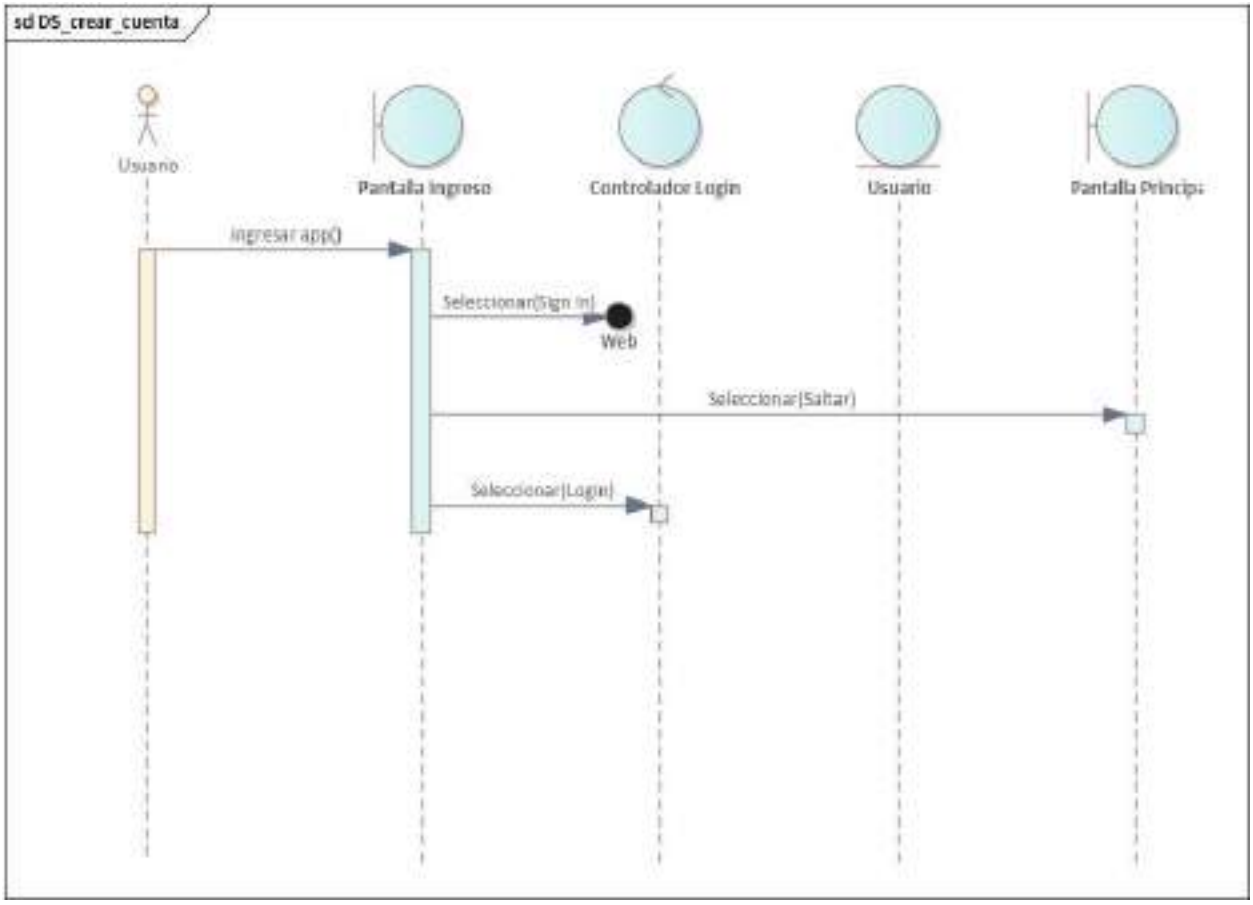


*Figura 2 – 152 Diagrama de Secuencia: Crear Cuenta*

## II.3.3.6.8.6 Diagrama de Secuencia: Desconectar

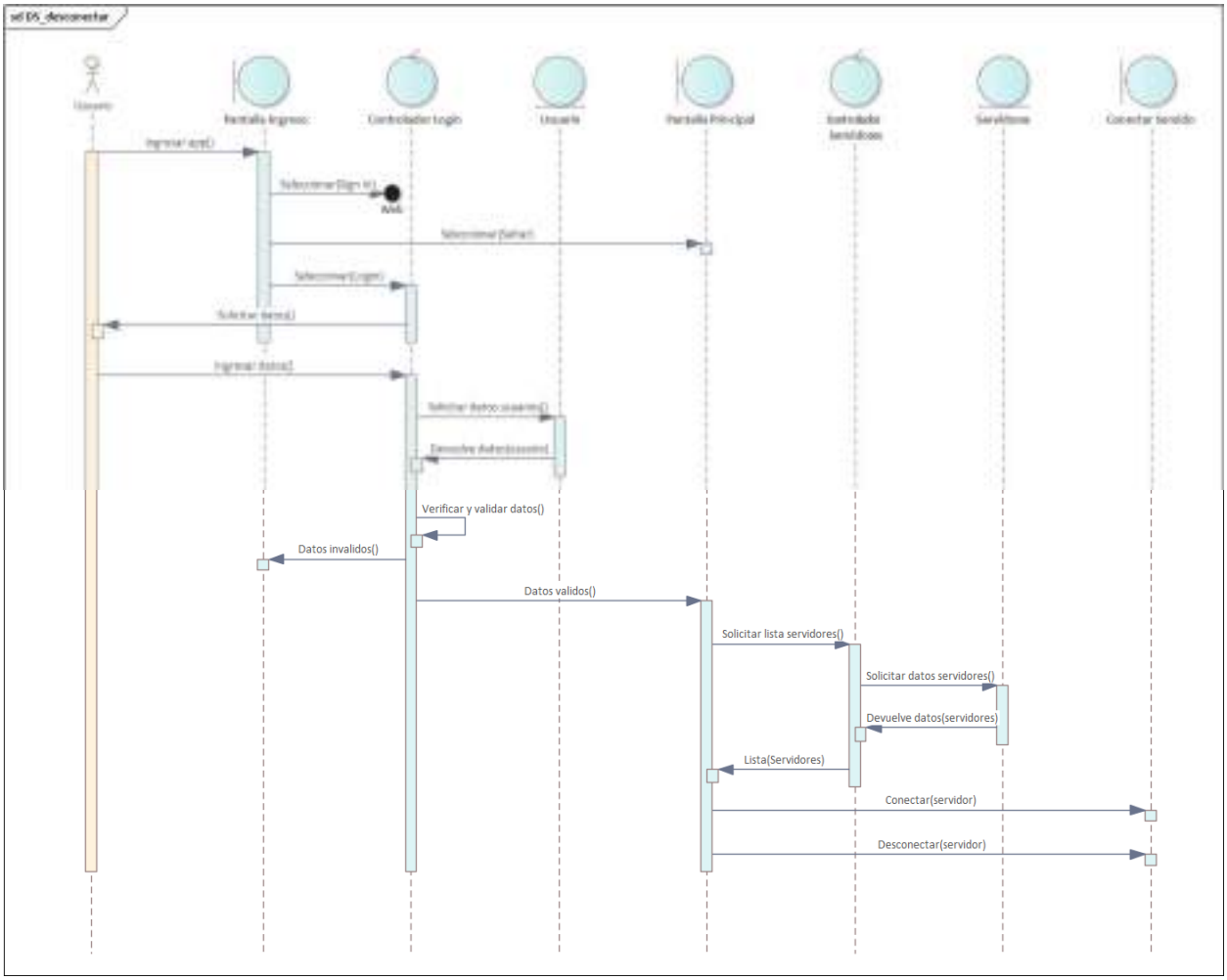


*Figura 2 – 153 Diagrama de Secuencia: Desconectar*

## II.3.3.6.8.7 Diagrama de Secuencia: Ingreso

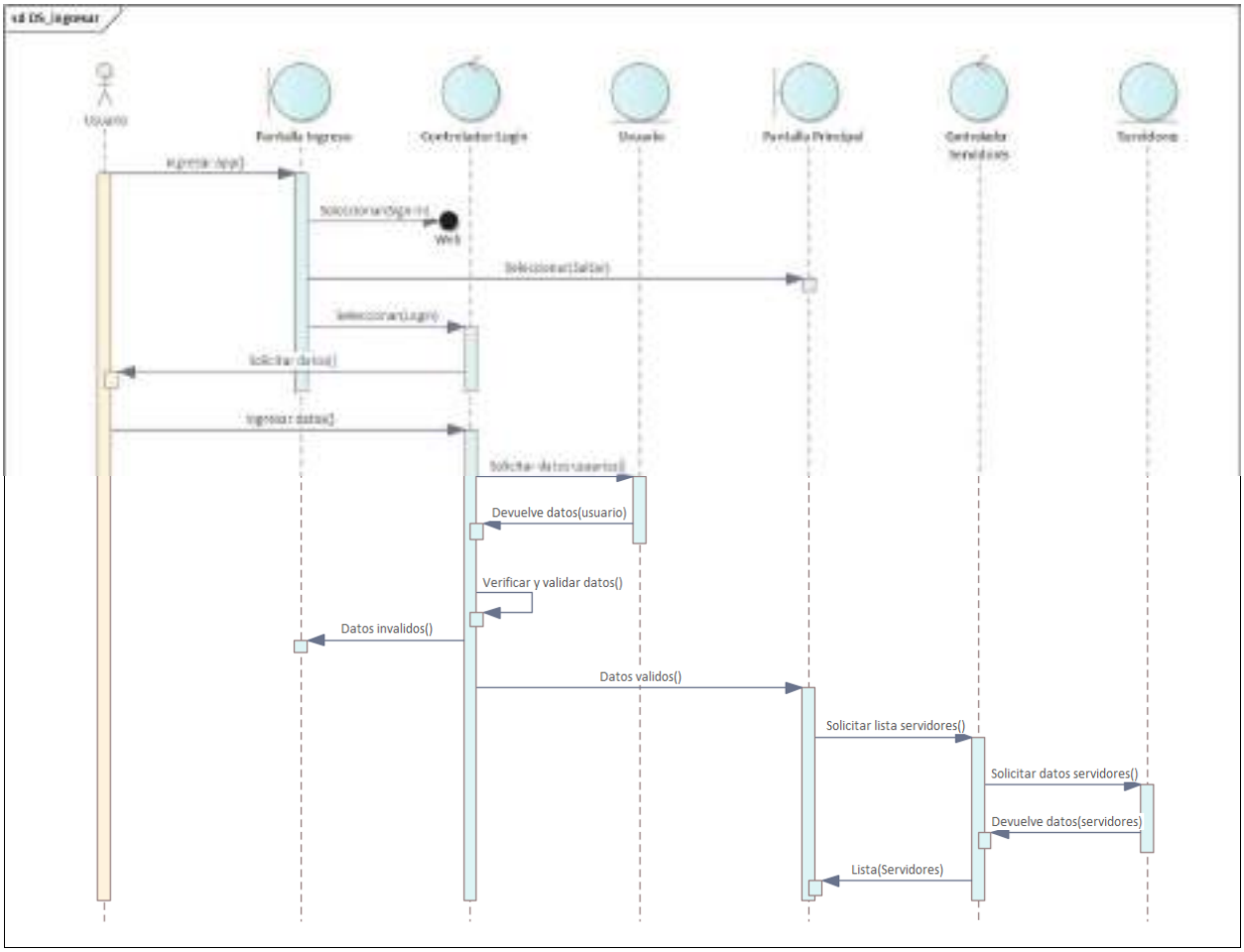


*Figura 2 – 154 Diagrama de Secuencia: Ingreso*

### II.3.3.6.8.8 Diagrama de Secuencia: Iniciar Sesión

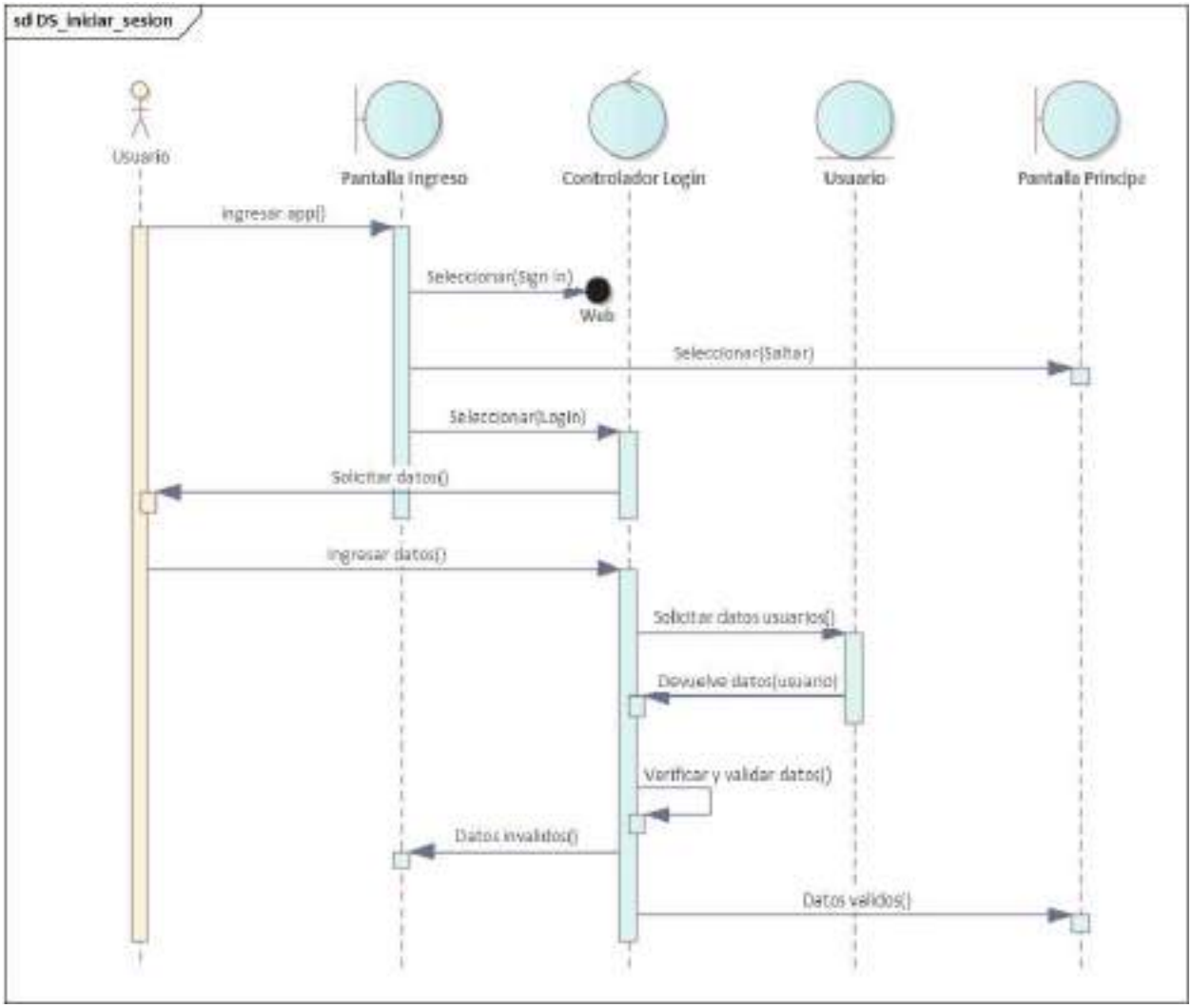


*Figura 2 – 155 Diagrama de Secuencia: Iniciar Sesión*

### II.3.3.6.8.9 Diagrama de Secuencia: Saltar

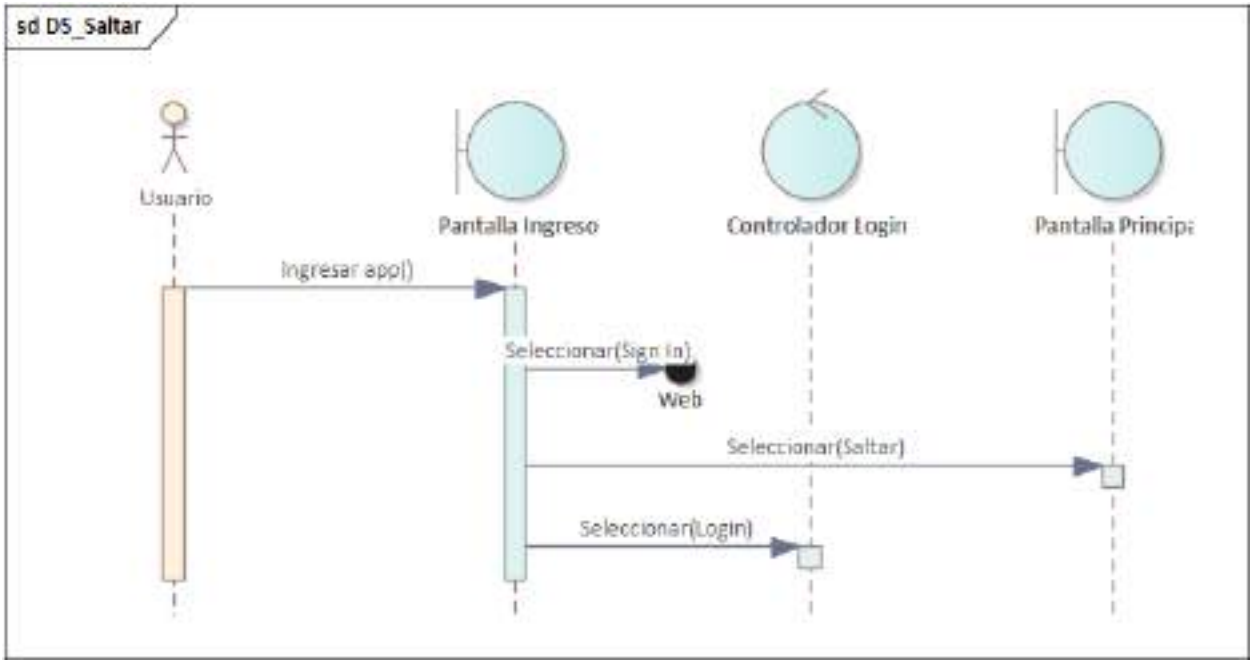


*Figura 2 – 156 Diagrama de Secuencia: Saltar*

### II.3.3.6.8.10 Diagrama de Secuencia: Seleccionar Servidor

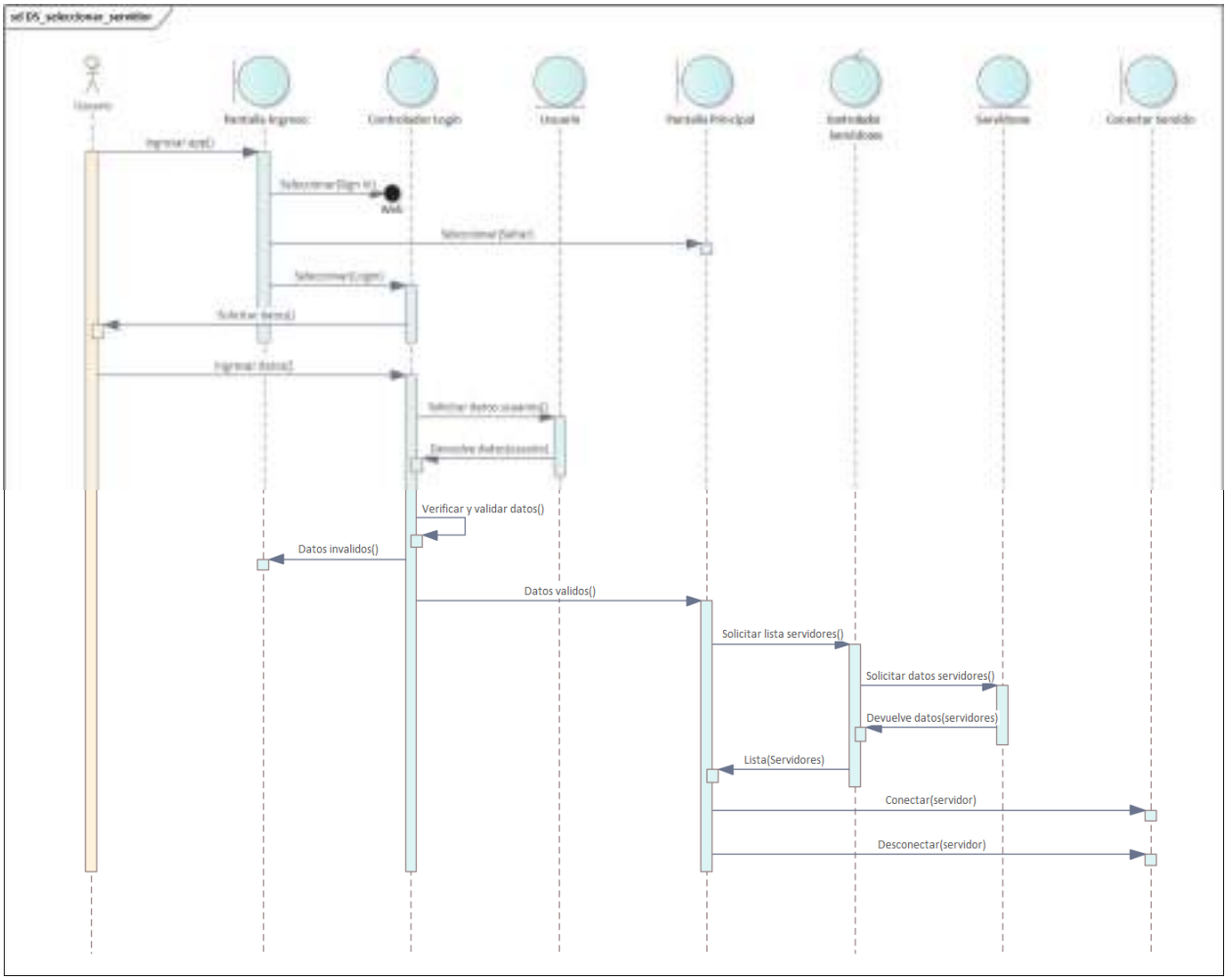


*Figura 2 – 157 Diagrama de Secuencia: Seleccionar Servidor*

### II.3.3.6.9 Prototipo de Interfaces de Pantalla

#### II.3.3.6.9.1 Pantalla (Mensaje de Bienvenida 1)


*Figura 2 – 158 Pantalla Mensaje de Bienvenida 1*

**II.3.3.6.9.2 Pantalla (Mensaje de Bienvenida 2)**


*Figura 2 – 159 Pantalla Mensaje de Bienvenida 2*

**II.3.3.6.9.3 Pantalla (Mensaje de Bienvenida 3)**


*Figura 2 – 160 Pantalla Mensaje de Bienvenida 3*

**II.3.3.6.9.4 Pantalla (Cargando Servidores)**

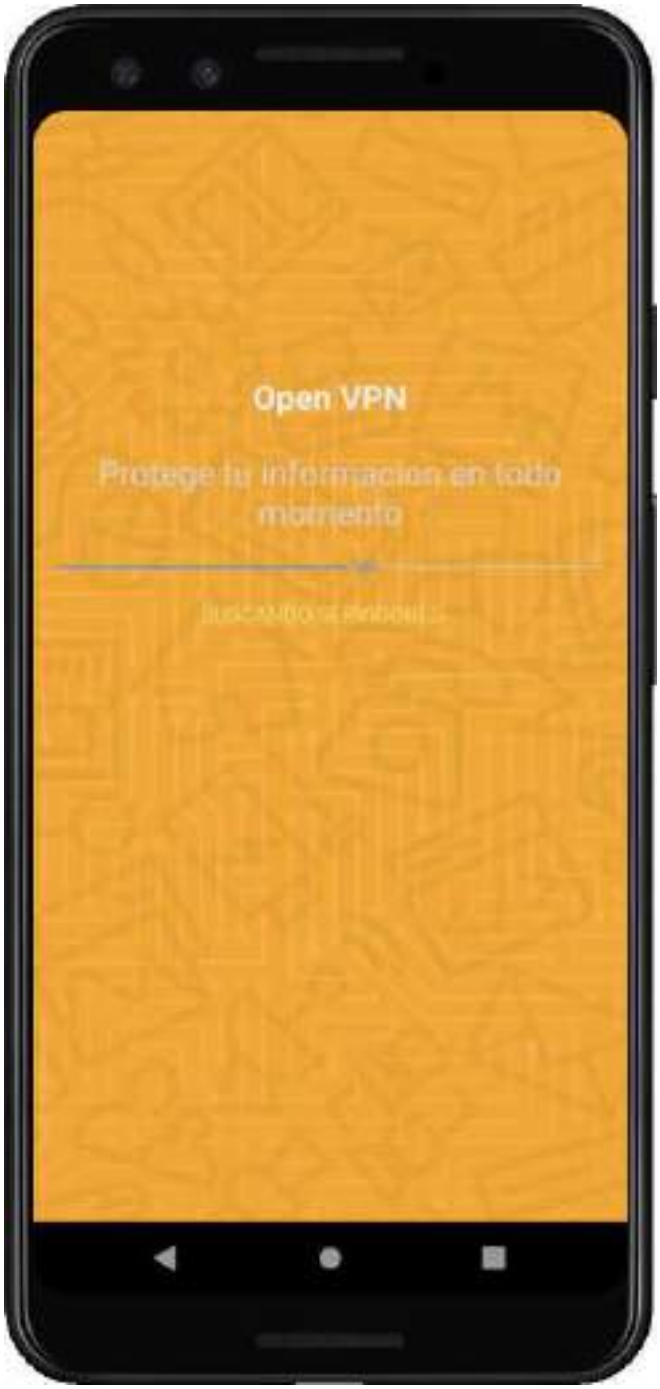


*Figura 2 – 161 Pantalla Cargando Servidores*

**II.3.3.6.9.5 Pantalla (Ingreso)**


*Figura 2 – 162 Pantalla Ingreso*

**II.3.3.6.9.6 Pantalla (Principal)**


*Figura 2 – 163 Pantalla Principal*

**II.3.3.6.9.7 Pantalla (Servidor País)**

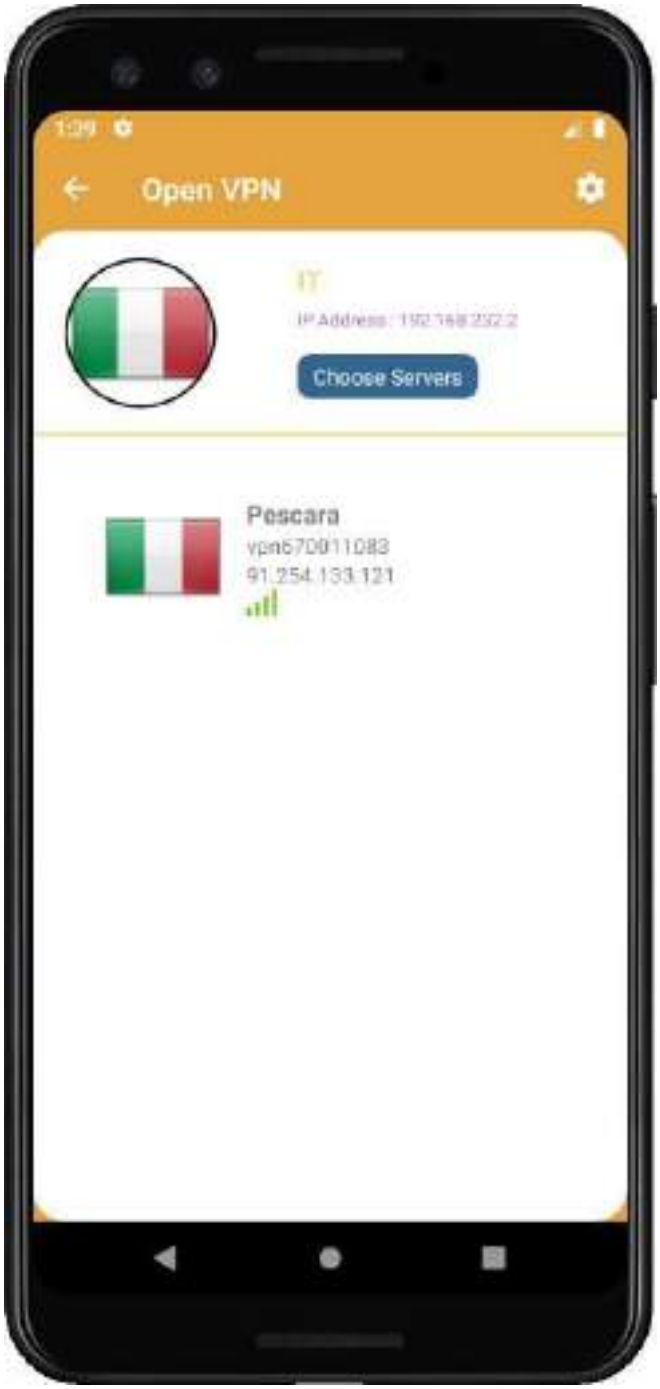


*Figura 2 – 164 Pantalla Servidor País*

**II.3.3.6.9.8 Pantalla (Servidor Seleccionado)**


*Figura 2 – 165 Pantalla Servidor Seleccionado*

**II.3.3.6.9.9 Pantalla (Moverse Otro País)**

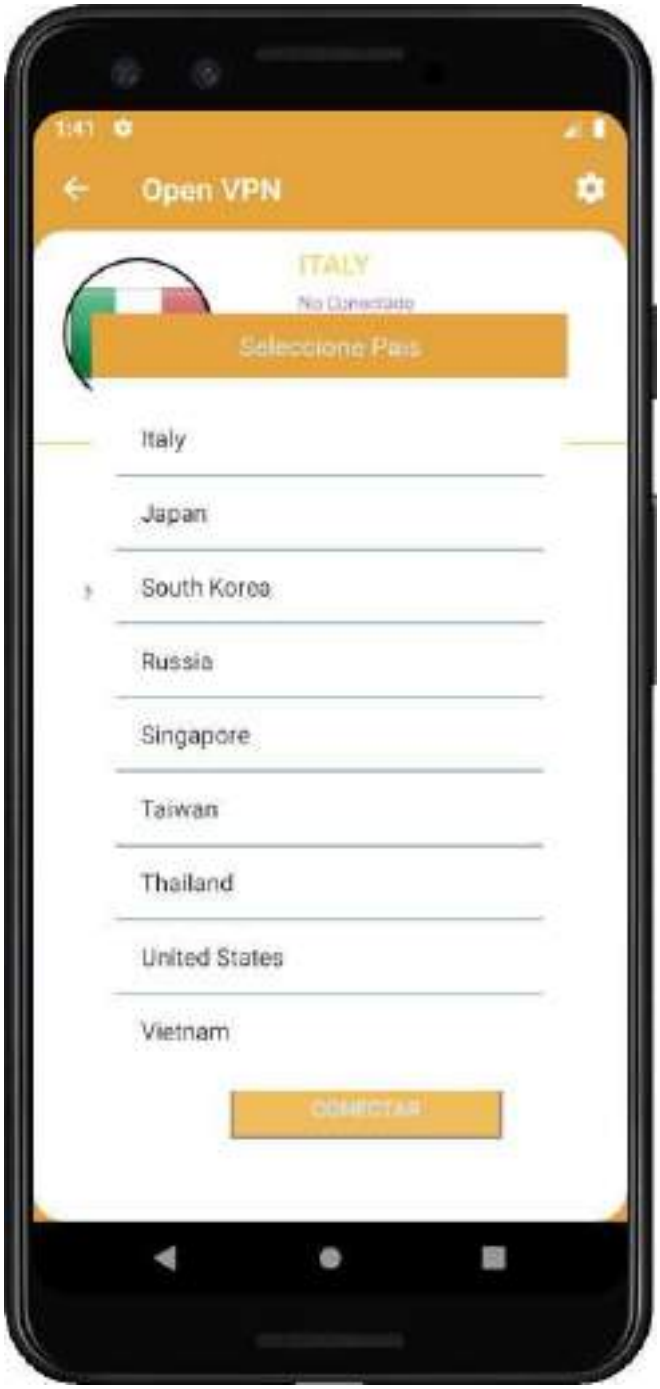


*Figura 2 – 166 Pantalla Moverse Otro País*

### II.3.3.6.9.10 Pantalla (Conectado Servidor)

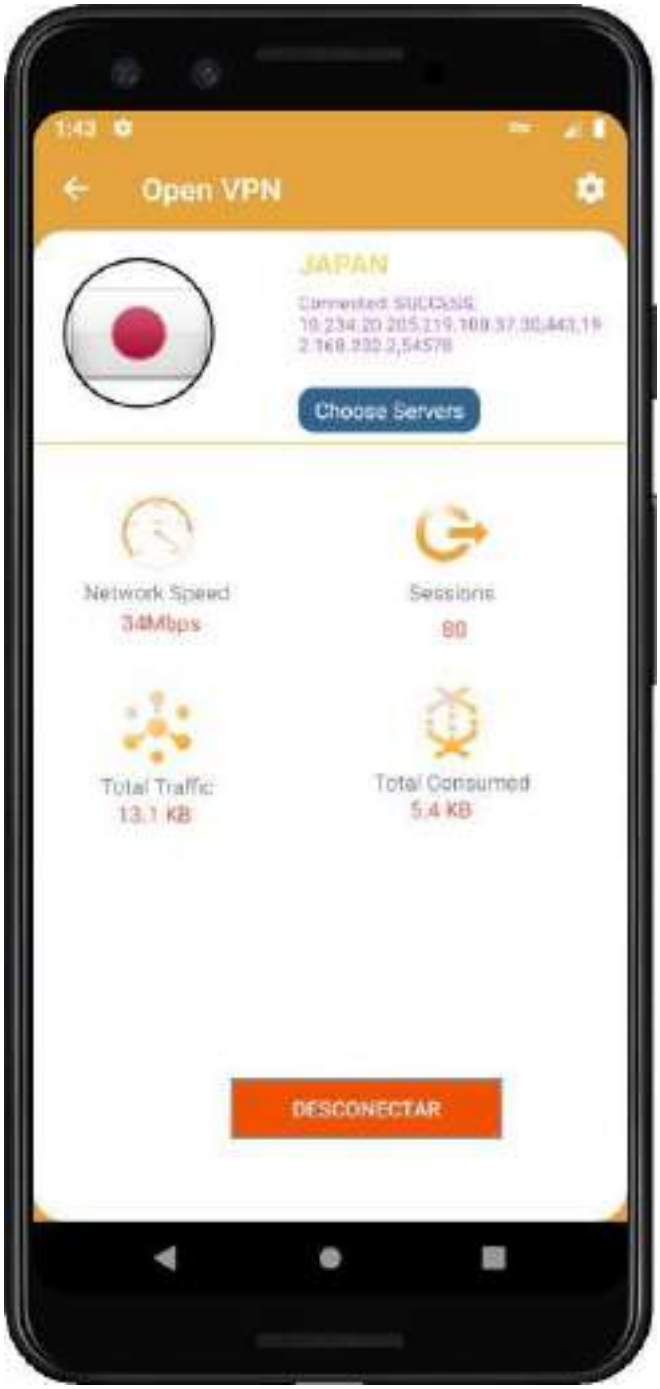


*Figura 2 – 167 Pantalla Conectado Servidor*

### II.3.3.6.9.11 Pantalla (Configuraciones)


*Figura 2 – 168 Pantalla Configuraciones*

### II.3.3.6.9.12 Pantalla (Configuraciones segundos reconexión automática)


*Figura 2 – 169 Pantalla Configuraciones segundos reconexión automática*

### II.3.3.6.9.13 Pantalla (Escoger país para conectarse por defecto)

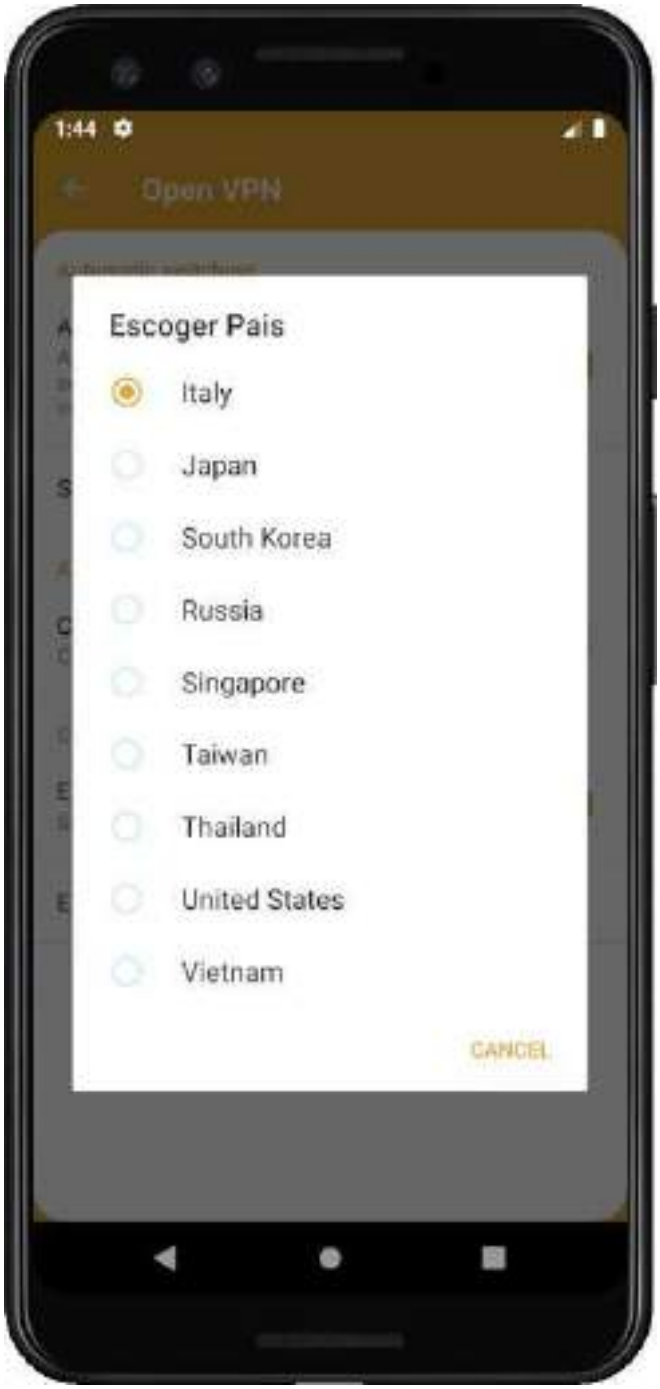


*Figura 2 – 170 Pantalla Escoger país para conectarse por defecto*

### II.3.3.6.9.14 Pantalla (Navegación)

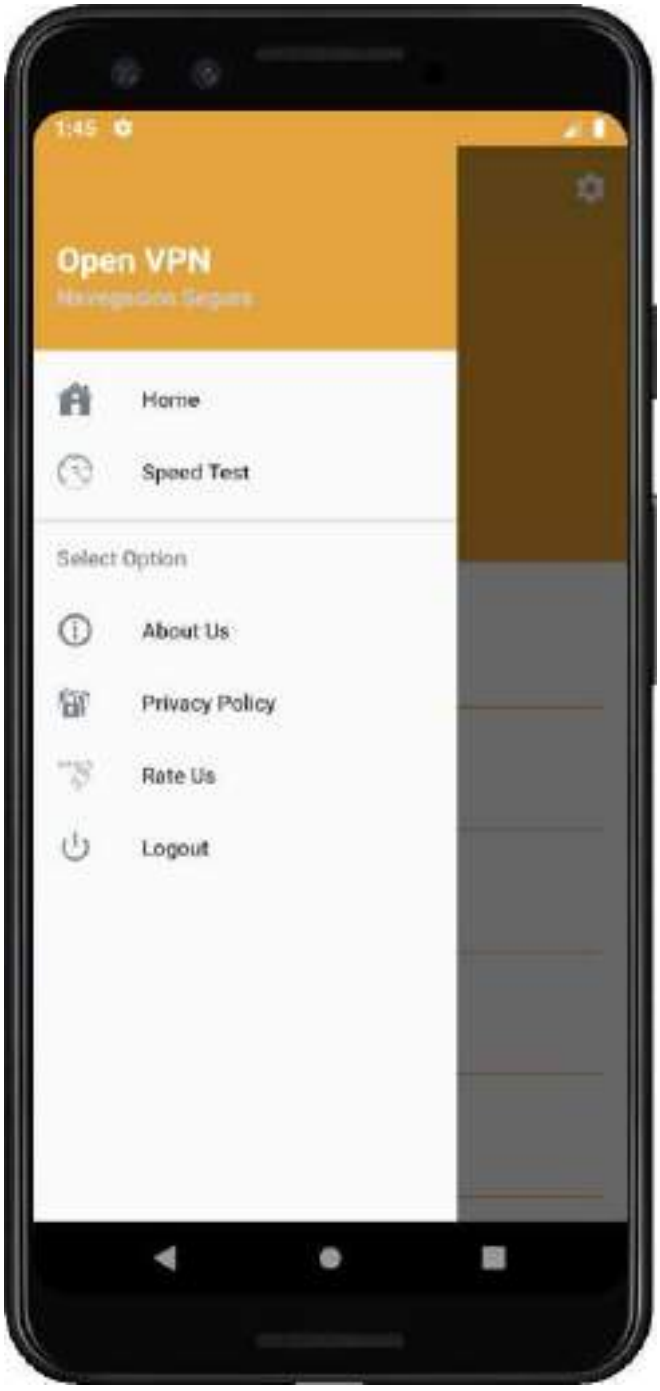


*Figura 2 – 171 Pantalla Navegación*

### II.3.3.6.9.15 Pantalla (Prueba de Velocidad)


*Figura 2 – 172 Pantalla Prueba de Velocidad*

### II.3.3.6.9.16 Pantalla (Prueba de Velocidad Realizada)


*Figura 2 – 173 Pantalla Prueba de Velocidad Realizada*

### II.3.3.6.9.17 Pantalla (Información sobre la Aplicación)


*Figura 2 – 174 Pantalla Información sobre la Aplicación*

### II.3.3.6.9.18 Pantalla (Políticas de Privacidad)


*Figura 2 – 175 Pantalla Políticas de Privacidad*

### II.3.4 Medios de verificación (Componente 3)

#### II.3.4.1 Pruebas de Seguridad Conexión Directa

Realizando la prueba de IP check podemos ver que la pagina detecta con facilidad todos nuestros datos y no solo los nuestros, sino que también los de nuestro ISP dejando ver que él está pasando por un DNS de Brasil para llegar al internet, lo cual es cierto ya que Bolivia no tiene una conexión directa a la internet, sino que pasamos por las conexiones marítimas en Brasil.


*Figura 2 – 176 Prueba IP Check página Perfect Privacy sin VPN*

Realizando la prueba WebRTC Leak podremos observa que al conectarse directamente al internet y solicitar a la página ingreso estamos no solo compartiendo nuestra IP publica que si no también dentro de la solicitud encontré que nuestra IP local también se está mostrando lo cual es un problema bastante grande ya que podría dirigir a nosotros directamente y a nuestra información, incluyendo también poniendo en riesgo nuestros dispositivos.


*Figura 2 – 177 Prueba WebRTC Leak Test página Perfect Privacy sin VPN*

Realizando la prueba de DNS se detectan los DNS del ISP que llegaría a ser Tigo brindando la información y mostrando que ellos usan 2 servidores DNS uno para paquetes locales y otro para quetes externos dado que también existen IP publican en Bolivia para servicio como llegan a ser las páginas y servicio de la universidad que usas como ISP a TIGO y Entel Simultáneamente.

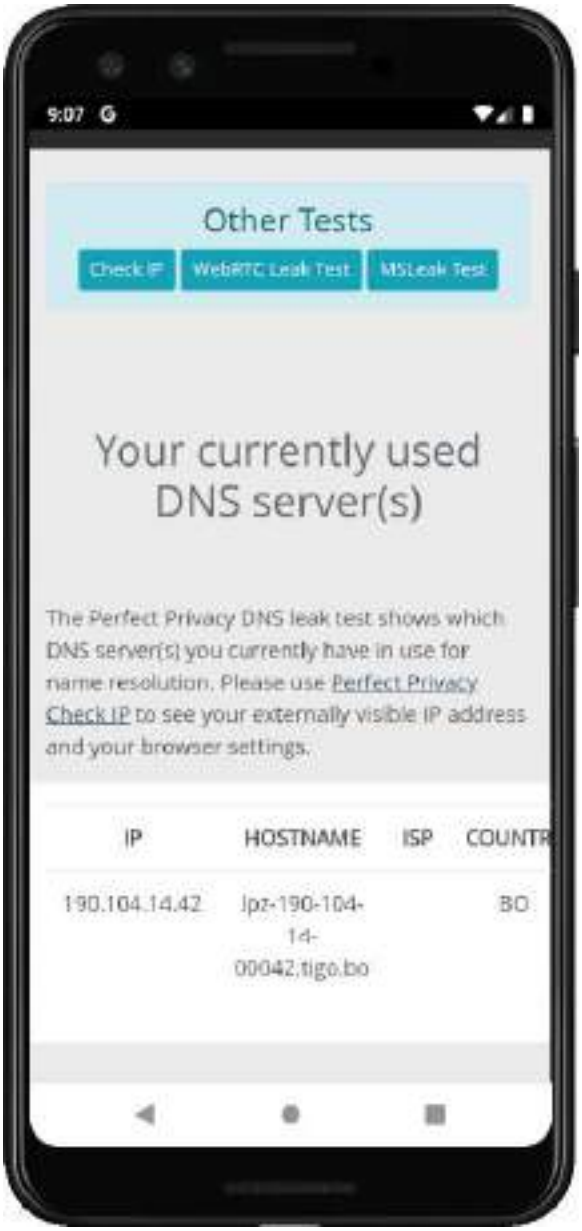


*Figura 2 – 178 Prueba DNS página Perfect Privacy sin VPN*

La última prueba es ver cuál es la velocidad de nuestra conexión a la internet cuando no estamos usando un VPN para protegernos, el plan con el que cuento debería darnos 60MB de ancho de banda entre baja y subida.


*Figura 2 – 179 Prueba velocidad Internet página SpeedTest by Ookla sin VPN*

### II.3.4.2 Pruebas de Seguridad Conexión VPN

a prueba nos muestra que tenemos un IP en el país de nuestro servidor que es el Estado Unidos en la ciudad de Santa José además de cambiar nuestro DNS y mostrar ahora que estamos saliendo directamente de nuestro hosting que es Vultr. También muestra que nuestras solicitudes no contienen ningún tipo de rastreos o registros de navegación ni de tipo HTTP o HTTPS también indicando que solo tenemos activado JS y no así Java o Flash.


*Figura 2 – 180 Prueba IP Check página Perfect Privacy con VPN*

El DNS test nos muestra que tampoco ve que estemos haciendo más de 2 saltos en cuanto a nuestras solicitudes a su página lo que es bueno ya que ni siquiera puede ver nuestro DNS principal si no que solo los de nuestro servidor, las IPs todas son de nuestros servidores y los saltos.

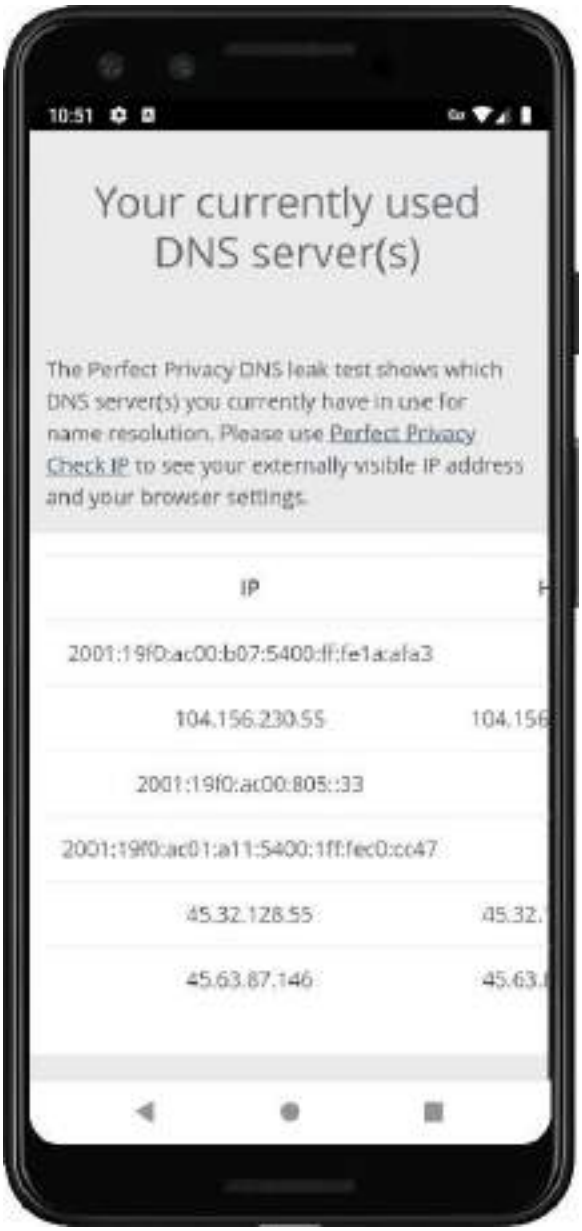


*Figura 2 – 181 Prueba DNS página Perfect Privacy IP con VPN*

El DNS test también nos muestra que nuestras solicitudes están saliendo de Vultr gracias a que el hostname está dentro de la información que puede obtener la página cuando entramos a ella.


*Figura 2 – 182 Prueba DNS página Perfect Privacy Hostname con VPN*

Por último, el WebRTC Leak Test no muestra que no pueden encontrar rastro alguno de nuestra IP real por lo tanto el servicio de OpenVPN que instalamos está protegiendo nuestra identidad en la red a no permitir que nadie puede obtener nuestra IP real.


*Figura 2 – 183 Prueba WebRTC Leak Test página Perfect Privacy con VPN*

Para finalizar las pruebas al servicio OpenVPN que levantamos veremos en la localización actual cual es nuestra velocidad y ping dado que todo estos saltos y la encriptación de nuestras solicitudes tienen a reducir lastimosamente nuestra velocidad de conexión a cambio de brindarnos seguridad. Lo haremos en la página SpeedTest by Ookla.


*Figura 2 – 184 Prueba velocidad Internet página SpeedTest by Ookla con VPN*

### II.3.4.2.1 Diagrama de Red

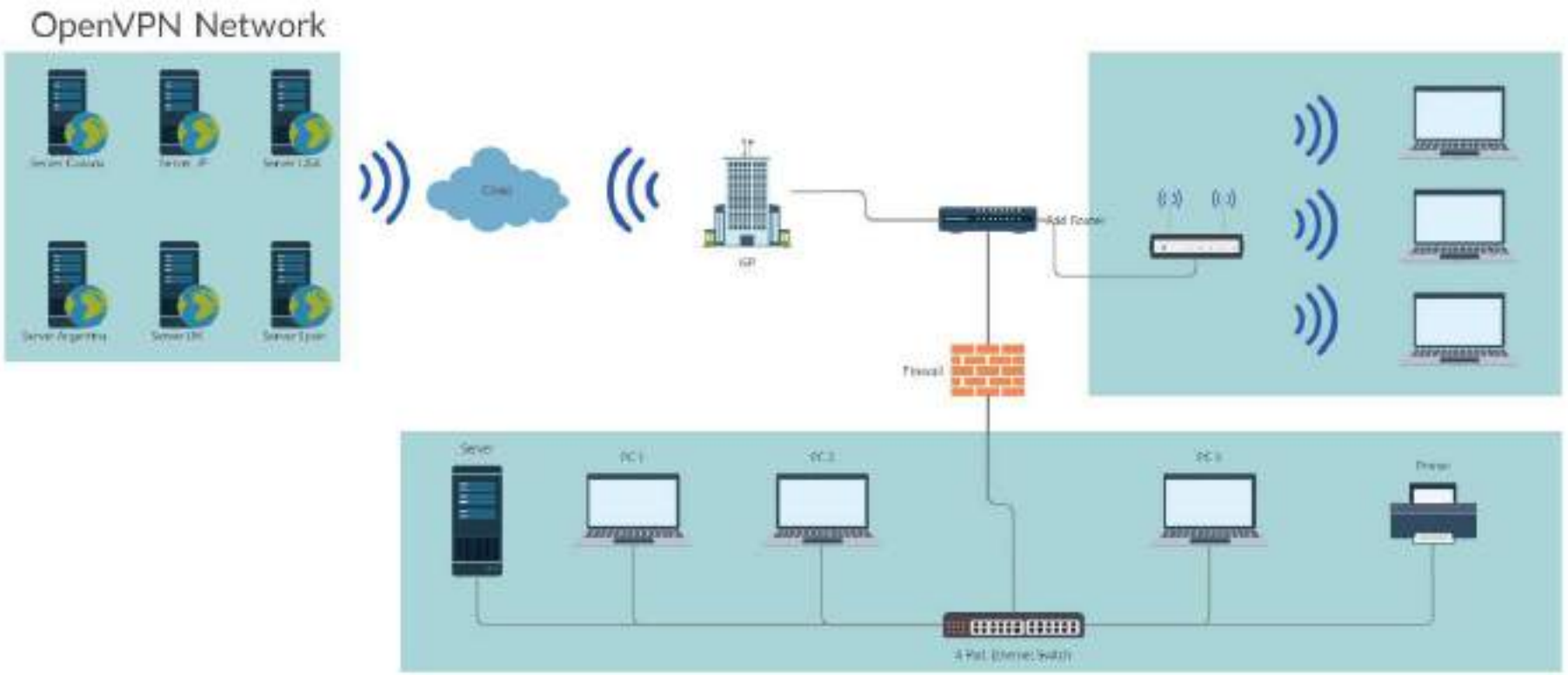


*Figura 2 – 185 Diagrama de R*

### II.3.4.2.2 Diagrama de Actividades del Proyecto

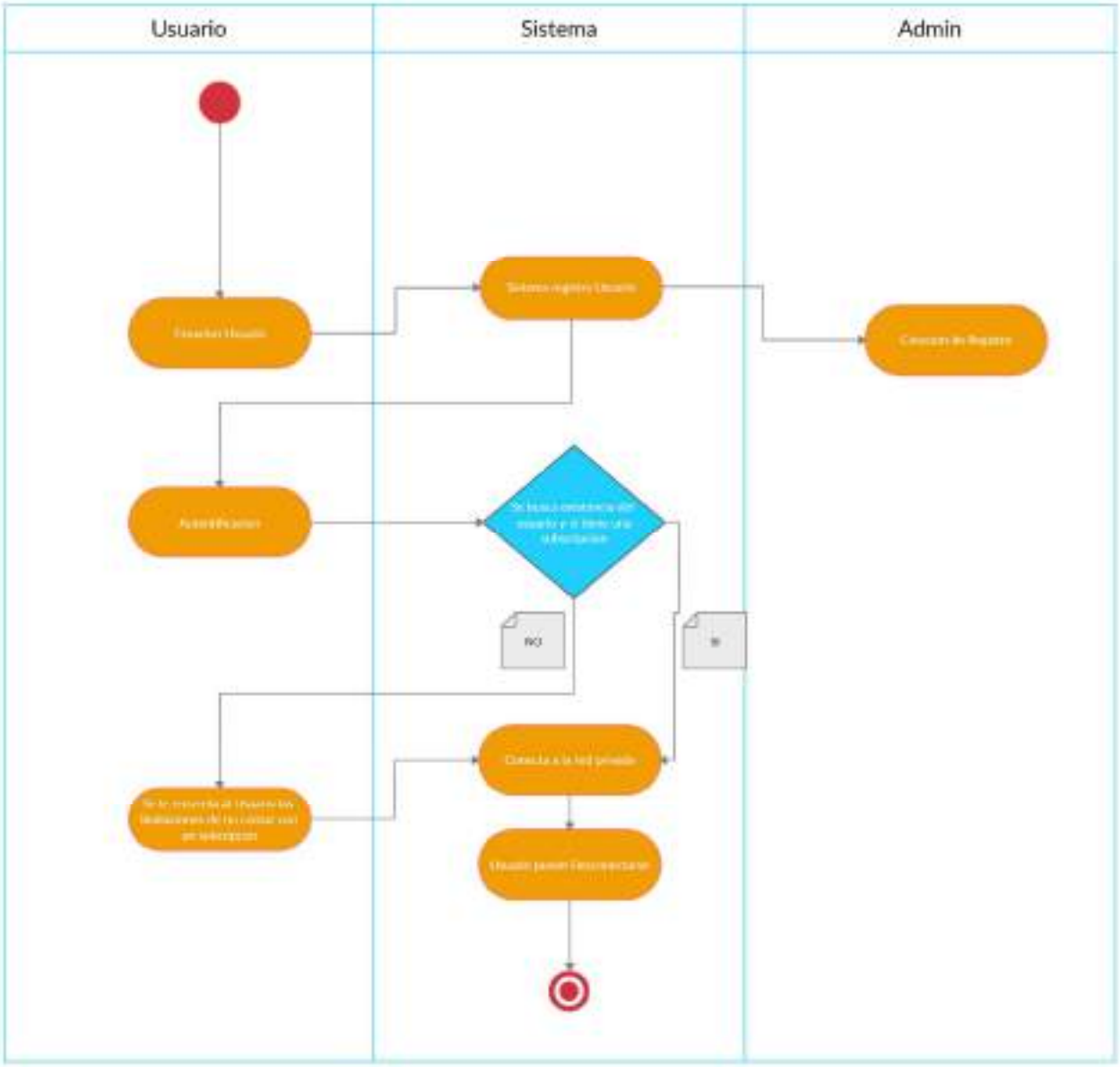


*Figura 2 – 186 Diagrama de Actividad del Proyecto*

# CAPÍTULO III
# CONCLUSIONES Y RECOMENDACIONES

# CAPÍTULO III: Conclusiones y Recomendaciones

## III.1 Conclusiones

Se concluye con el presente proyecto, que estudia las redes y el internet mismo, como todo hoy en día está involucrado con la internet la "Red de Redes" vemos los procesos y teórica que involucrara que todo el mundo pueda estar conectado.

Tomando en cuenta los Objetivos Planteados se llega a las siguientes conclusiones:

- Se desarrollo el sistema web de gestión de los usuarios de la VPN "Fast Tunnel VPN" en su totalidad según los alcances y limitaciones del proyecto.
- Se realizo un estudio en general de servicios de Hosting en busca de los mejores en cuanto a seguridad y normas que manejan.
- Se estudio a servicios de VPN similares a la hora de diseñar las características para la aplicación como NordVPN, PIA y Tunnel Bear.
- Se desarrollo la Red privada virtual basada en OpenVPN con servidores en los países más demandados.
- Se implemento el método de pagos en línea para la suscripción al servicio con el uso de in-app purchases IAPs pagos.
- Se desarrollo la aplicación en Android para que los usuarios de ese sistema operativo puedan usar el VPN.
- Todas las solicitudes de los dispositivos conectados al VPN están correctamente protegidas.
- Con el desarrollo del proyecto se ha logrado ofrecer una opción para las personas que desean conectarse a la internet de una manera más segura tanto de manera gratuita como de una manera pagada.
- La aplicación cuenta con una interfaz super amigable y muy fácil de entender a la hora de que los usuarios quieran usarlo aun siendo su primera vez entenderán lo más básico de inmediato.

## III.2 Recomendaciones

A partir del presente proyecto se propone las siguientes recomendaciones, con el fin de buscar el mejoramiento del sistema.

- Incrementar el número de servidores disponibles como así también la localización en las que están disponibles para incrementar las opciones de los usuarios.
- Desarrollar aplicaciones para otras plataformas además de Android.
- Estudiar otros tipos de infraestructuras disponibles para la creación de redes privadas virtuales que podrían ser otras opciones o con otros puntos fuertes.
- Actualizar constantemente la aplicación y desarrollar versiones más compatibles con versión o dispositivos más antiguos.
- Incrementar las opciones del sistema web, sus características, pero manteniendo como principio que entre menos información se tenga de los usuarios es más seguro para ellos y es de nuestro interés priorizar su seguridad y anonimidad.