ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE PROTECCIÓN PARA PERÍMETRO DE RED DEFINIDO POR SOFTWARE PARA LA RED DE ALTEL S.A.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELÉCTRONICA Y TELECOMUNICACIONES

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

LÓPEZ CRUZ CARLOS ENRIQUE

VÁSCONEZ ARIAS NATHALY VALERIA

DIRECTOR: ING. CARLOS ALFONSO HERRERA MUÑOZ

Quito, abril 2021

AVAL

Certifico que el presente trabajo se desarrolló por Carlos Enrique López Cruz y Nathaly Valeria Vásconez Arias bajo mi supervisión.

Ing. Carlos Alfonso Herrera Muñoz
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Nosotros, Carlos Enrique López Cruz y Nathaly Valeria Vásconez Arias, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no se presenta previamente para ningún grado o calificación profesional; y, que se consulta las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración se deja constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos que estipula la Ley, Reglamentos y Normas vigentes.

Carlos Enrique López Cruz	Nathaly Valeria Vásconez Arias

DEDICATORIA

El presente trabajo de titulación lo dedico principalmente a Dios, por ser la inspiración y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mi madre y abuela, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. Son definitivamente lo mejor del mundo

Lo dedico también a mi compañera de vida, Yanara, quien me ha acompañado los últimos años y me ha impulsado a crecer de forma constante y superar las adversidades.

Carlos

DEDICATORIA

Para mi ángel, Luis, que ha cumplido su promesa de no dejarme sola ni un solo día.

Valeria

AGRADECIMIENTO

Agradezco a Dios ya mi madre por bendecirme toda la vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Agradezco a Yanara, por ser el impulso y el apoyo en momentos de debilidad.

Finalmente, a mis profesores al Ingeniero Carlos Herrera por su guía para el cumplimiento del proyecto de titulación y amigos en las aulas, que hicieron de este paso por la universidad una de las épocas más felices de mi vida.

Carlos

AGRADECIMIENTO

Agradezco a Dios por guiarme a lo largo de mi vida y ser mi fortaleza en los momentos más difíciles, sé que sin su infinito amor no hubiera alcanzado mis metas.

Gracias a mi familia que ha sido mi motor para cumplir cada sueño en mi vida, a mi mamá por todo su esfuerzo y dedicación, por su paciencia y amor, por animarme a que no me de por vencida. A Emi por ser la mejor hermana del mundo, gracias por ser mi mejor amiga y cómplice y a Luisito por ser un ejemplo para mí a pesar de ser menor. A mi abuelita y mis tíos, Mary, Karo, Darwin y a Cris por ser mi segundo papá, gracias por todo su amor y su apoyo en los mejores momentos de mi vida, pero sobre todo en los peores.

Gracias a mi ángel, mi papá, que no me ha dejado sola ni un solo día, gracias por enseñarme el significado del verdadero amor.

Gracias a Marianita y Julio por su apoyo y amor durante este tiempo, se han convertido en una parte muy importante en mi vida.

A mi compañero de tesis por compartir todo su conocimiento conmigo, gracias por toda tu paciencia Carlitos, eres un gran maestro y amigo.

Finalmente, a nuestro director de tesis el Ing. Carlos Herrera por su guía para realizar la tesis, a mis profesores y amigos en las aulas, que este uno de los mejores tiempos de mi vida.

Valeria

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURA

ÍNDICE DE TABLA

RESUMEN

El presente trabajo de titulación propone la implementación de un prototipo de sistema de protección para brindar seguridad y privacidad a través de SDP, perímetro definido por software, por sus siglas en inglés, en la red de la empresa ALTEL S.A.

Para esto se analiza la evolución de las redes, con énfasis a los conceptos de perímetro de red y la influencia de los servicios en la nube, el aumento de tráfico de datos en los últimos años y cómo este desarrollo cambió los conceptos de requerimientos de los usuarios y las empresas en general.

En el capítulo 1 se presenta todo lo referente a conceptos que son necesarios conocer para comprender y sustentar las bases que permiten aplicar la solución de perímetro definido por software.

En el capítulo 2 se describe una metodología propuesta y diseñada por los autores del este Trabajo de Titulación, para poder aplicar de forma efectiva la solución de perímetro definido por software en una red corporativa.

En el capítulo 3 se presenta la implementación de un prototipo de aplicación de una solución de protección de perímetro definida por software.

Se realiza un repaso de los conceptos con relación a ciberseguridad para engranar estos a una metodología de diseño de soluciones de protección para servicios locales y de nube que permite a los usuarios contar con los beneficios de la seguridad de una red local pero esta vez con movilidad libre, sin restricción en los dispositivos que usa y sin afectar su experiencia al consumir recursos corporativos a través de internet.

Se analizan las dificultades para proteger la red por el rápido crecimiento que presenta, con el fin de proponer e implementar una metodología que permite diseñar un prototipo de sistema de protección.

Finalmente se realizará un análisis de resultados que facilita la verificación del cumplimiento de los objetivos que se declaran mediante la evaluación de la implementación de un prototipo de sistema de protección SDP y se demuestra la gestión mediante una plataforma de administración web.

PALABRAS CLAVE: Ciberseguridad, SDP, *Software Defined Perimeter*, *Cloud Protection*, CASB, NaaS.

ABSTRACT

This qualification work proposes the implementation of a prototype protection system to provide security and privacy through SDP, a software-defined perimeter, in the network of the company ALTEL S.A.

This analyzes the evolution of networks, emphasizing the concepts of network perimeter and the influence of cloud services, increasing data traffic in recent years, and how this development has changed the concepts of requirements of users and businesses in general.

Chapter 1 presents everything about concepts that need to be known to understand and support the foundations for applying the software-defined perimeter solution.

Chapter 2 describes a methodology designed by the authors to effectively implement the software-defined perimeter solution in a corporate network.

Chapter 3 introduces the implementation of an application prototype of a software-defined perimeter protection solution.

A review of the concepts associated with cybersecurity is reviewed to link them to a methodology for designing protection solutions for on-premises and cloud services that allows users to have the security benefits of an on-premises network but this time with free mobility, without restriction on the devices it uses and without affecting their experience consuming corporate resources over the Internet.

It analyses the difficulties in protecting the network by the accelerated growth it presents, to propose and implement a methodology that allows to design a prototype protection system.

Finally, a results analysis will be carried out that facilitates the verification of the fulfillment of the objectives set by evaluating the implementation of a prototype SDP protection system and demonstrates management through a web management platform.

KEY WORDS: Cybersecurity, SDP, Software Defined Perimeter, Cloud Protection, CASB, NaaS

1 INTRODUCCIÓN

En la búsqueda constante de facilitar la escalabilidad, movilidad, disponibilidad, agilidad, y capacidad de almacenamiento de las redes, la computación en la nube adquiere gran popularidad y cada vez, es más común el uso de servicios que se conocen como IaaS (*Infraestructure as a Service*), SaaS (*Software as a Service*), PaaS (*Platform as a Service*) y en general aplicaciones a las cuales se accede fácilmente desde cualquier parte del mundo mediante Internet. Por otro lado, la evolución de los sistemas de comunicación inalámbricos permite el acceso desde múltiples puntos geográficos.[1]

Tanto los servicios en la nube, como las comunicaciones inalámbricas hacen cada vez más compleja la tarea de los administradores de estos sistemas en cuanto a seguridad se refiere, tareas como controlar los accesos, permisos y proteger la información de estas aplicaciones o sistemas es mucho más complejo. En los últimos años es común ser víctimas de ataques informáticos o de virus y software malicioso, que permite a los atacantes hacer movimientos laterales, derramamiento de información en sistemas que comparten infraestructura, suplantación de identidades, acceso sin autorización, almacenamiento y distribución de *malware*, entre otras. Esto afecta la disponibilidad, integridad y confiabilidad de la información.

El presente Trabajo de Titulación se enfoca en implementar un prototipo de protección de red para la empresa ALTEL S.A., este puede ofrecer capacidades de protección para escenarios en que los recursos de información necesarios, están en la red local y también en servicios en las nubes de diferentes proveedores, para esto, se realiza el análisis del concepto de SDP, el desarrollo de la metodología para el diseño y el diseño para un segmento de usuarios, donde se hacen pruebas piloto de funcionamiento, operatividad, carga y seguridad, se revisa todos los conceptos base necesarios para comprender de forma efectiva lo descrito y que esto sea factible de aplicar por cualquier empresa en busca de una solución de protección con los retos actuales y los cambios que vienen en el corto y mediano plazo en cuanto a infraestructura y servicios de red.

1.1 OBJETIVOS

El objetivo general de este Proyecto de Titulación es:

- Implementar un prototipo de Sistema de Protección para Perímetro de Red Definido por Software para la Red de ALTEL S.A. mediante el uso de la plataforma PRISMA ACCESS de la empresa Palo Alto Networks.

Los objetivos específicos de este Proyecto de Titulación son:

- Estudiar la evolución del perímetro de las redes, su seguridad y componentes de arquitecturas de red actuales y los mecanismos de protección que se fundamentan en Perímetro Definido por Software SDP.

- Proponer una metodología para el diseño de un prototipo de sistema de protección con base en perímetro definido por software para la red de ALTEL S.A.

- Diseñar un prototipo de sistema de protección para perímetro definido por software para la red de ALTEL S.A. mediante la metodología definida.

- Implementar una prueba para el prototipo de sistema de protección que se diseñó, con base en el perímetro definido por software para la red de ALTEL S.A.

- Realizar pruebas de funcionamiento y validación de los resultados que se obtendrán con la implementación de la prueba de prototipo.

1.2 ALCANCE

Este Trabajo de Titulación propone el desarrollo de un prototipo de red para brindar seguridad y privacidad a la red a través del SDP en la empresa ALTEL S.A. mediante la realización de cinco fases:

- Fase I: Se realizará el estudio de la evolución de las redes, la seguridad y su impacto en el concepto del perímetro.

- Fase II: Se propondrá una metodología que permita diseñar un prototipo de sistema de protección para perímetro definido por software para la red de ALTEL S.A.

- Fase III: Se realizará el diseño del prototipo de un sistema de protección para perímetro definido por software para la red de ALTEL S.A.

- Fase IV: Se implementará un prototipo de sistema de protección para perímetro definido por software para la red de ALTEL S.A.

- Fase V: Se realizará un análisis de resultados que permitirá verificar el cumplimiento de los objetivos que se declararon.

Este Trabajo de Titulación se enfoca a la implementación de un prototipo que cubre un segmento de la red para usuarios administrativos y servicios básicos de red, que incluye lo siguiente:

- Dos usuarios
- Dos *laptops*
- Servicio de correo electrónico con *Google Mail*
- Servicio de ofimática en la nube con GSUIT
- Servicio de almacenamiento de archivos tipo *SaaS* con *Drive*
- Infraestructura en modalidad *IaaS* (un servidor en *AWS*)
- Un dispositivo móvil con sistema *Windows*

Para el acceso a los servicios desde la red local y desde diferentes puntos externos, se emplea los servicios de Internet en general.

Para la demostración final se presenta la interfaz web de administración de la plataforma *SaaS* PRISMA ACCESS de la empresa Palo Alto Networks enfocada en SDP, implementada como prototipo de protección del perímetro local, y extendido de la empresa auspiciante.

1.3 MARCO TEÓRICO

1.3.1 SASE – SECURE ACCESS SERVICE EDGE

Es una categoría de tecnología de redes introducida por Gartner en 2019, agrupa **soluciones de red** y **seguridad** en un servicio global que se encuentra en la nube.

La **Figura 1.1** Modelo SASE indica todas las capacidades que debe tener un servicio que opera como Perímetro Definido por Software basado en el concepto de SASE.

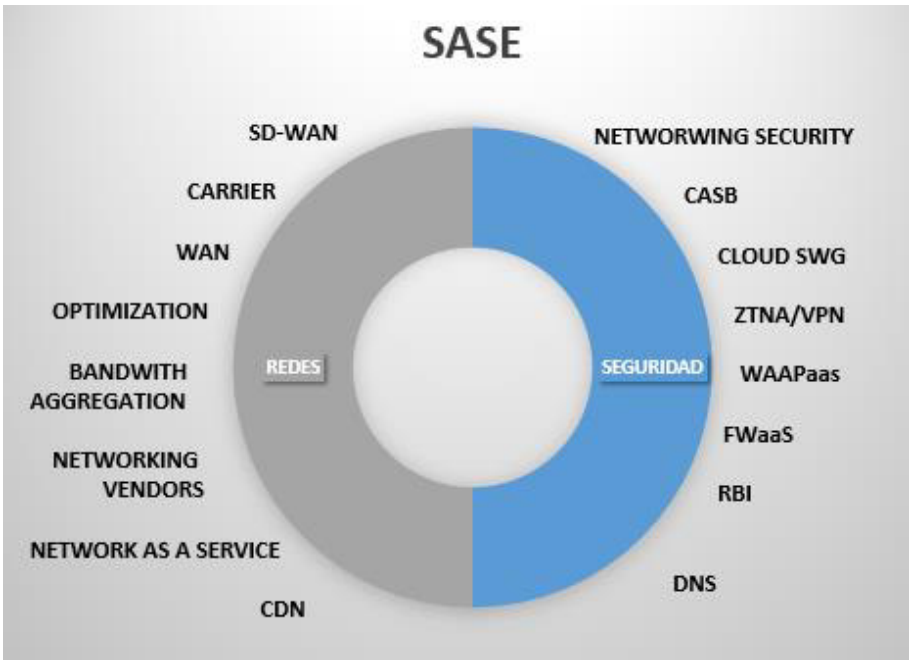

Figura 1.1 Modelo SASE

Al considerar la evolución del perímetro y que un usuario puede acceder a Internet desde cualquier lugar y usar cualquier dispositivo de punto final, es necesario establecer un esquema de seguridad que se adapte a cada situación, ubicación y necesidad particular de los usuarios, lamentablemente con equipamiento como routers, firewalls, software como antimalware, no se puede cubrir con todos los requerimientos de seguridad que son necesarios hoy en día. [2]

Por tanto, es necesario contar con un servicio que considere los conceptos propuestos, en la Figura 1.1 Modelo SASE. Estos servicios permiten extender el perímetro de una forma sencilla hasta el dispositivo final mediante el uso de esquemas como *Zero Trust o ZT,* por sus siglas en inglés, firewall como un servicio, análisis de comunicaciones a DNS que

tengan reputación de actividad maliciosa y bloquearlos, redes como servicio para asegurar el transporte de datos desde el origen a un destino explícito en la red interna o en la nube, caché de contenido en la nube del proveedor de SDP para reducir el impacto en la red de destino por volumen de tráfico con el uso de *Content Delivery Network o* CDN, por sus siglas en inglés, entre otros.

Todos los esquemas, modelos, equipos y soluciones de seguridad detalladas pasan a ser pequeños aportes de un macro servicio en la nube, facilita a los administradores la implementación de políticas en las infraestructuras de red globales que son escalables y tienen altas prestaciones y rendimiento.

1.3.2 REDES

1.3.2.1 Definición

Una red informática es un conjunto de dispositivos que interactúan entre sí, mediante conexiones físicas y lógicas. Este tipo de conexiones entre dispositivos permiten compartir información, recursos y servicios entre usuarios que se encuentran en distintos lugares geográficos.

Las redes informáticas evolucionan rápidamente a causa de la necesidad constante de recibir, procesar y enviar mayor cantidad de información a mejores velocidades, pero este crecimiento representa un innumerable conjunto de retos como la protección de la información de personas no autorizadas a acceder. [3]

1.3.2.2 Clasificación

Existen varios criterios para clasificar las redes como, por ejemplo, por la cantidad de dispositivos que las conforman, por su uso, redes personales o corporativas, por su topología, por su relación en cliente servidor o punto a punto, entre muchas más, sin embargo, la clasificación por el alcance o área de cobertura es la que comúnmente se utiliza.[4]

Uno de los principales problemas en las redes era el alcance que podían llegar a tener, es decir, que tan amplio era el espacio geográfico que podían llegar a cubrir con el conjunto de dispositivos que las conforman, por esta razón se las clasifica por su alcance, como se observa en la Figura 1.2 y de esta manera desarrollar distintas tecnologías para cada una de las clasificaciones.

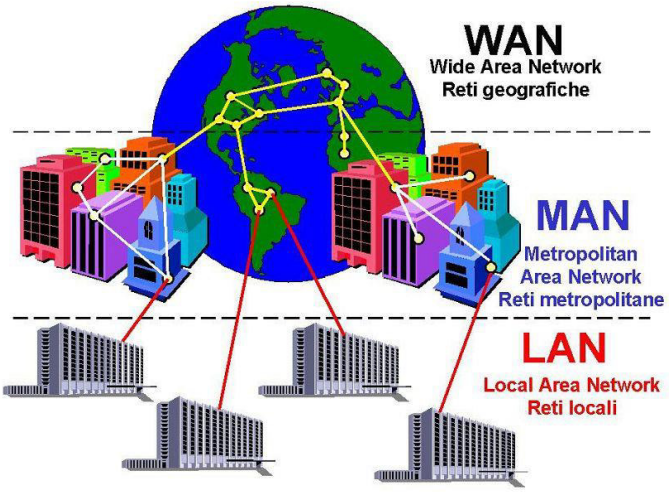

Figura 1.2 Clasificación de redes por su alcance

Al considerar el criterio de cobertura o alcance, las redes se clasifican en:

- Redes de Área Personal (PAN): Cubren el espacio geográfico de una persona, normalmente interconecta sensores que el usuario lleva en su cuerpo.
- Redes de Área Local (LAN): Cubren el espacio geográfico de una casa, oficina, piso o edificio.
- Redes de Área Metropolitana (MAN): Envuelven un espacio como una ciudad.
- Red de Área Extendida (WAN): Cubren varias ciudades, países e incluso continentes.

1.3.2.3 Conceptos de capas y protocolos

Para ampliar la compresión respecto al funcionamiento de las redes es necesario revisar el modelo de referencia actual que se usa para el diseño de redes y sus aplicaciones, ISO/OSI, consta de 7 capas, como se muestra en la Figura 1.3.

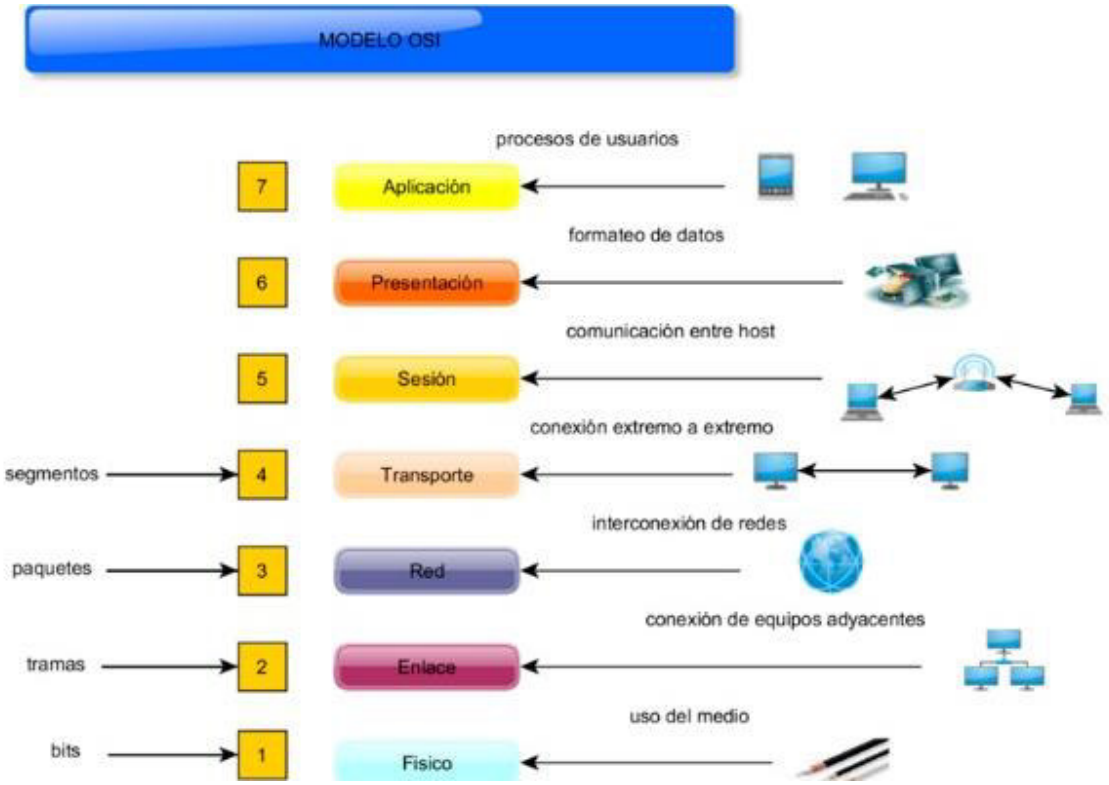

Figura 1.3 Modelo de referencia ISO/OSI

El Modelo OSI define 7 capas, las cuales son las siguientes:[5]

- Física: Establece la manera en la que la información se transmite al medio ya sea alámbrico o inalámbrico.
- Enlace: Define la mejor manera de conectan los equipos adyacentes para lograr una comunicación confiable, mediante el control de errores, de secuencia y de flujo.
- Red: Se encarga de la interconectar las redes, es decir, define el direccionamiento de los dispositivos y las redes.
- Transporte: Su objetivo es establecer conexiones confiables de extremo a extremo, asegurando que los paquetes lleguen sin errores y en el mismo orden que fueron enviados.
- Sesión: Su función es proporcionar mecanismos de comunicación con el host.
- Presentación: Prepara la información de las aplicaciones para mostrarlo al usuario.

- Aplicación: Es la capa que se encarga de las aplicaciones de usuario final y sus procesos.

Como se menciona anteriormente, el modelo OSI es una referencia, ya que, la arquitectura de las redes es TCP/IP y es aquí donde se definen los protocolos y servicios particulares que tendrá la red. En la actualidad la mayoría de las redes usan esta arquitectura que consta de 4 capas, para lograr esto, varias de las capas del modelo ISO/OSI se combinan con objeto de mejorar y facilitar las operaciones y diseño. A continuación, la Figura 1.4 ilustra las capas: [6]

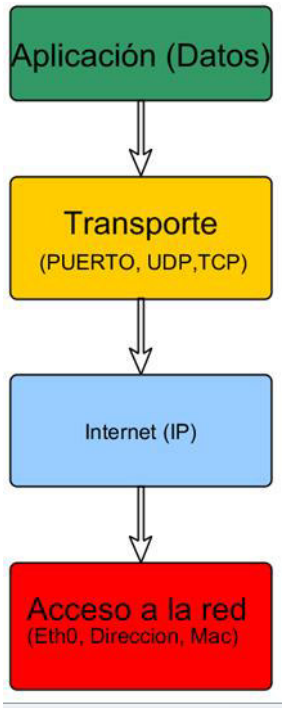

Figura 1.4 Capas del modelo TCP/IP

Las capas de la arquitectura TCP/IP son las siguientes:

- Acceso a la red: Esta capa realiza las funciones de la capa física y enlace del modelo OSI. Se encarga de todos los aspectos para que el protocolo IP acceda a un enlace físico con las características de la tecnología de red que se utilice.

- Internet: Su función se asemeja al desempeño de la capa de red en el modelo OSI. Selecciona la mejor ruta para que los paquetes de información alcancen su destino mientras viajan por la red. El protocolo IP es un protocolo no orientado a conexión que realiza el máximo esfuerzo. Al decir no orientado a conexión no significa que

no enviará correctamente los datos, sino que IP no realiza la verificación y la corrección de errores, para esto se apoya con los protocolos de las capas superiores.

- Transporte: Esta capa realiza la misma función que la capa que lleva el mismo nombre en el modelo OSI. Establece una conexión lógica entre el equipo que envía la información y quien la recibe.

- Aplicación: Esta capa desarrolla las funciones que realizan las capas sesión, presentación y aplicación del modelo OSI. Contiene protocolos de alto nivel para presentar la información al usuario.

El uso de estos conceptos llevó a las redes a un auge importante durante las últimas décadas. En general todas las redes alrededor del mundo están conectadas mediante una macro red conocida como la Internet que se conoce como la red de redes

Así se llega a tener múltiples redes privadas de muchas organizaciones que trabajar con recursos y servicios locales como se detalla en la Figura 1.5**¡Error! No se encuentra el origen de la referencia.**, y al mismo tiempo se accede a servicios públicos que comparten múltiples usuarios en diversas partes del mundo a través de redes públicas mediante el empleo de servicios de Internet.[7]

Figura 1.5 Conexión de área local

1.3.2.4 ISP - Proveedor de servicios de internet.

Para poder acceder a servicios en Internet existen empresas que facilitan las conexiones e implementan la infraestructura necesaria para sostener la transmisión de datos a gran

escala en una o varias ciudades, países o continentes. Esta infraestructura consiste en cables, equipos y herramientas necesarias para que el transporte de información sea efectivo, también involucra personal que se especializa en la administración, diseño e implementación de estos complejos sistemas[8]

El equipamiento que utiliza el ISP, entre otros, son cables, conmutadores y enrutadores, estos dos últimos son dispositivos que ayudan en el transporte de la información, al decidir las mejores rutas, las interfaces de entrada y salida de información, etc. Estos equipos se ubican en sitios conocidos como nodos de conmutación, que son centros de procesamiento de información o simplemente *Datacenter* en inglés.

Los *Datacenters* evolucionan para proveer no solo servicios de transporte de datos por los ISP sino para también proveer servicios a las empresas de aplicaciones para los usuarios finales como correo electrónico, infraestructura rentada, soporte y mantenimiento. [9]

Por ejemplo, existen ISP proveen servicios como *hosting*, es decir, si una empresa requiere un servidor de DNS, el ISP lo crea, mantiene y actualiza, si se requiere correo, página web, aplicación web, etc, de igual forma. Por otro lado, también proveen de servicios como *housing*, que es, el alquiler de un espacio físico en un *Datacenter*, si una empresa desea implementar servicios para sus empleados como el correo electrónico necesita tomar en cuenta elementos como:

- La infraestructura: Las conexiones eléctricas y los equipos de protección como reguladores de voltaje y corriente, las conexiones de red, el hardware que es el servidor o máquina física sobre la que instala el sistema y la aplicación, el sistema de enfriamiento para evitar que los equipos se sobrecalienten.

- El software: Se requiere un sistema operativo y una aplicación que sea compatible con este sistema y preste el servicio de correo electrónico.

- Los recursos humanos: Mínimo se necesita una persona que administre todos los recursos que se mencionan antes.

Esto puede resultar muy costoso y tedioso al momento de implementarlo es por esto, que las empresas deciden alquilar estos servicios a los ISP, que ya tienen esta infraestructura disponible y el costo lo dividirá entre sus “n” clientes. A este servicio se le llama housing.[10]

La diferencia entre el hosting y el housing es que el primero, nada es del cliente, salvo un servicio y quizá el software, en el segundo hasta los servidores son del cliente y lo demás como conexiones, sistemas de enfriamiento, servicios eléctricos, etc. son del proveedor.

1.3.2.5 Evolución de las redes

1.3.2.5.1 Virtualización

Toda aplicación requiere un entorno para ser puesta en producción, en el ejemplo del correo electrónico, se mencionó que se necesita un sistema operativo, este a su vez está sobre un servidor, este servidor está compuesto principalmente de memoria RAM, almacenamiento o discos y procesadores. Para poder dimensionar cuanto de cada uno de estos recursos es necesario para un servicio normalmente se considera un sobredimensionamiento consciente para evitar que el servicio deje de estar disponible por falta de recursos, en la hora pico de uso del correo electrónico, por ejemplo[11].

Lamentablemente esto es ineficiente ya que habrá una gran cantidad de recursos de memoria, procesamiento y disco que la mayor parte del tiempo se “desperdicia” – por decirlo de alguna manera –, esto dado que siempre se dimensiona para el peor escenario que por lo general son las horas pico.

Con el fin de romper este paradigma surgió la virtualización que es un sistema intermedio entre el servidor (el hardware) y el sistema operativo cuya función es utilizar de forma más eficiente los recursos de memoria, procesamiento y disco. Así, en un mismo equipo físico con un sistema de virtualización que comúnmente se llama hipervisor, se puede tener varios sistemas operativos con múltiples aplicaciones y los recursos se asignarán de forma semi dinámica o dinámica de acuerdo con la necesidad de cada aplicación.

En la Figura 1.6 se indica, el diagrama de funcionamiento de un hipervisor, donde se tiene un equipo de hardware o servidor, el sistema del hipervisor y las máquinas virtuales con un hardware virtual, un sistema operativo y su aplicación, así en nuestro ejemplo el mismo servidor podría eventualmente tener tanto el correo electrónico de la empresa como su página web e incluso otros servicios más como un servidor de archivos, el directorio de usuarios, el aplicativo de nómina, la aplicación de ventas, entre otros.

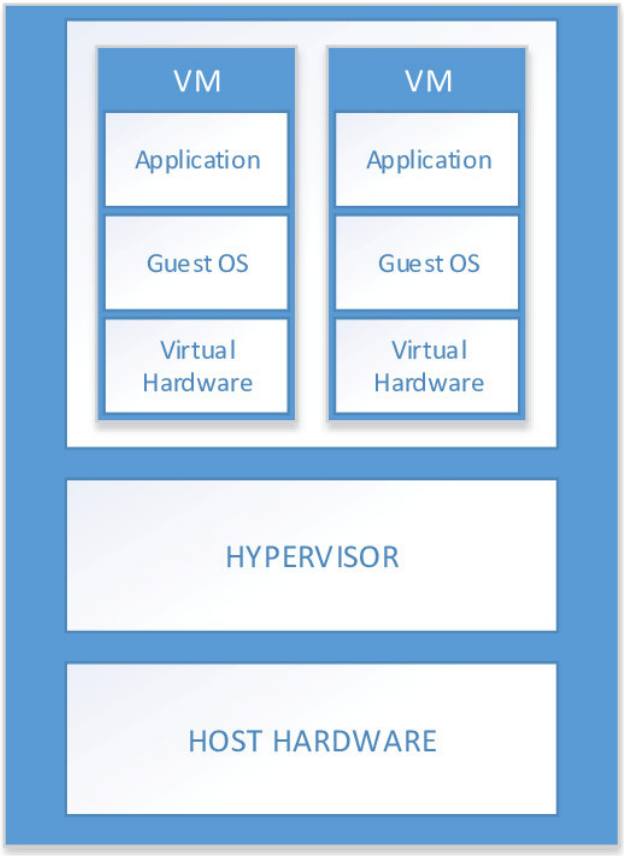

Figura 1.6 Diagrama de un hipervisor

1.3.2.5.2 Cloud

A pesar de que la virtualización solucionó en gran medida el problema de la subutilización de recursos, aún queda el problema de la infraestructura asociada a mantener operativo el hardware como los sistemas eléctricos, de enfriamiento y el cableado. Otro punto importante para considerar es la disponibilidad de los servicios, aún con toda la infraestructura al alcance de las empresas ¿qué podría ocurrir si hay un desastre natural, un corte de energía eléctrica o interrupción en el servicio de internet? Se requiere entonces un respaldo de todo eso en un sitio geográficamente distante para que no le afecte un desastre natural local o incluso continental, que tenga servicios eléctricos con otro proveedor de esto, independiente al primero y lo propio con el proveedor de internet. Esto último no necesariamente requiere otro sitio físico, se puede tener varios proveedores de internet en la misma oficina[12].

Ahora la pregunta es ¿Pueden las empresas darse el lujo de montar un *Datacenter* de respaldo? La respuesta es NO, sin lugar a discusión, ya que como se mencionó anteriormente era mejor rentar la infraestructura, y más aún si es uno de respaldo.

Para solucionar esta problemática nacen los servicios de *cloud* o nube, que son centros de datos gigantescos con recursos en renta para empresas que no desean o no tienen los recursos para montar sus propios *Datacenter* alrededor del mundo.

1.3.2.5.3 Evolución del Cloud

La computación en la nube y sus servicios tienen una evolución muy importante en la última década, en el mismo ejemplo del correo electrónico, hace una veintena de años cada empresa tenía su propio servidor de correo y existían pocos servicios de correo públicos. Hace algo más de una decena de años, los ISP proveían este servicio como un hosting. Hoy en día este servicio es una aplicación en la nube.

En este punto se debe identificar que existen nubes públicas y privadas, las públicas son aquellas a las que puede acceder cualquier persona o empresa y las privadas están orientadas a un gremio o sector en concreto o incluso a una organización en particular[13].

Los servicios provistos por estas nubes varían de acuerdo con el tipo. Se tienen servicios:

- **IaaS (Infraestructure as a Service):** Este servicio proporciona a las organizaciones un *Datacenter* virtual, que se conocen como VDC, por sus siglas en inglés. Estos *Datacenter* virtuales poseen todo, lo hace parte de un sitio físico, servidores, equipos de seguridad, sistemas operativos, aplicaciones, redes virtuales e incluso equipos de comunicación como *routers* o *switches* virtuales.

- **SaaS (Software as a Service):** La empresa que contrata este tipo de servicios no puede administrar la infraestructura atrás del software, pero si el aplicativo como tal. Por ejemplo, puede administrar el correo electrónico, al cliente de este servicio se le provee una interfaz de administración vía web o consola a través de la cual puede aprovechar todos los recursos y servicios disponibles del correo como crear, editar o eliminar cuentas, poner políticas, dar soporte y mantenimiento a usuarios finales, proveer seguridad e interconectar con otras aplicaciones son algunos ejemplos.

- **PaaS (Platform as a Service):** En estos servicios el cliente puede gestionar no solo la aplicación sino la plataforma asociada a la aplicación, por ejemplo, un software de desarrollo que permita escribir código fuente y diseñar otras aplicaciones.

Existen otras opciones como STaaS (*Storage as a Service*) que es almacenamiento como un servicio, aquí caen aplicaciones como OneDrive, Drive, Dropbox, etc. Sin embargo, con lo descrito se tiene el patrón que siguen estos servicios.

El éxito obedece al deseo de las empresas de liberarse de las complicaciones asociadas a tener infraestructuras costosas propias y sus inversiones en instalación y mantenimiento. Incluso los equipos como *switches* o *firewalls* tienen a ser como servicio, la vida útil de estos es limitada y las empresas constantemente deben cambiarlos y actualizarlos por nuevas tecnologías, esto afecta sus inventarios y trae procesos engorrosos de depreciación, reciclaje y bodegaje. Si estos equipos se contratan no como equipos sino como un servicio, la empresa proveedora es la responsable de todo esto y los riesgos que esto trae también se transmiten a los proveedores como fallas de fábrica, daños en partes y piezas o la administración y gestión.

Según encuestas realizadas en 2017 por la empresa *Ofcom* de origen británico y dedicada a evaluar tendencias a cerca de los consumidores, esto en concordancia con encuestas realizadas por la BBC, una empresa de igual forma británica dedicada a medios de comunicación, revelan que en los últimos años la tendencia es dejar de ocupar las computadoras como se las conoce y migrar todas las funcionalidades a los dispositivos móviles y tabletas.[14]

En la Tabla 1.1, se puede ver la tendencia de importancia entre un teléfono móvil en comparación con la importancia de la computadora, según los usuarios.

Año	**Personas que piensan que la computadora es más importante que un teléfono inteligente**	**Personas que piensan que un teléfono inteligente es más importante que una computadora**
2015	30%	32%
2020	15%	66%

Tabla 1.1 Tendencia a dejar de usar la computadora

Este cambio de preferencia de los usuarios, que antes veían más importante el uso de la computadora y que hoy en día se ha reemplazado por los dispositivos móviles, se debe a las ventajas de movilidad, acceso desde redes externas a las organizaciones, accesos a recursos desde cualquier parte del mundo y ya no solamente desde la red interna. Por otro lado, es necesario extrapolar la protección que tiene cuando está en la red interna, a los equipos donde los usuarios los necesiten utilizar, incluso cuando requieran moverse de forma constante por diferentes sitios de una ciudad, ciudades de un país o países del mundo para cumplir con diversas actividades inherentes a su rol en la organización.

1.3.3 CIBERSEGURIDAD

1.3.3.1 Concepto

Se define por el CERT - *Center for Emergency Response Technologies,* de Estados Unidos como el arte de proteger las redes, dispositivos y datos contra el acceso sin autorización o el uso con fines delictivos, también indica que es la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información[14].

Existen miles de riesgos al tener una ciberseguridad deficiente, como la pérdida de información confidencial, afectación a la reputación o hasta la caída de todos los sistemas de la organización.

1.3.3.2 Ciberseguridad para redes

Existe un sin número de herramientas que permiten solucionar riesgos o inconvenientes de seguridad concretos, por ejemplo, plataformas de *antimalware* que minimizan el riesgo de que un malware o virus que ingrese a un sistema. Los *firewalls,* por otra parte, evitan que servicios de red sin autorización ingresen a redes privadas o crucen ciertas fronteras de un segmento de red a otro[16].

Existen también otras soluciones de protección dedicadas para las redes como los IPS o sistemas de prevención de intrusos, los sistemas DLP o sistemas de prevención de fuga de información. También las soluciones de análisis de vulnerabilidades y parches de seguridad de aplicaciones y sistemas.

Para proteger adecuadamente las redes se debe también reforzar las configuraciones de los servidores, servicios, aplicaciones y sistemas, esto se hace mediante procesos de endurecimiento de estas configuraciones o *Hardening,* en inglés.

Parte importante de la protección y seguridad de las redes es el control sobre las acciones que pueden o no ejecutar tanto los administradores de las redes y los sistemas, así como los usuarios, para esto se desarrollan políticas de seguridad.

1.3.3.3 Tipos de amenazas a la red y al host

Según la empresa Kaspersky Lab, fabricante de soluciones *antimalware* en el primer trimestre de 2020, se neutralizaron por su parte 727 mil millones de ataques en 203 países, provenientes de al menos 442 mil millones de URL únicas. Estas amenazas se las pueden clasificar como amenazas al punto final, al usuario y de red, de acuerdo con el objetivo del ataque, como, las computadoras o servidores, los usuarios y las aplicaciones y servicios de red[17].

Es importante considerar que el 100% de los dispositivos en una red y las personas que ocupan sus servicios son vulnerables a ataques.

Para dispositivos finales se tiene los siguientes ejemplos de tipos de amenazas:[18]

- *Adware*: Son amenazas que introducen publicidad al navegar en internet y capturan las actividades del usuario para perfilar su comportamiento.

- Troyanos: Son amenazas que vienen dentro de otros archivos válidos, se ejecutan en segundo plano y dan acceso a un atacante o realizan un daño particular como robo de datos, credenciales o afectación a los sistemas.

- *Ransomware*: Son amenazas que permiten realizar secuestro digital de información, posterior a este secuestro el atacante exige un pago para devolver la información, comúnmente mediante monedas virtuales no rastreables como bitcoins.

- *Backdoors*: Son amenazas que proveen al atacante una puerta trasera o escondida de acceso a los equipos o activos.

- RAT – *Remote Administration Tool*: Son amenazas que permiten al atacante tener el control y la administración de los dispositivos que alcanzó el ataque.

Para los usuarios finales:[18]

- *Phishing*: Son ataques en los que se pesca usuarios sin capacitación y mediante técnicas de ingeniería social, que son técnicas para engañar, logran que las

victimas ejecuten acciones como transferencias, entreguen credenciales o instalen *malware*.

- *Spear Phishing*: Son ataques similares al phishing pero que tienen como objetivo una persona en concreto.

- *Spam*: Son amenazas no activas que pueden persuadir a la victima de realizar actividades no apropiadas o que comprometan la seguridad.

Para las aplicaciones y servicios de red[19]

- Inyección de SQL: Son ataques en los que a través de una caja de texto de una aplicación web se insertan comandos hacia la base de datos, con afectación, desde daño a la información hasta la fuga de datos sensibles.

- *Cross Site Scripting*: En estos ataques se puede inyectar scripts en una página web que contengan código malicioso y se interpretan por el navegador del usuario, esto permite al atacante inyectar en los equipos de las victimas otras amenazas como las que se describieron antes.

- *Defacement*: Un atacante entra a la configuración de una página web y la deforma, se usa frecuentemente por ciber terroristas para realizar un ataque y dejar una bandera o logo que los identifique como autores del ataque.

- DoS: Los ataques de denegación de servicio buscan realizar tantas peticiones a un mismo servicio que los recursos de los equipos como memoria o procesador se saturen y dejen de responder, esto logra indisponibilidad de los servicios de red.

- DDoS: Es similar a los ataques de denegación de servicios, pero en lugar de ser un equipo atacante son varios, esto hace más difícil su detección.

- *Buffer Overflow*: Muchos servicios trabajan con colas de tráfico o información en buffers, cuando estos se saturan hay paquetes o información que se pierde, estos ataques buscan obligar a los equipos a saturar su buffer para que desechen la información importante y almacenen en la cola o buffer basura.

1.3.3.4 Evolución de la ciberseguridad

La ciberseguridad evoluciona de forma constante, durante el tiempo se puede ver un crecimiento que se asocia a los riesgos y amenazas existentes en las redes, también obedece a la necesidad de defenderse de cibercriminales.

El primer hacker con esta calificación fue Nevil Maskelyne, quien en 1903 logró interceptar comunicaciones realizadas mediante telégrafo inalámbrico. [21]

El primer cibercriminal por su lado fue Jhon Draper que pudo generar llamadas gratis al modificar un silbato que venía en las cajas de cereales a una frecuencia X y con esto podía realizar llamadas gratuitas que afectaban una central telefónica.

El primer *malware* en la historia fue un *malware* de nombre Creeper, que llegó a las computadoras a través de la ARPANET que es la generación anterior al Internet actual. El *malware* mostraba un mensaje en el computador y se ejecutaba de forma autónoma. Por sus efectos se tuvo que crear el primer antivirus de nombre Reaper, que buscaba al *malware* y lo eliminaba. A grandes rasgos el primer *antimalware* fue también un *malware*, pero con mejores propósitos.

Tanto los *malwares* como los *antimalware* evolucionaron muchísimo hasta llegar a tener las plataformas conocidas como EDR, que son herramientas de detección y respuesta en el punto final o *Endpoint Detection and Response* por sus siglas en inglés. Estas plataformas permiten cazar *malware* previamente descubierto, así como responder a los ataques nuevos o de día cero.

1.3.3.5 Políticas de ciberseguridad.

Para minimizar estos riesgos se crearon cientos de recomendaciones como buenas prácticas para mejorar la ciberseguridad, sin embargo, no se puede garantizar al 100%.

En el trabajo de titulación “Políticas de auditoría de seguridades en redes locales” que lideró por el Ing. William Humberto Andrade Hinojosa en el 2007 para la carrera de Ingeniería en Sistemas, se elaboran políticas de auditoría mediante encuestas a un grupo finito de empresas para levantar políticas de seguridad en redes locales y con conexión a Internet, estas se implementan en una empresa para detectar el cumplimiento de las normas de seguridad como también los puntos vulnerables y se emiten recomendaciones a seguir para hacer de la red un sitio más seguro. Con esto se afirma la necesidad de evolucionar en seguridad a la vez que se crece en servicios de telecomunicaciones.[22]

1.3.4 PROTECCIÓN DEL PERÍMETRO DE LA RED

Cuando las soluciones de seguridad se implementan sobre los equipos de punto final, que son los terminales que emplean los usuarios, se hace referencia a la seguridad interna o de punto final, cuando se ubica en la frontera de un grupo de terminales se habla de seguridad perimetral o de borde.

1.3.4.1 Seguridad Perimetral

La seguridad perimetral pretende ofrecer soluciones a los riesgos en las comunidades entre diversas redes, la más trivial, por ejemplo, es bloquear o permitir el acceso a ciertos puertos o protocolos desde ciertos segmentos de red. Para analizar esto a mayor profundidad, se debe definir lo que es el perímetro de la red.[19]

La Figura 1.7 muestra el perímetro tradicional de la red, y permite describir mejor la idea, un grupo de terminales de usuarios como computadores, servidores, impresoras, teléfonos celulares o tabletas por detrás de un enrutador de acceso a internet o de un firewall normalmente pertenecen a un perímetro de red, que puede ser el borde por donde las comunicaciones de la red *LAN – Local Area Network* cruzan hacia el internet o en general a las redes WAN *Wide Area Network,*. Como se puede apreciar en la Figura 1.7 este borde se protege por un equipo que se denomina ***Firewall***, que controla permisos o bloqueos de puertos y protocolos que dependen del origen o destino de las comunicaciones.

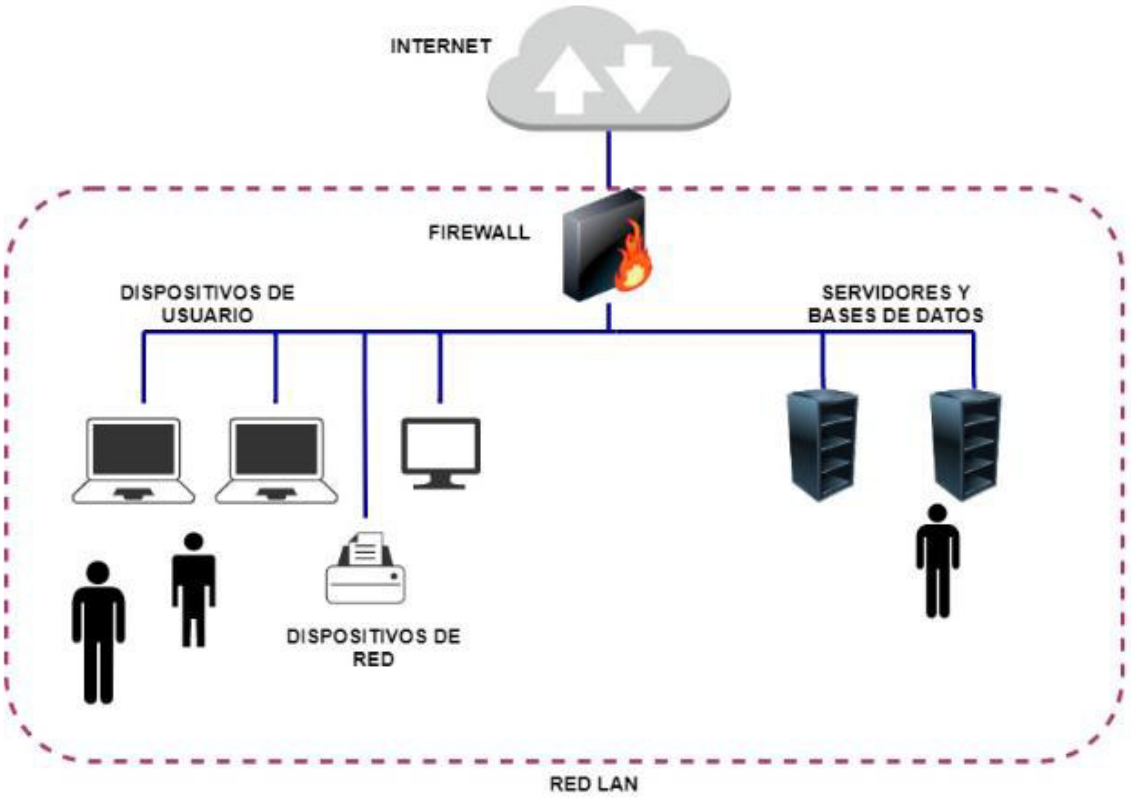

Figura 1.7 Perímetro tradicional de la red

Esto evolucionó, hasta el punto de que los equipos que protegen el perímetro de la red tienden capacidades de detectar y prevenir intrusos

Por tanto, los equipos de protección ofrecen diferentes reglas de protección y filtrado en cada una de estas capas, aquellos que llegan hasta la capa *aplicación* se llaman firewalls de nueva generación o de capa 7. Algunos equipos de protección perimetral realizan muchas funciones y se conocen como UTM - *Unified Threat Management*, que dependen del tamaño de la red cada función es preferible delegarla a una solución específica.

1.3.4.2 Perímetro extendido.

Con el paso de los años, el perímetro de la red se extendió, hasta la casa de los usuarios, oficinas remotas y nuevas necesidades surgieron como tener movilidad y necesidad de acceso desde cualquier punto del globo a ciertos recursos corporativos.

Un primer paso de esta evolución o extensión del perímetro luce como lo que se muestra en la imagen anterior, en la Figura 1.7 en donde se observa que el perímetro crece con

más firewalls o sistemas VPN – *Virtual Private Network,* que permiten extender la red hasta ciertas zonas donde está el usuario:

En la **Figura 1.7**Figura 1.8 se muestra como las diversas necesidades, han extendido el perímetro de la red.

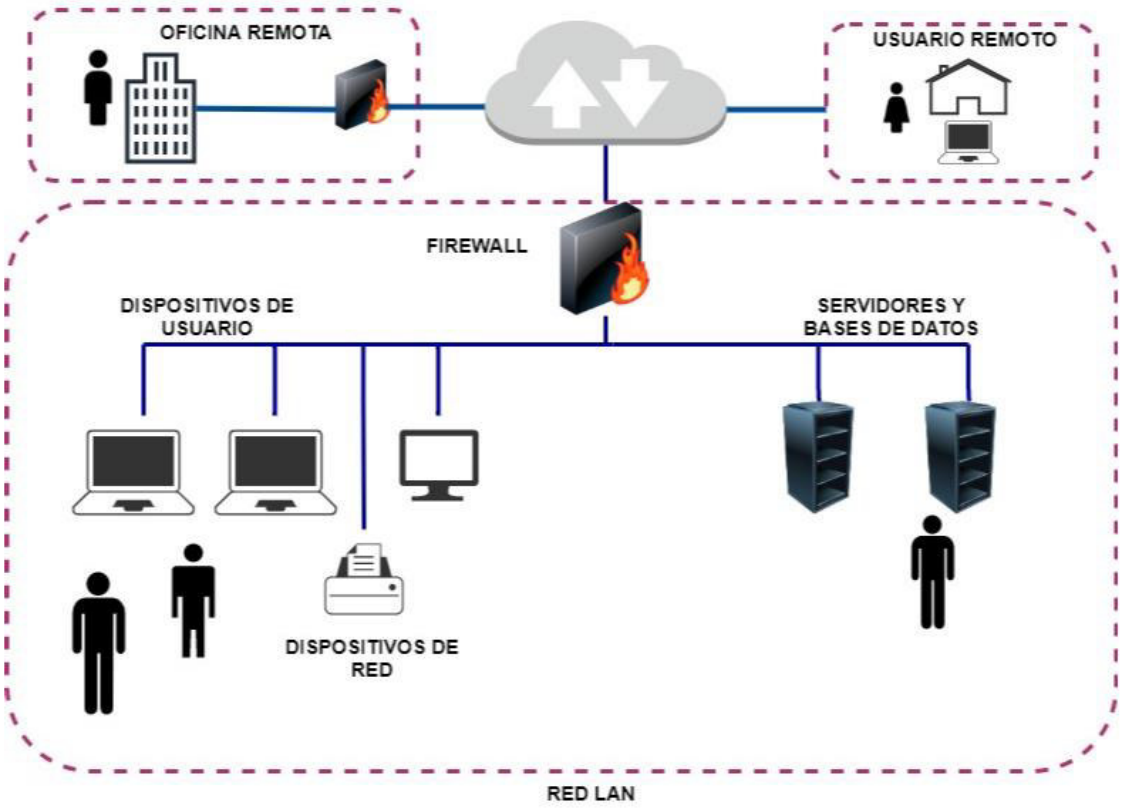

Figura 1.8 Perímetro extendido

Esto llevó a que sea necesario definir el acceso a la red WAN de una forma diferente a la del perímetro tradicional y ahora los firewalls o UTM vienen con capacidades que se conocen como SD-WAN o red de área extendida definida por software que permite que se envíe de forma automática la información a través del mejor camino.

Ahora el panorama es aún más amplio, el perímetro se extendió con el ingreso de servicios en la nube que consideran el *Cloud Computing* que provee soluciones informáticas en sitios que se distribuyen a través del mundo en diferentes centros de datos accesibles solamente por internet.

En la Figura 1.9 se puede observar una serie de servicios que se prestan por diversos proveedores en el mundo, soluciones que son software como servicio, infraestructura como

servicio y plataformas como servicio, SaaS, IaaS, PaaS, por sus siglas en inglés y a las que los usuarios necesitan acceso a más de la red local.

Figura 1.9 Servicios en la nube

Esto hace del perímetro de la red algo tan extendido y difuso que se tuvo que redefinir la forma en la que se protege.

En el trabajo de titulación "Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, se utilizó tecnología UTM (*Unified Threat Managment*)" que lideró el Ing. Fernando Flores en el 2008 para la carrera de Ingeniería Electrónica y Redes de Información, realiza un estudio de seguridad perimetral utilizando tecnología UTM, también un análisis de los módulos que lo conforman y posibles las soluciones de seguridad que pueden proveer al perímetro con diferentes proveedores de esta tecnología. Finalmente se proporciona una visión del estado actual de la red de una empresa y se sugiere soluciones de seguridad. Sin embargo, no considera la movilidad de los usuarios y el dinamismo de salir del perímetro de la red y realizar trabajo de forma remota. [22]

1.3.4.2.1 SDN – Redes definidas por software[22]

Las redes definidas por software son arquitecturas de red con las siguientes características:

- Dinámica
- De fácil administración
- Flexible
- Buen retorno sobre las inversiones

Esto es útil particularmente para tráfico que requiere gran ancho de banda requerimientos muy cambiantes en las aplicaciones de hoy en día. Al igual que SDP separa el plano de control del plano de datos esto permite a los administradores reprogramar los servicios que prestará la red directamente dependiente de sus necesidades.

Esto se vuelve factible por el reemplazo de elementos de hardware como balanceadores de carga y firewalls a soluciones de software. De esta forma se tiene las políticas en el plano de control y el plano de datos trabaja con conmutadores físicos que responden al control que envía el software de administración.

1.3.4.2.2 NFV - Virtualización de las funciones de red

La virtualización de funciones de red o NFV, por sus siglas en inglés introduce una nueva forma de ver las redes, se considera una mejora que logra reemplazar los equipos de hardware de propósito específico como routers, balanceadores de carga y firewall por equipos que se basan en software, el software por su parte se ejecuta en servidores genéricos compatibles mediante técnicas de virtualización.[20]

1.3.4.3 NaaS - Network as a Services

Son servicios que permiten a sus clientes contar con características dinámicas de red que son utilizadas bajo demanda. Uno de los casos de uso más comunes es cuando se requiere abrir una nueva sucursal, se puede tener acceso a la nube o a red WAN de una compañía de forma sencilla, prenderlo y apagarlo cuando se lo necesite, reduce costos y evita invertir en equipos como routers o switches de costos altos[21].

1.3.4.4 SD-WAN – Software Define Wide Area Network

Las redes de área extendida o WAN son ampliamente utilizadas por corporaciones que tiene operación o sucursales en diferentes ubicaciones geográficas distantes, interconectar estas ubicaciones puede representar un reto importante en cuanto a requerimientos técnicos como inversión económica. Una forma de disminuir esos costos y los requerimientos técnicos es evitar el uso de hardware específico para el efecto y permitir que esto sea definido por software, a través de equipos capaces de crear conexiones WAN mediante protocolos de comunicación segura. Por medio de servicios de Internet “montan” una red WAN bajo demanda y seleccionan las mejores condiciones disponibles para transportar el tráfico de una ubicación a otra. [26]

1.3.4.5 ZT - Zero Trust

Confianza cero, por sus siglas en inglés, se trata de un modelo, se basa en tres conceptos fundamentales, uno de ellos es tener un control estricto de acceso, al proporcionar privilegios mínimos a los usuarios, el segundo, acceder a los recursos de forma segura sin importar la ubicación geográfica y por último inspeccionar todo el tráfico de datos de la red en busca de actividades anómalas.

Esto permite ocultar todas las aplicaciones para que no sean visibles desde la internet o redes públicas inseguras, colocar un punto central que valide el tráfico proveniente de los usuarios externos, se mejora la seguridad comparada con las VPN, que en el último tramo permiten el tráfico sin cifrar y consideran este último tramo como un segmento seguro o confiable, eliminar los segmentos de red con altos privilegios, es decir, no se asume ningún usuario, equipo o segmento de red como confiable, absolutamente todo se inspecciona y se monitorea las actividades, estado y comportamiento de los equipos y usuarios para establecer políticas de autorización de accesos a recursos de red y aplicaciones así como para autenticación.

1.3.4.6 CASB - Cloud Access Security Broker

Según la empresa Gartner, se define un CASB como una solución que permite mejorar la seguridad de las aplicaciones locales o de nube que tiene la organización mediante la aplicación de políticas por usuario que controlan las actividades que estos pueden realizar, crear, editar, eliminar, mover, acceder, copiar, descargar, etc, son algunas de las cosas que se pueden permitir, monitorear o bloquear a los usuarios en las aplicaciones mediante soluciones de este tipo.

1.3.5 SDP – SOFTWARE DEFINE PERIMETER

SDP fue originalmente propuesto por Cloud Security Alliance (CSA), esto fue una iniciativa de red Black Core de Global Information Grid (GIG).

SDP propone un modelo de seguridad para proteger de manera dinámica las redes actuales. Este modelo de seguridad se basa en autenticar, autorizar y segmentar antes de obtener acceso a la infraestructura de la organización, como resultado, se evita ciberataques, facilita la administración, y mejora la seguridad de los recursos en la nube de las organizaciones.

SDP adopta una arquitectura de confianza cero al autenticar y verificar un host para cada sesión, esto puede ser altamente efectivo al abordar los incidentes de propagación lateral de amenazas que se encuentra a menudo en las organizaciones.

1.3.5.1 Arquitectura SDP

Consta de tres elementos los host SDP que inician, los hosts que aceptan conexiones y los controladores SDP que gestionan las interacciones a través de un canal de control, por lo tanto, se separa el plano de control del plano de datos para obtener un sistema totalmente escalable como se muestra en la Figura 1.10.

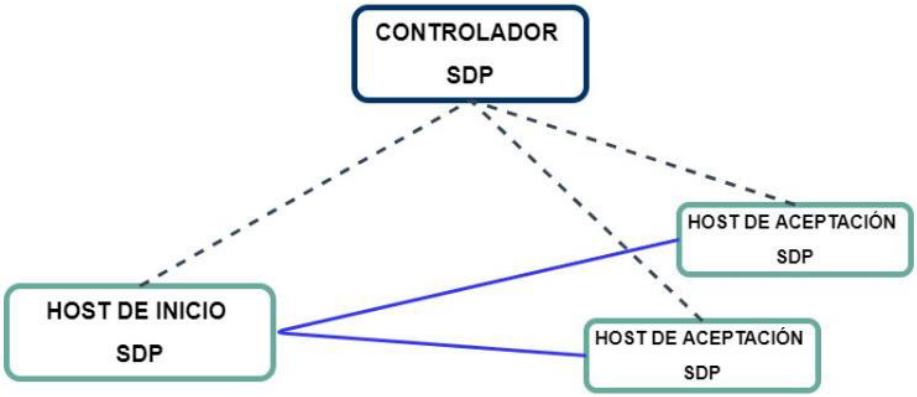

Figura 1.10 Arquitectura SDP

Controlador SDP: es el elemento central de SDP, actúa como intermediario de confianza para el control de los mensajes entre el host SDP y los controladores de seguridad.

Realiza la emisión de certificados y autenticación de dispositivos, además determina los servicios y aplicaciones a los que cada host de inicio está autorizado a acceder en el host receptor.

Ayuda a la configuración de túneles mTLS en tiempo real entre el host de inicio SDP y el host de aceptación.

Cliente SDP O Host Iniciador: Los clientes SDP envían una solicitud para realizar la conexión. Esta solicitud se envía al controlador SDP que autentica al host iniciador mediante la petición de información sobre el hardware o el software del *host Iniciador*. Una vez realizada la autenticación se crea un túnel mTLS, que conecta el IH con el servidor autorizado.

Host que aceptan SDP: este acepta servicios o aplicaciones previamente autorizados. Está configurado para rechazar todo los paquetes y solicitudes de todos los hosts excepto el controlador SDP.

El host SDP generalmente está protegido por un enlace SDP que actúa como el protector. Esta puesta de enlace es el punto de terminación del mTLS del IH. Esto sucede después de que el controlador SDP proporciona la puerta de enlace la dirección IP y los certificados IH verificados y autenticados.

1.3.5.2 Capas de seguridad

Autenticación de paquete único (SPA): Permite descartar el flujo de información no autorizada.

La información del primer paquete enviado es encriptada desde el dispositivo del cliente al controlador SDP, donde se verifica y auténtica la identidad antes de dar acceso. El dispositivo envía el SPA a la puerta de enlace para rechazar el tráfico no autorizado y permitir el paso del tráfico de datos de los dispositivos permitidos.

Validación de dispositivo (DV): Verifica que el dispositivo pertenece al usuario autorizado, y de esta manera añade una capa adicional de seguridad al garantizar que la clave encriptada se mantenga en este dispositivo. Con mTLS solo se comprueba que la clave no sea revocada y que no caduque, pero DV nos permite saber si el dispositivo fue robado o lo está utilizando otro dispositivo.

Firewall Dinámico: La principal regla de este tipo de firewalls es negar todas las conexiones a diferencia de los firewalls estáticos que poseen miles de reglas.

SDP adopta el firewall dinámico en la puesta de enlace al eliminar y agregar reglas que permiten a los usuarios autenticados y autorizados acceder a las aplicaciones y servicios.

Enlace de Aplicación (AppB): Es el proceso obligatorio de las aplicaciones autorizadas para utilizar los túneles TLS creados por SDP. Esto permite que los dispositivos autenticados y autorizados puedan comunicarse a través de los túneles mientras que las aplicaciones no autorizadas se mantengan bloqueadas.

Estos protocolos son los que dificultan a los usuarios y atacantes acceder a aplicaciones y servicios protegidos.

Vale la pena mencionar que la complejidad de este marco se basa principalmente en la función Hash utilizada como parte del cifrado / descifrado del paquete SPA ya que las otras cuatro capas de seguridad del marco ya existen. Por ejemplo, los firewalls dinámicos se usan en la capa 3.

2. METODOLOGÍA

Por lo expuesto en el capítulo 1, es evidente la necesidad de proteger sistemas en organizaciones que mantienen un esquema de operación de red que cuentan con servicios locales y de nube. Estas organizaciones requieren brindar a los usuarios la posibilidad de acceder a los recursos de red de manera segura en cualquier parte y desde cualquier dispositivo que requieran.

Para la implementación de soluciones de perímetro definido por software, se considera un modelo de protección de redes como “conocer solo lo que necesite”, que se implementa por el Departamento de Defensa de los Estados Unidos. Además de limitar el acceso a los usuarios de acuerdo únicamente a lo que necesitan saber, existe una forma de proveer seguridad que se conoce como **confianza cero** o ZT por sus siglas en inglés *Zero Trust,* que indica que todo usuario y dispositivo siempre se debe autorizar y autenticar antes de ingresar a la red, aún si su “saber o conocer” se justifican por su cargo, los beneficios de SDP incluyen movilidad y no se atan a una VPN o dispositivo por lo que se llevan a cabo en la nube.

2.1 DIAGRAMA DE LA METODOLOGÍA PROPUESTA PARA IMPLEMENTACIÓN DE SDP

Para implementar correctamente de sistemas de SDP, el presente trabajo de titulación propone una metodología basada en 6 pasos, tal como se indica en la Figura 2.1.

Figura 2.1 Pasos para la implementación de la metodología

Estos 6 pasos abarcan lo necesario para implementar exitosamente un esquema de protección a la red mediante perímetro definido por software.

2.2 DETALLE DE LA METODOLOGÍA

2.2.1 PASO I - INVENTARIOS DE ACTIVOS Y USUARIOS[27]

Se debe realizar correctamente el levantamiento de inventario de los activos de la organización, se entiende como un **activo** como un recurso de software o hardware con el que cuenta la organización.

En el inventario de activos debe al menos constar la siguiente información:

- **Identificador**, es un código para una rápida identificación y normalmente es alfanumérico y secuencial.
- **Nombre**, es el nombre con el que el activo se conoce dentro de la organización o como lo llaman los usuarios o administradores.
- **Tipo**, corresponde a la naturaleza del activo, por ejemplo, hardware o software.
- **Descripción**, es un pequeño detalle de la funcionalidad que presta el activo.

- **Proceso al que pertenece**, debe contener el nombre del proceso, con la debida documentación, en caso de existir o si es un proceso empírico debe ponerse un nombre al proceso que el activo presta soporte.
- **Nivel de clasificación de información**, debe definirse como la confidencialidad de la información que alberga el activo.
- **Ubicación que puede ser física o electrónica**, debe estipular donde se encuentra el activo, en caso de ser físico, debe tener también una ubicación física, en caso de ser electrónico debe tener una dirección electrónica, como es el caso de los servicios en la nube.
- **Propietario**, es el dueño del activo dentro de la organización, generalmente el jefe o gerente del área a la que el activo sirve.
- **Custodio**, es el responsable de la administración del activo, generalmente el técnico que lo administra.
- **Criticidad**, es el nivel de importancia que tiene el activo para el proceso.
- **Usuarios con acceso**, es un inventario de los usuarios y los accesos o permisos que tienen sobre este y su información.

Realizar de forma correcta este inventario es necesario para poder definir el alcance de los activos que estarán bajo la protección de la plataforma de perímetro definido por software, la factibilidad de implementación de la solución y ayudará a definir cómo protegerlo de forma adecuada.

2.2.2 PASO II - MATRIZ DE ACCESOS

Es un inventario de los usuarios y los accesos o permisos que tienen sobre los activos de información, en esta matriz es importante especificar al menos:

- **Usuario**, tendrá el nombre del usuario que requiere acceder al activo.
- **Rol**, debe detallar el rol o cargo que tiene el usuario, esto normalmente se usa como justificación de por qué ese usuario debe tener acceso a un activo. De acuerdo con su rol en la organización se determina si es necesario o no que el usuario acceda. Esto permite la implementación de acceso con base en la necesidad del saber.
- **Activo**, detalla a que activos debe tener acceso el usuario de acuerdo con su rol.

- **Origen del acceso**, esto debe describir desde donde es necesario que el usuario acceda, desde la red interna de la organización, desde cualquier parte en internet, o ambas.

2.2.3 PASO III - DEFINICIÓN DE ALCANCE

Para avanzar como la correcta implementación de un sistema de SDP es necesario que la empresa o sus responsables determinen que procesos, activos o usuarios estarán seguros con la solución.

La definición del alcance debe ser tratada con la gerencia de la organización de forma que se defina los procesos o usuarios que se van a beneficiar de la solución.

Puede darse el caso de que ciertos recursos, por criticidad sean necesarios acceder únicamente desde las instalaciones de la organización, desde la red interna o con cientos equipos y aplicativos muy específicos de acuerdo con el giro de negocio y las políticas internas de cada empresa. En este caso estas políticas deberán ser debidamente implementadas también en la solución.

Por tanto, la definición del alcance debe responder a beneficios para 3 aristas, personas, proceso y herramientas y estar en total sincronía con estos.

Los beneficios que derivan de la implementación de una plataforma de SDP son múltiples, sin embargo, no todos son necesarios o aplicables en el 100% de las empresas por lo que en la definición del alcance se debe definir también que funcionalidades se van a emplear y justificar el por qué, esto se puede realizar mediante el uso de recursos como **términos de referencia** en que se listan las funcionalidades necesarias para una empresa en particular una vez se realizan los pasos uno y dos.

A continuación, se presenta una lista de las posibles funcionalidades que puede tener una plataforma con SDP:

- **Funcionalidades de red**
    - **Soporte para SD-WAN** Los canales de datos exclusivos son costos y difíciles de conseguir por problemas como la ubicación geográfica por lo que muchas organizaciones ahora usan soluciones que tienen redes de área extendida privadas definidas por software, la solución de SDP debe ser compatible con estas soluciones.

- **NaaS** Una parte fundamental del SDP es el core de funcionamiento de la solución y un SDP establece una conexión segura desde donde esté el usuario hasta el recurso que quiere acceder, esto es posible mediante el uso de redes como servicio, que son redes virtuales montadas sobre las redes tradicionales MPLS que brindan ciertas funcionalidades particulares como seguridad, transporte rápido y seguro de tráfico entre los centros de datos del proveedor de esta red con equipos dedicados para este fin pero que cuentan con múltiples características de seguridad y minimizan los riesgos de ataques como Man-In-The-Middle mediante una red virtual privada y segura que transporta información sobre otra red cuyo core no es la seguridad sino el transporte.

- **VPN IPsec** Por la necesidad de acceder a recursos locales de una empresa desde cualquier sitio, va a ser necesario establecer algunas conexiones VPN sitio a sitio, que se realizan mediante IPsec por lo que es mandatorio que una solución de SDP pueda realizar estas conexiones sin importar el fabricante del equipo que recibe la conexión, el primer sitio será la nube donde está el SDP y el otro el sitio físico, virtual o de nube donde están los recursos que se desean acceder.

- **VPN SSL** De igual forma que las VPN IPsec existe la posibilidad de que un recurso se pueda acceder desde una VPN host a host, por lo que el SDP simulará ser uno de los hosts, el que requiere acceso y actuará como proxy para redirigir al usuario final al segundo host, que es el recurso al que el usuario quiere o necesita acceder.

- **Políticas de reenvío de tráfico** SDP es un servicio que provee una red como servicio es necesario poder establecer políticas en el reenvío de tráfico para permitir o bloquear lo que el administrador considere como necesario para la correcta y segura operación de la red.

- **Calidad de Servicio** Muchas aplicaciones requieren ciertas condiciones particulares respecto al rendimiento de la red como retarlo o latencia o ancho de banda para funcionar correctamente por lo que es importante que la solución de SDP permita configurar calidad de servicio, esto generalmente es necesario para aplicaciones como telefonía IP u otras que trabajan en tiempo real.

- **Funcionalidades de seguridad**

    - **Descripción y análisis de tráfico SSL** Para proveer seguridad a nivel de telecomunicaciones es necesario analizar el tráfico que se transporta por la red en búsqueda de contenido no que no se permite o malicioso, muchas amenazas son transportadas en tráfico que se cifra para que las soluciones de protección de red tradicional no lo detecten, se inventó el análisis profundo de paquetes para que los sistemas de prevención de intrusos puedan analizar la carga útil que llevan los paquetes de red, para realizar esto se requiere al descripción y análisis de tráfico encriptado mediante SSL o TLS.

    - **Agente de seguridad de acceso a la nube (CASB)** Para poder autenticar y autorizar los usuarios es necesario que exista un agente o un bróker que realice esta función, las soluciones que realizan esto de forma dedicada se conocen como CASB, para proveer servicios de SDP, este es un componente esencial, también es primordial para la aplicación del concepto de Zero Trust.

    - **Gateway de navegación web mediante servicio en la nube** Uno de los servicios principales que tienen actualmente los usuarios de las redes a más del correo, servidores de archivos, contabilidad, etc, se tiene la navegación a internet, esto brinda múltiples beneficios, pero trae riesgos, con los IPS, Gateways de navegación locales y firewalls de nueva generación se puede proteger a los usuarios durante su experiencia de navegación en internet, se analiza la reputación de los sitios web, IP, categoría, contenido, etc, de acuerdo a esto se aplican políticas de seguridad. También se aplican políticas de control de acuerdo con las necesidades o condiciones de cada empresa como el bloqueo de navegación a redes sociales desde dispositivos corporativos.

    - **Acceso a la red que utilice metodología Zero Trust** Es necesario que cada equipo y usuario que acceda se autentique y autorice a entrar en la red y que todo lo que compone la infraestructura que presta un servicio sea una caja negra para el usuario final, es decir que no sea visible para él. Si un equipo de punto final se compromete por un atacante, este se detiene antes de ingresar a la red para evitar que el atacante use el equipo con *malware* como salto para comprometer la red corporativa.

- **Firewall como servicio** Las reglas más comunes de control en el perímetro corresponden a reglas de permisos o bloqueos basadas en IP, puertos y protocolos, para simular el perímetro de la red tradicional ahora en SDP se requiere replicar esta funcionalidad.
- **DNS seguro** Los servicios de resolución de nombres de dominio a menudo se emplean para redireccionar al usuario a sitios maliciosos o fraudulentos, es necesario analizar la reputación y comportamiento de los DNS para brindar seguridad completa a los usuarios.
- **Prevención de fuga de información** El tráfico se analiza y su contenido también, es prioridad para las organizaciones controlar el contenido de la información que entra o sale de sus activos, para esto la información se clasifica y se define en que activos puede estar almacenada, ser leída o modificada y por qué usuarios. Estas políticas se deben aplicar en los puntos que permiten el acceso o salida de información en la red, así como en los puntos finales, en el esquema de perímetro tradicional se ubican en la puerta del perímetro, en el caso de SDP debe ser una funcionalidad que esté presente en toda la solución ya que el perímetro ahora se define mediante software.
- **Sandboxing** Muchas amenazas son desconocidas, para poder definir si existe o no una amenaza, se emula el ambiente final donde debe llegar un paquete de información, como si fuera una caja de arena que filtra el contenido denso, contenido que en este caso sería malicioso. Junto con lo descrito anteriormente se requiere esta función para todo el contenido que no se conoce, así se emula y se decide si es malicioso o no.

Existen servicios de diferentes fabricantes que ofrecen más funcionalidades, estos se deben evaluar de acuerdo con la necesidad de cada empresa.

2.2.4 PASO IV – IMPLEMENTACIÓN

La implementación debe llevarse con base en las siguientes fases:

- **Fase I – Preparación de requerimientos,** en esta fase se analiza todo lo necesario para implementar la solución de SDP, que puede ser:
  - Licencias de Software
  - Hardware

- Documentación e información como los inventarios
- Socialización a los administradores y usuarios

- **Fase II – Implementación piloto,** en esta fase se realiza un despliegue parcial de la solución, lo que permite evaluar el impacto de implementarla y determinar posibles riesgos, estos riesgos se deben ser analizar y atender por el implementador y los involucrados. El presente trabajo realizará la implementación hasta este punto, a petición de la empresa patrocinadora.
- **Fase III – Implementación total,** una vez que se realiza el despliegue del piloto y este se ajusta hasta que ya no presente riesgos o impactos negativos para la organización se extrapolará la implementación a todos los activo, procesos o usuarios de la organización. Esta fase normalmente se conoce como despliegue masivo, porque replica lo que tuvo éxito en el ambiente piloto a toda la organización.
- **Fase IV – Monitoreo y afinamiento,** a pesar de haber sorteado todos los posibles impactos y riesgos en la fase II existe la posibilidad de que el despliegue masivo presente inconvenientes, por lo que se recomienda monitorear y hacer afinamientos durante al menos 15 días después de finalizar el despliegue total.

2.2.5 PASO V - DOCUMENTACIÓN

Una vez se realiza todo lo anterior, es necesario que se documenten las actividades en una memoria técnica con todas las configuraciones realizadas, en caso de que alguien requiera consultarlas, también puede ser que existan cambios que en la siguiente fase se realicen como mejoras o que los miembros del equipo de despliegue abandonen la organización, de esta forma siempre se tendrá una fuente de consulta que indique qué se hizo, cómo se hizo y por qué se hizo.

La memoria técnica debe contener:

- Información de resumen de la solución implementada
- Registros de acceso
- Arquitectura
- Diagrama de red
- Detalle de las configuraciones.

Todo esto para que cuando sea necesario revisarla sea comprensible para el lector.

2.2.6 PASO VI - MEJORA CONTINUA

La organización continuará su evolución en el tiempo, ninguna empresa es estática, nuevos productos, servicios, personal, mercado, etc, requerirán nuevos activos y los usuarios acceso a estos. Los activos existentes se pueden actualizar, migrar o reemplazar, por lo que la mejora continua es una parte importante del proceso de adopción de una nueva tecnología como SDP.

Para el desarrollo de la metodología y facilitar su gestión, se **anexa** a este proyecto una plantilla de libro de Excel con modelos de inventario de activos y matriz de accesos que puede ser empleada por cualquier organización.

3 RESULTADOS Y DISCUSIÓN

El presente capitulo presenta la aplicación de la metodología propuesta, la solución seleccionada para el prototipo de implementación y sus resultados, así como la discusión de éstos.

3.1 LEVANTAMIENTO DE LA INFORMACIÓN

Con base en la metodología planteada, se realiza el levantamiento de información de activos, usuarios, cuentas y servicios que requieren y que formarán parte del servicio, se emplea el formulario de levantamiento de información propuesto en este Trabajo de Titulación, tal como se indica en la Figura 3.1.

IDENTIFICADOR	NOMBRE	TIPO	DESCRIPCIÓN	PROCESO AL QUE PERTENECE
AT001	win-mobile	Laptop	Laptop de uso general, para trabajo fuera de oficina	Ventas
AT002	win-subnet1	Desktop	Equipo ubicado en la matriz, subred 1	Ventas
AT003	win-subnet2	Desktop	Equipo ubicado en la matriz, subred 2	Servicios gestionados
AT004	NGFW-Branch-UI	Appliance Virtual	Firewall de borde de la matriz	Administrativo
AT005	Panorama	Appliance Virtual	Manager de los firewall	Administrativo
AT006	Prisma	SaaS	Servicio SDP de Palo Alto Networks	Administrativo

Figura 3.1 Evidencia del levantamiento de activos de la organización

La información recopilada incluye:

- El inventario de activos
- La matriz de accesos
- El alcance que se desea

3.2 MATRIZ DE ACCESOS

Para efectos del trabajo de titulación se emplea una matriz de accesos con base en 5 roles como se muestra en la **Figura 3.2**:

- **Proveedor:** Este rol indica que el usuario pertenece a otra empresa, sin embargo, requiere acceso a la infraestructura interna con el objetivo de brindar soporte de tercer nivel sobre las herramientas que ofrece la empresa a sus clientes
- **Usuario:** Este rol se asigna a los técnicos empleados del equipo técnico que brindar soporte técnico de nivel uno y dos a los clientes de la empresa.
- **Vendedor:** Este rol se asigna a los asesores comerciales de la fuerza de ventas de la empresa.
- **Preventa:** Este rol se asigna a los ingenieros de preventa que apoyan la gestión de los asesores comerciales de la empresa.
- **Gerente:** Este es un rol que se asigna a los ejecutivos de gerencia a cargo de las diferentes áreas funcionales de la empresa.

USUARIO	ROL	ACTIVO	ORIGEN DEL ACCESO
Contractor	Proveedor	192.168.XXX.XX/24	Any
Employee	Usuario	192.168.XXX.XXX/24	Any
Sales	Vendedor	192.168.XXX.XX/24	Any
Presales	Preventa	192.168.XXX.XX/24	Any
Manager	Gerente	192.168.XXX.XX/24	Any

Figura 3.2 Matriz de Accesos

3.3 PLANTEAMIENTO DEL ALCANCE

A partir del levantamiento de información se define el alcance para la solución, se considera los siguientes aspectos:

- Las necesidades de conectividad remota que actualmente se cubre con VPN tradicional.

- Las necesidades de acceso a equipos según el usuario por tener equipos de uso compartido.
- La seguridad en el equipo.
- La protección de perímetro para defensa de ataques de intrusión.
- La necesidad de movilidad de los miembros de la organización por su operación en el país y sus alianzas estratégicas en diversos países de Europa, Asia, Norteamérica y Sudamérica.

3.4 SOLUCIÓN IMPLEMENTADA

La necesidad de cobertura de la empresa ALTEL S.A. abarca los países marcados en rojo en la Figura 3.3, en donde se puede apreciar que ALTEL S.A con sede en Ecuador opera apoyada por su alianza estratégica desde varios países que son España, Emiratos Árabes Unidos, Estados Unidos, Chile y Ecuador.

Figura 3.3 Distribución de la operación de la empresa ALTEL

Por la forma de operar de la empresa requiere que sus colaboradores estén en constante movimiento, al ser un proveedor de servicios de seguridad de la información, atiende clientes en estos países con personal compartido que necesita movilidad sin límites, también, este personal y sus dispositivos de computación requieren protección especializada para los datos de los clientes y los de la propia empresa.

Actualmente la topología de la red se distribuye como se muestra en la Figura 3.4:

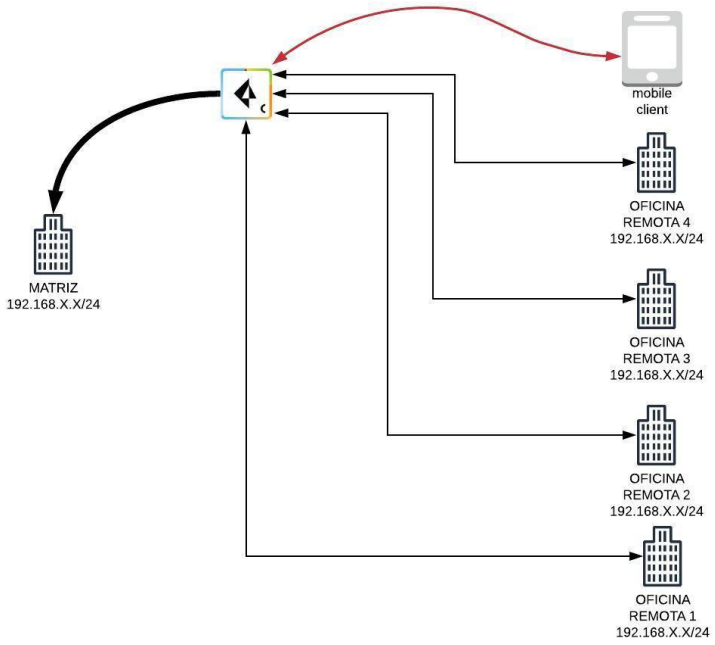

Figura 3.4 Topología de la red

La distribución de redes y recursos empresariales es tradicional, en cuanto a seguridad en el perímetro cuenta con un firewall de frontera que protege los equipos dentro de la red y qué a través de la VPN, permite acceso remoto.

Sin embargo, a pesar de que se permite el acceso remoto con las VPN estas transportan cualquier tráfico incluso inseguro o de amenazas. Por lo que se solventa este inconveniente con la implementación de SDP.

El SDP permite extender la misma protección de perímetro que tiene la empresa hasta los dispositivos que están fuera de la red, incluso en movilidad como es el caso del dispositivo “win-mobile”

El SDP es un servicio SaaS, software como servicio en la nube. Se establece una conexión VPN S2S, sitio a sitio con la nube del proveedor y esta nube se convierte en el punto de acceso global, el proveedor tiene centros de datos para acceso en todo el mundo, en donde esté el usuario se conectará al punto de acceso más cercano, se convierte en el borde extendido de la red de la empresa.

La Figura 3.5 muestra los puntos disponibles en América Latina para conexión a través del servicio provisto por la empresa Palo Alto Networks para Latinoamérica:

Figura 3.5 Puntos de acceso en América Latina del servicio SaaS.

Para información de puntos de acceso a nivel global se puede consultar el siguiente enlace de referencia:

- https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/list-of-prisma-access-locations.html

Para entender un poco mejor la necesidad de contar con SDP en esta organización, hay que considerar que la operación de empresa está distribuida en 5 países, en varios de estos países la operación se encuentra activa en más de una ciudad, y a su vez el personal de una ciudad puede operar desde distintos edificios, dando lugar a una operación como se muestra en la Figura 3.6:

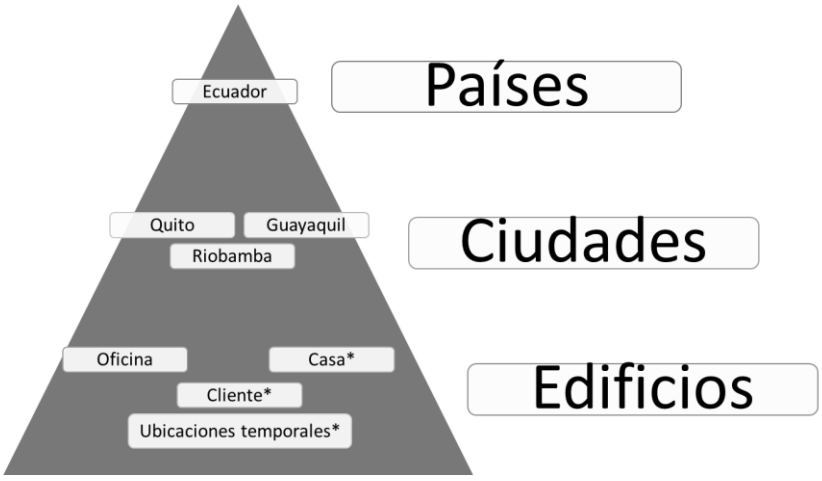

Figura 3.6 Microsegmentación de la operación. (* Indica ubicación cambiante)

Las necesidades de conectividad y seguridad en las diferentes sucursales de la empresa donde se dispone de oficinas están cubiertas por soluciones de protección especializada como Firewalls, sistemas de prevención de intrusos en la red, sistemas *antimalware* e incluso soluciones de autenticación de usuarios y equipos. Sin embargo, esto no ocurre cuando los usuarios con sus dispositivos abandonan el edificio donde se encuentra la oficina.

Es físicamente imposible ubicar estos sistemas de seguridad en cada posible ubicación que tendrá el usuario. En la Figura 3.6 se observó que el mismo usuario podía trabajar en la oficina, en caso de estar en modalidad de *homeoffice,* necesita trabajar desde su casa, en ocasiones movilizarse a visitar clientes e incluso requiere trabajar durante periodos de movilización en desde cafeterías, aeropuertos, terminales de autobús, etc.

En forma macro se puede dividir la necesidad en dos pilares fundamentales que son:

- Networking
- Seguridad

La parte de Networking es importante porque el usuario requiere consumir los servicios de la compañía que residen en servidores internos para uso del personal, desde cualquier ubicación, pero al ser servicios de uso privado no deben ni pueden estar expuestos a internet.

La parte de seguridad por protección de la información en los dispositivos y de la infraestructura de la compañía a la que se brinda acceso al dispositivo. En caso de que el dispositivo sea comprometido por un atacante puede ser la puerta de entrada a comprometer toda la infraestructura.

La aplicación de SDP como una solución a estos desafíos cubre los requerimientos de ALTEL S.A. y de las empresas que como ALTEL, se encuentren en la búsqueda de soluciones que permitan solventar estas necesidades.

La implementación del piloto consistió en desplegar la solución mediante un agente, que permite extender el perímetro de la red y por tanto la protección interna con la que cuenta la empresa hasta el punto final, sin importar la ubicación geográfica de este o la red de acceso que esté empleando.

La Figura 3.7, permite visualizar de forma didáctica como se extiende el perímetro hasta el nuevo borde y como a través de un agente en el equipo o un portal de usuario se puede extender la protección hasta el equipo de punto final.

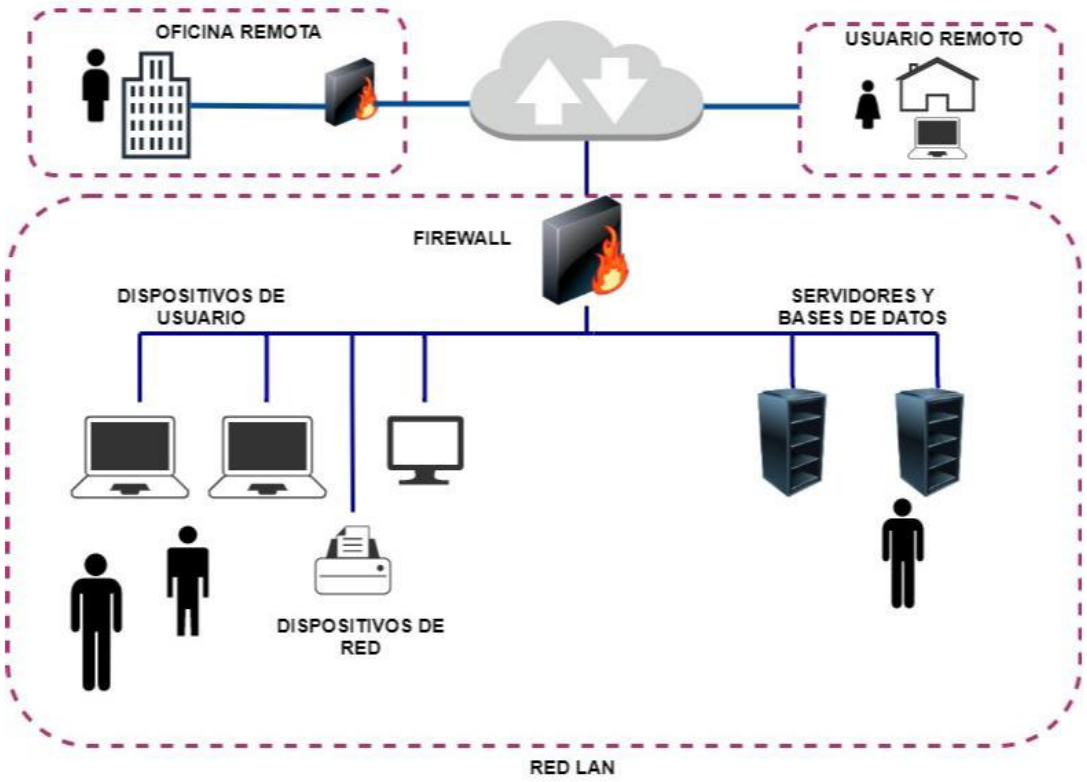

Figura 3.7 Perímetro Extendido

La Figura 3.7 permite observar, que la RED LAN en principio está protegida por un elemento de seguridad, el firewall, adicional del software de protección que reside en cada dispositivo según su sistema operativo.

Este firewall, en realidad tiene más elementos de seguridad, tales como:

- Protección para la navegación web
- Protección para la resolución de nombres de dominio
- Sistema de prevención de intrusos
- Detección y control de *malware* en la red

3.5 ARQUITECTURA DE LA SOLUCIÓN IMPLEMENTADA

La solución consta de un servicio SaaS y de un agente que permite consumir este servicio en los dispositivos finales, como se muestra a continuación en la Figura 3.8. Se puede observar que existe un agente, es decir, un software cliente que se instala en el equipo de punto final del usuario. Este software permite conectar el dispositivo con el servicio de SDP alojado en la nube mediante el uso de internet.

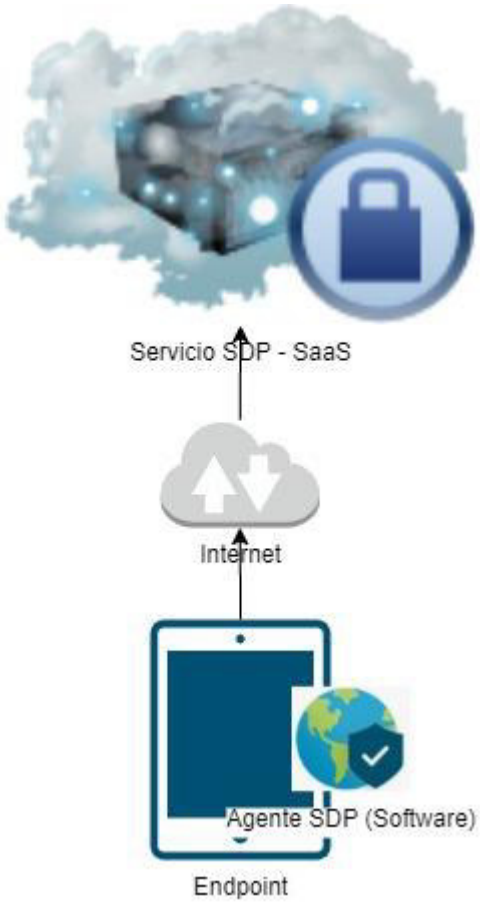

Figura 3.8 Arquitectura de la solución implementada

El agente se puede activar a discreción del usuario o mediante una política se puede establecer que siempre esté activo y que el usuario pueda desactivarlo.

Su funcionamiento consiste en establecer un túnel de conexión segura hasta la nube del proveedor de SDP, siempre que el software esté activado. La siguiente figura ilustra como sería una conexión con el buscador de Google con el software cliente de SDP activo, así como con el software de SDP no activo.

En el primer escenario, el dispositivo final, que puede ser un teléfono móvil, una tableta o una computadora de escritorio o laptop, con etiqueta **"1"**, sin el agente, accede directamente a la navegación web **"3"**, mediante una red de acceso de internet cualquiera **"2"** sin pasar por un sistema de seguridad, como en el caso de la Figura 3.7**Figura 1.8**, si estaba protegido por el firewall, sistema de prevención de intrusos, *antimalware* de red, etc.

En la Figura 3.9 se muestra el segundo escenario donde podemos ver que al estar el dispositivo fuera de la red, con el agente de SDP activo **"1"**, mediante el uso de internet **"2"**, primero accede al servicio de SDP en la nube **"3"** y luego al servicio donde prevente navegar, en el ejemplo los servicios de Google.

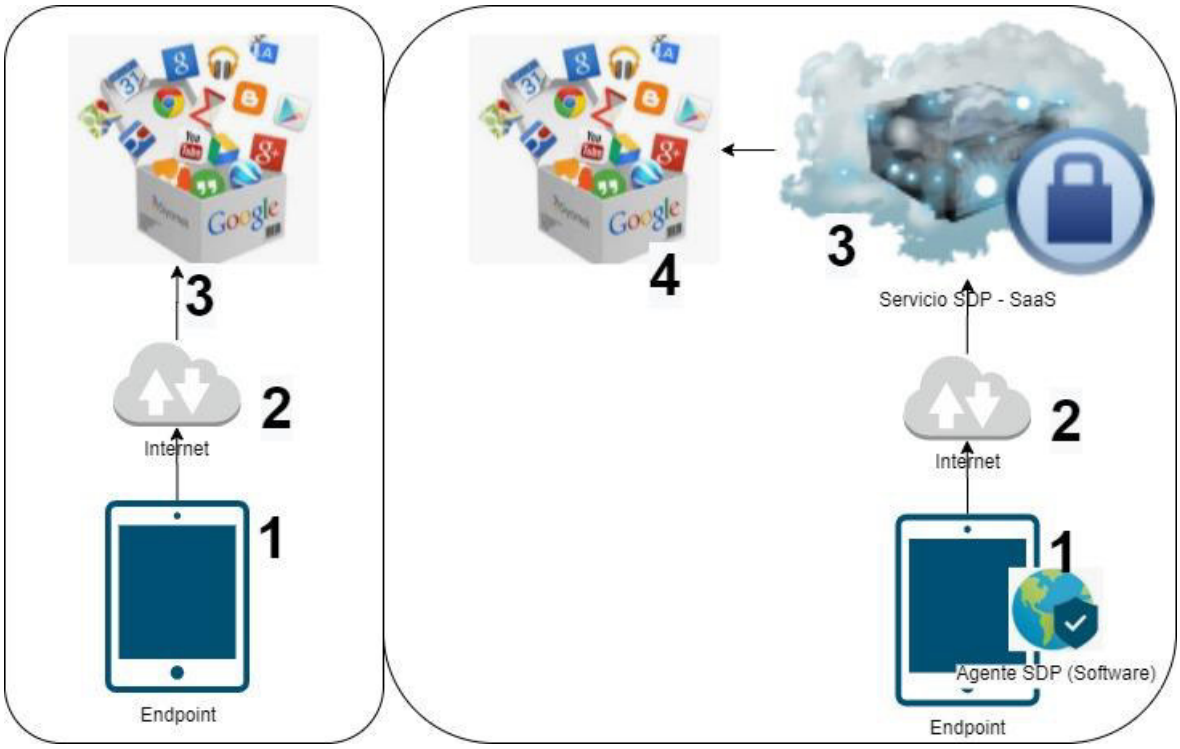

Figura 3.9 Diagrama de conexión sin el agente SDP y con el agente SDP.

Este tipo de servicio puede presentar un desafío en cuanto a retardo de las comunicaciones, por esta razón se debe evaluar que el proveedor de SDP tenga puntos de acceso al servicio distribuidos alrededor del mundo al menos en los países donde la empresa cliente tiene operaciones.

En este caso, como la operación es en 5 países, la solución SDP debe tener centro de datos o "nubes" para acceder al servicio lo más cercana posible al usuario final.

Así, por ejemplo. Como se muestra en la Figura 3.10, el usuario ubicado en el país 3 debe conectarse al punto de acceso 3, que es el punto de acceso al servicio de SDP más cercano

a él, geográficamente. Este usuario no debería acceder, en el ejemplo, al punto de acceso 1, ya que al estar en otro continente el retardo en las comunicaciones podría afectar el rendimiento de las aplicaciones que intenta acceder. Lo propio ocurre con los demás usuarios, sin importar la ciudad o país donde estén buscarán la conexión al punto de acceso más cercano de la lista disponible, que se representa en color verde y se evitaría los accesos innecesarios a sitios lejanos como el que se ilustra en color rojo.

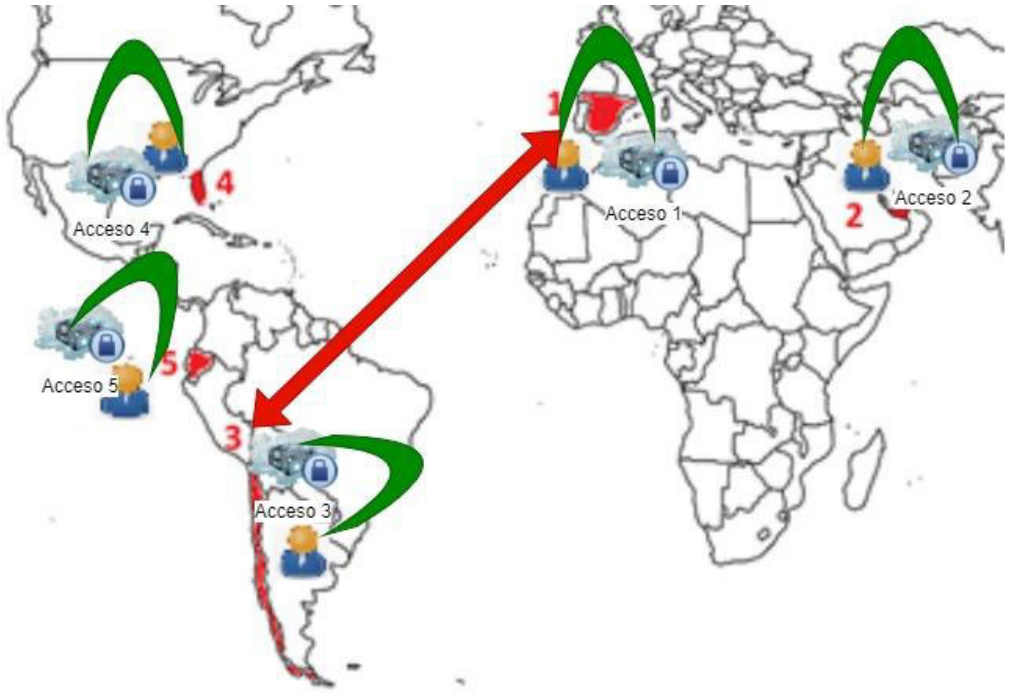

Figura 3.10 Conexión al punto de acceso SDP más cercano

En los puntos de acceso el proveedor del SDP brinda sus servicios de transporte de datos como de seguridad. En el caso del transporte de datos, por ejemplo, el usuario en el país 3 accedió al punto de acceso al servicio 3, que es su punto de acceso al servicio SDP más cercano. Entre los puntos de acceso existe conectividad especializada de alta velocidad, usualmente MPLS, que conecta todos los puntos de acceso y de forma dinámica se crea un camino hacia el servicio que el usuario requiera.

A continuación, se observa en la Figura 3.11 que el usuario del país 3, quiere conectarse no solo a internet de forma segura, sino que intenta acceder a un servicio de la Red LAN de la empresa que está ubicado en el centro de datos del país 2, conexión que vemos en color café, al otro lado del mundo. Para esto el punto de acceso SDP 3, se comunica, con

la infraestructura del proveedor de SDP que se localiza en la ubicación 4 y luego salta a la de la ubicación 2, conexión que vemos en color azul.

Figura 3.11 Conexión a servicios de un Centro de Datos remoto

Para completar la comunicación, la infraestructura del proveedor de SDP ubicada en el punto 2, debe poder acceder a los servicios del *datacenter* de la ubicación 2. Esto lo hace mediante un túnel IPsec para conexión site-2-site, como se puede ver en la Figura 3.12, en color celeste. Este firewall a su vez controla todo el tráfico de entrada y salida de la Red LAN de ese centro de datos.

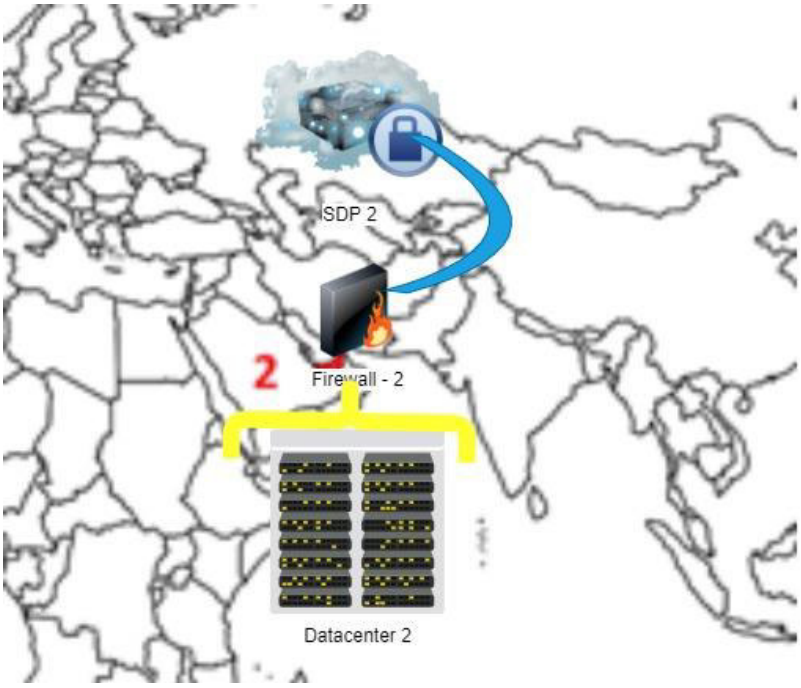

Figura 3.12 Conexión desde el SDP hacia el *datacenter* de cada ubicación.

En conclusión, cada ubicación debe estar conectada a la nube del proveedor de SDP mediante IPsec para estar disponible cuando un usuario requiera un servicio de la red interna. Todos los demás servicios de seguridad, control web, *antimalware* a nivel de red, etc, se proveen directamente desde la nube del proveedor de SDP.

Así se repite el proceso por cada ubicación local, de forma sencilla. El usuario por su parte solo necesita el agente en su dispositivo y de acuerdo con su perfil podrá acceder a la infraestructura o información que requiera según su necesidad.

3.5.1 CONEXIÓN HACIA NUBES PÚBLICAS.

Una parte importante de los servicios SDP es la capacidad que se ofrece de conectar a los dispositivos de usuario a servicios de nube pública, en condiciones normales un usuario puede acceder a un servicio de nube pública desde cualquier lugar. En este caso nos enfocaos en AWS, la nube conocida como *Amazon Web Services,* Este servicio consiste en infraestructura alojada en la nube que es accesible mediante servicios IP, para este proyecto de titulación se tiene lo siguiente:

Una cuenta de pago de la plataforma, que como se puede observar provee todos los servicios y pago por consumo de lo que la empresa contratante requiera, en este caso, infraestructura para servidores en la nube, el detalle de la cuenta se muestra como indica la Figura 3.13.

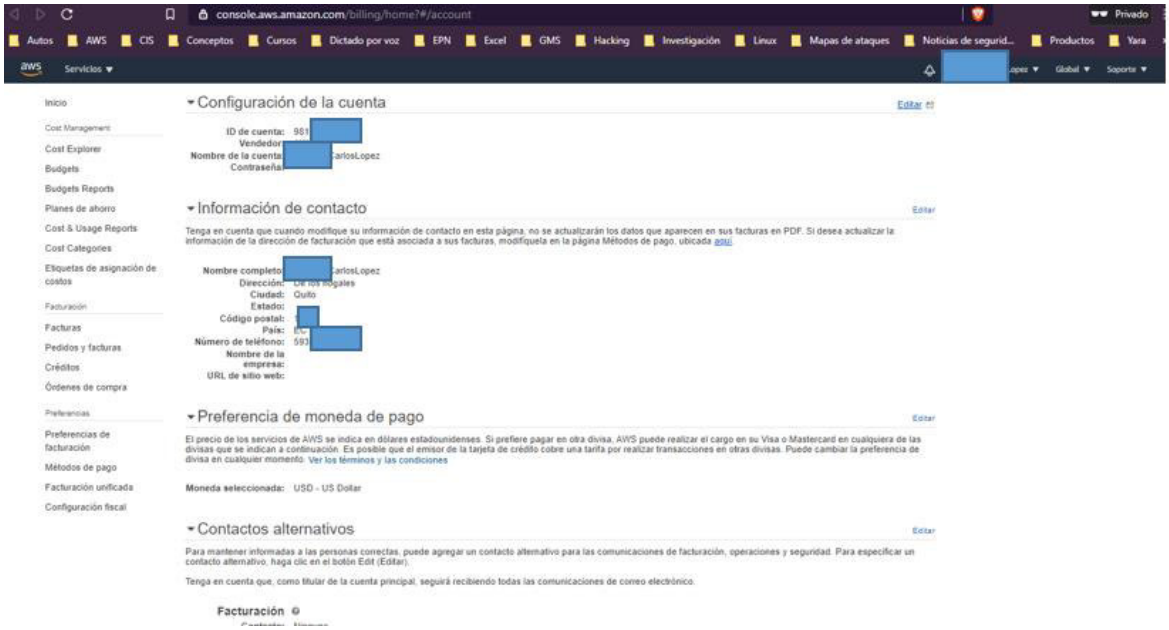

Figura 3.13 Cuenta en AWS para la implementación del piloto de SDP

Para efectos de la prueba se dispone de un equipo virtual, como se puede apreciar en la Figura 3.14, el equipo se encuentra desplegado con la tecnología EC2, que es propia de AWS, para desplegar servidores virtuales de cualquier sistema operativo, se puede desplegar un sistema en blanco o un sistema con la aplicación, base de datos o configuración que se requiera, previamente preparado, por ejemplo para un servicio web se puede desplegar el servidor con la aplicación IIS para el servicio web y una base de datos SQL, por ejemplo. Sin embargo, aquí se desplegó un equipo Linux con la aplicación EMPIRE, que es necesaria para la empresa, misma que se accede mediante web por el puerto 8080 mediante el uso del protocolo HTTP.

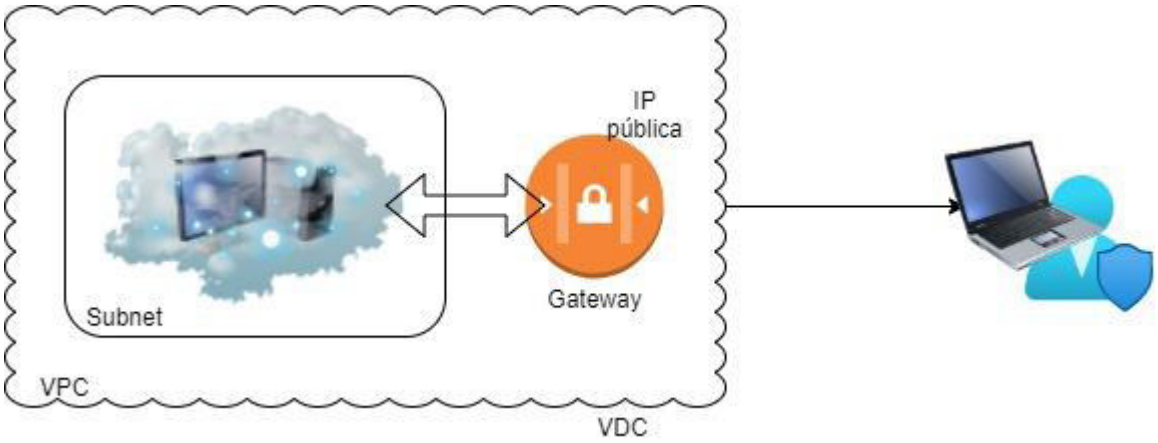

Figura 3.14 Diagrama base AWS – ALTEL

La arquitectura de AWS consta de subredes internas que forman lo que se conoce como VPC que se traduce como Nube Privada Virtual de AWS, varios VPN pueden estar en una zona o región en donde AWS tiene los datacenter físicos, en este caso se ubica en OHIO en Estados Unidos. Para el acceso, AWS provee un Gateway virtual configurado al que se puede conectar mediante una IP pública o un nombre de dominio DNS. La seguridad provista por AWS, se basa en listas de acceso o ACL que se configuran ingresando la IP desde donde se desea acceder y el puerto al que se necesita el acceso. Y es aquí donde SDP se necesita.

Como se observa en la Figura 3.15 se dispone de 3 VPC, cada uno con sus reglas de acceso.

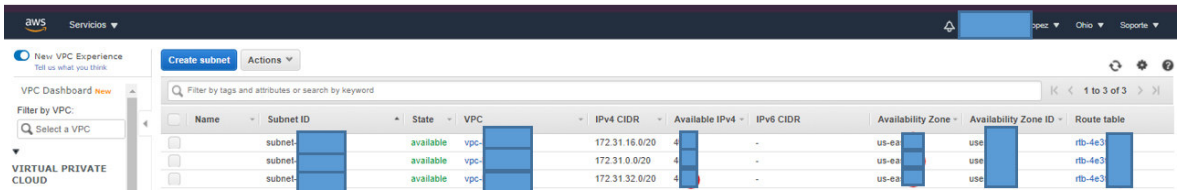

Figura 3.15 VPC disponibles de ALTEL S.A.

Cada uno de estos VPC dispone de uno o varios grupos de reglas de acceso que permiten o deniegan tráfico con base en parámetros de la capa 3 y 4 del modelo ISO/OSI como se muestra en la Figura 3.16:

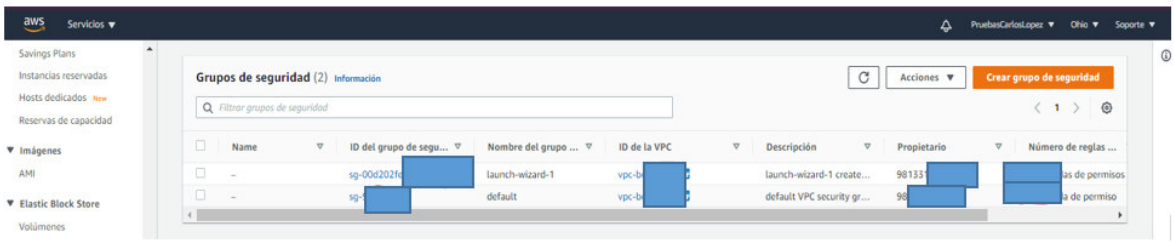

Figura 3.16 Grupos de seguridad de acceso a un VPC de ALTEL S.A.

Estos grupos de seguridad controlan las comunicaciones a las instancias de AWS, que no son más que las máquinas virtuales. Este acceso se da mediante una IP pública, como se mencionó antes y se puede ver en la Figura 3.17.

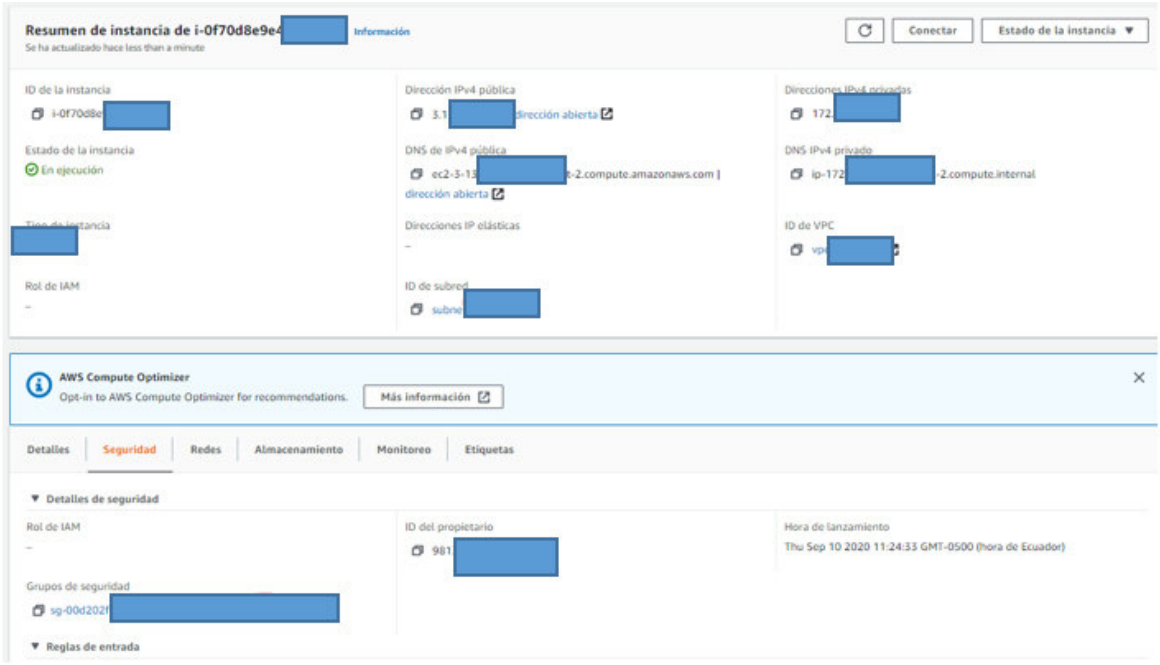

Figura 3.17 Instancia EC2 del piloto para ALTEL S.A. e IP pública asignada.

Las reglas pueden ser configuradas de manera sencilla como se muestra en la Figura 3.18

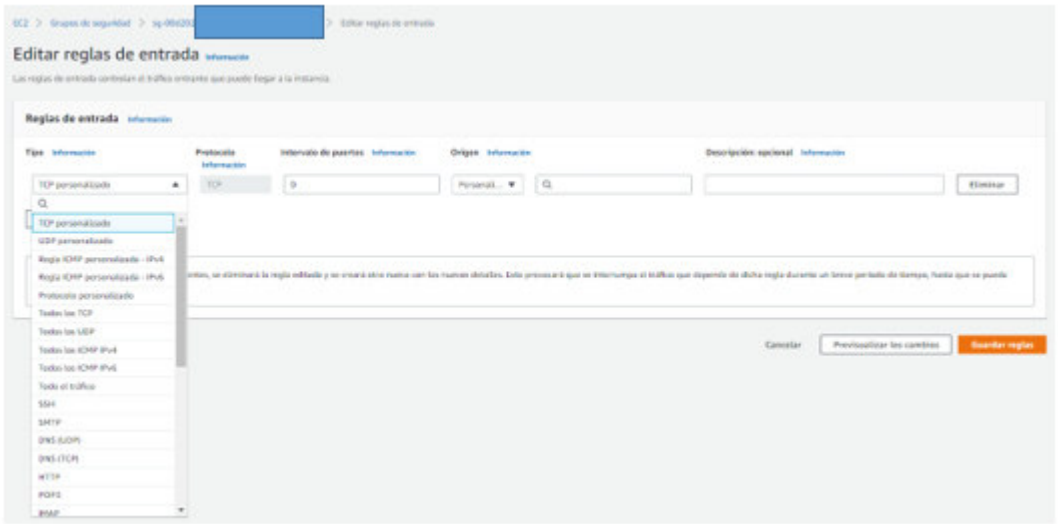

Figura 3.18 Creación de reglas de acceso en AWS.

En este punto es donde surge el inconveniente que se soluciona con la aplicación de SDP, los usuarios que emplean el sistema EMPIRE, desplegado en el servidor que instaló la empresa ALTEL en AWS, no acceden a este servidor desde un solo lugar, sino que acceden desde las redes de los clientes de la empresa, desde sus casas, aeropuertos, etc,

esto por la necesidad de realizar los trabajos para el que el servidor es requerido. Por tanto, se tiene 2 opciones, la primera, es volver el acceso completamente público, es decir que se puede acceder desde cualquier IP pública que consulte el servicio, como se muestra en la regla descrita en la Figura 3.19. Desde cualquier sitio, buscando el puerto 8080 y 80 en TCP, permitir el acceso.

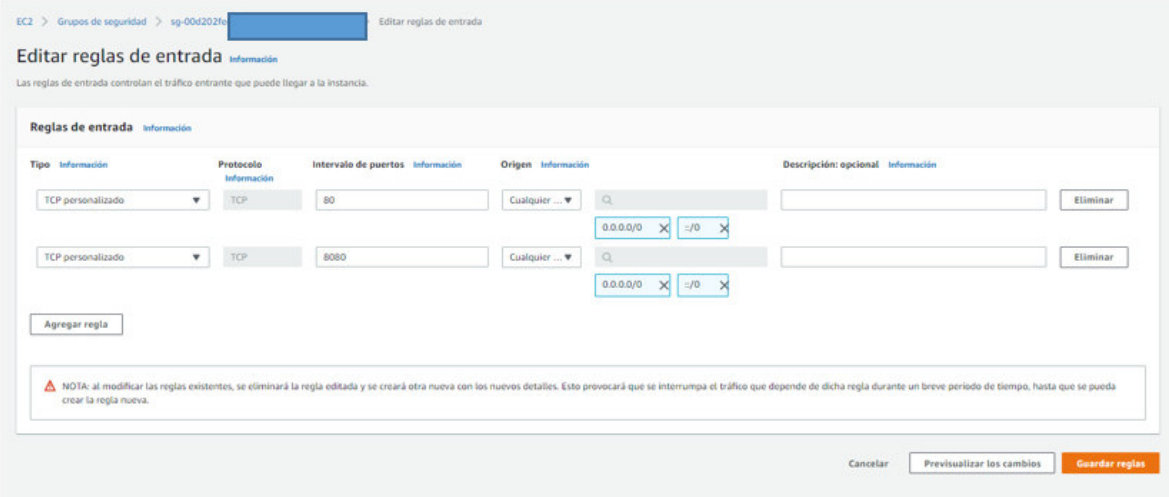

Figura 3.19 Acceso libre desde cualquier lugar por los puertos 80 y 8080 con TCP

Esto crea una brecha de seguridad enorme, puesto que cualquier atacante podría encontrar alguna manera de vulnerar el servidor a través de esos puertos, una manera de prevenir esto es colocando un firewall para aplicaciones web que proteja este servicio, sin embargo, el servicio que se ofrece por este equipo, no es un servicio web propiamente es un centro de comando para pruebas de ciberseguridad, por lo que, no es eficiente desplegar esta solución y su costo no es comparable al beneficio. Una segunda opción sería colocar de forma manual las direcciones IP desde donde se conecta cada usuario y actualizar cada vez que cambien, esto tampoco es eficiente ya que el trabajo operativo que implica y la molestia al usuario son altos y no aceptables.

Por tanto, con la solución de SDP se puede brindar el acceso de forma dinámica al usuario en donde se encuentre, manteniendo la privacidad de la aplicación y el servidor. Como se aprecia en la Figura 3.20 el usuario ya no se conecta a la IP pública de AWS, sino que lo hace a la nube de SDP como lo hizo en los escenarios descritos antes y es la infraestructura del proveedor de SDP quien se conecta a la nube privada de la empresa ALTEL, mediante un API desarrollado para este propósito. Esto elimina los inconvenientes listados anteriormente y mantiene la flexibilidad al usuario de consumir el servicio cuando y desde donde lo necesite. Otro factor importante es que este permiso se asignará de acuerdo con

su rol en la organización, sin olvidar la seguridad y la prevención de ingreso de amenazas o atacantes al servidor y la aplicación desplegada en la nube.

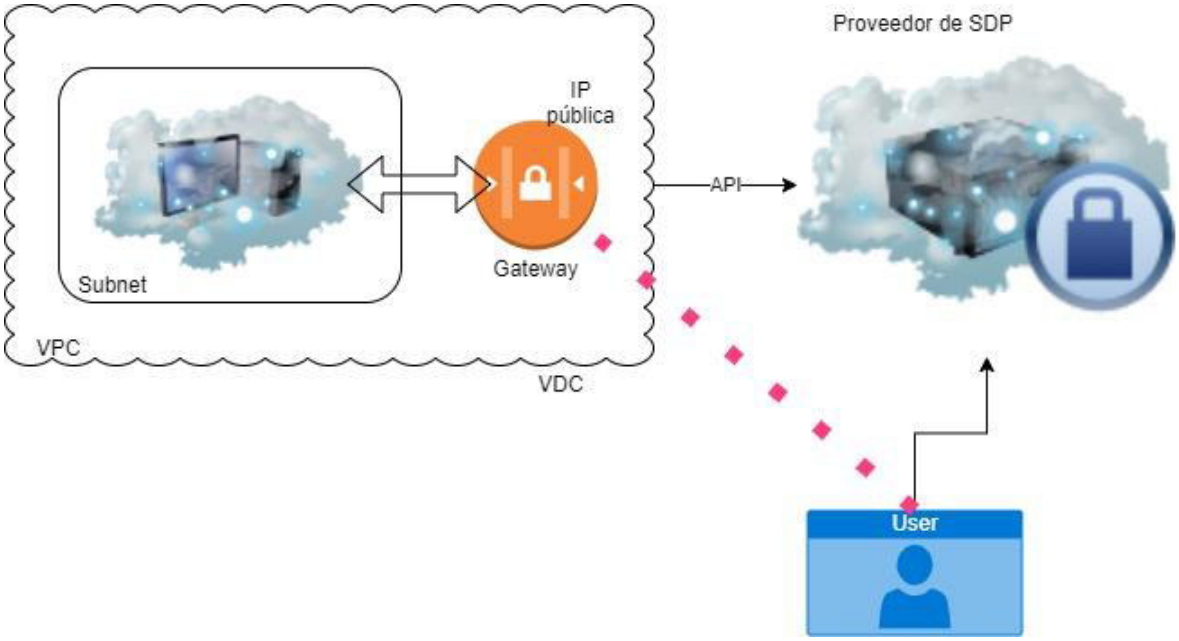

Figura 3.20 Conexión a AWS, empleando SDP.

Podemos ver esto en la implementación piloto mediante el uso de *plugins* o conectores que se emplean para realizar la conexión desde la plataforma de SDP de Palo Alto Networks, hacia la nube de AWS como se muestra en la Figura 3.21.

Figura 3.21 Configuración del conector AWS en Palo Alto Networks

Por tanto, para prestar el servicio todas las conexiones que entren a la nube de AWS, de cualquier usuario, serán previamente revisadas por los controles de FaaS, se llevan de

forma segura mediante la NaaS provista por el SDP y las políticas de acceso se asignan con base en el usuario. En la Figura 3.22 podemos ver la configuración de túnel.

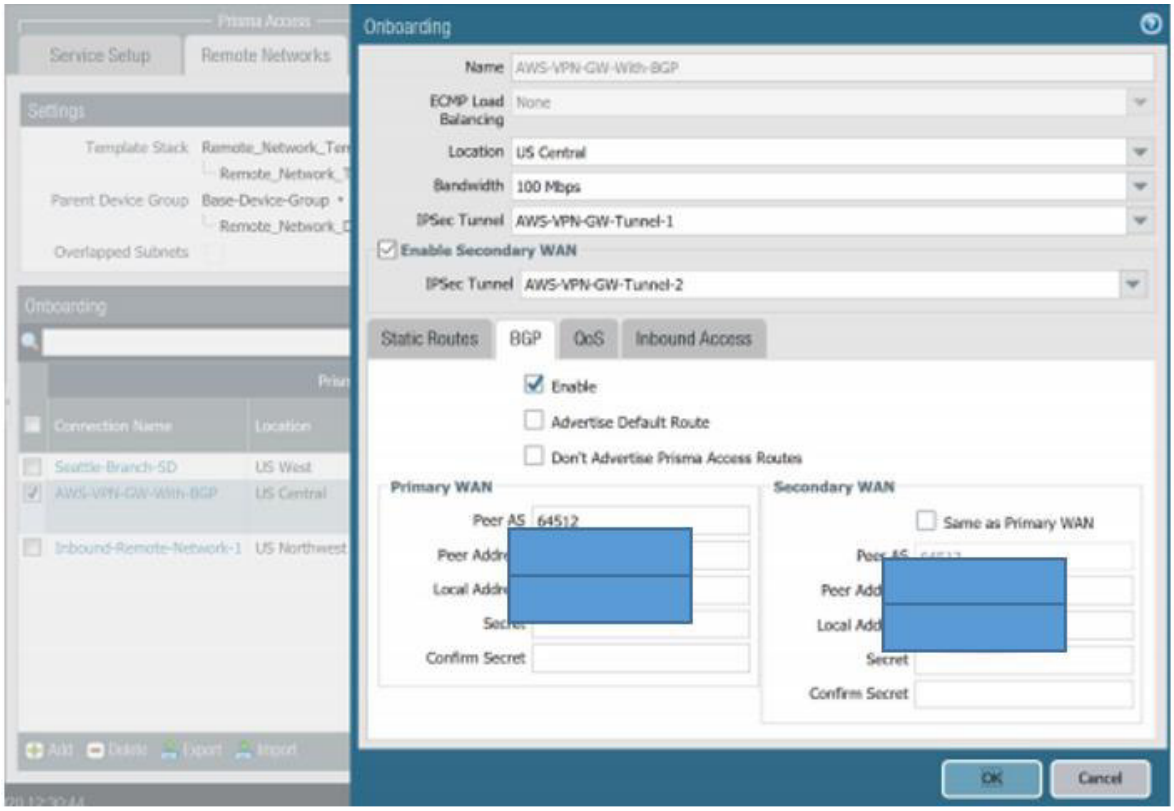

Figura 3.22 Configuración de túnel entre AWS y Palo Alto Networks

Esto se puede ver también en la parte de la consola de servicios de nube en la plataforma Panorama, que es el administrador de la infraestructura de Palo Alto Network como se muestra a continuación en la Figura 3.23

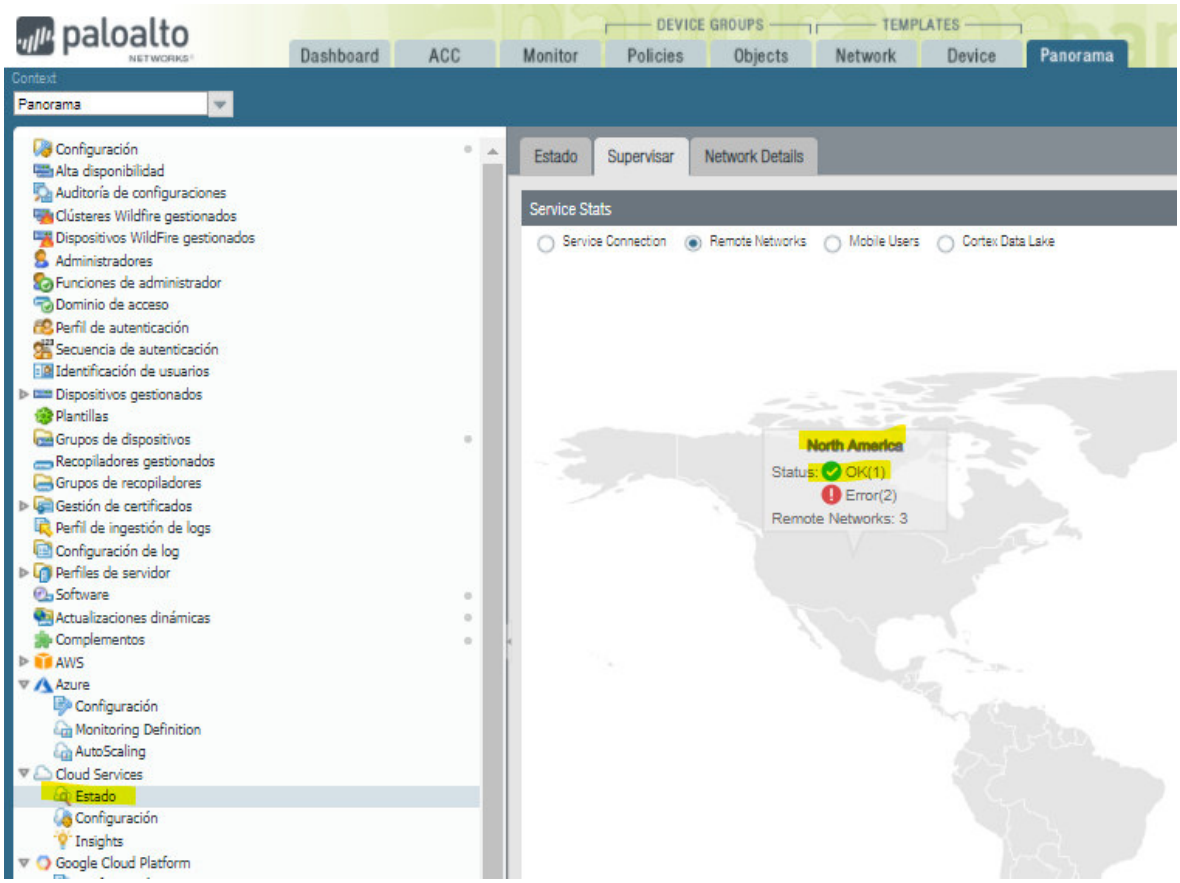

Figura 3.23 Conexión de la nube de Palo Alto Networks al servidor en AWS.

3.5.2 CONEXIÓN HACIA SERVICIOS SAAS.

Al igual que el acceso a los servidores o servicios ubicados en las premisas de la empresa y aquellos a los que se accede en la nube pública de AWS. Es necesario proteger el acceso de los usuarios a las plataformas que se prestan como un software como servicio – SaaS. Al ser un servicio SaaS, por sí mismo cubre la necesidad de movilidad y brinda acceso desde cualquier sitio al usuario a través de una conexión web.

Los servicios SaaS normalmente se consideran como *Shadow IT,* este es un concepto de reciente aparición y trata de englobar toda aquella información o acciones que se realizan sin el control de los departamentos de IT en las empresas, una vez que se conectan las aplicaciones a la protección de un SDP en el caso de uso de la aplicación como servicio SaaS, se tiene visibilidad completa de lo que se tiene en las aplicaciones y lo que ocurre con cada elemento, esto facilita la administración, en la siguiente Figura 3.24 se puede observar que se realiza un inventario completo del contenido de la solución SaaS, se categoriza y activa un monitoreo constante a través de API.

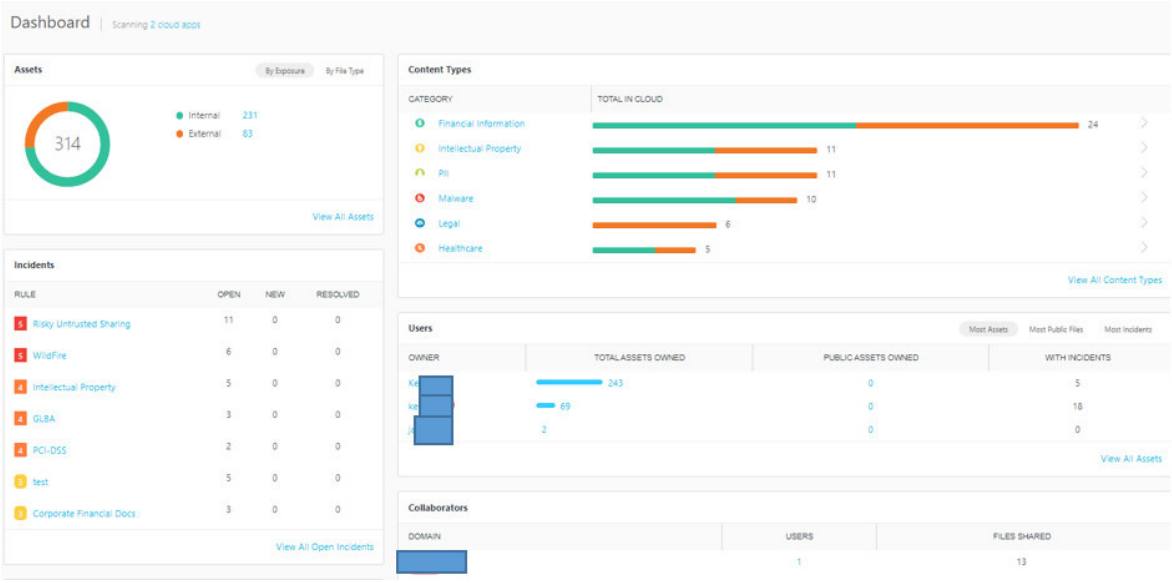

Figura 3.24 Dashboard de la solución para protección de servicios SaaS mediante SDP.

Para el piloto se configuró la protección para los servicios de BOX y de Google, a continuación, en la Figura 3.25, podemos observar las aplicaciones

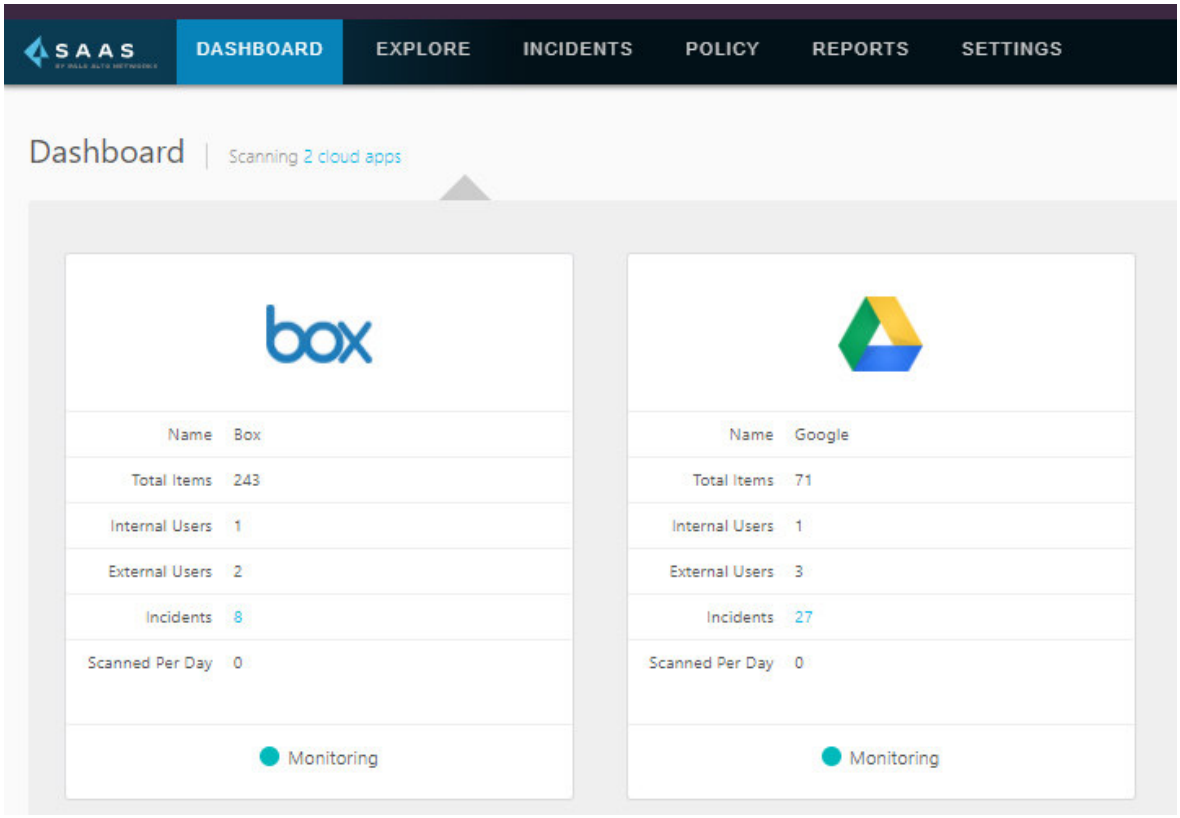

Figura 3.25 Servicios SaaS que se monitorean

A estos servicios a más de proteger su acceso mediante la aplicación del esquema de ZT o confianza cero, se añade la protección ante amenazas, es decir, si un usuario intenta compartir un documentos, enlace o archivo malicioso, la protección de *antimalware* y prevención de fuga de información sensible en el SDP, como se puede observar en la Figura 3.26.

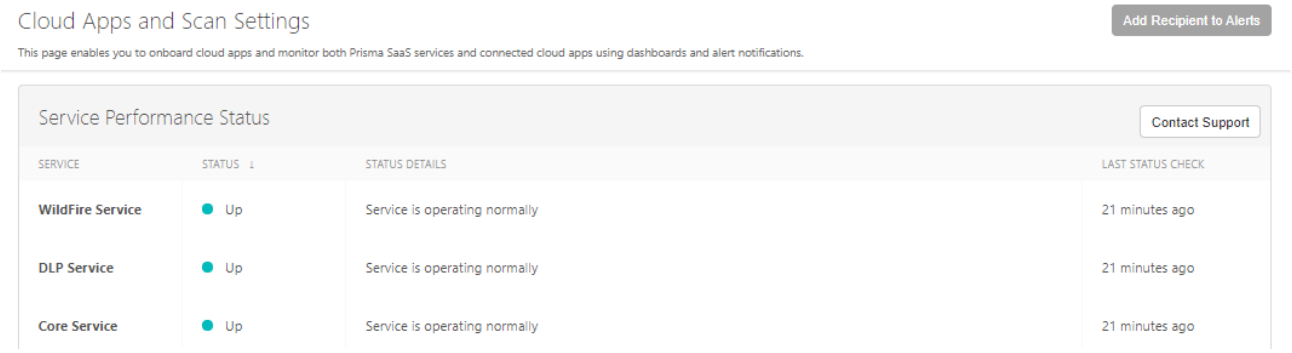

Figura 3.26 Módulos de protección habilitados para aplicaciones SaaS

La protección *antimalware* permite realizar monitoreo de los archivos que entran y salen de la aplicación SaaS en búsqueda de *malware*. Esta protección se configura por tipo de archivo, como se muestra en la Figura 3.27.

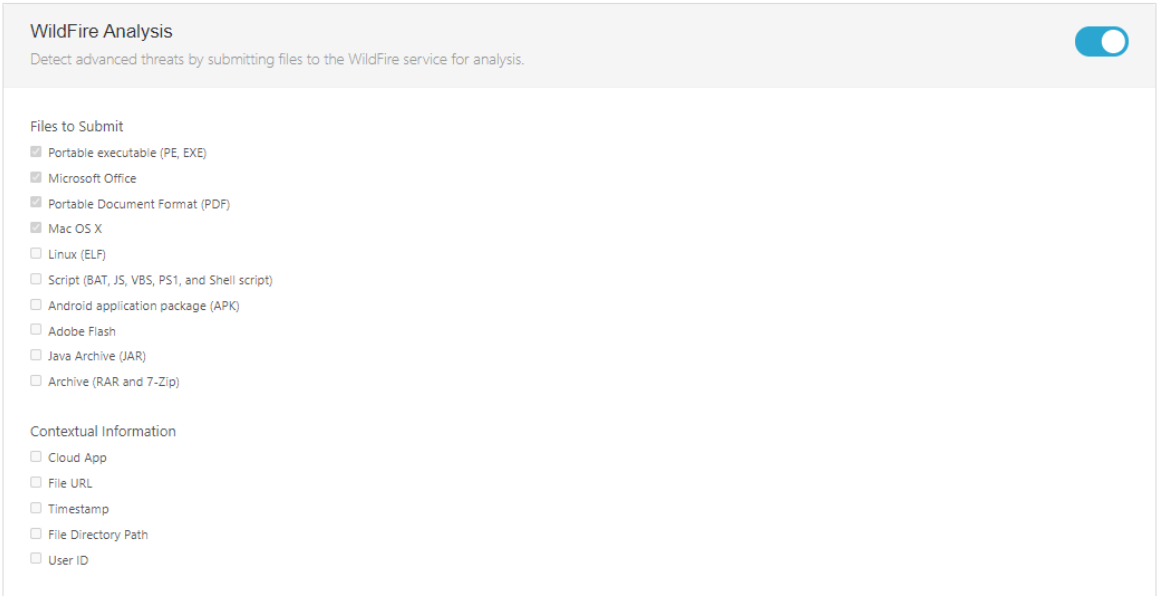

Figura 3.27 Protección antimalware habilitada

La protección de prevención de fuga de información o DLP evita que salga información confidencial de estos servicios a dispositivos no autorizados por la empresa ALTEL SA. Si

un usuario tiene las credenciales adecuadas para descargar un archivo, lo podrá hacer siempre que el dispositivo de destino de la información pertenezca a la empresa, si abre la aplicación SaaS en otro dispositivo, aún si dispone de las credenciales de administrador del documento, no lo podrá descargar a ese dispositivo por no estar autorizado para almacenar información catalogada como sensible, la configuración de esto lo podemos ver a continuación, en la Figura 3.28, se observa las categorías para detectar datos financieros, legales o de salud mediante el uso de aprendizaje de máquina o *Machine Learning.*

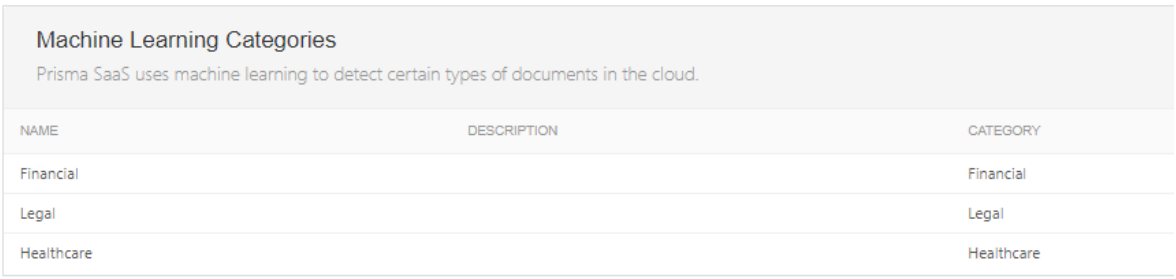

Figura 3.28 Configuración de DLP

A continuación, en la Figura 3.29 se ve un ejemplo de los resultados de los documentos que fueron detectados por contener información que puede ser sensible y no se permiten descargar o cargar a sitios no confiables, lo cual refuerza la seguridad de las aplicaciones SaaS.

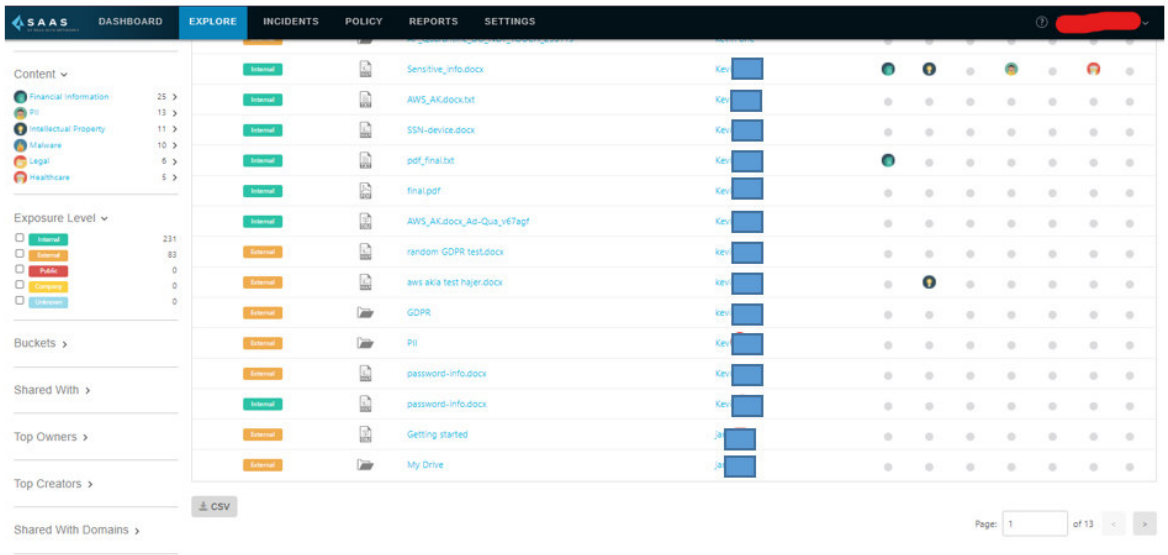

Figura 3.29 Documentos que contienen información sensible.

En conclusión, la misma protección que se tenía en el punto final del usuario, dentro de la red corporativa atrás de varios elementos de seguridad como Firewall, WAF, DLP, *Antimalware*, etc, se tiene sin problemas en cualquier dispositivo o punto de acceso en internet para los usuarios fuera de la red corporativa.

A continuación, en la Figura 3.30, podemos ver las conexiones que permiten al usuario acceder de forma segura a las aplicaciones desde cualquier lugar a través del uso de SDP.

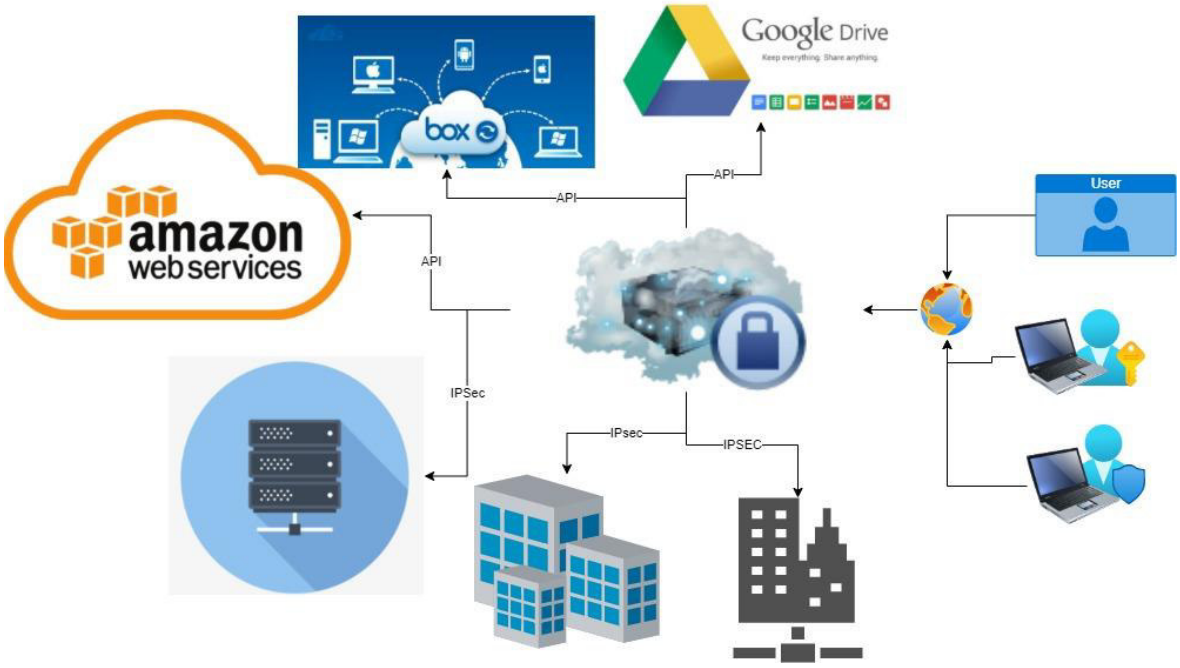

Figura 3.30 Resumen de las conexiones a todos los servicios probados.

A los servicios y servidores en el *datacenter* principal o en una oficina local, se accede mediante conexiones IPSec desde la nube del proveedor de SDP hacia el o los firewalls de la empresa, extendiendo las características de protección y control en la red.

Al servicio de infraestructura en la nube pública de AWS, la conexión se la realiza mediante un API, que es una interfaz de programación de aplicaciones, con esto se puede, de igual forma, extender la protección de la red, en caso de tener un firewall en la infraestructura de nube, también se podría conectar mediante IPSec como el caso de la infraestructura en las premisas de la empresa, en este proyecto se probó un servidor virtual, sin embargo, aplica para todos los servicios en la nube incluso lo que es *ServerLess,* una tecnología que permite desplegar infraestructura mucho más optimizada ya que el servidor tiene solo las

funciones necesarias para una aplicación en concreto, lo que optimiza enormemente el uso de recursos y disminuye costos.

A los servicios SaaS las conexiones se realizaron también mediante un API, a través de ella se puede monitorear todo lo que sucede con el servicio SaaS, el SDP, principalmente se usa para brindar acceso seguro y protección mediante políticas, sin embargo, se pueden tener más usos como la prevención de fuga de información en estas aplicaciones sobre la que los administradores de TI tienen menos o ningún control.

Finalmente, se indican todas las funcionalidades activadas y probadas durante el despliegue del prototipo de protección SDP de la solución Prisma de la empresa Palo Alto Networks, en la red de prueba de ALTEL SA.

- **Funcionalidades activadas a nivel de red**

    - **Soporte para SD-WAN** La solución de SDP permite tener una red WAN, es decir una red de área extendida que cubre varios continentes mediante únicamente el uso de software y comunicaciones que viajan a través de internet. Para esto en el caso de ALTEL S.A. se prueba el piloto mediante el uso de la solución GlobalProtect de Palo Alto Networks. Esto se realiza mediante conexiones que mayormente son MPLS pero que para Altel S.A son transparentes es decir están listas para ser utilizadas con el servicio de SDP contratado. Para poder conectar las “últimas millas”, por llamarlo de alguna manera, se usan tunes Ipsec, así todas las redes LAN de cada una de las ubicaciones, pueden verse entre sí como si fueran una red LAN extendida alrededor del mundo en 5 países con diversas ubicaciones y su red WAN definida por software, que interconecta las diferentes LAN.

    - **NaaS** Se valida las funcionalidades de transporte de datos que se realiza entre los nodos SDP del proveedor, estas conexiones se prestan como un servicio y son dinámicas, es decir se crean y eliminan redes tan rápido como el usuario se conecta a un punto de acceso SPD y requiere consumir servicios de ciertas localidades de acuerdo con su perfil en la empresa.

    - **VPN IPsec** En cada ubicación geográfica que se tiene servicios de red para los usuarios se conecta mediante túnel Ipsec al proveedor de SDP.

    - **VPN SSL** Dentro del software de Globalprotect se dispone de conexión VPN SSL a ciertos activos de información de interés del usuario. Así en el caso de que desde un computador se autentica un usuario interno, es decir un

empleado de ALTEL, se asigna permisos de acceso remoto a ciertos recursos de la empresa y si se conecta un contratista o proveedor se asigna acceso a otros recursos y no se requiere más que la autenticación mediante usuario, contraseña y en caso extremo un doble factor de autenticación biométrico como un código enviado al celular del usuario.

- **Políticas de reenvío de tráfico** Según el rol que el usuario desempeña en la organización se le asignan políticas de navegación, por ejemplo, en el caso del usuario contratista que no pertenece a ALTEL, si el usuario está navegando sin el agente SDP puede navegar libremente a redes sociales, páginas de entretenimiento, etc, pero no podrá acceder a servidores internos, una vez que activa el cliente SDP, podrá navegar a servidores internos pero su navegación a entretenimiento, redes sociales y cosas similares, se limita, puesto que no es política de la compañía poner la infraestructura a disposición de los usuarios para el entretenimientos sino para labores estrictamente apegadas a su rol de trabajo.

  Del mismo modo una política configurada en el sitio 3, por ejemplo, se distribuye a todos los nodos SDP, de manera que cuando el usuario se conecta desde otra ubicación geográfica las políticas de navegación están aplicadas como si estuviera dentro del perímetro de la red Local en la empresa, a través de la Red LAN.

- **Calidad de Servicio** Muchas aplicaciones requieren ciertas condiciones particulares respecto al rendimiento de la red como retarlo o latencia o ancho de banda para funcionar correctamente por lo que es importante que la solución de SDP permita configurar calidad de servicio, esto generalmente es necesario para aplicaciones como telefonía IP u otras que trabajan en tiempo real.

- **Funcionalidades de seguridad**

  - **Descripción y análisis de tráfico SSL** Para aplicar las políticas y controles de seguridad todo el tráfico cifrado es abierto, se analiza y se vuelve a empaquetar, cifrar y reenviar a su destino final, este análisis ocurre en los nodos que prestan el servicio de SDP.

- **Agente de seguridad de acceso a la nube (CASB)** Esta tarea se llevó a cabo a través del uso del agente de GlobalProtect que realiza esta función, esto gracias a la aplicación del concepto de Zero Trust.
- **Gateway de navegación web mediante servicio en la nube** Se logró proteger a los usuarios durante su experiencia de navegación en internet, se analizó la reputación de los sitios web, IP, categoría, contenido, etc, de acuerdo con esto se aplicaron políticas de seguridad. También se aplican políticas de control de acuerdo con las necesidades o condiciones de cada empresa como el bloqueo de navegación a redes sociales desde dispositivos corporativos.
- **Firewall como servicio** Dentro de cada acceso SDP que se pudo ver se encuentra prácticamente todo un Firewall que se presta como servicio por el proveedor de SDP, este firewall, es de nueva generación e incluye protección a nivel de prevención de intrusos en la red, prevención de *malware*, etc.
- **DNS seguro** El servicio de SDP cuenta con una base de reputación de nombres de dominio que permite validar la reputación y controló de forma efectiva el intento de acceso a sitios maliciosos e incluso evitó la descarga de contenido de *malware*.
- **Prevención de fuga de información** Se probó los accesos a recursos de la compañía basándose en el usuario, así un empleado tenía acceso a ciertos recursos y un proveedor o contratista a otros, limitando las posibilidades de pérdida o fuga de información.
- **Sandboxing** Se validó con muestras de *malware* de la familia EICAR diseñadas para probar soluciones de seguridad que el contenido de los archivos se emula en el sandbox que el servicio de SDP incluye.

3.5.3 DIRECCIONAMIENTO IP

La implementación se realizó de acuerdo a la Tabla 3.1 con las direcciones IP:

Elemento	Dirección
MATRIZ	
Red de la matriz	192.168.250.0/24
HQRestrictedServer	192.168.250.50/24
HQServer	192.168.250.100/24
SUCURSAL	
Acceso WAN enlace 1	172.16.10.0/24
Acceso WAN enlace 2	172.16.20.0/24
Sub Red 1 de la sucursal	192.168.74.0/24
SR1 – Gateway	192.168.74.1/24
Tunnel.1	192.168.74.251/32
Tunnel.2	192.168.74.252/32
Win-subnet1	192.168.74.100/24
Sub Red 2 de la sucursal	192.168.174.0/24
SR2 – Gateway	192.168.174.1/24
Win-Subnet2	192.168.174.100/24

Tabla 3.1 Direccionamiento IP de la red IP de ALTEL

3.5.4 PRUEBAS REALIZADAS

Se consideraron 5 escenarios de prueba para verificar todo lo implementado y descrito en este capítulo, que son:

1. Asegurar a un usuario móvil

   Con esta prueba se pretende demostrar que la protección que se tiene dentro de la red local mediante el uso de firewall y sistema de prevención de intrusos en la red se extiende a través del uso de SDP al dispositivo final sin importar su ubicación geográfica.

2. Asegurar el acceso remoto a la red LAN

   Esta prueba permite verificar que se puede acceder a recursos locales mediante el uso del sistema SDP, sin importar la ubicación geográfica o física del dispositivo.

3. Acceder a un equipo de la oficina remota mediante un enlace de acuerdo con los permisos del usuario

   Una solución actual de VPN permite transportar datos desde una ubicación remota hacia la red interna, sin embargo, el perfil asignado a la comunicación no está asociado al rol del usuario, se requiere entonces, VPN de nueva generación que sincronicen los permisos de la VPN con los permisos del usuario y esto no se ha implementado con éxito en las organizaciones por la cantidad de configuraciones manuales que se tendría que realizar y las limitaciones de las soluciones de VPN en granularidad de estas configuraciones. La prueba pretende validar que con el usuario se asignan o eliminan permisos a nivel de red de forma sencilla, brindando o quitando acceso a un sistema restringido.

4. Acceder a un equipo de la oficina remota con dos enlaces, activo-pasivo para redundancia.

   Una de las preocupaciones de la empresa auspiciante es la introducción de un punto de falla en la arquitectura, es decir, que pasa si uno de los puntos de acceso del SDP del proveedor no está disponible, esto podría ocasionar que no esté disponible toda la infraestructura que se accede a través del SDP. Por esta preocupación se probó el acceso considerando 2 canales de comunicación, un canal activo y un canal pasivo.

5. Acceder a un equipo de la oficina remota con dos enlaces, activo-activo para redundancia.

   Debido a la preocupación anterior, también se probó mediante conexión activo-activo.

3.5.5 RESULTADOS OBTENIDOS:

La implementación del prototipo se realizó empleando la solución de Palo Alto Networks, la Figura 3.31nos muestra la consola en donde podemos operar todos los ambientes empleados para las pruebas, se dispone de acceso a los Firewall de la oficina principal, de las oficinas remotas o sucursales, un administrador de todos los Firewall e IPS a través de Panorama, que es el *dashboard* de administración centralizada, y el acceso a los sistemas operativos de los servidores y equipos por probar mediante RDP o escritorio remoto.

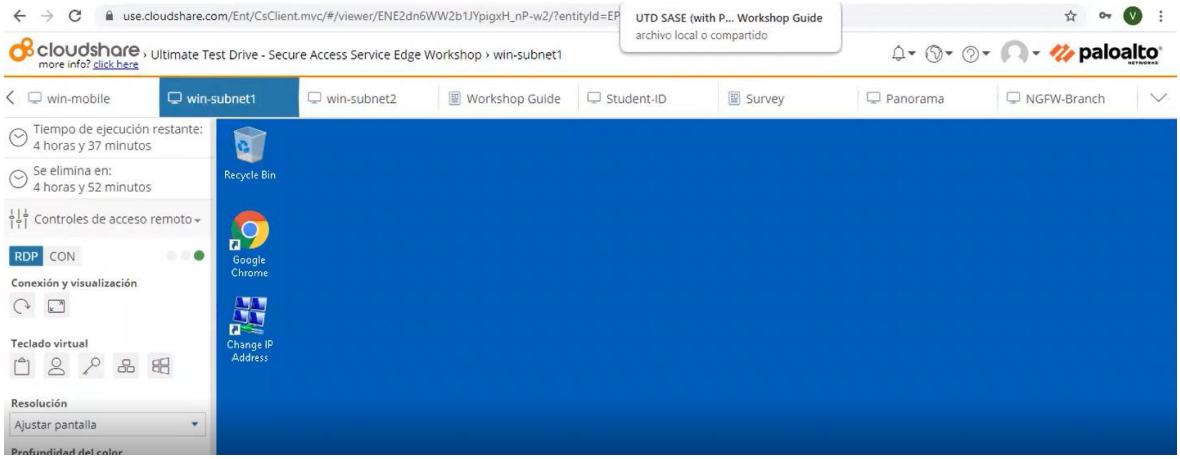

Figura 3.31 Dashboard de administración de la implementación del prototipo.

3.5.6 Asegurar a un usuario móvil

Para la protección de dispositivos móviles se utiliza el agente GlobalProtect, que permite seguridad constante y acceso a Internet, ya que, determina automáticamente la mejor puerta de enlace para el usuario y canaliza el tráfico a esta ubicación.

Una vez instalada la aplicación en los dispositivos se debe habilitar e ingresar las credenciales de usuario se verá un icono en el escritorio como se muestra a continuación en la Figura 3.32.

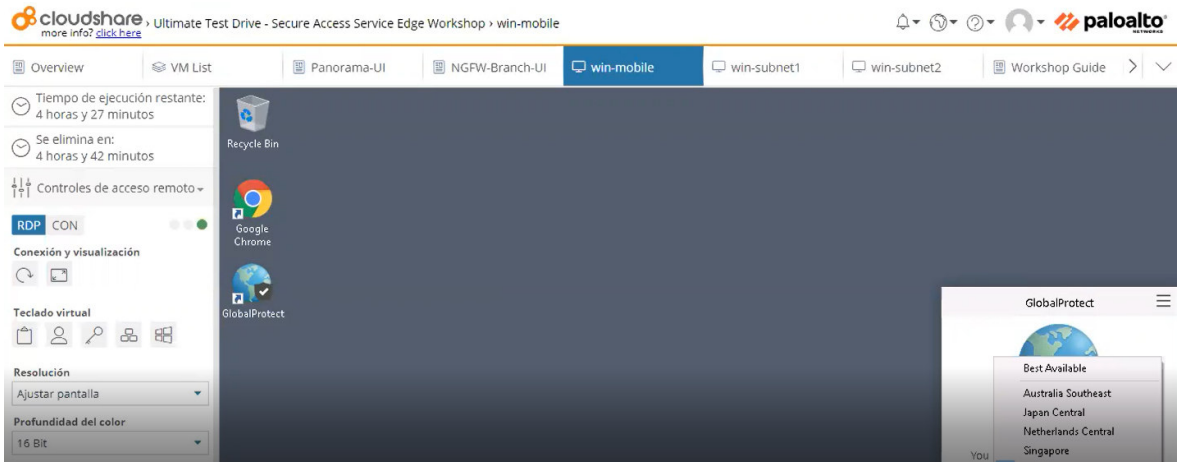

Figura 3.32 Dispositivo móvil con el agente de GlobalProtect listo.

Como se muestra en la Figura 3.33 al habilitar la conexión se establece un túnel SSL/IPsec que brinda una conexión segura con la puesta de enlace más cercana disponible de Prisma Access.

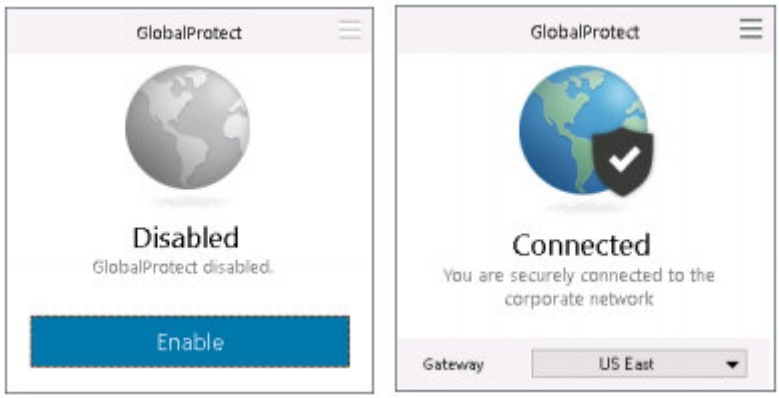

Figura 3.33 Agente de GlobalProtect

Posterior a este paso, el dispositivo móvil se puede visualizar en la consola de administración. En la consola de administración se muestra un resumen del estado de los dispositivos, el número de puerta de enlace y cuántos móviles se encuentran con conexión actualmente.

Para probar que la aplicación funciona correctamente se abre el navegar desde el dispositivo móvil y se ingresa la siguiente página http://2016.eicar.org/download/eicar.com que es un archivo de prueba contra *antimalware*.

En la Figura 3.34 se observa el mensaje de bloqueo de la página.

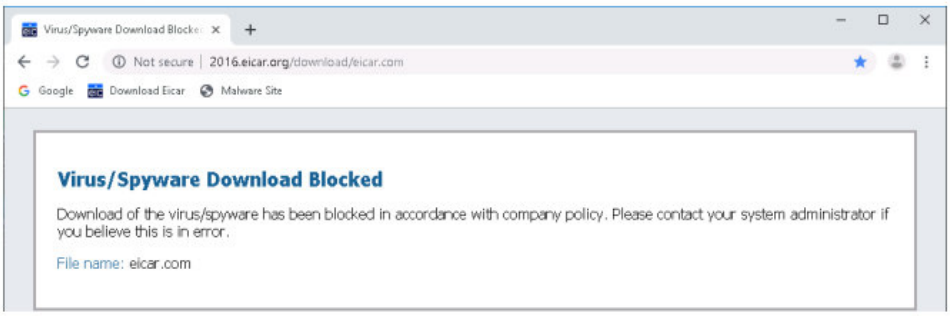

Figura 3.34 Detección de amenaza en la red y bloqueo

Al realizar una segunda prueba, se ingresa a un sitio web de *malware* como, por ejemplo https://businesstobuy.net/, la herramienta la bloquea, porque la detecta como una herramienta de filtrado de URL, como muestra la Figura 3.35.

Figura 3.35 Detección de *malware* y bloqueo.

Con estas pruebas se demuestra que la seguridad se entrega desde la nube y se adapta a la puerta de enlace más cercana a los usuarios.

La herramienta incluye capacidades de seguridad como filtrado de URL, prevención de amenazas y WildFire que es un servicio en la nube diseñado para identificar y bloquear ataques de día cero.

Las herramientas SDP permiten eliminar la necesidad de trasladar el tráfico de los usuarios a las oficinas o centros de datos. El tráfico se analiza y limpia en el primer punto de acceso disponible en la infraestructura del proveedor de SDP.

3.5.7 Asegurar el acceso remoto

Los administradores de la herramienta Prisma Access pueden controlar el acceso de los usuarios a las aplicaciones empresariales, ya sea, de forma individua o por grupo de usuarios y de acuerdo con el estado del dispositivo.

Para que los accesos se realicen con éxito se tiene levantados los túneles mediante IPSec como se muestra en la Figura 3.36.

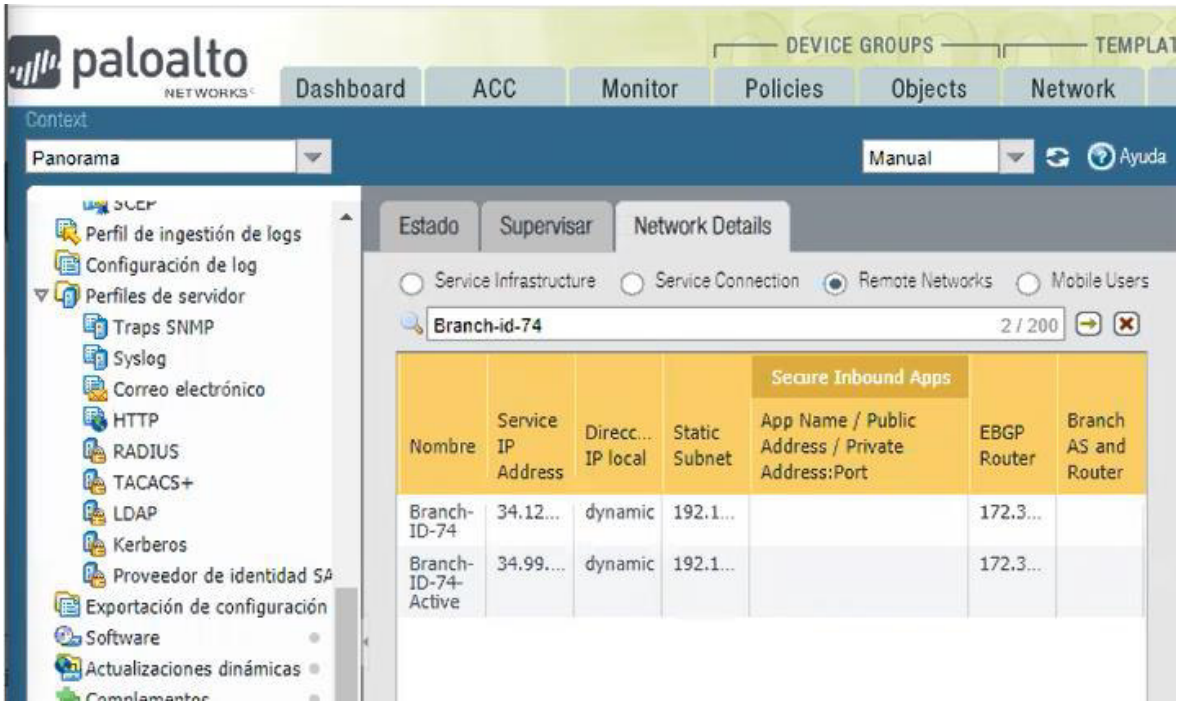

Figura 3.36 Túneles de conexión.

El agente GlobalProtect requiere como primer paso que, los usuarios se autentifiquen correctamente para configurar el túnel. La autenticación se puede realizar por diversos métodos como la autenticación multifactor (MFA), Radius, Active Directory y certificados.

Una vez que se realiza esta configuración el túnel el usuario tendrá acceso solo a aplicaciones específicas y solo en dispositivos con autorización, estos accesos se convierten en puertas de los enlaces, como se muestra a continuación en la Figura 3.37:

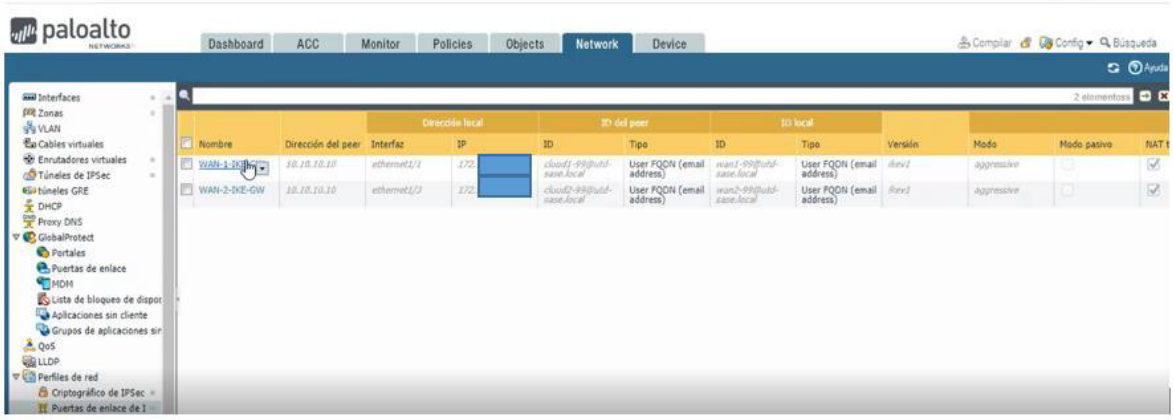

Figura 3.37 Puertas de enlace disponibles.

Como se muestra en la Figura 3.38, a cada usuario se asigna un perfil, que depende de las tareas que desempeña en la organización, por lo que, tendrá acceso únicamente a las aplicaciones que le ayudan con el desarrollo de sus actividades.

	Name	Location	Source			Destination	
			Zone	Address	User	Zone	Address
1	Secure-Internet-Traffic	Mobile_User_Device_Group	PrismaAccess-Remote-Users	any	any	Internet	any
2	Secure-Access-to-HQ-Restrictted-Server	Mobile_User_Device_Group	PrismaAccess-Remote-Users	any	employee	HQ	Restricted-Server
3	Deny-Access-to-HQ-Restricted-Server	Mobile_User_Device_Group	PrismaAccess-Remote-Users	any	contractor	HQ	Restricted-Server
4	Secure-Access-to-HQ-and-Branch-Office	Mobile_User_Device_Group	PrismaAccess-Remote-Users	any	contractor	Branch-Office	any
					employee	HQ	

Figura 3.38 Políticas de acceso basadas en el usuario.

Para ALTEL se crearon 2 perfiles de usuario, *employee* para técnicos en ingenieros preventa los cuales manejan su información dentro del servidor HQRestrictedServer y *contractor* para empleados o proveedores que se contratan ocasionalmente por la empresa y sus aplicaciones e información se encuentra en el HQserver, como se muestra en la Tabla 3.2.

SERVIDOR	**IP**	**ACCESO**
HQRestrictedServer	192.168.250.50/24	Técnicos e Ingenieros preventa
HQServer	192.168.250.100/24	Contratistas

Tabla 3.2 IP de perfiles de usuario

Al ingresar con las credenciales de contratista comprueba el acceso al servidor HQServer que corresponde a la IP 192.168.250.100.

En la Figura 3.39 se muestra que los contratistas tienen acceso al servidor HQServer.

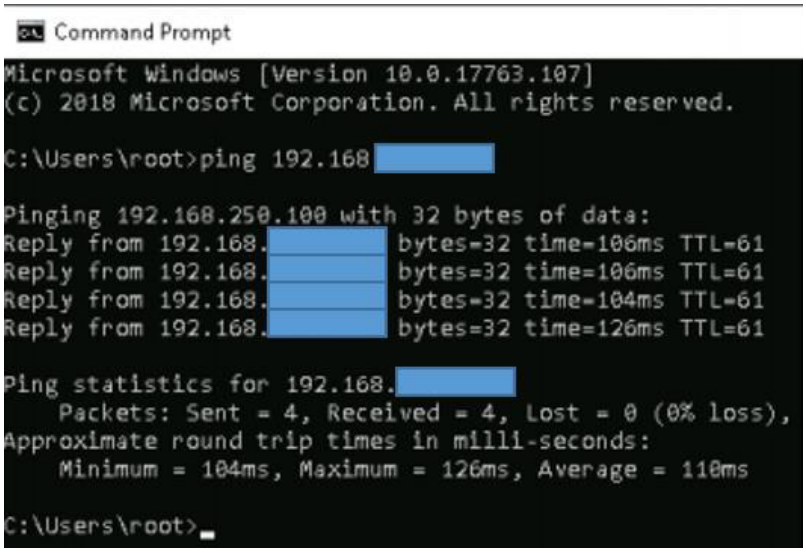

Figura 3.39 Evidencia de conexión exitosa.

Como muestra la Figura 3.40 el ping falló como se esperaba porque los contratistas no tienen acceso al servidor HQRestrictedServer.

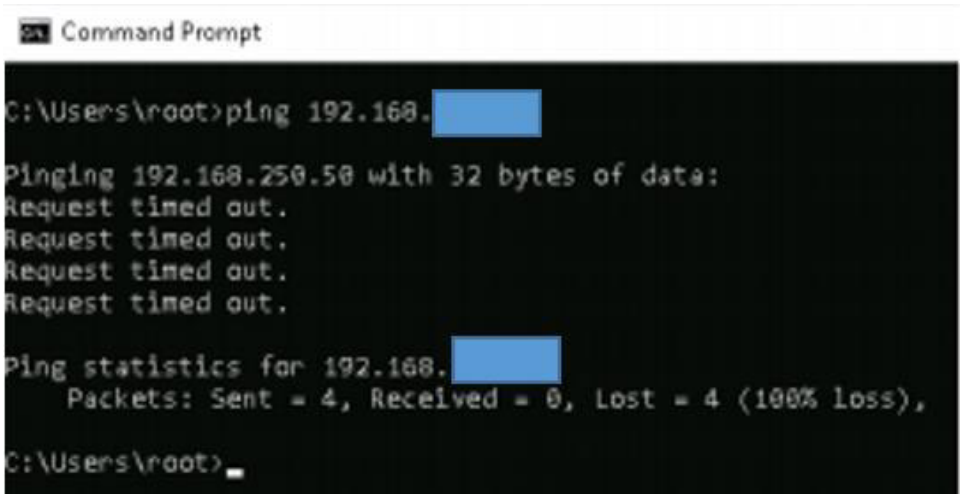

Figura 3.40 Evidencia de conexión no exitosa

La correcta configuración y autenticación del túnel no proporciona automáticamente acceso a las aplicaciones internas. Se valida si el usuario dispone o no de los permisos de acceso granulares a cada servicio desplegado en la red interna.

Se observa que la autenticación y autorización se da en función de cargo del usuario, al grupo que pertenece, del dispositivo que lo solicita, a la aplicación a la que accedes y los puertos y servicios que se utilizan.

3.5.8 Acceder a un equipo de la oficina remota con un enlace basado en el usuario

El concepto SDP permite brindar seguridad constante a todas las sucursales de una organización sin necesidad de implementar hardware costoso o retroceder el tráfico al centro de datos.

Para incorporar una oficina remota es necesario configurar un túnel IPSEC desde la sucursal actual hasta Prisma Access.

Para configurar un túnel VPN, los pares o puertas de enlace VPN deben autenticarse entre sí, mediante claves precompartidas o certificados digitales, y de esta manera establecer un canal seguro que se utilizará para proteger el tráfico entre los anfitriones de cada lado.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ike-gateway

Para la configuración de la puerta de enlace IKE es importante tener clara la dirección IP del dispositivo remoto con el que forma el túnel IPsec, para poder colocarlo en la configuración como muestra la Figura 3.41.

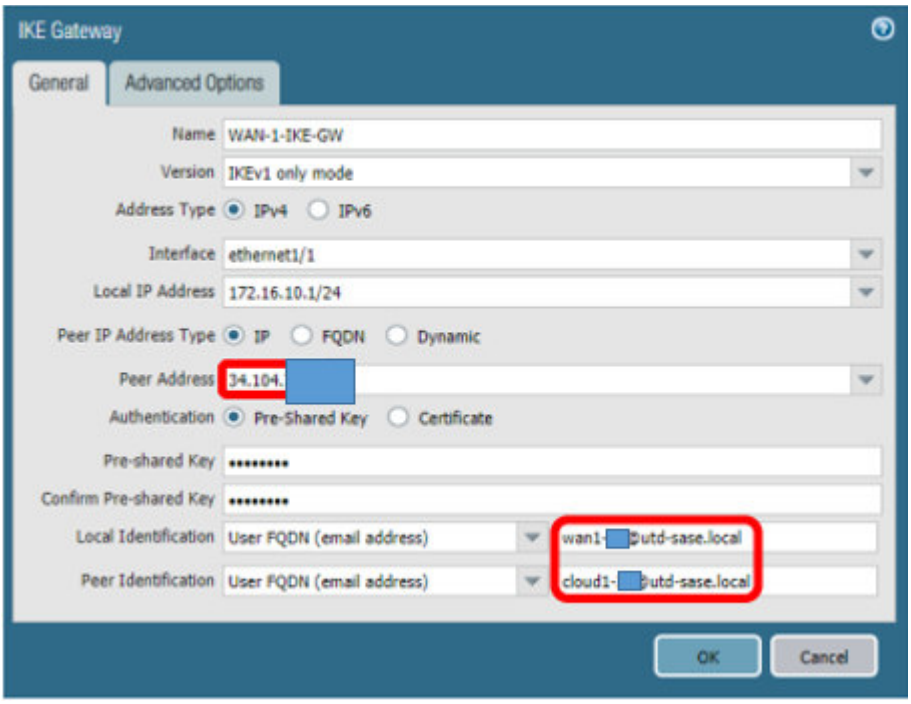

Figura 3.41 Configuración del Gateway para la conexión al sitio remoto

Los firewalls de Palo Alto Networks que inician y terminan las conexiones VPN a través de dos redes se denominan Gateway IKE. Para configurar el túnel VPN y enviar tráfico entre puertas de enlace IKE cada par debe tener una dirección IP estática o dinámica o un FQDN, Fully Qualified Domain Name, que es un nombre de dominio completo que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo. Para crear la ruta estática como se muestra en la Figura 3.42

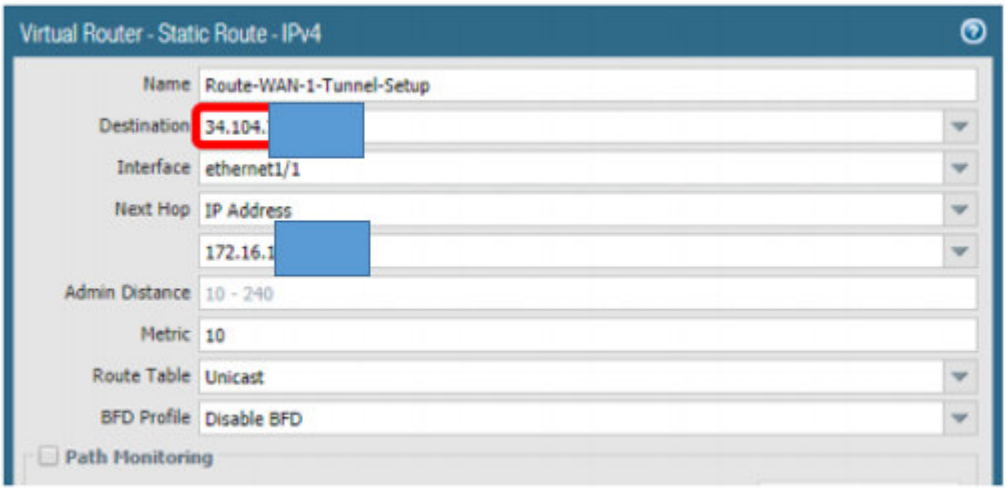

Figura 3.42 Configuración del túnel para el acceso al sitio remoto

Acceder a un equipo de la oficina remota con dos enlaces, activo-activo para redundancia.

Para asegurar la calidad del servicio es necesario mantener un nivel de disponibilidad que garantice a los usuarios el acceso permanente a las aplicaciones o servicios de la organización, por este motivo se recomienda la configuración sistemas de redundancia.

Por lo expuesto anteriormente, se considera la configuración un túnel IPSec redundante desde cada una de las sucursales, y con distinta ubicación geográfica del túnel principal.

Los túneles IPSec redundantes se deben configurar individualmente y especificar el ancho de banda y su ubicación geográfica como muestra la Figura 3.43, de manera similar a lo que se realizó con los túneles IPSec principales. Desde la sucursal remota se puede tener más de una conexión activa a Prisma Access, lo que permite que ambos túneles (principal y redundante) mantengan una conexión simultánea.

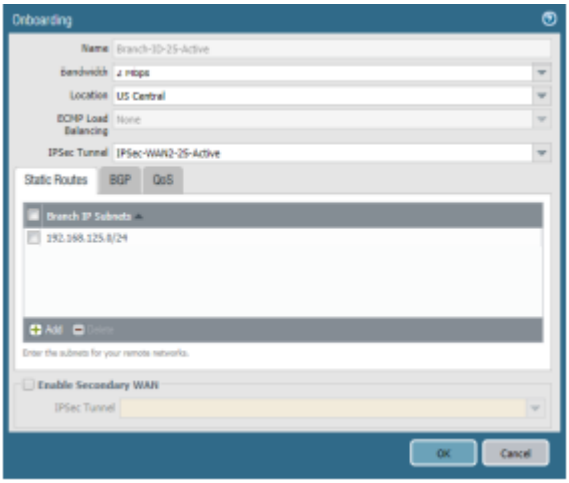

Figura 3.43 Configuración Ipsec para la conexión a la sucursal remota.

Al realizar pruebas con los túneles IPSec de redundancia desde las sucursales, se obtuvo los mismos resultados que al usar los túneles IPSec principales. Se valida que los usuarios mantienen los accesos que se otorgaron originalmente.

Como se muestra en la Figura 3.44, se puede observar que todo el tráfico es analizado y protegido como si el dispositivo estuviera en la red interna a pesar de que está en otra ubicación geográfica y se conecta mediante el agente de SDP

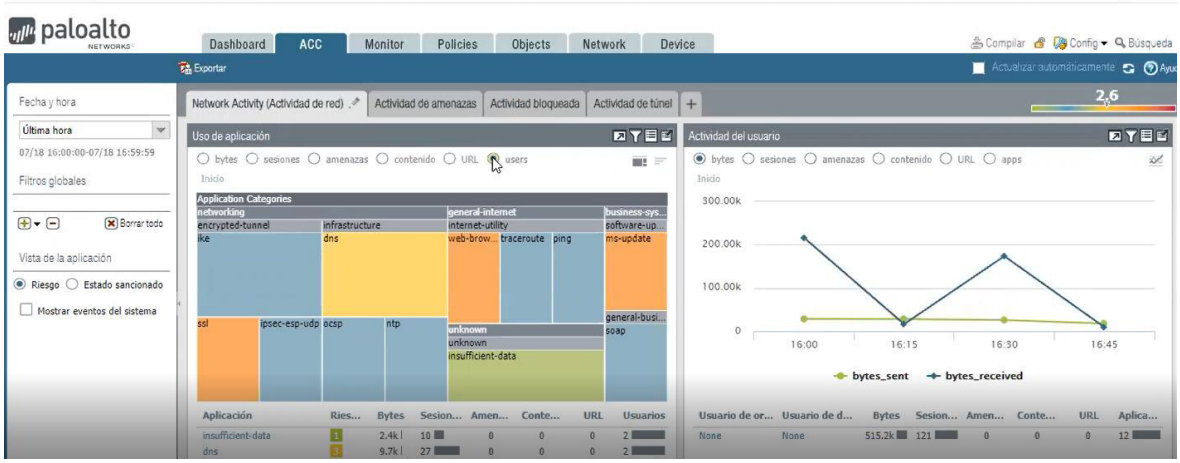

Figura 3.44 Resultado de final de comunicaciones de los dispositivos remotos.

3.6 COSTOS DE IMPLEMENTACIÓN DE SDP EN ALTEL SA

Para desplegar la solución probada, se debe considerar los costos descritos en la Tabla 3.3, estos costos se encuentran en **dólares americanos**.

En esta tabla podemos ver que se probó con licenciamiento que incluye acceso para 10 usuarios, porque es lo mínimo que la empresa que provee el SDP vende.

- El ITEM 1, es el acceso a infraestructura local mediante el uso de SDP, acceso a los servicios en el datacenter local, acceso a las oficinas de las sucursales, equipos en la red LAN, etc.
- El ITEM 2 es la protección y acceso mediante SDP a la infraestructura en la nube pública de AWS.
- El ITEM 3, permite proteger a los usuarios y la información que acceden a plataformas de SaaS como Google Drive y Box; finalmente,
- El ITEM 4 son las horas hombre invertidas en el proyecto, considerando el valor promedio del costo que maneja la empresa auspiciante del proyecto de titulación.

Puesto que, los aliados estratégicos de la empresa ALTEL, tienen en su portafolio de soluciones a Palo Alto Networks, no fue necesario solicitar cotizaciones o considerar costos de internación al Ecuador, impuestos y demás, estos se los maneja en otro país, por lo que se considera únicamente los valores que la empresa debe costear, en caso de otras empresas de deben considerar impuestos, ISD y valores de internación al país y uso de software extranjero como lo estipula la ley:

ITEM #	**Cantidad**	**Descripción**	**Valor Unitario (En USD)**	**Valor Total (En USD)**
1	10	Prisma Access (x 10 usuarios)	$ 400,00	$ 4.000,00
2	10	Prisma Cloud (x10 usuarios	$ 3.750,00	$ 3.750,00
3	10	Prisma SaaS (x 10 usuarios)	$ 3.750,00	$ 3.750,00
4	800	Horas Hombre	$ 20,00	$ 16.000,00
			TOTAL	**$ 27.500**

Tabla 3.3 Costo de implementación del prototipo

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

A través del desarrollo del presente Proyecto de Titulación se logró diseñar e implementar un sistema de protección con una solución de Perímetro Definido por Software para la empresa ALTEL S.A mediante el uso de Prisma de la empresa Palo Alto Networks. Este sistema de protección le permite a Altel asegurar sus dispositivos y la de sus colaboradores alrededor del mundo y de esta manera evitar la pérdida o divulgación de información sensible de la compañía y de sus clientes

Se implementó un prototipo de Sistema de Protección para Perímetro de Red Definido por Software para la Red de ALTEL S.A. mediante el uso de la plataforma PRISMA de la empresa Palo Alto Networks para cubrir las necesidades de comunicación, movilidad y al mismo tiempo asegurar la información sensible que maneja la organización.

Se realizó el estudio de la evolución del perímetro de las redes, la seguridad y los componentes de la arquitectura actual, así como los mecanismos de protección basados en perímetro definido por software, para definir una metodología que asegure un perímetro que no se encuentra definido.

Estudiamos los componentes en las arquitecturas de red actuales y los mecanismos de protección basados en Perímetro Definido por Software SDP y comparamos los mecanismos de protección tradicionales con SDP, y se observó que, en cuánto a costos y administración se trata SDP lleva a ventaja respecto a la protección tradicional mediante Firewalls y VPN, por la facilidad de movilidad que nos proporciona SDP..

Se realizaron pruebas de funcionamiento y validación de los resultados de manera satisfactoria, al ser Altel una empresa con colaboradores a nivel mundial. De esta manera se confirmó las ventajas de SDP al asegurar un perímetro que no se encuentra definido.

La solución de SDP, permite extender el perímetro de las redes hasta el dispositivo final del usuario, sin importar donde esté ubicado geográficamente y los permisos de acceso, navegación, la protección a nivel de red como prevención de intrusos, detección y control de malware, prevención de fuga de información, carga y descarga de datos sensibles para la organización en dispositivos no autorizados, se ejecutó de manera efectiva en el equipo de punto final.

El acceso a los servicios de SDP es amigable al usuario, la empresa que provee la solución empleada para este prototipo posee centros de datos alrededor del mundo con una

presencia lo suficientemente amplia para cubrir las necesidades de la organización auspiciante, por esta razón no presenta inconvenientes ni retardos a nivel de red.

Se realizaron pruebas mediante ataques simulados con la utilidad EICAR y se logró verificar que después de activar la protección mediante el agente de SDP, estos ataques fueron contenidos de manera exitosa.

4.2 RECOMENDACIONES

Es imprescindible contar con información coherente del inventario de activos y de aplicaciones a las que los usuarios deben acceder, en el caso de la empresa auspiciante, esta información proviene de una consultoría de clasificación de información y activos, que permite asignar los permisos de acceso a los usuarios con base en el rol que desempeñan para la organización.

Es necesario considerar y limitar el alcance del proyecto de implementación, en este caso se cubrió todos los casos de uso, estos casos de uso son, acceso a la infraestructura local, acceso a la infraestructura de nube y a servicios de SaaS. En general, no todas las organizaciones van a tener todo, por lo que se recomienda realizar un análisis de esto para no incurrir en gastos innecesarios.

Es necesario tener bien definido el nivel de acceso que tiene cada usuario a la información de la empresa esto permite definir reglas de manera más rápida y eficaz, evitando la perdida de información y divulgación de esta a usuarios no autorizados.

Es de vital importancia capacitar a las empresas de la importancia de la seguridad informática ya que pequeños cambios en las actividades de los usuarios pueden evitar la ataques a la red.

Para la aplicación efectiva de la metodología propuesta es necesario que la empresa que desee implementar protección mediante SDP, realice el proceso de manera consultiva, es decir llevando la documentación de los usuarios, activos, accesos, requerimientos, alcances y demás de manera sistemática y ordenada, esta información es la que constituye la base para el diseño de la solución por implementar y de la calidad de esta información depende directamente el éxito del proyecto. Las plataformas de SDP, como en este caso Prisma, vienen listas para operar, sin embargo, requieren la configuración de reglas y políticas, estas reglas deben ser cuidadosamente definidas con los administradores de las tecnologías de la información con base en los levantamientos de información y alcances.

4.3 REFERENCIAS BIBLIOGRÁFICAS

[1] F. Doelitzscher, A. Sulistio, C. Reich, H. Kuijs, and D. Wolf, "Private cloud for collaboration and e-Learning services: from IaaS to SaaS," *Computing*, vol. 91, no. 1, pp. 23–42, 2011.

[2] E. L. R. Lucion and R. C. Nunes, "Software Defined Perimeter: improvements in the security of Single Packet Authorization and user authentication," in *2018 XLIV Latin American Computer Conference (CLEI)*, 2018, pp. 708–717.

[3] W. Charfi, M. Masmoudi, and F. Derbel, "A layered model for wireless sensor networks," in *2009 6th International Multi-Conference on Systems, Signals and Devices*, 2009, pp. 1–5.

[4] J. R. Darιn, *Fundamentos de Redes Informáticas: 2textordfeminine Edición*. IT Campus Academy, 2016.

[5] G. Tolosa, "Protocolos y Modelo OSI," *Recuperado de http://www. tyr. unlu. edu. ar/TYR-publica/02-Protocolosy-OSI. pdf*, 2014.

[6] M. Fernández Barcell and others, "Protocolo TCP/IP," 2014.

[7] K. Ashton and others, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[8] D. F. Á. Amézquita, J. C. P. Herrera, A. L. G. Zuluaga, and L. Y. M. Hernández, "Proveedores de Servicios de Internet y de contenidos, responsabilidad civil y derechos de autor," *Studiositas*, vol. 4, no. 3, pp. 51–64, 2009.

[9] M. Yrigoyen-Quintanilla and C. M. Torres-Paredes, "Implementación de un Datacenter académico virtualizado," *Interfases*, no. 008, pp. 93–124, 2015.

[10] I. G.-J. Sidera, "Los contratos informáticos de hosting y housing en relación con la normativa española de protección de datos de carácter personal," *Revista de la contratación electrónica*, no. 78, pp. 3–39, 2007.

[11] M. N. Osaba, "Virtualización en redes definidas por software," 2016.

[12] R. Miralles, "Cloud computing y protección de datos," *IDP. Revista de Internet, Derecho y Polιtica*, no. 11, pp. 14–23, 2010.

[13] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS," in *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*, 2015, pp. 148–155.

[14] J. P. Maroto, "El ciberespionaje y la ciberseguridad," in *La violencia del siglo XXI. Nuevas dimensiones de la guerra*, 2009, pp. 45–76.

[15] R. H. Gil, D. F. Amorós, and J. R. C. Fernández, "La ciberseguridad. Historia y evolución de la criptologιa. 1textordfeminine Parte," 2011.

[16] J. Dordoigne, *Redes informáticas-Nociones fundamentales (5textordfeminine edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...)*. Ediciones Eni, 2015.

[17] M. Szylkowska, "Amenazas cibernéticas y riesgo de proliferación en el área de logιstica: un resumen del problema," in *Anales de la Real Academia de Doctores de España*, 2019, vol. 4, no. 1.

[18] P.-E. Martιn, "Inseguridad cibernética en América Latina: Lιneas de reflexión para la evaluación de riesgos," *Instituto Español de Estudios Estratégicos*, vol. 8, 2015.

[19] J. M. Miranda and H. Ramirez, "Estableciendo controles y perιmetro de seguridad para una página web de un CSIRT," *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, no. 17, pp. 1–15, 2016.

[20] J. C. C. Sandoval, "Virtualización de las Funciones de Red," *Network*, 2019.

[21] P. Costa, M. Migliavacca, P. Pietzuch, and A. L. Wolf, "NaaS: Network-as-a-Service in the Cloud," in 2nd {USENIX} Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services (Hot-ICE 12), 2012.

5 ANEXOS

5.1 ANEXO A

El anexo A, constituye un libro de Excel que se puede emplear como guía para levantar información y ejecutar de forma exitosa la metodología que se planteó en este proyecto de titulación.

En la Figura 5.1, se muestra la caratula del documento, en esta caratula se tiene el control documental y un resumen del archivo, es recomendable seguir este formato para guardar todos los documentos de un proyecto, esto facilitará su identificación y comprensión a futuro o por personas ajenas al proyecto.

CONTROL DOCUMENTAL	
ENTIDAD:	
CLASIFICACIÓN:	**Confidencial**
TITULO:	Levantamiento de información
VERSIÓN:	Versión 1.0
FECHA DE EDICIÓN:	
FICHERO:	Anexo1-Plantillas.docx
HERRAMIENTAS DE EDICIÓN:	Microsoft Office Word
AUTORES:	Carlos López y Valeria Vasconez
RESUMEN:	Levantamiento de información necesaria para dimensionar e implementar una solución de SDP
DESCARGO	El presente documento es de propiedad intelectual de la entidad por lo que su acceso, copia total o parcial por personal no autorizado está terminantemente prohibido y su desacto será atendido de acuerdo a la legislación vigente de propiedad intelectual, código civil y penal ecuatoriano sergún sea el caso.

Figura 5.1 Plantilla para levantar información.

Inventario de activos

En la Figura 5.2, se muestra un ejemplo del levantamiento de activos que se debe realizar para el correcto dimensionamiento y diseño de una solución de seguridad como SDP, las organizaciones que lo empleen pueden añadir columnas a discreción según su necesidad para convertirlo en algo más completo para su uso particular.

IDENTIFICADOR	NOMBRE	TIPO	DESCRIPCIÓN	PROCESO AL QUE PERTENECE	NIVEL DE CLASIFICACIÓN D
AT001	win-mobile	Laptop	Laptop de uso general, para trabajo fuera de oficina	Ventas	Confidencial
AT002	win-subnet1	Desktop	Equipo ubicado en la matriz, subred 1	Ventas	Confidencial
AT003	win-subnet2	Desktop	Equipo ubicado en la matriz, subred 2	Servicios gestionados	Confidencial
AT004	NGFW-Branch-UI	Appliance Virtual	Firewall de borde de la matriz	Administrativo	Confidencial
AT005	Panorama	Appliance Virtual	Manager de los firewall	Administrativo	Confidencial
AT006	Prisma	SaaS	Servicio SDP de Palo Alto Networks	Administrativo	Confidencial

Figura 5.2 Matriz de accesos

La Figura 5.3 muestra una matriz de acceso basada en 5 roles, sin embargo, las organizaciones que opten por emplear esta metodología deben incluir todos los roles que hagan parte de su organigrama.

USUARIO	ROL	ACTIVO	ORIGEN DEL ACCESO
Contractor	Proveedor	192.168.XXX.XX/24	Any
Employee	Usuario	192.168.XXX.XXX/24	Any
Sales	Vendedor	192.168.XXX.XX/24	Any
Presales	Preventa	192.168.XXX.XX/24	Any
Manager	Gerente	192.168.XXX.XX/24	Any

Figura 5.3 Alcance de la solución

Es importante conocer el alcance de que tendrá el proyecto y limitar de manera adecuada para que sea realizable y sus objetivos sean demostrables, en este caso, como se muestra en la Figura 5.4, para el prototipo se activó todo el alcance, no es necesario siempre hacer esto, dependerá de la necesidad de cada empresa.

Categoría	Detalle	SI/NO
Seguridad como servicio	SSL Decryption	Si
	CASB	Si
	Cloud SWG	Si
	ZTNA	Si
	FWaaS	Si
	DNS	Si
	DLP	Si
	Sandboxing	Si
Red como servicio	SD-WAN	Si
	QoS	Si
	Policy Based Forwarding	Si
	Network as a Service	Si
	IPSec VPN	Si
	SSL VPN	Si

Figura 5.4 Alcance de Protección de Altel

5.2 ANEXO B

Prototipo de Perímetro Definido por Software desplegado en la empresa auspiciante de este trabajo de titulación:

- **Fabricante**: Palo Alto Networks
- **Solución**: Prima
- **Licenciamiento**: Prisma Access, Prisma Cloud, Prisma SaaS.

El prototipo mediante el cual se probó el Perímetro Definido por Software, constaba de una plataforma en la nube que centralizaba el acceso a todas las consolas de las plataformas de seguridad necesarias para la prueba y constaba de:

- **Overview**: es un resumen de lo que tiene acceso en el prototipo.
- **VM List**: Es el listado de equipos virtuales o de nube a los que se puede acceder desde esta consola.
- **Panorama**-UI: Es la consola que permite el manejo de todos los firewalls de la organización, incluyendo la conexión a la nube.
- **NGFW-Branch-UI:** Es la consola del firewall de la sucursal con la que se realizaron las pruebas de los conceptos de SDP para efectos de este trabajo de titulación.

- **Win-mobile:** Es el equipo que requiere acceso desde cualquier sitio y se necesita que la protección del perímetro se extienda hasta este dispositivo, para efecto del prototipo, se accede al dispositivo mediante escritorio remoto RDP, propio de los sistemas operativos Windows de la empresa Microsoft.
- **Win-Subnet1:** Es un servidor ubicado en un segmento de red 1, este equipo es un destino de la conexión mediante realizada desde Win-mobile con el agente de SDP instalado.
- **Win-Subnet2:** Es un servidor ubicado en un segmento de red 2, este equipo es un destino de la conexión mediante realizada desde Win-mobile con el agente de SDP instalado.

A continuación, se muestra la consola del prototipo empleado:

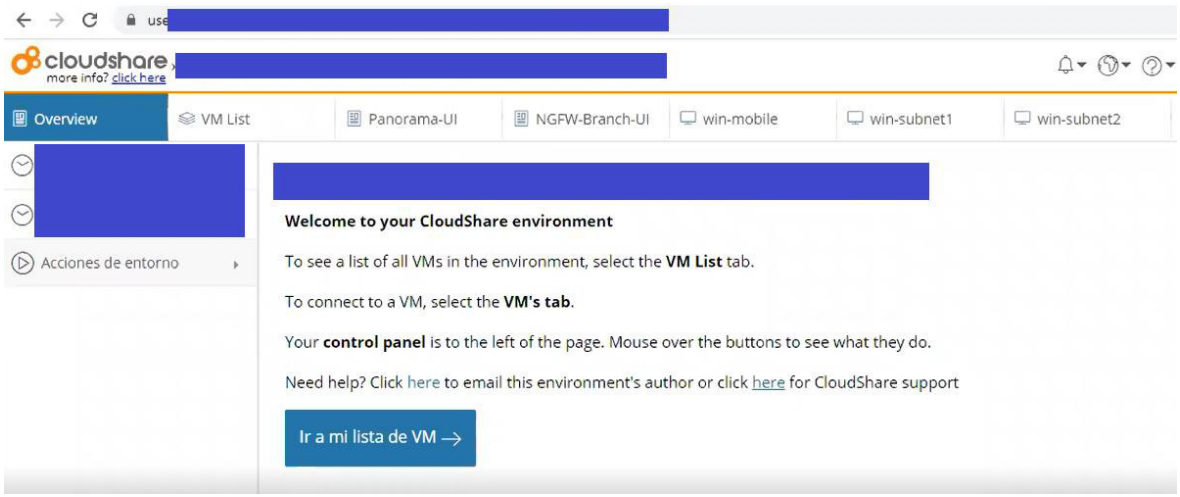

Figura 5.5 Dashboard del prototipo de SDP.

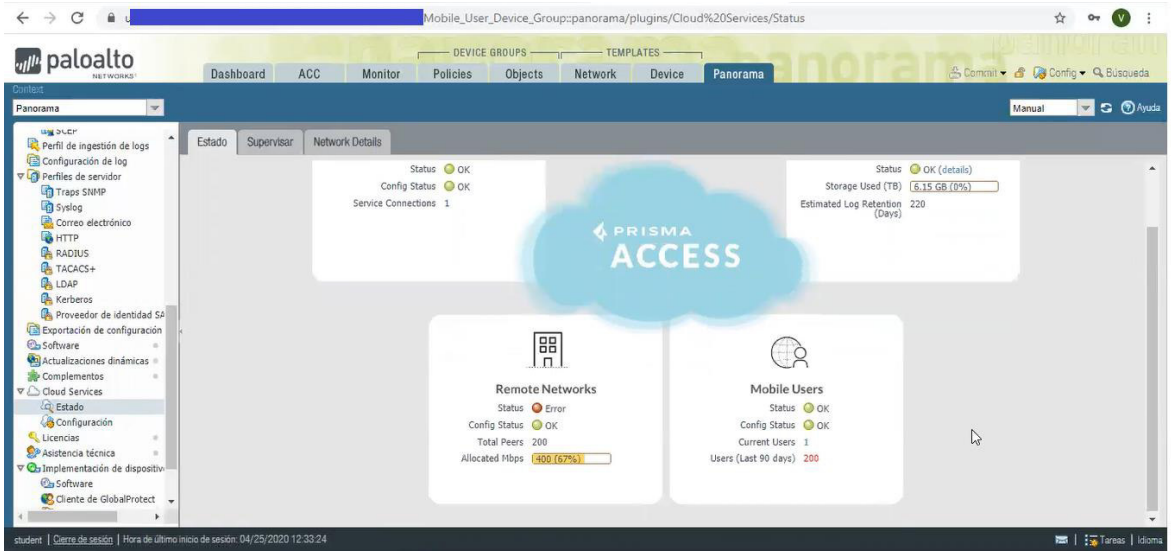

Figura 5.6 Consola del Panorama

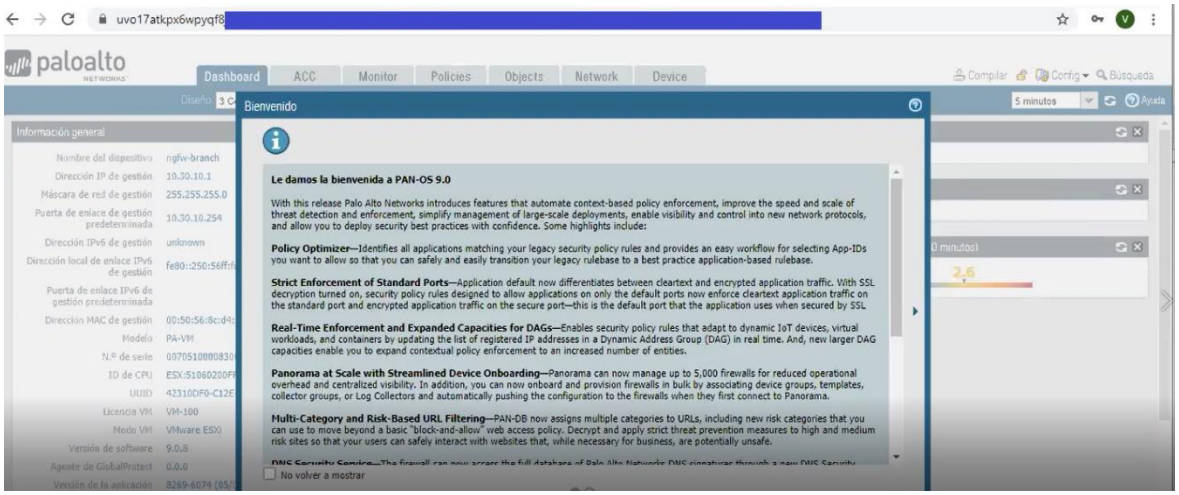

Figura 5.7 Consola del **NGFW-Branch-UI**

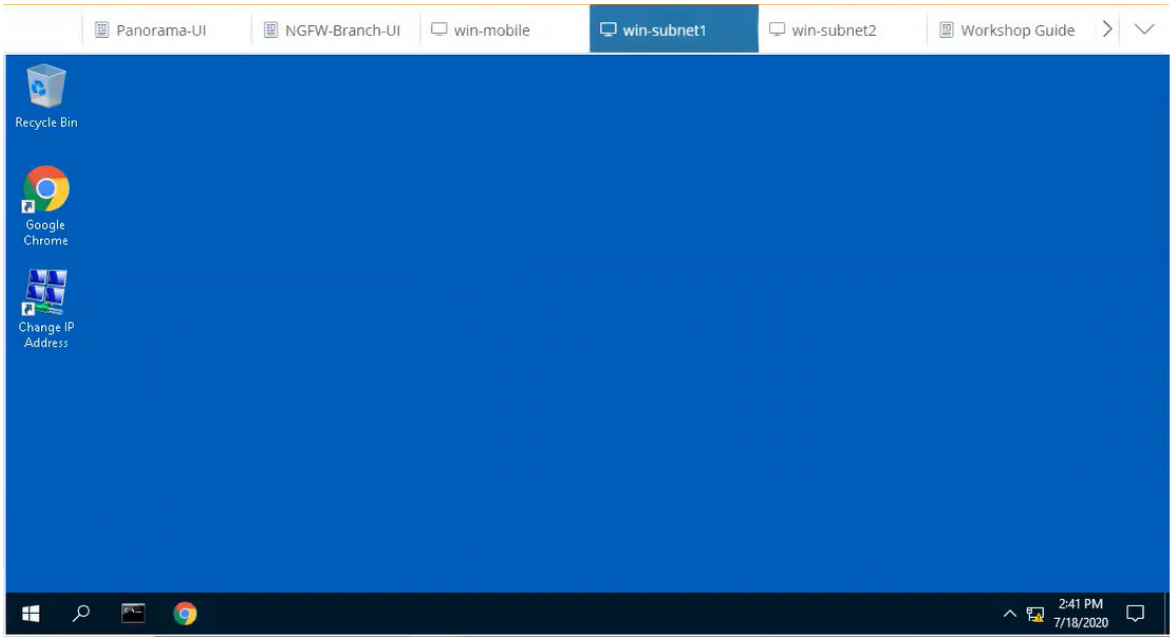

Figura 5.8 Consola del **win-subnet1**

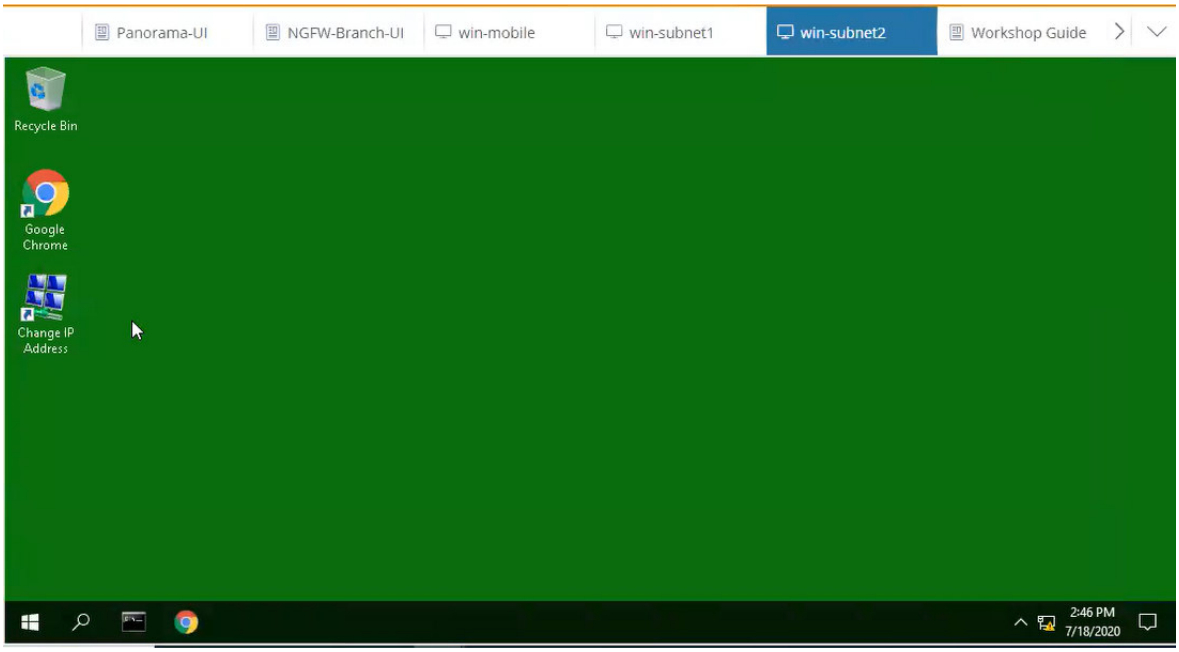

Figura 5.9 Consola del **win-subnet2**

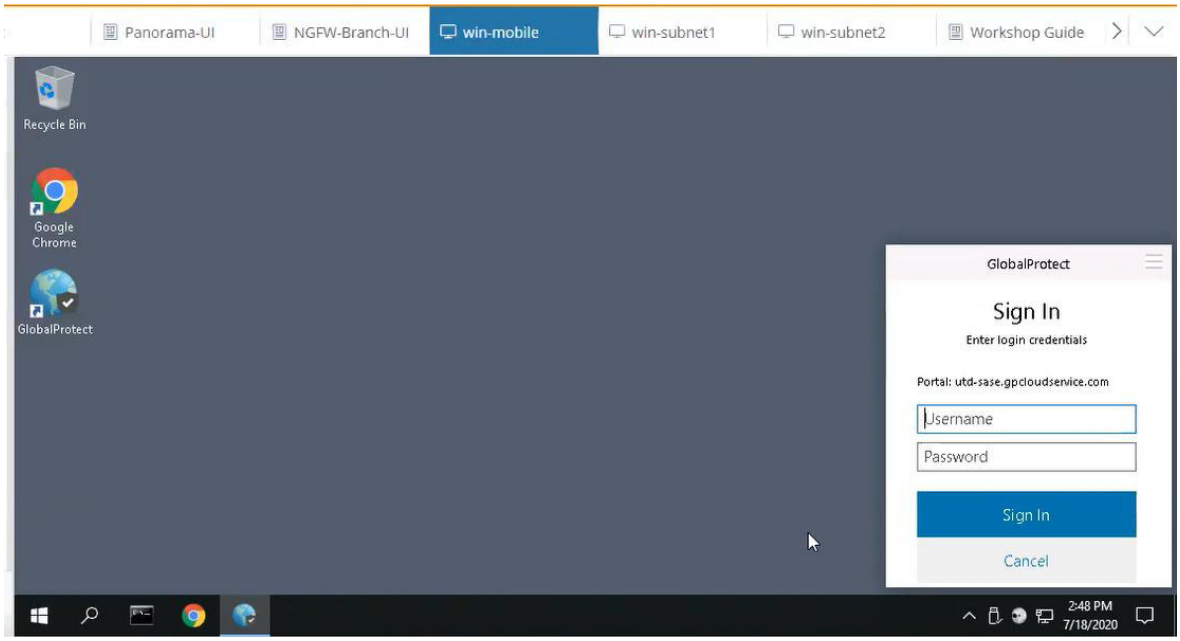

Figura 5.10 Consola del **win-mobile con agente de SDP – Global Protect**

Para la conexión a la nube de AWS y de Google, se usó consolas independientes:

Google – Servicios SaaS:

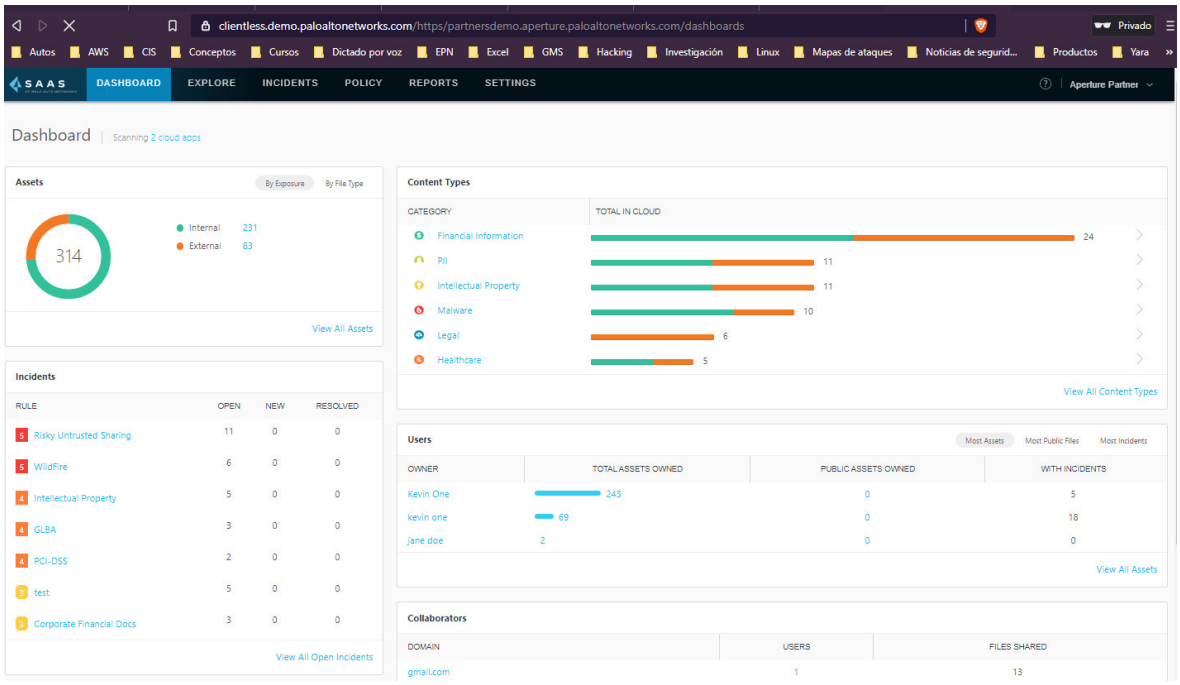

Figura 5.11 Consola de para la gestión de Google y Box

Amazon AWS – Servicios IaaS:

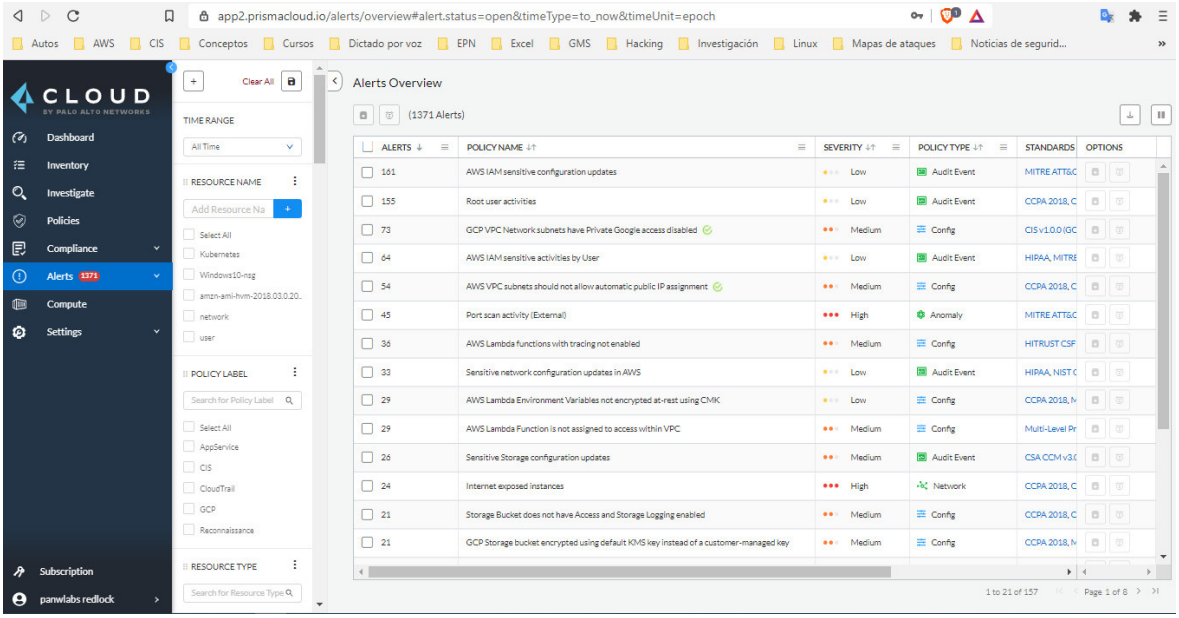

Figura 5.12 Consola de para la gestión de AWS.

ORDEN DE EMPASTADO