FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE UNA RED VPN PARA EL TRABAJO REMOTO EN LA EMPRESA CLI GESTIONES ADUANERAS S.A. LIMA 2020”

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniera de Sistemas Computacionales

Autora:
Midori Medalith Idrogo Mendoza

Asesor:
Mg. Leonardo José Torres Argomedo

Lima - Perú

2021

DEDICATORIA

A Dios por forjar mi camino, a mis padres Ricardo y Mirodi que siempre me apoyaron a seguir adelante y a mi hermana Mayteé, quien es mi motor para lograr mis metas.

AGRADECIMIENTO

A la empresa CLI Gestiones Aduaneras por la confianza y el brindarme la facilidad para hacer uso de la información requerida en este informe durante el periodo laborado.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El siguiente informe consiste en la experiencia laboral desempeñada en la empresa CLI Gestiones Aduaneras S.A., donde se explicará la implementación de una red VPN para la conexión remota de los usuarios debido al virus del COVID 19 que llegó al Perú.

Para que la continuidad del negocio no se vea afectado, los colaboradores se conectarían remotamente a través de equipos virtuales los cuales se encontraban nateados para su conexión. Sin embargo, se presentaron inconvenientes de lentitud en la conexión, problemas para acceder a los sistemas y recursos específicos, además de la inseguridad en los puertos lógicos abiertos en los servidores, por tal motivo se opta por implementar una red VPN que permita a los usuarios conectarse a la red interna de manera más rápida y acceder a los sistemas y recursos conectándose a los equipos de la organización.

Para la implementación de la VPN, se configuró una VPN Open Source con OpenVPN, ya que era un servicio del firewall de la empresa, Endian Firewall Comunity, tras la configuración y las pruebas realizadas se logra mejorar la calidad en el acceso y seguridad de los sistemas y servicios de red en el trabajo remoto con la VPN.

CAPÍTULO I. INTRODUCCIÓN

1.1. Contextualización de la Experiencia

El presente informe expone la experiencia adquirida en la empresa CLI Gestiones Aduaneras S.A. a la cual ingresé en el año 2019 tras un proceso de selección en el cual se solicitaba el puesto de Asistente de Soporte en el área de Sistemas.

Durante el primer año laborando en la organización mis funciones fueron dar soporte a los usuarios en los problemas técnicos de hardware y software, siendo algunas de las tareas la revisión de los backups, inventariar los activos de la empresa, administra la red de la agencia, establecer políticas en el proxy, así como la instalación y configuración de los equipos de los usuarios, crear los accesos y validar los permisos de los usuarios a los sistemas y gestionar los incidentes con el sistema de aduanas SINTAD.

Para el primer trimestre del año 2020, se inició el periodo de cuarentena a causa del virus COVID 19, “Decreto Supremo N° 044-2020-PCM, que declara el Estado de Emergencia Nacional, por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID 19” (Diario El Peruano, 2020). el que fue decretado por el presidente Martin Vizcarra, por tal motivo fue necesario adaptarse a la modalidad del trabajo remoto.

Para brindar el acceso remoto a los colaboradores se crean 5 máquinas virtuales, las cuales fueron asignadas a los colaboradores por áreas, y para lograr la conexión remota se le coloca a cada máquina una IP con puertos abiertos que permitiría acceder al sistema de aduanas SINTAD, así como a las unidades de red de la empresa.

Los requisitos solicitados a los usuarios fueron que debían contar con un equipo (Pc o Laptop) con sistema Operativo Windows 7 o Windows 10 y que además estos cuenten con

un antivirus actualizado y operativo, esto con el fin de minimizar el riesgo de infección en la red de la empresa. Lamentablemente no se obtuvieron los resultados esperados con respecto al trabajo remoto, ya que durante la cuarentena se reportaron diferentes incidentes como errores con la multisesión, lentitud en la conexión, lentitud al acceder al sistema de SINTAD, inconvenientes con la accesibilidad a información específica, lentitud en el servicio de Webmail, entre otros.

Culminados los 90 días de la cuarentena, la empresa decide realizar trabajo semipresencial, es decir se dividió al personal en dos grupos, los cuales se turnaban, una semana presencial y una semana de forma remota. Cuando el personal trabajaba de forma remota reportaba los mismos inconvenientes a pesar de ser menos colaboradores conectados, por ello se decide implementar una red VPN para mejorar la conexión remota para cuando los colaboradores se encuentren laborando remotamente.

Tras el decreto de urgencia por el COVID 19 muchas empresas tuvieron que cerrar sus instalaciones ya que muchas de estas no cumplían con los protocolos que había impuesto el estado, ComexPerú (2020), indica que se cuenta con 3.1 millones de mypes, lo cual a diferencia del año 2019 se observa un decrecimiento del 48%, lo que indica un impacto significativo en el rubro empresarial.

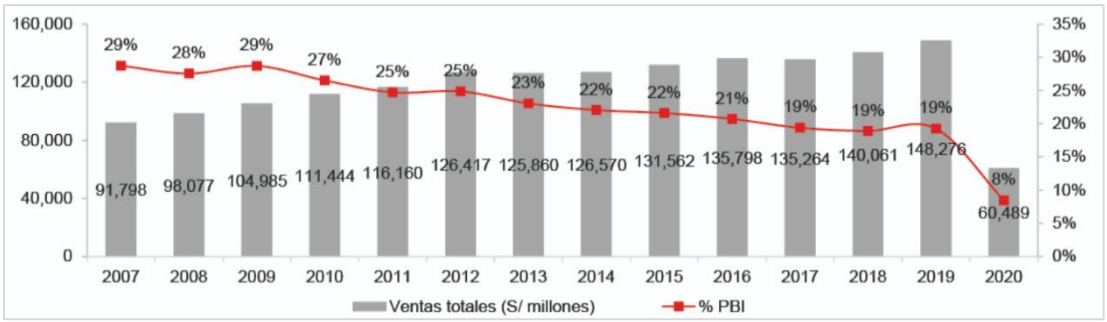


Figura 1. Ventas de las Mypes en Perú (S/ millones)
Fuente: Enaho. Elaboración: ComexPerú

Para la implementación se ejecuta el servicio Open VPN el cual se encontraba como un servicio dentro del firewall Endian Comunity que tiene la empresa, se activa el servicio y se realizan pruebas de tal forma que no se presenten errores al conectarse, así como verificar que no se presente lentitud en las conexiones con muchos usuarios, finalmente se decide que los usuarios se conecten a sus equipos de oficina y de esa forma puedan acceder a los recursos que desean como si estuvieran en la modalidad presencial. Una vez culminado el periodo de pruebas, se procede a organizar al personal para realizar la configuración de la VPN en sus equipos (personales, prestados por la empresa y equipos de oficina enviados a sus hogares); previamente se crean las credenciales de los usuarios en el firewall, las cuales por política de la empresa no deben ser brindadas a los colaboradores y solo deben ser gestionadas por el personal de soporte.

Finalmente se brindan las capacitaciones al personal para que tengan claro la nueva modalidad de conexión y durante tres meses se realiza el seguimiento para determinar el buen funcionamiento de la VPN.

Durante las semanas en que el personal realizaba el trabajo remoto, se empezó a observar que las incidencias reportadas empiezan a disminuir, logrando que el personal tenga un trabajo remoto de mejor calidad.

1.2. Descripción de la empresa

CLI Gestiones Aduaneras S.A. pertenece a la Corporación de Logística Integral (CLI), fue creada el 05 de diciembre del 2008, inicia sus operaciones en enero del 2010 con el RUC es el Nº 20478175524 y su dirección fiscal en AV. Elmer Faucett Nro. 2000 Int. D Urb.

Industrial Grimanesa (Frente Al Edificio De Lima Cargo City) Prov. Const. Del Callao.

Actualmente realiza la atención a sus principales clientes de manera satisfactoria, lo cual lo lleva a acumular una experiencia de más de 10 años en la prestación de sus servicios como el agenciamiento aduanero, así como brindando sus propios servicios en todo lo concerniente a la cadena logística, carga internacional, gestión en los trámites de aduanas y el transporte brindado de la carga local.

1.1.Misión.

La misión que tiene la organización es: "Fidelizar a nuestros socios comerciales y contribuir a que logren el éxito a partir de la prestación de un servicio óptimo, con alta tecnología, innovación y profesionalismo" (CLI Gestiones Aduaneras S.A.)

1.2.Visión.

La visión de la empresa es: "Ser la corporación más reconocida y competitiva en prestar servicios de gestión aduanera y logística integral, diferenciándonos por la calidad de nuestro servicio, alto profesionalismo de nuestros colaboradores e innovación tecnológica" (CLI Gestiones Aduaneras S.A.).

1.3.Principales Servicios.

Gracias al gran crecimiento de la empresa, se efectúa un planeamiento orientado a la modernización gracias a la tecnología, personal altamente calificado y capacitado, permitiendo brindar un buen servicio a los clientes y operadores, quienes se encuentran satisfechos, además se han obtenido certificaciones en CALIDAD, BASC, OEA, Sistema de Gestión Anti Soborno y homologación de SGS obteniendo la categoría A+ (00805/18).

a. Transporte.

CLI Proyectos obtuvo la certificación ISO9001 la cual garantiza la trazabilidad que tienen todas sus operaciones ya que cuenta con una flota de transporte pesado y liviano los cuales son cubiertas a nivel nacional, así como el traslado de mercadería general y mercadería IMO.

b. Logística Integral.

Atiende un servicio de puerta a puerta y sobre todo a medida de todo lo que requiere y necesita el cliente.

c. Agenciamiento de Carga Internacional.

Este servicio brindado cuenta con un certificado importante que es el de IATA ya que pertenece al Global Logistic Family permite que se pueda llegar a diferentes países.

d. Agenciamiento de Aduana.

Gracias a la confianza que ha depositado cada cliente en CLI y el posicionamiento entre las mejores 10 agencias aduaneras, ratifica el buen servicio ofrecido, actualmente se tiene oficinas en Paita, Mollendo, Tacna y Pisco.

VÍA DE DESPACHO	TIEMPO (DIAS)
AEREO	3 DÍAS
MARÍTIMO	5 DÍAS
Total General	4 DÍAS

Figura 2. Promedio en la atención de despachos.

Fuente*:* Página Oficial de CLI Gestiones Aduaneras

1.4.Organigrama.

CLI mantiene un organigrama vertical, donde está liderado por el Gerente General, quien junto al área comercial se encargan de captar nuevos clientes, a su lado se encuentra la gerencia logística quien está a cargo de él buen funcionamiento de la parte operativa de la empresa. A partir de ello se cuenta con diferentes áreas que componen toda la empresa. Las áreas críticas son Servicio al cliente, Liquidación, Revisión. La agencia cuenta con 115 colaboradores.

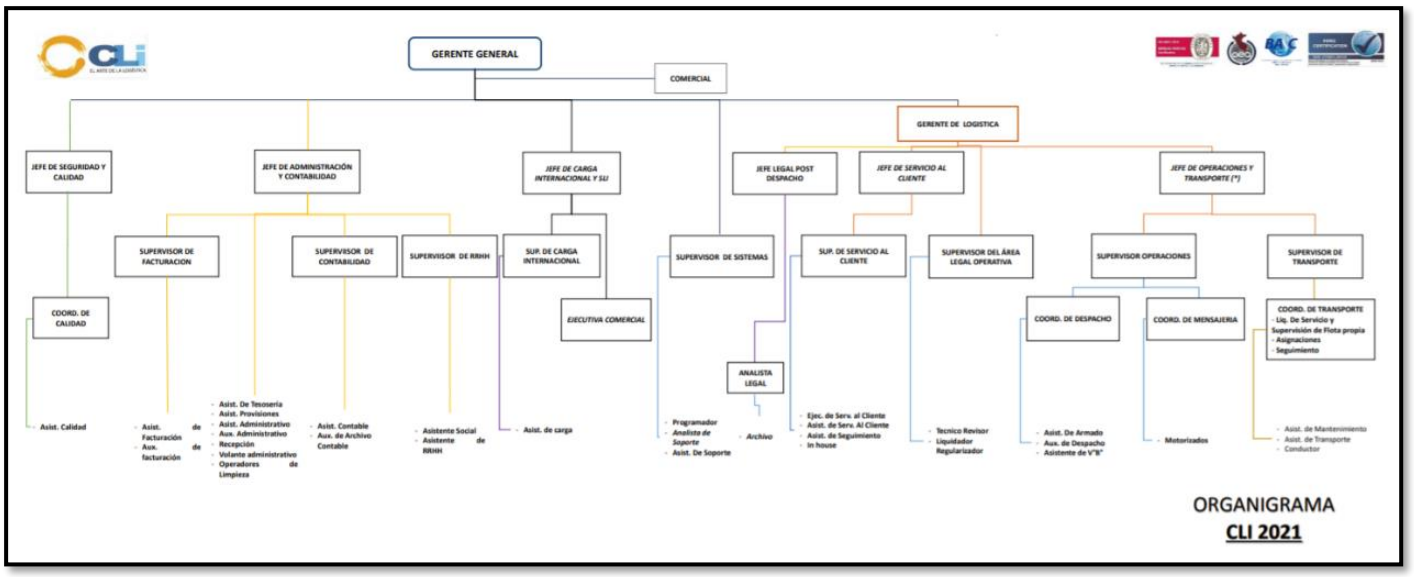


Figura 3. Organigrama de CLI Gestiones Aduaneras.
Fuente: CLI Gestiones Aduaneras, área de Seguridad y Calidad

1.5.Mapa de Procesos.

A continuación, el funcionamiento y la distribución de los procesos y actividades de la organización.

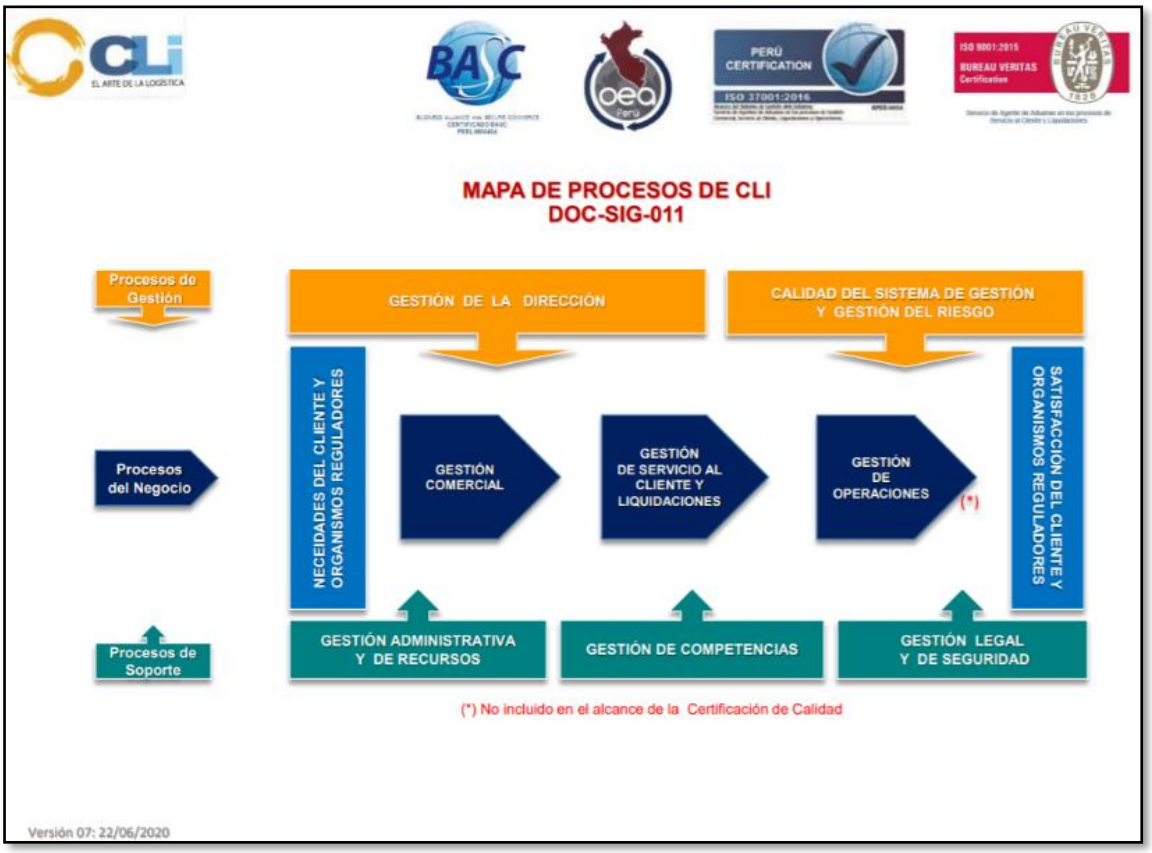


Figura 4. Mapa de procesos de CLI Gestiones Aduaneras.

Fuente: CLI Gestiones Aduaneras, área de Seguridad y Calidad

1.6.Principales Clientes y Operadores.

a. Clientes.

Nuestra mejor carta de presentación y garantía es la confianza que depositan todos nuestros clientes. Para acceder a nuestra plataforma en línea y aprovechar las bondades de este servicio, CLI les otorgara a sus clientes un usuario y contraseña a partir de su primera operación con nosotros.

Entre nuestra variada cartera de clientes podemos mencionar:

Figura 5. Principales Clientes.

Fuente: Página Oficial de CLI Gestiones Aduaneras

b. Operadores.

A quienes CLI le brinda el servicio de agenciamiento de aduana para sus principales clientes, dicha alianza demuestra la confianza de los operadores con CLI en el crecimiento de su negocio. Entre nuestros operadores tenemos:

Figura 6. Principales Operadores.

Fuente: Página Oficial de CLI Gestiones Aduaneras

CAPÍTULO II. MARCO TEÓRICO

2.1.Antecedentes

2.1.1. Nacionales

- Martel, M. (2019), en su tesis titulada "Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764" en la universidad de Ciencias Aplicadas realizó un diseño de comunicación mediante VPN entre sus locales, con el objetivo de poder optimizar sus recursos y además de poder agilizar las transacciones diarias que realizaban las empresas. La solución brindada era lograr la interconexión de la sede principal y sus diferentes sucursales, por ello la solución buscada debe englobar los siguientes criterios como: escalabilidad, seguridad de datos, disponibilidad de información, y sobre todo economía. Por ello el diseño de redes privadas virtuales solucionan de una forma más flexible y económicas para las empresas que necesitan lograr una comunicación de manera segura con sus clientes, proveedores y/o sucursales, desestimando la implementación de redes dedicadas las cuales son muy costosas las cuales son implementadas para el mismo fin. Este tipo de conexiones por VPN además de lograr reducir costos y establecer una conexión segura ofrece escalabilidad ya que se puede adaptar para una mayor cantidad de puntos de venta que requiera la organización y con mínimas inversiones en el ISP América Móvil Perú SAC.
- De la Cruz, S. y Vera, J. (2019), en su tesis titulada "Implementación de una VPN con Open Source para la gestión de aplicaciones de Intranet en la Universidad Nacional Pedro Ruiz Gallo", realizaron una investigación donde el objetivo era determinar que el uso de una Red

VPN Open Source, Softether VPN, mejorará la gestión de aplicaciones de una intranet en la Universidad Nacional Pedro Ruiz Gallo, una vez evaluados los requisitos de hardware que requerirían para tal implementación, se elaboró la topología física y lógica teniendo en cuenta la seguridad y el acceso rápido que se requiere lograr. se pudo demostrar que la implementación de una red VPN logró a través de una simulación, optimizar la gestión de las aplicaciones de la intranet de la universidad demostrando además la seguridad, confidencialidad y disponibilidad de las aplicaciones garantizadas.

- Espinoza, C. (2018), en su tesis titulada "Propuesta de una Red Privada Virtual para mejorar el Servicio de Comunicación en las Tiendas Mass para la empresa Supermercados Peruanos S.A.", de la universidad Autónoma del Perú, realizó una investigación cuyo objetivo fue proponer una solución mediante una Red Privada Virtual que le permita mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A. esto se realiza bajo la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar) de Cisco Systems, esta metodología proporciona los procesos, habilidades y técnicas que se necesitarían dicha implementación de la Red Privada Virtual. Esta mejora se constatará en el enlace entre dos o más sucursales que se encontraban geográficamente a kilómetros de distancia. Se pudo obtener resultados positivos ya que en primer lugar se pudo reducir los tiempos de latencia con enlaces 3G pasando de un intervalo de <900ms-1500ms> a <10ms-20ms>, además se reducen los saltos de paquetes de datos para llegar a sus destinos de red de <4host-11host> a 5host, de ese modo también se logra reducir los tiempos de ingreso a los sistemas ya que anteriormente un usuario demoraba de <4min-7min> a tan solo tardar 7 segundos.

2.1.2. Internacionales

- Quezada, H. (2016), en su tesis titulada "Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja", realizó un diseño de una VPN para lograr el acceso a las bases de daros científicas de la Universidad Nacional de Loja, cuya finalidad era poder obtener un servicio que permita que los miembros de la universidad accedan de manera remota a los recursos que brinda la red interna del campus de la universidad desde una red fuera de la institución y la mejor manera de hacerlo sería mediante una conexión VPN debido a sus altos niveles de seguridad, integridad y autenticidad que este tipo de redes virtuales ofrece. La herramienta a usar fue Open VPN la cual se basaba en una tecnología SSL-TLS la cual permitía que los usuarios puedan acceder remotamente de una forma segura, además la configuración del Open VPN permitía una comunicación directa con los servicios de la red interna. Así mismo con la implementación de la red VPN se consiguió un servicio de acceso a biblioteca virtual que permitía el acceso a los servicios internos como la base de datos científicos, libros electrónicos, revistas digitales, desde una red externa a la institución.
- Cansino, D. (2012), en su tesis titulada "Diseño e Implementación de una Red Privada Virtual segura para las oficinas de Caminosca S.A basado en plataforma Gnu/Linux" de la Universidad Politécnica Salesiana de Quito, realizó un diseño e implementación de una red privada virtual segura para las oficinas de CAMINOSCA S.A. basado en plataforma GNU/Linux, esto con el fin de poder intercambiar información por medio de la VPN entre los usuarios de la oficina principal hacia las sucursales ofreciendo seguridad, confidencialidad y rapidez de esa manera los usuarios podrán desarrollar sus diferentes

actividades en casa área respectiva comunicándose e intercambiando información. Los usuarios que se encontraban en las sucursales accedían a la información que se encontraba en la oficina principal de una manera más rápida sin temor a que esta información pueda ser filtrada.

- Quishpe, L. (2021), en su tesis titulada "Estudio para la Implementación de una Red Privada Virtual (VPN) Utilizando Herramientas de software libre, caso de estudio Comisión Fulbright del Ecuador", cuyo objetivo principal es implementar una red VPN que permita la institución y sus colaboradores puedan disponer de las herramientas y servicios mediante el trabajo remoto con tecnología actual y que sea segura para la institución. Para ello requirieron de los siguiente: servicio de internet PYME de 75 Mbps con IP Publica para la conexión VPN, computador Clon para ser usada como servidor VPN, se optó por el software OpenVPN y servidor proxy a Squid. Luego de evaluar la red privada, verificar la conectividad y realizar las pruebas correspondientes a los paquetes, accesos se verifica que la implementación fue satisfactoria ya que permite una conexión encriptada con un óptimo funcionamiento y seguridad necesaria.

2.2.Marco Conceptual

2.2.1. Hipervisor

De acuerdo a la informática, Menciona Niño (2020) que el termino virtualización hace referencia a la abstracción de los recursos que tiene una computadora a la cual se le denominará **Hipervisor o VMM** (Virtual Machine Monitor). Este Hipervisor hace referencia a una capa abstracta entre el hardware del equipo físico y el hardware de la máquina virtual, donde se pueden crear diferentes dispositivos o recursos como por ejemplo un servidor, un dispositivo

de almacenamiento, una red, incluso un sistema operativo, donde se dividen los recursos de uno o más entornos de ejecución.

Por otro lado, la página oficial de VMWare (s.f), indica que un Hipervisor es un monitor de máquinas, este permite crear y ejecutar diferentes máquinas virtuales, en simples palabras, permite que un equipo host preste soporte a diferentes equipos virtuales llamados también invitados compartiendo de ese modo recursos entre ellos como por ejemplo la memoria o el procesador. Así mismo indica que los hipervisores permiten que se pueda aprovechar de una mejor manera los recursos de un sistema, así como proporcionar mayor movilidad TI ya que se puede trasladar de un servidor a otro fácilmente ya que se encuentran en un mismo host.

2.2.2. Tipos de Hipervisor

2.2.2.1. Tipo 1 Nativo:

Este tipo de imprevisores, también conocidos como bare-metal o unhosted, se ejecutan sobre hardware real, es decir sobre un equipo físico, para poder controlar el hardware y monitorizar los sistemas operativos virtuales. Los equipos virtuales que se ejecuten de manera simultánea lo realizan a otro nivel entre ellos se tiene VMWare Esxi, VMWareEsx, Xen, Citrix, XenServer y Microsoft Hyper-V Server (Gutiérrez, 2014).

2.2.2.2. Tipo 2 Hosted:

En este tipo de Hipervisores o monitores son ejecutados sobre un sistema operativo convencional, en el cual se virtualizan diversos sistemas operativos, esta virtualización se encuentra situada en una capa más alejada del hardware y el rendimiento es mucho menor, ejemplo de ellos son VirtualBox, VMWare Workstation, WEMU (Gutiérrez, 2014).

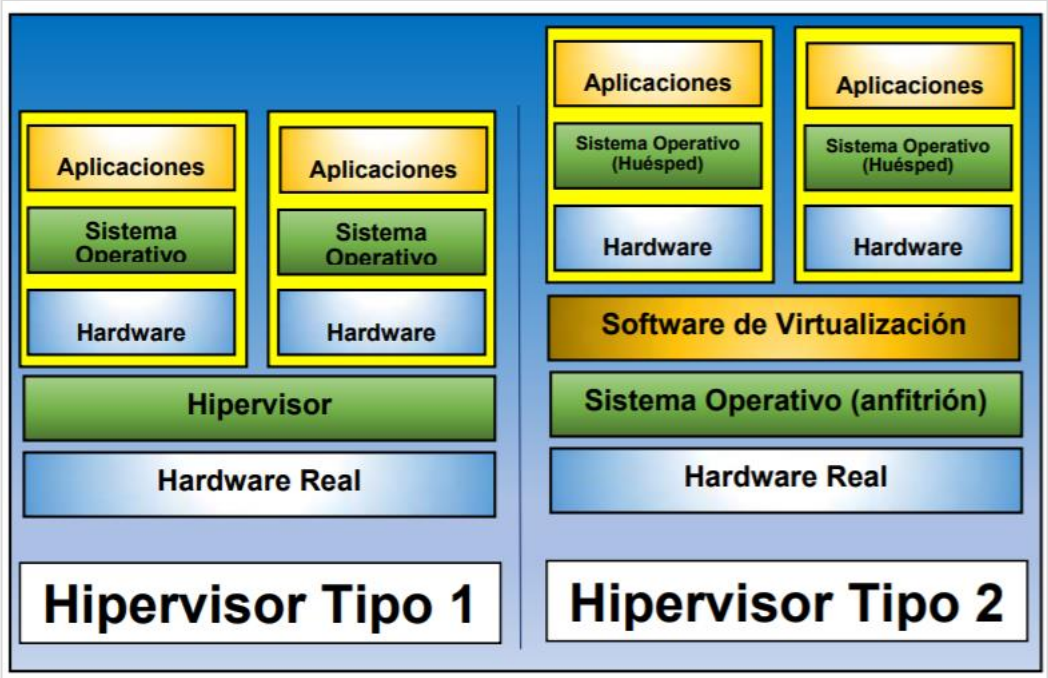


Figura 7: Tipos de Hipervisor

Fuente: Gutiérrez A. (2014). Virtualización de Servidores de la Infraestructura Informática de la Universidad de Quintana Roo, Unidad Chetumal

2.2.3. VMWare ESXi:

De acuerdo a página oficial de VMWare (s.f.), indica que VMWare Esxi es un hipervisor bare metal, se instala de manera directa en un servidor físico, permitiendo que se pueda acceder de manera directa a los recursos y a su vez que estos sean controlados. Así mismo VMWare Exi permite que se puedan realizar particiones del Hardware, de tal forma que se pueda consolidar de manera eficaz y se pueda reducir costes.

Las principales características de este son:

- Consolida el hardware para poder mejorar la capacidad a utilizar.
- Aumenta el rendimiento.
- LA Administración TI se encuentra centralizada.
- Reduce los recursos del hardware que solo va a ejecutar el hipervisor.

2.2.4. Firewall

De acuerdo a Tanenbaum, A. y Wetherall, D. (2012), los Firewalls conocidos como (servidores de seguridad) hacen referencia a la estrategia medieval de seguridad, es decir, escavan un foso defensivo profundo alrededor del castillo, esto hacia que todo aquel que entre o salga tenía que pasar por un único puente levadizo. Por tal razón en las redes sucede lo mismo, una organización puede tener diferentes redes LAN que se conectan de forma arbitraria, pero todo el tráfico que entra y sale debe pasar por un puente levadizo electrónico llamado FIREWALL.

Es así como el Firewall actúa como un filtro de paquetes ya que inspecciona cada uno de los paquetes que ingresan y salen. Todos los paquetes que cumplan con un filtro establecido en las reglas por un administrador se reenviarán de forma normal, mientras que los que no cumplan se descartarán. Dichos filtros que están bajo un criterio son propuestos como reglas o tablas que listarán todos los orígenes y destinos que serán permitidos, bloqueados, alguna permitirá monitorear los paquetes que entran y sales de las máquinas (Tanenbaum, A. y Wetherall, D, 2012).

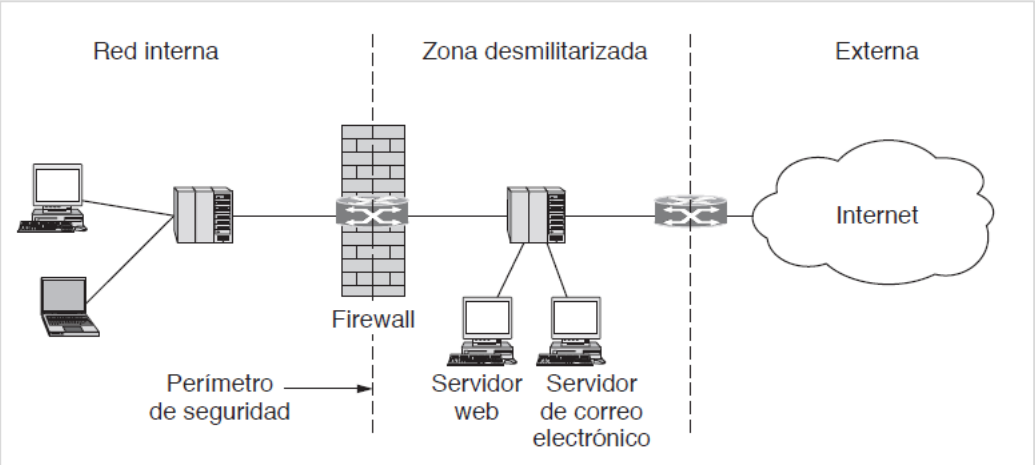


Figura 8. Firewall en una red interna

Fuente: Informática Forense y software libre, Poniendo en marcha un estacón de trabajo con SLAckware13.0.

A pesar que se pueda tener un firewall muy bien configurado, existen brechas que pueden causar problemas de seguridad, por ejemplo, Un Firewall está configurado para permitir solo paquetes de entrada de redes específicas, un intruso de fuera puede ingresar a la red por medio de IPS falsas para evadir dicha regla. Si un colaborador quiere filtrar un documento sensible, puede encriptarlo o fotografiarlos y enviárselos como JPEG. Los Firewalls suelen proporcionar un solo perímetro como defensa, frecuentemente es usado para una defensa por capas, si esta defensa es violada, todas las demás se cerrarán, por ello es recomendable que los equipos finales (equipos de escritorio) puedan tener sus propios firewalls activos, es una manera de poder minimizar los riesgos que se puedan presentar (Tanenbaum, A. y Wetherall, D, 2012).

2.2.5. Endian Firewall Comunity

Endian Comunidad (s.f.). indica que Endian Firewall Community (EFW) está basado en Linux y que puede transformar un dispositivo con características específicas en una solución de Gestión Unificada de Amenazas (UTM). Este sistema está diseñado para poder simplificar la seguridad y poder proteger las redes utilizado código abierto e incluye características de seguridad como firewall de paquetes con estado, seguridad para la web y para el correo electrónico, antivirus, también de código abierto y además ofrece VPN para SSL y IPsec.

Según la Guía de Instalación de Endian escrita por Guijarro, Tapia, Viteri y Zambrano (2018), las características mínimas de un equipo son las siguientes:

- CPU: se puede usar un Intel x86 compatible (500MHz mínimo, 1GHz recomendado), Intel Core 2 Duo, Xeon, procesadores Pentium y Celeron.
- Procesador Múltiple: Soporte incluido para Multiprocesador simétrico (SMP)

- RAM: debe tener 256MB mínimo (512MB recomendados)
- Disco Duro: Discos SCSI, SATA, SAS o IDE requeridos (8GB mínimo)
- Software RAID: Para software RAID1 (mirroring) dos discos del mismo tipo (las capacidades no deben ser iguales).
- Tarjeta de Red: Ttarjetas de red Gigabit y NIC fibra.

De acuerdo a Carrasco, I. y Vera, A. (2010) definen al Firewall Endian como una distribución de Linux que trabaja como un cortafuego que proporciona una interfaz web intuitiva que permite su fácil administración y está basado en Linux From Scratch. Para su configuración requiere de pocos requerimientos de hardware y está orientado a usuarios domésticos o a empresas pequeñas.

Así mismo Carrasco, I. y Vera, A. (2010) indica que Endian puede ser implementado en diferentes topologías de red, que puede ser desde una LAN con salida a internet, hasta la creación de una zona desmilitarizada (DMZ), el cual soporta además una red inalámbrica.

Las zonas son divididas en:

- Roja: zona de internet.
- Verde: LAN, red de área local (red interna).
- Naranja: DMZ, zona desmilitarizada.
- Azul: Wireless, zona inalámbrica.

Además, Endian abarca las siguientes características con funciones “Out the Box”

- Firewall con inspección de los estados.
- Antivirus (Http/FTP)
- Filtros para el contenido Web.

- VPN SSL/TLS
- IDS
- NTP, DHCP, entre otros.

2.2.7. VPN

Una red privada virtual, también conocida como VPN, se define según CISCO (s.f.), como una conexión que se encuentra cifrada para internet a través de un dispositivo a una red. Esto ayuda a que la transmisión de datos o información se realice de una manera más segura, evita además que personas que no se encuentran autorizadas puedan espiar este tráfico y el usuario pueda trabajar de manera remota. VPN es un entorno que se utiliza de manera frecuente en las empresas.

CISCO (s.f.) menciona que existen dos tipos de VPN:

Por acceso remoto: esto se refiere a que mediante un dispositivo se va realizar la conexión a la red de la empresa, estos dispositivos son conocidos como “Terminales”, estos pueden ser una computadora, una laptop, una Tablet o incluso un Smartphone, estos en definitiva deben cumplir ciertos requisitos para que se pueda efectuar esta conexión

Sitio a Sitio: este tipo de VPN lo que hace es conectar a la oficina de una empresa con las diferentes sucursales que se tenga, esto debido a que la distancia de las agencias no permite realizar una configuración de red directa, es tal caso se utilizan equipos dedicados para que se pueda establecer la conexión.

Por otro lado, Tanenbaum, A. y Wetherall, D. (2012), indica que las VPN son redes que se encuentran superpuestas sobre redes públicas, pero que estas adoptan muchas propiedades que tienes las redes privadas, estas son llamadas virtuales ya que solo son una

ilusión, al igual que aquellos circuitos virtuales que no son reales. Muchos de los Firewall tienen la capacidad integrada de VPN en sus configuraciones, incluso algunos enrutadores tradicionales cuentan con este servicio integrado. Debido a que los firewalls son la herramienta principal de seguridad en una organización es natural que los túneles empiecen y terminen en el firewall, lo cual establece una separación entre la red de la empresa y el internet (Tanenbaum, A. y Wetherall, D, 2012).

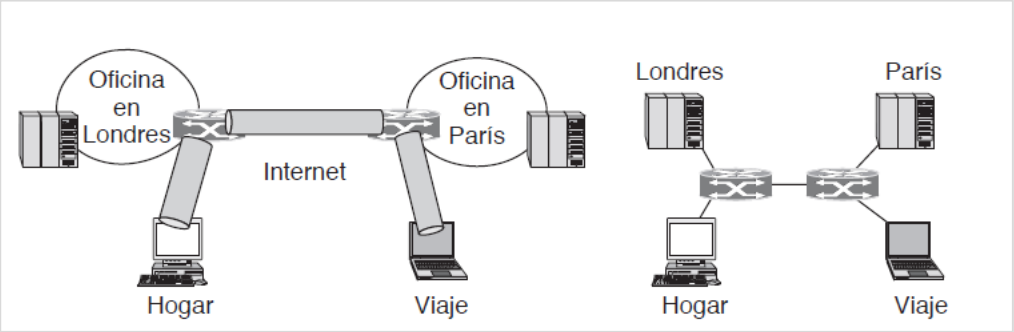


Figura 9. Red Privada Virtual

Fuente: Informática Forense y software libre, Poniendo en marcha un estacón de trabajo con SLAckware13.0.

2.2.8. Escenarios de VPN

De acuerdo al Centro Criptológico Nacional de España (2017), indica que existen tres escenarios, una de ellas es VPN entre las sedes que tiene una organización (VPN de sitio a sitio), la segunda es la VPN entre un cliente que se encuentra remoto y una de las sedes de la organización (VPN de acceso remoto) finalmente la VPN entre equipos (VPN de equipo a equipo).

- **VPN de sitio a sitio**, este tipo de escenario es empleado en las organizaciones para poder mantener la comunicación entre dos redes, las cuales pertenecen a

una organización, por ejemplo, la comunicación entre una sede y la oficina principal (Centro Criptográfico Nacional de España, 2017).

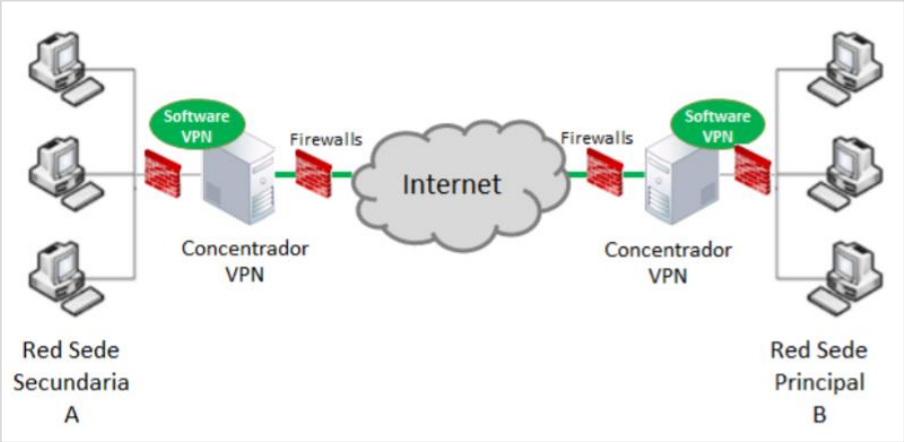


Figura 10. VPN de sitio a sitio

Fuente: Guía de Seguridad de las TIC CCN-STIC 836. 9-11

En estos escenarios no es necesario que en los equipos de los clientes deban ser instalado un software VPN, no requiere de una configuración particular para que se pueda establecer la conexión por VPN (Centro Criptográfico Nacional de España, 2017).

El concentrador para la VPN puede ser un dispositivo dedicado físico o también puede estar incorporado en un dispositivo de red como por ejemplo el router o firewall (Centro Criptográfico Nacional de España, 2017).

- **VPN de Acceso Remoto**: este tipo de escenarios se presenta cuando un usuario se comunica desde su hogar hacia la red de la organización, a través del internet (red pública). A diferencia del anterior, este si necesita un concentrador para que se pueda establecer la conexión VPN. Para que el usuario pueda acceder a un recurso de la organización, su equipo debió ser

configurado previamente para que pueda hacer conexión al cliente VPN (Centro Criptográfico Nacional de España, 2017).

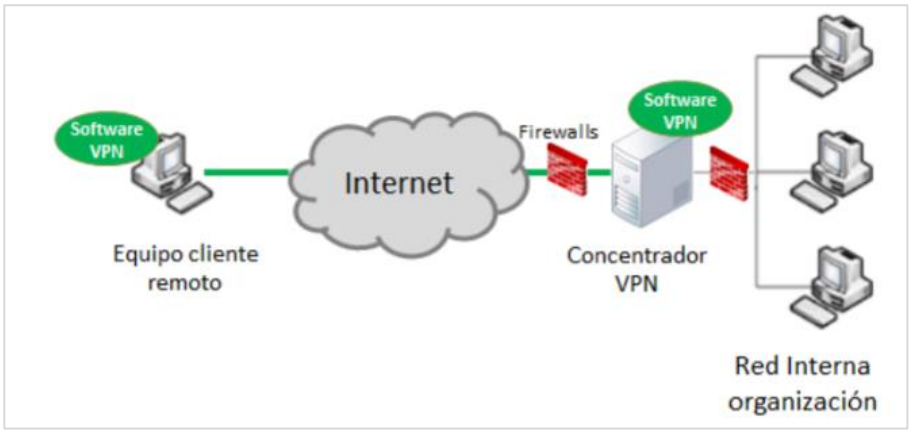


Figura 11. VPN de acceso remoto

Fuente: Guía de Seguridad de las TIC CCN-STIC 836. 9-11

En este escenario, todos los dispositivos clientes que se conecten, deben tener una configuración exclusiva con un software VPN y los usuarios deben ser autentificados previa conexión (Centro Criptográfico Nacional de España, 2017).

- **VPN de equipo a equipo:** En este último escenario, la comunicación será entre dos equipos, el cual será protegido de extremo a extremo, usualmente son utilizados para las conexiones a servidores que no se encuentran bajo un protocolo seguro o que pueden encontrarse en redes con riesgo como lo son los DMZ. La conexión VPN se realiza desde un cliente (origen) a un servidor (destino), en este caso el servidor debe tener configurado el software del cliente VPN y además debe estar configurado para aceptar las conexiones de

los clientes específicos con su respectiva autentificación (Centro Criptográfico Nacional de España, 2017).

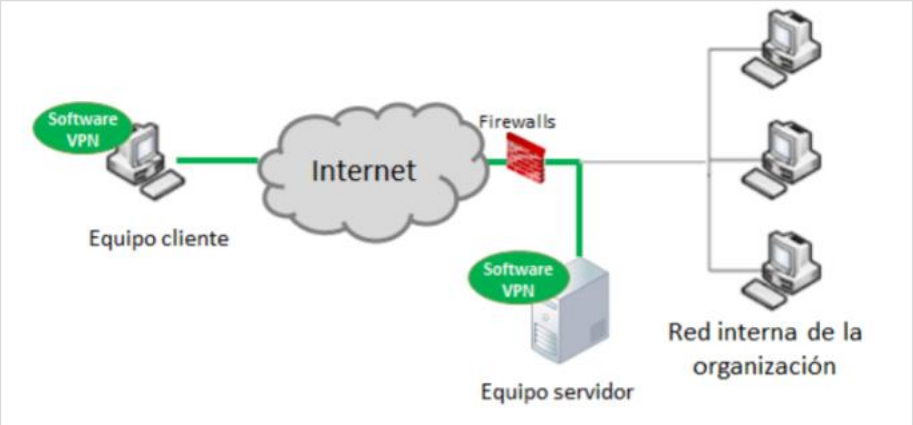


Figura 12. VPN de equipo a equipo

Fuente: Guía de Seguridad de las TIC CCN-STIC 836. 9-11

2.2.9. VPN según nivel de operación

De acuerdo al Centro Criptológico Nacional de España (2017), clasifica a la VPN de acuerdo a su nivel de operatividad con sus respectivas ventajas e inconvenientes tecnológicos de la siguiente manera:

Tabla1: Comparativa de VPN según Nivel de operación.

	Tecnología	Ventajas	Inconvenientes
APLICACIÓN	En cada aplicación SW	Ofrece una gran variedad en su configuración para asegurar la protección entre las aplicaciones que tienen comunicación.	La protección solo se da en el software específico. No aplica para aplicaciones comerciales. Si no se configura bien, podría quedarse desprotegido. No ofrece protección para la capa de red.

TRANSPORTE	SSL/TLS	Proporciona un buen algoritmo de cifrado utiliza además el protocolo TLS 1.2. Ofrece diferentes métodos para la autentificación Se puede configurar un proxy. Compatibilidad NAT. Reportes de auditoría. Permite la seguridad a endpoints. No se requiere un despliegue de software ya que usa una aplicación por Web.	No brinda protección a la capa de red. Solo aplica a aplicaciones web. Solo se autentifica el servidor en el cliente mas no viceversa. Se requiere de un instalador en el cliente o un plug-ins en el navegador web.
RED	IPsec	Protección para todo el tráfico IP independiente de la aplicación o protocolo que lo genera. Apto para protocolos y aplicaciones obsoletas o tradicionales de cliente/servidor. Soportado por casi todos los sistemas operativos. Proporciona mecanismos robustos de cifrado y autenticación. Puede usar una variedad de protocolos de autenticación.	Sólo protege comunicaciones IP. Requiere instalación de software cliente. Complejo de configurar, operar y mantener. Problemas de compatibilidad con NAT. No proporciona control de acceso granular a los recursos. No proporciona controles de seguridad a los endpoints (aunque depende del software cliente del producto IPsec).
ENLACE	PPTP	Se puede utilizar con redes no IP. + Establece un túnel entre equipo cliente y red de la organización.	Vulnerabilidades de seguridad conocidas. - Los mecanismos de autenticación no son robustos. - No es transparente al usuario, ya que debe instalar el software PPTP. - Necesario configurar filtrado de paquetes en dispositivos de red, para que admitan paquetes GRE. - Sólo soporta una sesión por túnel.

	L2TP	Se puede utilizar con redes no IP. Establece un túnel entre equipo cliente y red de la organización. Soporta múltiples sesiones por túnel. Mecanismos de autenticación adicionales (RADIUS). Se puede combinar con IPsec para un cifrado y autenticación más robustos.	No es transparente al usuario, ya que debe instalar el software L2TP.
	L2F	Se puede utilizar con redes no IP. Mecanismos de autenticación adicionales (RADIUS). No requiere instalación de software en el equipo cliente.	La comunicación entre el equipo cliente y el ISP no está protegida. Dependencia del ISP. No provee cifrado de datos adicional al de PPP, el cual ya ha sido reconocido como débil y vulnerable.

Fuente: Guía de Seguridad de las TIC CCN-STIC 836. 9-11

2.2.10. Open PVN

OpenVPN es una herramienta de código abierto creada por James Yonan, esta intenta ser una VPN universal la cual ofrece una gran flexibilidad. (OpenVPN, 2017).

En la página oficial de OpenVPN Yonan (2017), la describe de la siguiente manera:

> OpenVPN es un demonio VPN robusto y altamente flexible. OpenVPN admite seguridad SSL / TLS, puente ethernet, transporte de túnel TCP o UDP a través de un proxy o NAT, soporte para direcciones IP dinámicas y DHCP, escalabilidad a cientos o miles de usuarios y portabilidad a la mayoría de las principales plataformas de sistemas operativos.
>
> Admite el cifrado convencional utilizando una clave secreta previamente compartida (**modo de clave estática)** o seguridad de clave pública (**modo SSL /**

TLS) utilizando certificados de cliente y servidor. OpenVPN también admite túneles TCP / UDP no cifrados.

Diseñado para funcionar con la interfaz de red virtual TUN / TAP que existe en la mayoría de las plataformas.

2.2.11. Conexión Remota

CISCO (s.f.). indica que se debe proporcionar un acceso seguro y protegido, donde los usuarios se conecten y sus dispositivos accedan de una forma remota a la red de la corporación, la VPN permite que esta conexión sea segura debido a su solidez en la autentificación del usuario o del dispositivo.

De acuerdo a lo mencionado por Toala,2021, en su trabajo de investigación titulado Análisis de un Software Libre de Administración Remota para prácticas de los estudiantes en el Laboratorio de Telecomunicaciones de la Universidad Estatal del Sur de Manabí, indica que:

> Los programas de acceso remoto o conexión remota se consideran como un programa que permiten realizar accione en un equipo local las cuales son ejecutadas en otro equipo remoto, esto indica que se utiliza para que una persona pueda acceder y administrar un equipo sin necesidad d estar en la misma ubicación de manera física por medio de una interfaz gráfica de usuario (Fernández, 2020).

2.2.12. Trabajo Remoto:

Debido a la presencia del Covid19 El Peruano informa en la Resolución Ministerial Nº 072-2020-TR (2020) define al trabajo remoto como una prestación de servicios que ofrece un trabajador que puede encontrarse en su domicilio o desde un centro de aislamiento. Además,

indica que se realiza por diferentes medios o equipos de información (internet, telefónica u otros), los cuales permiten realizar las labores de oficina, pero desde otros lugares, esto siempre y cuando la naturaleza de sus funciones se lo permitan.

¿Qué factores que se debe tener en cuenta el/la empleador/a para determinar el trabajo remoto?

Para ello se recomienda evaluar los siguientes puntos:

- Determinar si por la naturaleza de sus funciones pueda desempeñar sus labores sin necesidad de estar físicamente en la oficina.
- Existen herramientas informáticas las cuales permiten que actividades administrativas, soporte o asesoría (áreas de contabilidad, legal, tecnología, entre otros) pueden ser trabajadores de manera remota sin que se afecte su productividad. Por otro lado, hay actividades que requieren que se manejen de forma presencial como limpieza, vigilancia o producción entre otros, en estos casos no aplicaría el trabajo remoto.
- Identificar a los grupos vulnerables, por edad o por enfermedades que identifiquen a ese grupo como vulnerable las cuales deben realizar trabajo remoto.

¿Qué obligaciones especiales corresponden a los/las empleadores/as en caso de trabajo remoto?

Los empleados deberán cumplir lo siguiente:

- No debe afectar la naturaleza del vínculo laboral, la remuneración, y demás condiciones económicas salvo aquellas que se encuentran vinculadas a la asistencia al centro de trabajo o cuando estas favorecen al tragador.
- Comunicar al colaborador por medio de un soporte físico (documento escrito) o como digital (correo electrónico, intranet, aplicaciones de mensajería), se debe indicar periodo del trabajo remoto, medios y las medidas para el desarrollo y salud en el trabajo.
- Debe informar al colaborador las medidas que se puedan considerar dentro del trabajo remoto.
- El empleador debe otorgar facilidades de accesos a los sistemas, plataformas o incluso aplicativos informáticos para que puedan desarrollar sus funciones en el trabajo remoto, además debe brindar las reglas que aplican a la confidencialidad y la protección de los datos.
- El empleador debe brindar la capacitación necesaria previa a implantación de sistemas, plataformas o aplicaciones informativos distintos a los usados por el trabajador.

¿Qué obligaciones especiales corresponden a los/las trabajadores/as que realizan trabajo remoto?

- Cumplir con la normativa vigente de seguridad de la información, protección y confidencialidad de los datos, así como guardar confidencialidad de la información proporcionada por el empleador para la prestación de servicios.

- Cumplir con las medidas y condiciones de seguridad y salud en el trabajo en la empresa.
- Se debe estar disponible, siempre durante la jornada laboral para las diferentes coordinaciones de carácter laboral.
- Se debe reportar y entregar lo encargado por el empleador en los horarios y periodos establecidos en la jornada laboral.
- El empleado debe ser partícipe de las capacitaciones programadas que disponga la empresa.
- El colaborador debe informar de manera inmediata cualquier desperfecto que pueda afectar el trabajo remoto. Culminado el descanso podrá reincorporar sus labores remotas siempre y cuando aún esté vigente dicha modalidad.
- El empleador debe informar los descansos médicos al empleador, Cumplir con la prohibición de subrogación de funciones.

¿Quién debe proporcionar los equipos y medios para el desarrollo del trabajo remoto?

Las herramientas necesarias para el desarrollo del trabajo remoto como equipos, internet, telefonía u otros medios pueden ser proporcionados por el empleador o por el trabajador.

¿Se debe compensar los gastos en los equipos que incurre el/la trabajador/a?

Si los medios o herramientas son brindados por el trabajador, se puede llegar a un acuerdo con el empleador para que se puedan derivar los gastos adicionales para el desarrollo del trabajo remoto.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

3.1.Descripción del Ingreso a la empresa

Terminado mi periodo de estudiante en la Universidad Privada del Norte, postulé a diferentes plazas acorde a mis conocimientos para poder comenzar una línea de carrera que refuerce mi profesión. Posteriormente, el día 27 de febrero, recibí una llamada del área de RRHH de la empresa CLI Gestiones Aduaneras S.A. para el puesto de Asistente de Soporte, quien me citó para una entrevista el día 28 de febrero a las 09:00 am. En la entrevista conocí al Supervisor del área de Sistemas, quien me realizó preguntas referentes al cargo y me explicaron las funciones que realizaría en la empresa, culminada la entrevista me indicaron que RRHH se pondría en contacto conmigo para indicarme si quedaba seleccionada para el puesto. Fue así que el día 04 de marzo se comunicó conmigo el área de RRHH para indicarme que formaría parte de la empresa CLI Gestiones Aduaneras S.A. y que empezaría a laborar con ellos el día 15 de marzo.

El día 15 de marzo ingresé a la empresa y realicé la firma del contrato, ingresé al área de sistemas donde se encontraba la señorita a la cual remplazaría, quien me brindó una inducción general de las funciones que realizaba, las cuales englobaban el apoyo a todos los usuarios en problemas técnicos del día a día, hasta la creación de usuarios, limpieza de equipos, instalación de sistemas, soporte de impresoras, manejo de inventarios, reportes en base de datos, entre otros.

Gracias a mi buen desempeño, fui promovida a Analista de Soporte, para entonces no solo veía los temas ya antes mencionados, sino que también me encargaba de la gestión de la red, el firewall, revisión del servidor de correos, revisión de los correos spam, participación en

las auditorías, elaboración y actualización de procedimientos y elaboración de manuales de uso de los nuevos sistemas elaborados por los programadores, entre otras funciones.

3.2.Identificación del Problema

En el año 2020, el presidente Martín Vizcarra declara estado de emergencia a nivel nacional según: "Decreto Supremo N° 044-2020-PCM, que declara el Estado de Emergencia Nacional, por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID 19" (Diario El Peruano, 2020).

Por tal razón se adoptan medidas de trabajo remoto ya que el gobierno lo exigía. "En el Decreto de Urgencia N° 026-2020 se puede aplicar durante la vigencia de la emergencia sanitaria declarada a nivel nacional mediante el Decreto Supremo N° 008-2020-SA por el plazo de noventa (90) días calendario" (Diario El Peruano, 2020, p. 2).

Como primera actividad se realiza un inventario del personal para saber si contaban con internet, laptop o PC. Seguidamente, se crean 5 máquinas virtuales en el Hipervisor Vmware Esxi 7 y a cada una de estas máquinas se le asigna un puerto distinto desde una IP pública nateada para que los usuarios se conecten a ellas desde sus casas durante el periodo de cuarentena.

Posteriormente, al personal que no contaba con equipo, se le entrega una laptop alquilada. La empresa había alquilado 20 laptops del proveedor Tansligra SAC, así mismo se cambió el plan de los equipos móviles para que el personal que no contase con internet en casa pudiera compartir internet desde sus equipos móviles del trabajo.

Finalmente, se brinda una capacitación al personal de cómo deben acceder tanto a las máquinas virtuales por la conexión a escritorio remoto de Windows y el acceso a los sistemas

dentro de él, así como el ingreso al Webmail, además se les brindó sus credenciales para la conexión remota y el correo.

Las primeras semanas fueron complicadas ya que los usuarios no se adaptaban a la modalidad. Lamentablemente la modalidad del trabajo remoto hizo que la productividad de los colaboradores disminuya considerablemente, siendo habitual que los usuarios reportaran inconvenientes en su conexión, acceso a archivos, dificultad en acceder al sistema y a la mayoría se les hizo muy difícil usar el correo Webmail ya que en oficina usaban el Outlook.

3.2.1. Problema General

¿Cómo mejorar el acceso y seguridad de los sistemas y servicios de red en el trabajo remoto?

3.2.2. Problemas Específicos

- ¿Cómo logar un acceso más estable en la conexión remota?
- ¿Cómo mejorar el nivel de seguridad en los puertos lógicos abiertos en los servidores?
- ¿Cómo mejorar los accesos a los recursos y servicios de la red corporativa en el trabajo remoto?
- ¿Cómo obtener un mejor control y monitoreo en trabajo remoto?

3.3.Objetivos

3.3.1. Objetivos Generales

Implementar una red VPN para mejorar la calidad en el acceso y seguridad de los sistemas y servicios de red en el trabajo remoto.

3.3.2. Objetivos Específicos

- Mejorar la estabilidad de conexión remota mediante una óptima configuración de la VPN en el dispositivo de Gestión Unificada de Amenazas (UTM).

- Mejorar la seguridad de la conexión remota mediante la implementación de los túneles cifrados en la VPN.
- Brindar acceso a los recursos y servicios de la red corporativa de forma más directa a través una conexión VPN.
- Implementación de reportes y alertas en el UTM para monitorear la productividad de los colaboradores.

Todos estos incidentes reportados se ingresaron en un Excel, donde se clasificaron los incidentes relacionados al trabajo remoto, como se muestra en la siguiente tabla donde se muestra el resume de las incidencias, para mayor detalle, consultar el Anexo1:

Tabla 1. Resumen de Incidencias reportadas en mayo 2020.

Tipos de Incidentes	MES	# Eventos	Porcentaje de Eventos
FALTA ACCESO A SISTEMAS Y ARCHIVOS	MAYO	30	17%
PROBLEMAS EN LA CONEXIÓN REMOTA	MAYO	100	56%
PROBLEMAS CON LOS CORREO	MAYO	27	15%
LENTITUD EN SISTEMAS	MAYO	20	11%
Total general		**177**	**100%**

Fuente: Elaboración Propia

Para poder organizar la información obtenida, usamos el diagrama Ishikawa o conocido también por diferentes autores como diagrama causa-efecto. De acuerdo a Martínez (2000), indica que este tipo de diagramas son usados para poder representar la relación que existe entre las causas que pueden originarse y el efecto producto de ellas.

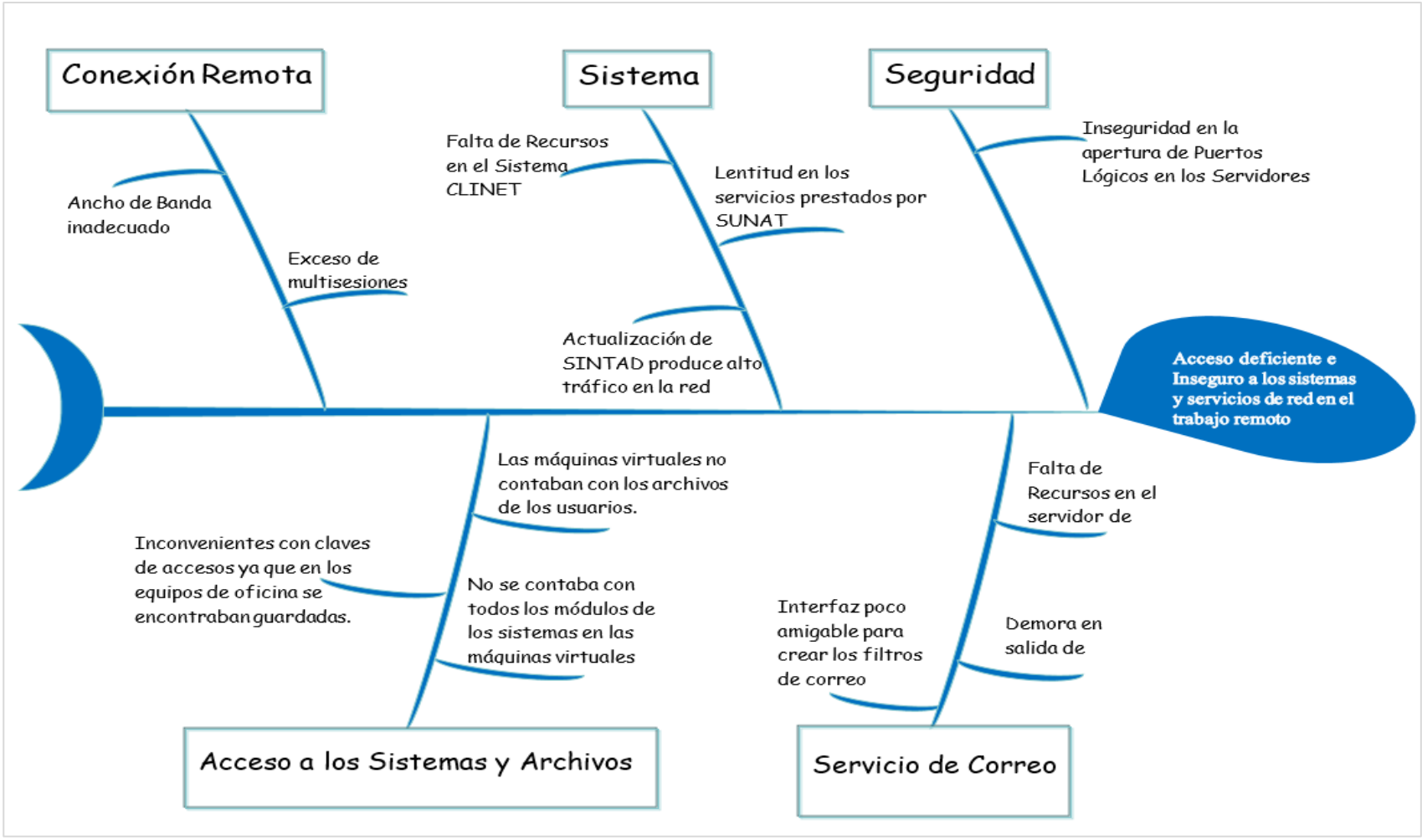


Figura 13. Diagrama Ishikawa

Fuente: Elaboración Propia

En el diagrama podemos observar que el problema que engloba los incidentes reportados es el acceso deficiente e inseguro a los sistemas y servicios de red en el trabajo remoto, y las causas que provocan este contratiempo están asociados a la conexión remoto, al sistema, a los accesos de los archivos y sistemas y al servicio de correo.

A continuación, utilizaremos la tabla de frecuencias para representar la información recolectada, según Tomás (2009) indica que este tipo de tablas son pieza fundamental para representar la información, ya que permite que un volumen de datos se reduzca de tal manera que facilite su visualización.

Tabla 2: Tabla de Frecuencias

Incidentes Reportados en el mes de Mayo	**Frecuencia**	**P. Acumulado**		**80-20**
Exceso de multisesiones	88	50%	88	80%
No se contaba con todos los módulos de los sistemas	13	57%	101	80%
Ancho de Banda Inadecuado	12	64%	113	80%
Las máquinas virtuales no contaban con los archivos de los usuarios.	11	70%	124	80%
Falta de Recursos en el Servidor de Correos	10	76%	134	80%
Lentitud en los servidores prestados por SUNAT	10	81%	144	80%
Interfaz poco amigable para la creación de filtros de correo	7	85%	151	80%
Inconvenientes con claves de accesos	6	89%	157	80%
Pérdida en el servicio de correo	6	92%	163	80%
Actualización de SINTAD produce alto tráfico de red	6	95%	169	80%
Demora en salida de correos	4	98%	173	80%
Falta de Recursos en CLINET	4	100%	177	80%
Inseguridad en la Apertura de Puertos lógicos en los servidores	-	-	-	-

Fuente: Elaboración Propia

Finalmente, con los datos obtenidos, aplicaremos el principio de Pareto, también conocido como principio de 80/20 el cual nos permite analizar la información de causas ante un problema priorizándolas según sus frecuencias y mediante un gráfico de la curva acumulada, por ello Koch (2015), establece que de una minoría de causas se puede obtener el esfuerzo que conduce a los resultados, rendimiento o recompensas, esto quiere decir que el 80% de lo que se puede conseguir en un trabajo es consecuente a un 20% del tiempo que se le dedica. Por ello prácticamente cuatro quintos del esfuerzo que pongamos en una tarea, prácticamente la totalidad, son irrelevantes y contrarios a lo que se puede llegar a esperar.

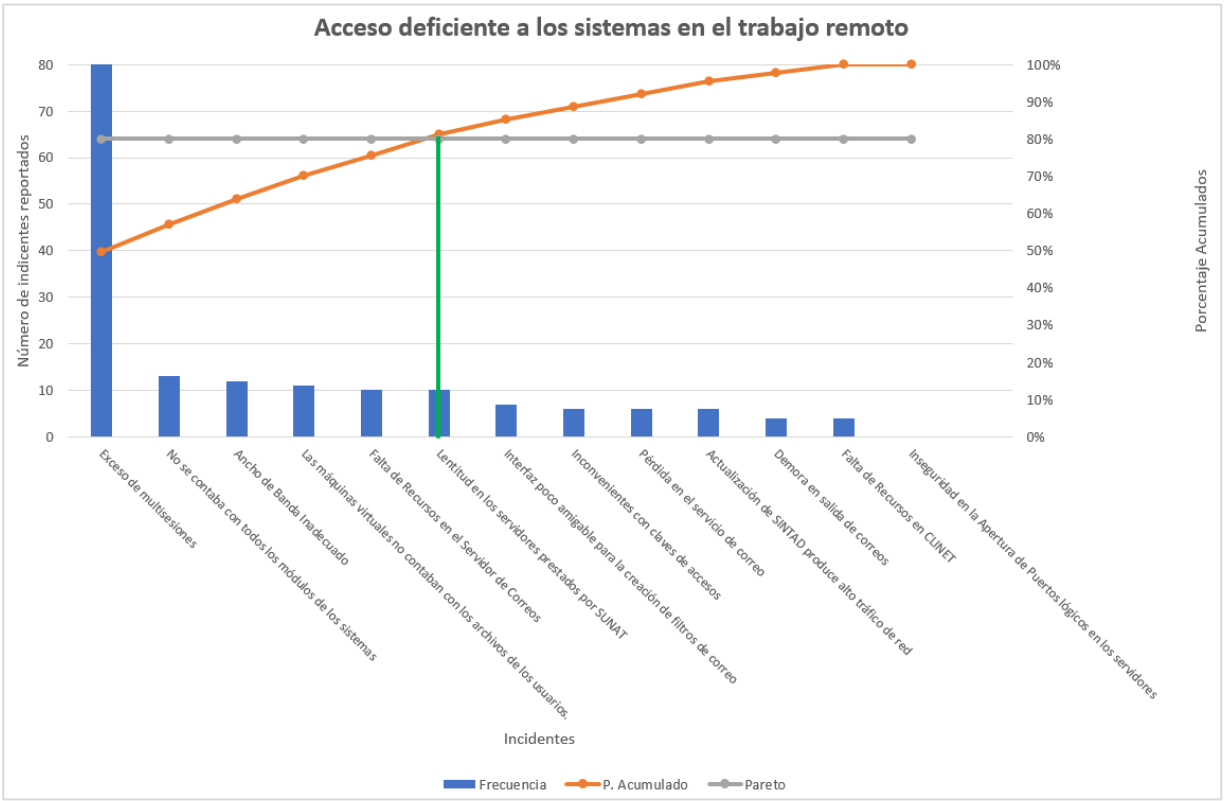


Figura 14. Diagrama del principio de Pareto 80/20

Fuente: Elaboración Propia

En el diagrama de barras observamos que se tiene un eje Y derecho y un eje Y izquierdo, en el izquierdo ubicamos las causas basadas en a frecuencia relativa y en el eje Y derecho ubicamos el porcentaje acumulado.

La curva observada, se basa en el porcentaje acumulado de cada causa, en el cual el 76% abarca a las 5 principales causas del problema, esto nos indica que debemos enfocarnos en poder brindar una solución que permita minimizar estos incidentes.

3.4.Desarrollo del proyecto

3.4.1. Planificación

Para la implementación de la VPN se investiga y propone que se sea ejecutado con la herramienta Open VPN, ya que el Firewall de la organización tenía el servicio compatible con este.

Figura 15. Servicio OpenVPN en Endian Firewall Comunity

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

De acuerdo a la página oficial de Endian, indica en su manual de uso que es recomendable usar OpenVPN. “Recomienda OpenVPN en situaciones en las que no es necesario admitir una infraestructura IPsec existente. Endian Firewall

incluye un cliente OpenVPN fácil de usar para Microsoft Windows, Linux y MacOS X" (2008).

Se validaron los requisitos necesarios en los equipos de los usuarios como el antivirus, sistema operativo, memoria RAM y la velocidad del internet hogar que cuenta cada usuario, como los equipos de la empresa eran Windows7, y otros Windows10, se establece que se contemplarán las versiones de OpenVPN para ambos casos.

A continuación, se muestra el cronograma donde se especifica la lista de actividades a realizar durante la implementación de la VPN:

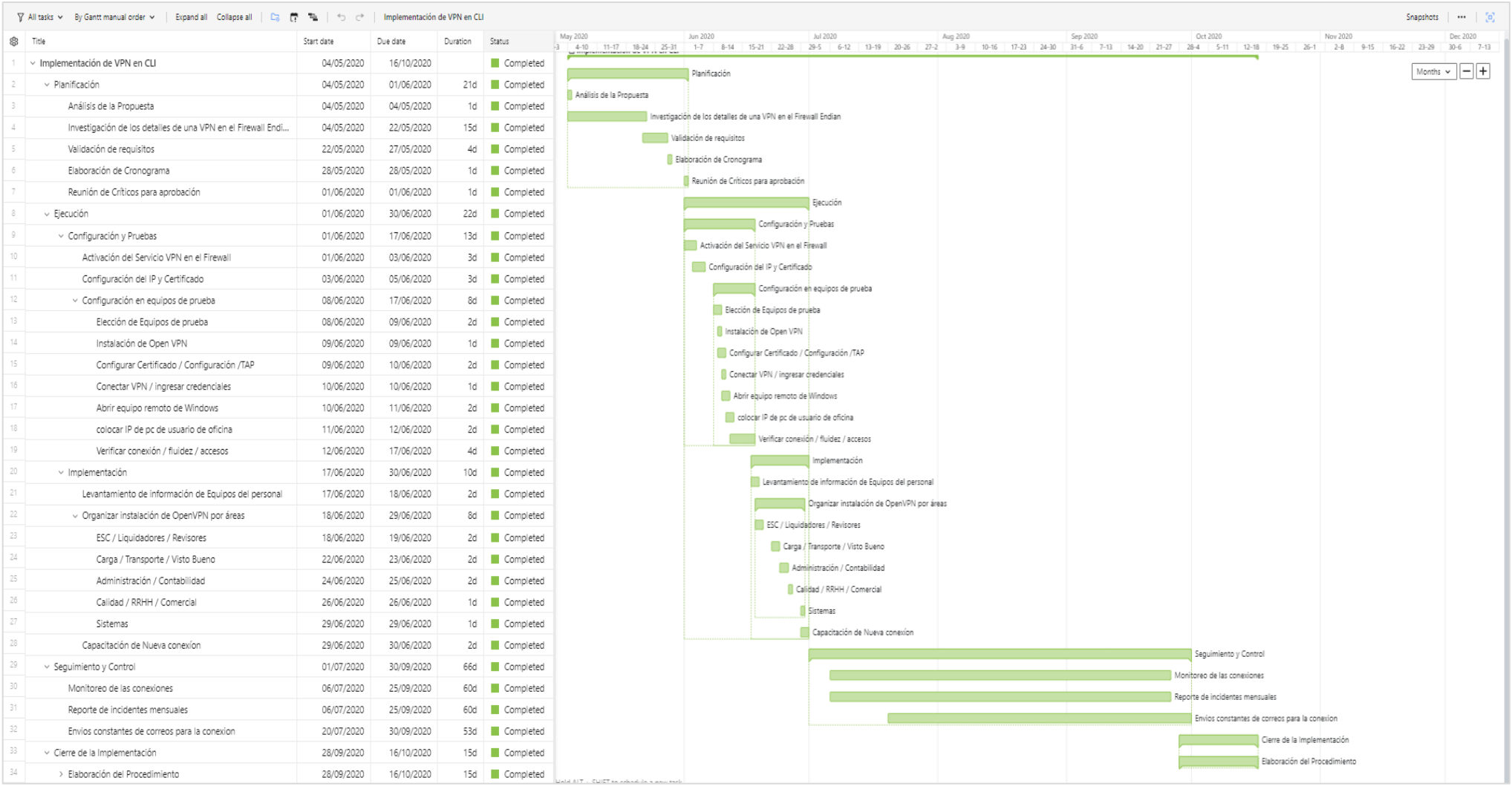
Title	Start date	Due date	Duration	Status
Implementación de VPN en CLI	04/05/2020	16/10/2020		Completed
Planificación	04/05/2020	01/06/2020	21d	Completed
Análisis de la Propuesta	04/05/2020	04/05/2020	1d	Completed
Investigación de los detalles de una VPN en el Firewall Endian	04/05/2020	22/05/2020	15d	Completed
Validación de requisitos	22/05/2020	27/05/2020	4d	Completed
Elaboración de Cronograma	28/05/2020	28/05/2020	1d	Completed
Reunión de Críticos para aprobación	01/06/2020	01/06/2020	1d	Completed
Ejecución	01/06/2020	30/06/2020	22d	Completed
Configuración y Pruebas	01/06/2020	17/06/2020	13d	Completed
Implementación	17/06/2020	30/06/2020	10d	Completed
Levantamiento de información de Equipos del personal	17/06/2020	18/06/2020	2d	Completed
Organizar instalación de OpenVPN por áreas	18/06/2020	29/06/2020	8d	Completed
Capacitación de Nueva conexíon	29/06/2020	30/06/2020	2d	Completed
Seguimiento y Control	01/07/2020	30/09/2020	66d	Completed
Cierre de la Implementación	28/09/2020	16/10/2020	15d	Completed

Figura 16 Actividades a realizar para la implementación de la VPN

Fuente: Elaboración Propia

Así mismo se diagramó, utilizando el diagrama de Gantt, todo el cronograma con sus respectivas actividades a realizar y en el periodo programado, para su

realización se usó wrike, esta es una herramienta web, que permite organizar tareas o proyecto.



	Title	Start date	Due date	Duration	Status
1	Implementación de VPN en CLI	04/05/2020	16/10/2020		Completed
2	Planificación	04/05/2020	01/06/2020	21d	Completed
3	Análisis de la Propuesta	04/05/2020	04/05/2020	1d	Completed
4	Investigación de los detalles de una VPN en el Firewall Endi...	04/05/2020	22/05/2020	15d	Completed
5	Validación de requisitos	22/05/2020	27/05/2020	4d	Completed
6	Elaboración de Cronograma	28/05/2020	28/05/2020	1d	Completed
7	Reunión de Críticos para aprobación	01/06/2020	01/06/2020	1d	Completed
8	Ejecución	01/06/2020	30/06/2020	22d	Completed
9	Configuración y Pruebas	01/06/2020	17/06/2020	13d	Completed
10	Activación del Servicio VPN en el Firewall	01/06/2020	03/06/2020	3d	Completed
11	Configuración del IP y Certificado	03/06/2020	05/06/2020	3d	Completed
12	Configuración en equipos de prueba	08/06/2020	17/06/2020	8d	Completed
13	Elección de Equipos de prueba	08/06/2020	09/06/2020	2d	Completed
14	Instalación de Open VPN	09/06/2020	09/06/2020	1d	Completed
15	Configurar Certificado / Configuración /TAP	09/06/2020	10/06/2020	2d	Completed
16	Conectar VPN / ingresar credenciales	10/06/2020	10/06/2020	1d	Completed
17	Abrir equipo remoto de Windows	10/06/2020	11/06/2020	2d	Completed
18	colocar IP de pc de usuario de oficina	11/06/2020	12/06/2020	2d	Completed
19	Verificar conexión / fluidez / accesos	12/06/2020	17/06/2020	4d	Completed
20	Implementación	17/06/2020	30/06/2020	10d	Completed
21	Levantamiento de información de Equipos del personal	17/06/2020	18/06/2020	2d	Completed
22	Organizar instalación de OpenVPN por áreas	18/06/2020	29/06/2020	8d	Completed
23	ESC / Liquidadores / Revisores	18/06/2020	19/06/2020	2d	Completed
24	Carga / Transporte / Visto Bueno	22/06/2020	23/06/2020	2d	Completed
25	Administración / Contabilidad	24/06/2020	25/06/2020	2d	Completed
26	Calidad / RRHH / Comercial	26/06/2020	26/06/2020	1d	Completed
27	Sistemas	29/06/2020	29/06/2020	1d	Completed
28	Capacitación de Nueva conexion	29/06/2020	30/06/2020	2d	Completed
29	Seguimiento y Control	01/07/2020	30/09/2020	66d	Completed
30	Monitoreo de las conexiones	06/07/2020	25/09/2020	60d	Completed
31	Reporte de incidentes mensuales	06/07/2020	25/09/2020	60d	Completed
32	Envios constantes de correos para la conexion	20/07/2020	30/09/2020	53d	Completed
33	Cierre de la Implementación	28/09/2020	16/10/2020	15d	Completed
34	Elaboración del Procedimiento	28/09/2020	16/10/2020	15d	Completed

Figura 17. Diagrama de Gantt del Proyecto

Fuente: Elaboración Propia

Una vez planteado el proyecto y la estrategia a usar, el Supervisor de Sistemas, propuso la implementación del mismo en la reunión llamada "**Críticos"**, la cual se realizaba de manera semanal donde participaban los gerentes con todos los jefes de áreas.

3.4.2. Ejecución

i.Activación del servicio

Para poder iniciar el servicio de VPN que tiene ya el firewall Endian Firewall Community, abrimos un navegador web, e ingresamos la ruta (IP) del firewall, ingresamos las credenciales respectivas, una vez logueados nos dirigimos al menú y seleccionamos la opción **VPN**, seguidamente nos dirigimos a la opción Open VPN Server, en esta opción observaremos dos opciones, de las cuales nos ubicaremos en la opción **Server configuration**, observaremos un interruptor el cual se encuentra en color gris, el cual luego de hacer clic sobre él se pintará verde.

A continuación, tras unos minutos de espera para que se pueda generar las certificaciones respectivas, raíz y host, se observará que ya se cuenta con la configuración predeterminada, el puerto a usar con el protocolo UDP, el TAP el cual será la interfaz ethernet virtual y se agregó la subnet respectiva.

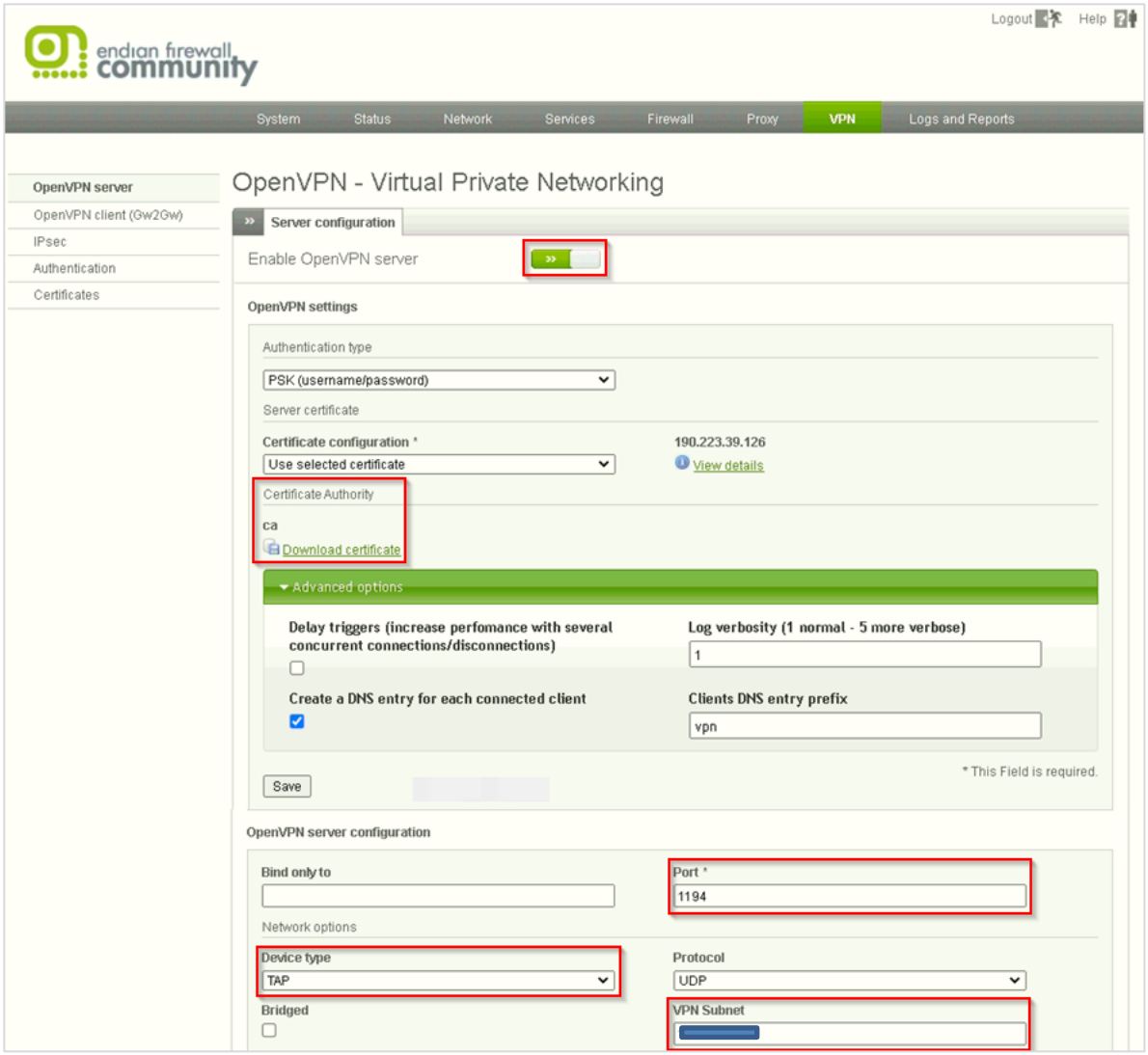


Figura 18. Activación del servicio VPN en el Firewall

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

Así mismo, se tenía que crear un usuario para poder probar la conexión, este usuario se creaba en la opción **Authentification**, en este caso se creó el usuario **midori** de prueba**.**

ii. Instalación de OpenVPN.

Para realizar las pruebas, se usó una laptop backup que se encontraba en almacén, este equipo tenía un sistema operativo de 64 bits, así que ingresamos al siguiente link https://openvpn.net/community-downloads/ para descargar el instalador del OpenVPN, seleccionamos la opción de descarga **Instalador MSI de Windows de 64 bits**, una vez culminada la descarga, procedemos a instalar el programa.

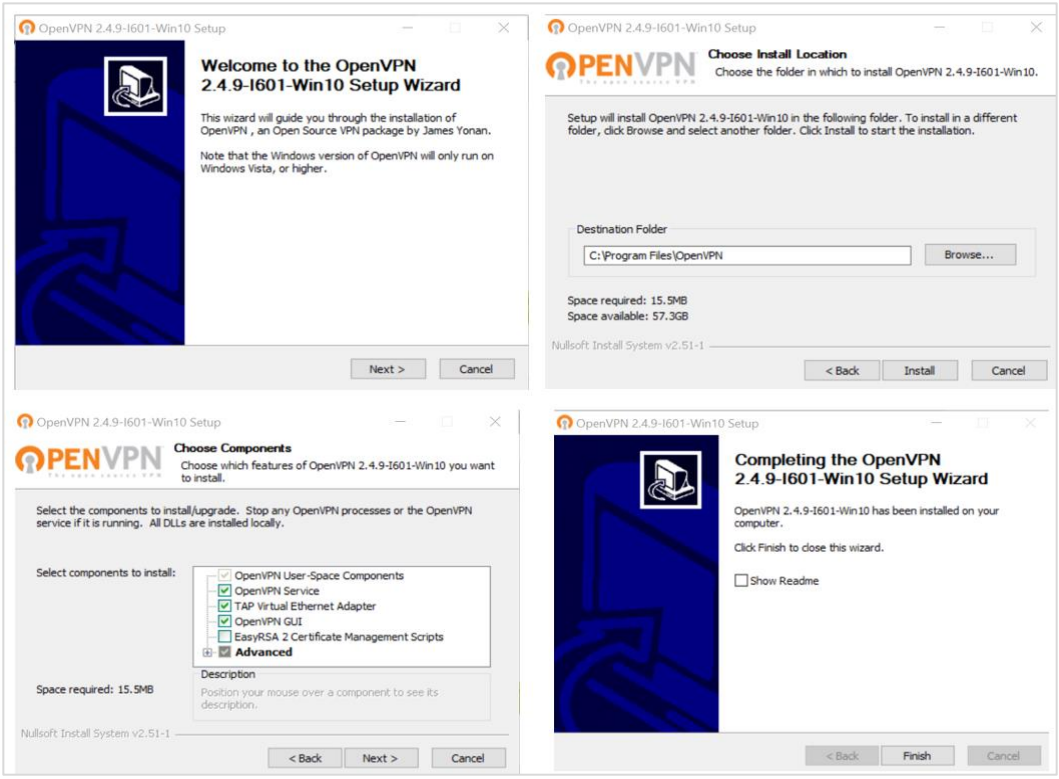


Figura 19. Instalación de OpenVPN

Fuente: Elaboración Propia

Una vez instalado OpenvPN, debemos colocar la configuración y el certificado en la siguiente carpeta, C:\Program Files\OpenVPN\config. Esto con el fin de que pueda aceptar un cliente Windows, multisesiones, y el reconocimiento del TAP para la conexión con la red de CLI. Uno de ellos es el Certificado cuya extensión es "**.pem"**, el cual se descarga del firewall y el segundo es un archivo de configuración cuya extensión es "**.ovpn".**

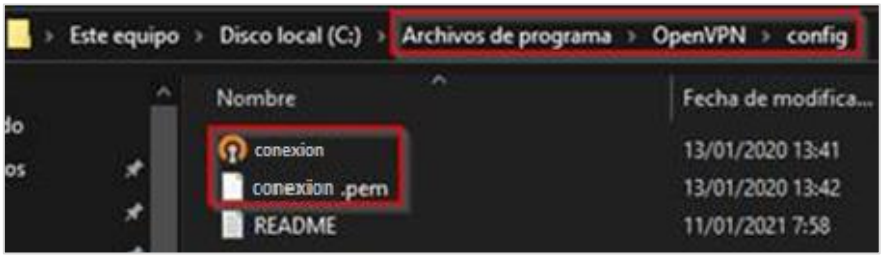


Figura 20. Certificado y configuración de Open VPN

Fuente: Elaboración Propia

En el archivo de configuración se coloca que la interfaz ethernet virtual (TAP) debe ser nombrada "**conexión"**, de lo contrario no se podrá realizar la conexión VPN, para ello se debe realizar el cambio en la configuración de la red.

Figura 21. Interfaz virtual Ethernet TAP

Fuente: Elaboración Propia

iii. **Estableciendo conexión VPN**

Culminada ya la instalación en el equipo, nos dirigimos al escritorio, hacemos doble clic sobre el ícono de OpenVPN, inmediatamente se observará que en la barra de herramientas se mostrará un ícono con un candado, en el cual haremos clic derecho y seleccionaremos la opción conectar.

Seguidamente ingresaremos nuestras credenciales y se establecerá la conexión y el ícono del candado se tornará de color verde.

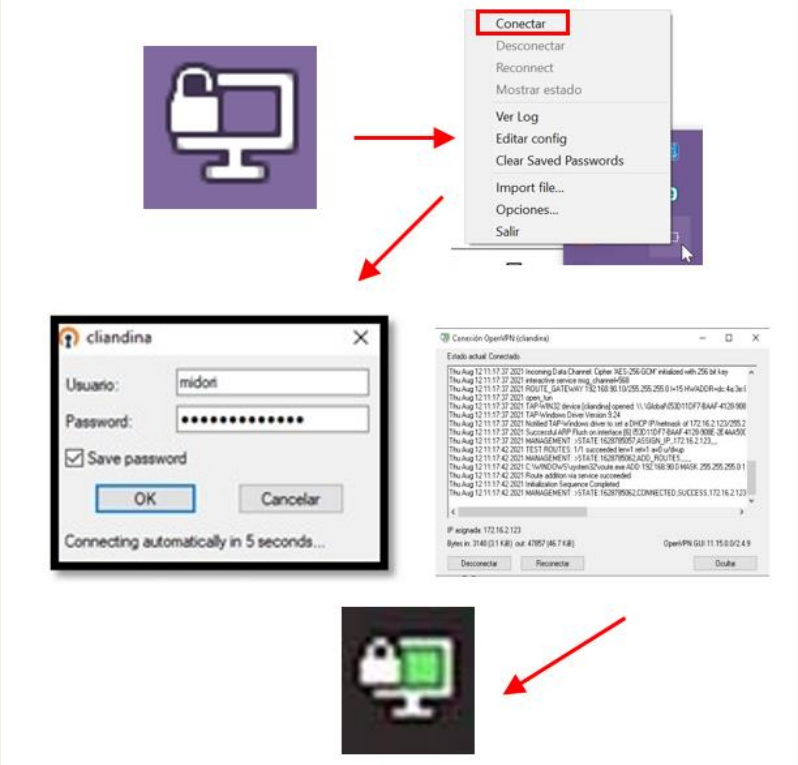


Figura 22. Estableciendo conexión VPN con CLI

Fuente: Elaboración Propia

Cabe mencionar que fueron diferentes intentos hasta poder establecer conexión sin errores, dichos inconvenientes se debieron a diferentes factores como, el firewall de Windows, banda ancha del internet del cliente, error al escribir la contraseña, error en los archivos de configuración, finalmente después de algunos intentos se logró establecer la conexión esperada.

iv. Probando la conexión a un equipo de CLI

Para verificar la conexión a un equipo de oficina, procedemos a abrir la conexión a escritorio remoto de Windows, en él colocamos la IP del equipo de oficina, en este caso nos conectaremos a una máquina indicando el IP y colocamos las credenciales (usuario y contraseña) y efectivamente, ya teníamos acceso al equipo de oficina, la cual nos permitirá trabajar como si estuviéramos de manera presencial.

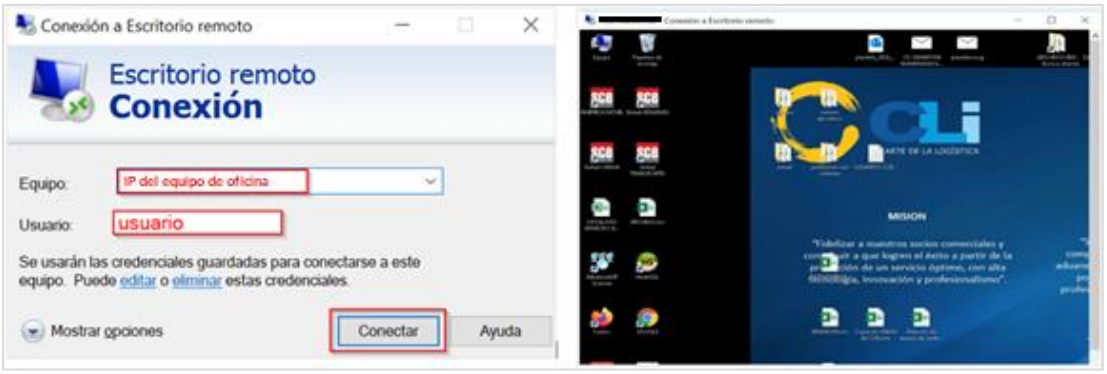


Figura 23. Conexión a equipo de oficina

Fuente: Elaboración Propia

3.4.3. Implementación

Al culminar las pruebas, se procede a crear los usuarios y sus respectivas credenciales en el Firewall.

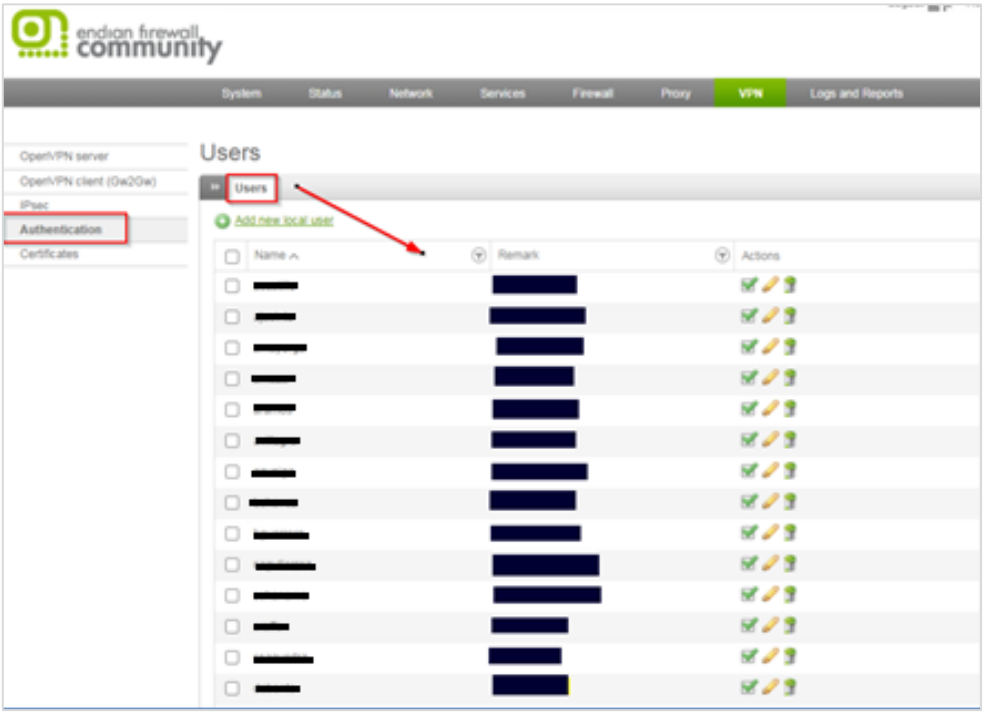


Figura 24. Creación de Usuarios VPN en el Firewall

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

En la figura 24 observamos los usuarios creados en el firewall en la sección de Autentificación.

Seguidamente se realiza un inventario donde se detallan los usuarios por área y los equipos con sus características por donde los usuarios se iban a conectar, cabe recalcar que al personal de alto riesgo durante la cuarentena se les brindo equipos de la empresa, y a los demás que no contaban con equipo propio se les brindó laptops de la empresa y laptops que alquilaron al proveedor Transligra SAC.

Características de los equipos donde se conectan los usuarios al Sistema									
	USUARIO			CLI			TRASLIGRA (alquiler)		
AREA	EQUIPO	SO	ANTIVIRUS	EQUIPO	SO	ANTIVIRUS	EQUIPO	SO	ANTIVIRUS
ESC	Laptop	Windows 10 64 Bits	Mcaffe						
ESC				Laptop	Windows 10 64 Bits	Bitdefender			
ESC				Laptop	Windows 10 64 Bits	Bitdefender			
ESC							Laptop	Windows 10 64 Bits	ESET
ESC							Laptop	Windows 10 64 Bits	ESET
ESC							Laptop	Windows 10 64 Bits	ESET
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC							Laptop	Windows 10 64 Bits	ESET
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC							Laptop	Windows 10 64 Bits	ESET
ESC	Desktop	Windows 7 64 Bits	ESET						
ESC	Laptop	Windows 10 64 Bits	kaspersky						
ESC	Laptop	Windows 10 64 Bits	Avira						
ESC				Desktop	Windows 7 64 Bits	Bitdefender			
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC	Laptop	Windows 10 64 Bits	ESET						
ESC							Laptop	Windows 10 64 Bits	ESET
ESC	Laptop	Windows 7 32 Bits	ESET						
ESC							Laptop	Windows 10 64 Bits	ESET
ESC	Laptop	Windows 10 64 Bits	Avira						
ESC							Laptop	Windows 10 64 Bits	ESET
ESC							Laptop	Windows 10 64 Bits	ESET
REVISORES				Desktop	Windows 7 64 Bits	Bitdefender			
REVISORES	Desktop	Windows 7 32 Bits	Avira						
REVISORES							Laptop	Windows 10 64 Bits	ESET
REVISORES							Laptop	Windows 10 64 Bits	ESET
LIQUIDADORES				Desktop	Windows 7 64 Bits	Bitdefender			
LIQUIDADORES	Laptop	Windows 7 32 Bits	Avira						
LIQUIDADORES							Laptop	Windows 10 64 Bits	ESET
LIQUIDADORES							Laptop	Windows 10 64 Bits	ESET
LIQUIDADORES				Laptop	Windows 7 64 Bits	Bitdefender			
LIQUIDADORES	Desktop	Windows 7 32 Bits	kaspersky						
LIQUIDADORES	Laptop	Windows 10 64 Bits	ESET						
LIQUIDADORES	Desktop	Windows 10 64 Bits	Mcaffe						
VISTO BUENO							Laptop	Windows 10 64 Bits	ESET
VISTO BUENO							Laptop	Windows 10 64 Bits	ESET
VISTO BUENO	Laptop	Windows 10 64 Bits	ESET						
CARGA	Laptop	Windows 10 64 Bits	kaspersky						
CARGA							Laptop	Windows 10 64 Bits	ESET
CARGA	Desktop	Windows 7 32 Bits	ESET						
CARGA				Laptop	Windows 10 64 Bits	Bitdefender			
TRANSPORTE							Laptop	Windows 10 64 Bits	ESET
TRANSPORTE							Laptop	Windows 10 64 Bits	ESET
TRANSPORTE	Laptop	Windows 10 64 Bits	Mcaffe						
TRANSPORTE	Desktop	Windows 10 64 Bits	Mcaffe						
TRANSPORTE	Desktop	Windows 7 32 Bits	ESET						
RRHH	Laptop	Windows 10 64 Bits	ESET						
RRHH	Laptop	Windows 10 64 Bits	ESET						
COMERCIAL	Laptop	Windows 10 64 Bits	kaspersky						
COMERCIAL	Desktop	Windows 10 64 Bits	Avira						
CONTABILIDAD							Laptop	Windows 10 64 Bits	ESET
CONTABILIDAD	Desktop	Windows 10 64 Bits	ESET						
CONTABILIDAD	Laptop	Windows 10 64 Bits	ESET						
ADMINISTRACION	Desktop	Windows 10 64 Bits	ESET						
ADMINISTRACION	Desktop	Windows 7 32 Bits	ESET						
ADMINISTRACION							Laptop	Windows 10 64 Bits	ESET
ADMINISTRACION							Laptop	Windows 10 64 Bits	ESET
ADMINISTRACION	Laptop	Windows 10 64 Bits	kaspersky						
ADMINISTRACION	Laptop	Windows 10 64 Bits	Mcaffe						
ADMINISTRACION	Desktop	Windows 7 32 Bits	ESET						
ADMINISTRACION	Desktop	Windows 7 32 Bits	ESET						
ADMINISTRACION	Laptop	Windows 10 64 Bits	ESET						
CALIDAD	Laptop	Windows 10 64 Bits	Avira						
CALIDAD	Laptop	Windows 10 64 Bits	ESET						
CALIDAD	Laptop	Windows 10 64 Bits	kaspersky						
PROYECTOS							Laptop	Windows 10 64 Bits	ESET
PROYECTOS				Laptop	Windows 10 64 Bits	Bitdefender			
PROYECTOS							Laptop	Windows 10 64 Bits	ESET
JEFATURA				Laptop	Windows 10 64 Bits	Bitdefender			
JEFATURA				Laptop	Windows 10 64 Bits	Bitdefender			
JEFATURA				Laptop	Windows 10 64 Bits	Bitdefender			
JEFATURA							Laptop	Windows 10 64 Bits	ESET
JEFATURA	Laptop	Windows 10 64 Bits	ESET						

Figura 25. Características de los equipos donde se conectan los usuarios

Fuente: Elaboración Propia

- **Cronograma de instalación por áreas.**

Al tener ya un alcance de los usuarios que trabajaban presencial y remoto y contar con las características de sus equipos con los que se conectarían se procede a realizar un cronograma de este y para realizar la instalación de una manera más rápida se subieron los instaladores y ambos archivos de configuración que se necesitarían a un drive.

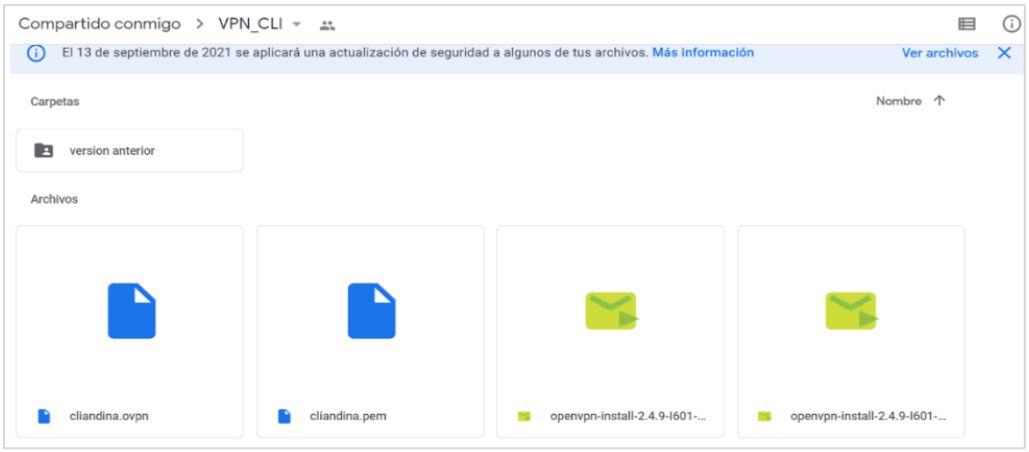


Figura 26. Drive con los instaladores del Open VPN y sus versiones
Fuente: Elaboración Propia

A continuación, se muestra el cronograma de instalación del OpenVPN a los usuarios por áreas. En primer lugar, se toman las áreas operativas (críticas), seguidamente las operativas menos críticas, y luego las áreas administrativas. Por cada usuario que se realizaba la instalación se le explicaba la nueva modalidad de ingreso y se les conectaba a los equipos de oficina, al personal de alto riesgo

solo se le indica que luego de activar el VPN podía utilizar los sistemas como si estuvieran en oficina.

Title	Start date	Due date	Duration
Organizar instalación de OpenVPN por áreas	18/06/2020	29/06/2020	8d
ESC / Liquidadores / Revisores	18/06/2020	19/06/2020	2d
Carga / Transporte / Visto Bueno	22/06/2020	23/06/2020	2d
Administración / Contabilidad	24/06/2020	25/06/2020	2d
Calidad / RRHH / Comercial	26/06/2020	26/06/2020	1d
Sistemas	29/06/2020	29/06/2020	1d

Figura 27. Cronograma de instalación por área
Fuente: Elaboración Propia

- **Capacitación al personal.**

  Para un mejor entendimiento de la nueva modalidad de conexión remota, luego de culminar la instalación del OpenVPN a todos los usuarios, se agenda una capacitación por la plataforma Microsoft Teams, esta se programó para el día 29/06/2020 de 9:00 am. a 10:00 am. en el cual se trató de absolver todas las dudas e interrogantes planteadas.

3.4.4. Seguimiento y Control

En esta etapa se monitoreó las conexiones desde la VPN, así mismo se realizó una bitácora de incidencias en la cual se observa que el primer mes en su mayoría el inconveniente fue el adaptarse a la nueva forma de conectar, y para ello se brindaba mensajes constantes de cómo se realizaba la conexión en correos recordatorios.

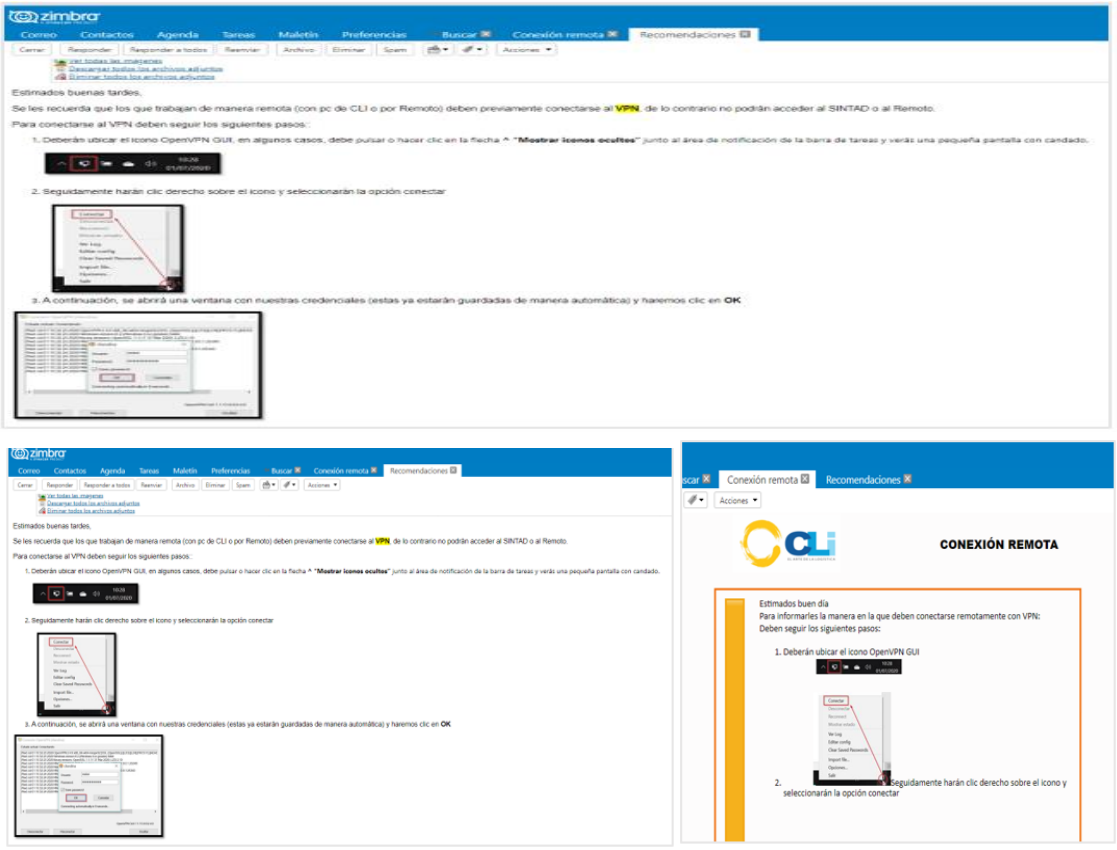


Figura 28. Correos de recordatorio de Conexión VPN

Fuente: Elaboración Propia

En la figura 28 se observan los correos enviados a los usuarios indicando y recordando la manera de conectarse por medio de la VPN.

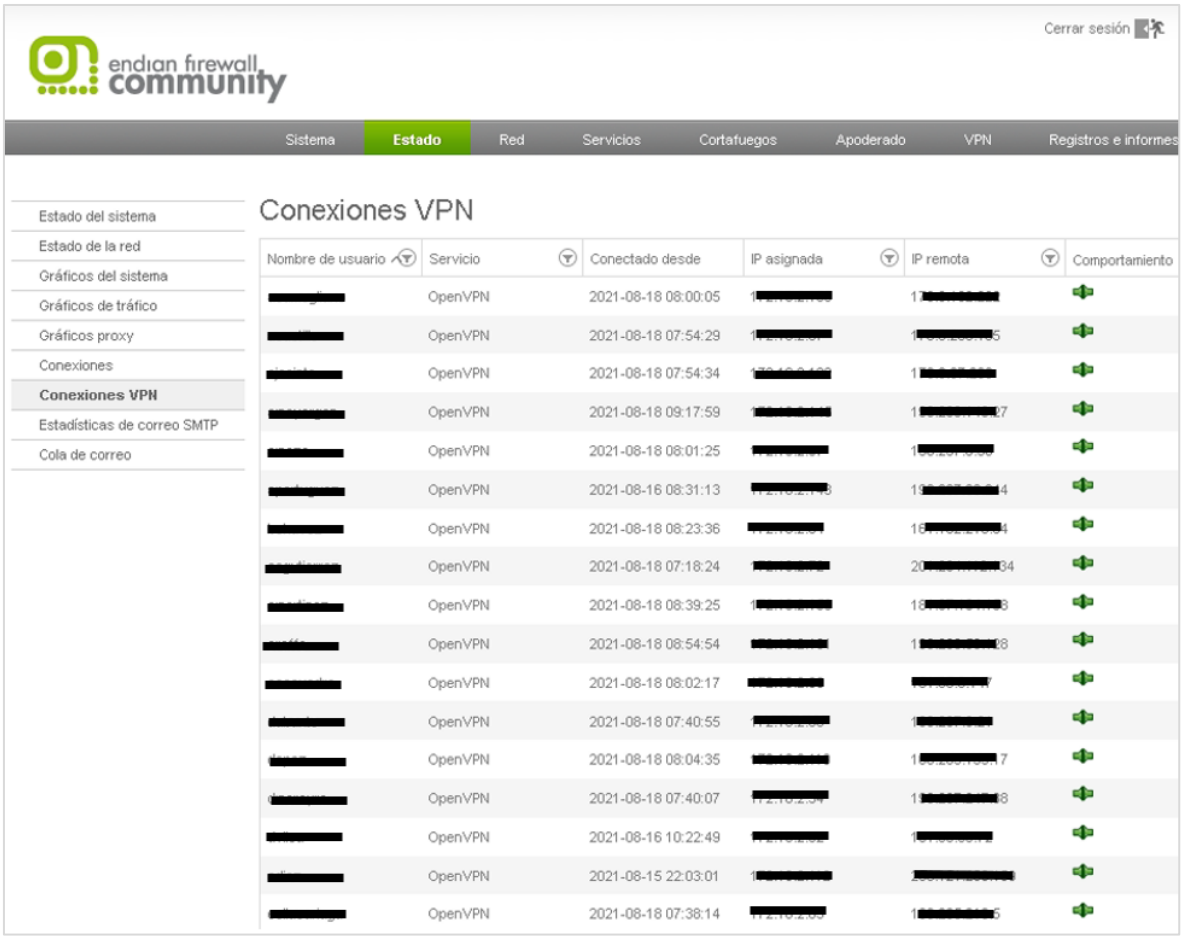


Figura 29. Monitoreo de la conexión VPN

Fuente: Elaboración Propia

En la figura 29 observamos que el firewall registra la fecha y hora en que lo usuarios realizan la conexión al VPN.

3.4.5. Cierre de la implementación

Finalmente se establece de manera formal el procedimiento donde se indica la forma de instalación, las diferentes modalidades en las que se puede brindar una conexión VPN, este fue presentado al área de Calidad para su gestión, autorización y publicación en el blog de la organización.

Figura 30. Publicación de Procedimiento para la conexión VPN

Fuente: Correo Corporativo de CLI Gestiones Aduaneras S.A.

En la figura 30 observamos la aprobación del documento donde se explica el procedimiento que se debe seguir para la conexión VPN.

3.4.6. Arquitectura de la Red Interna de la Organización CLI Gestiones Aduaneras S.A.

La organización presenta una red virtualizada en VMWare Esxi7, en donde se tienen diferentes servidores como el servidor de correos, el servidor de archivos, el servidor de la base de datos y el del Firewall Endian Comunity 3.2.5.

Además, cuenta con dos líneas de Internet, uno de Claro con 60 Mbps el cual es el principal y uno de América Móvil con 20 Mbps el cual es de contingencia, ambas líneas son administradas por el Firewall.

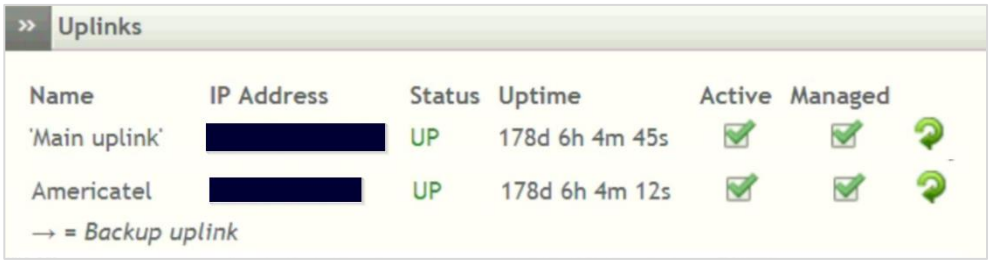


Figura 31. Administración de líneas UpLinks

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

En la figura 31 observamos las interfaces y enlaces Ascendentes, Uplinks, esta configuración permite tener más de una interfaz de red, en este se tiene la línea de Claro y de América Móvil activas, en cuanto el Firewall detecta que la principal cae, toma se segunda para que los usuarios no perciban la caída de la red principal.

3.4.6.1. **Arquitectura de la red antes de la implementación VPN:**

A continuación, se mostrará la arquitectura de la red antes de la implementación de la VPN:

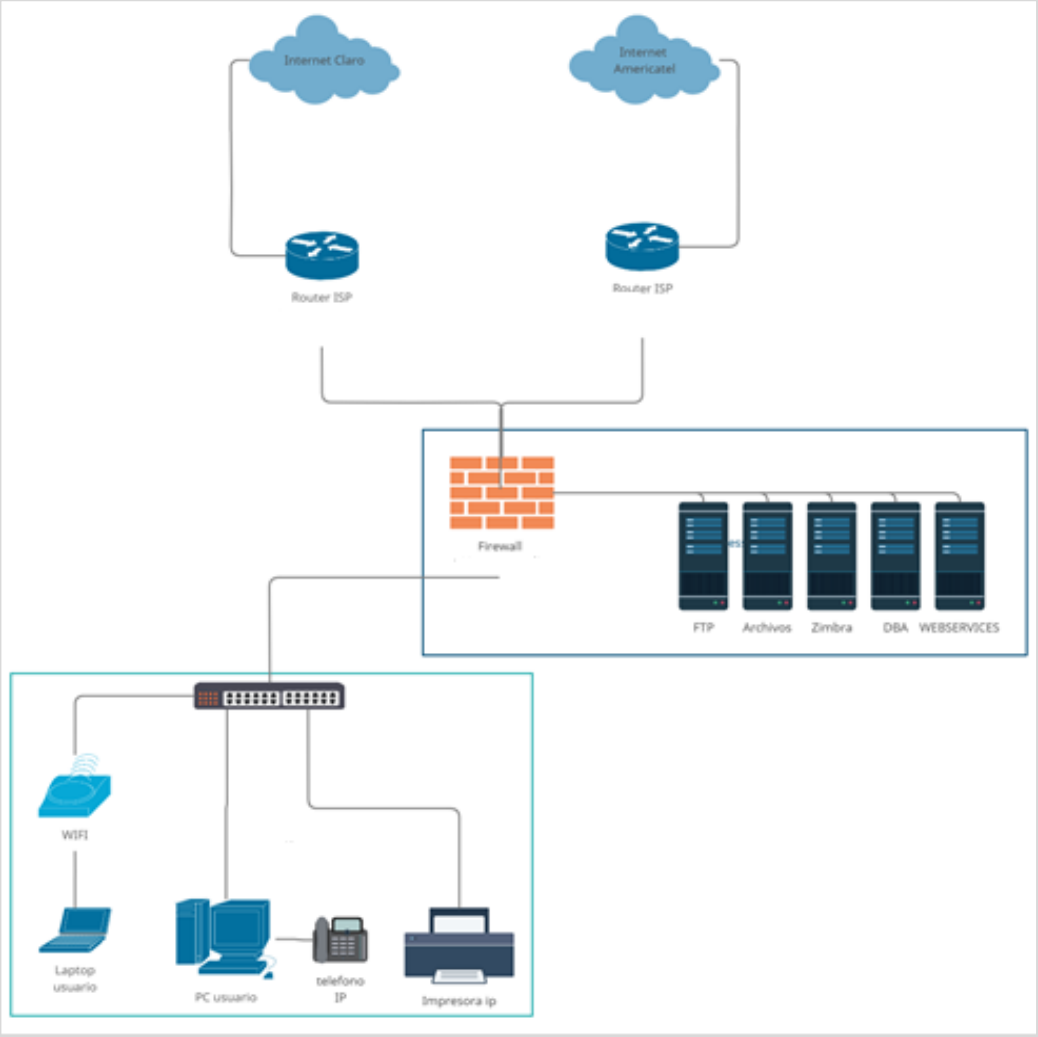


Figura 32. Arquitectura de la Red antes de la Implementación VPN
Fuente: Elaboración Propia

En la figura 32 observamos la arquitectura de la red interna de la organización, donde se muestra la virtualización de los servidores principales, la línea principal y la línea de contingencia de la red y así como la red LAN de la empresa.

3.4.6.2.**Arquitectura de la Red tras la implementación de VPN**

Tras la implementación de la VPN en la organización se diseñó el siguiente diagrama:

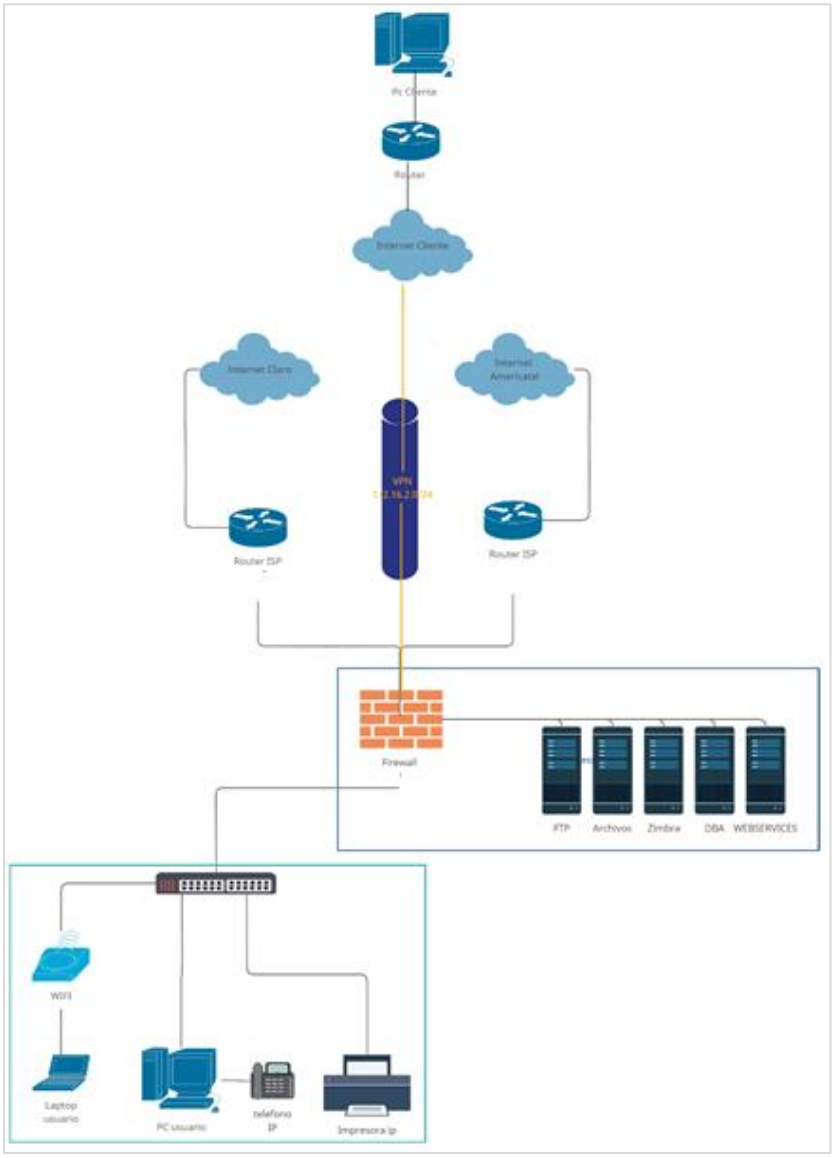


Figura 33. Arquitectura de la Red tras implementación de la VPN

Fuente: Elaboración Propia

En la figura 33 observamos el diseño de la red tras la implementación de la VPN, para mejorar las conexiones se aumentaron ambas líneas de internet, la principal de Claro 90 Mbps 1 a 1 fibra y la de contingencia de América Móvil a 40 Mbps 1 a 1 fibra.

3.4.7. Procedimiento de Conexión Remota

Para la conexión remota en un principio se realizó accediendo a máquinas virtuales mediante una IP Nateada con un puerto respectivo que hacía referencia a la máquina virtual a la cual estaría conectándose el usuario. Conexión

3.4.7.1. **Procedimiento de Conexión Remota antes de la VPN**

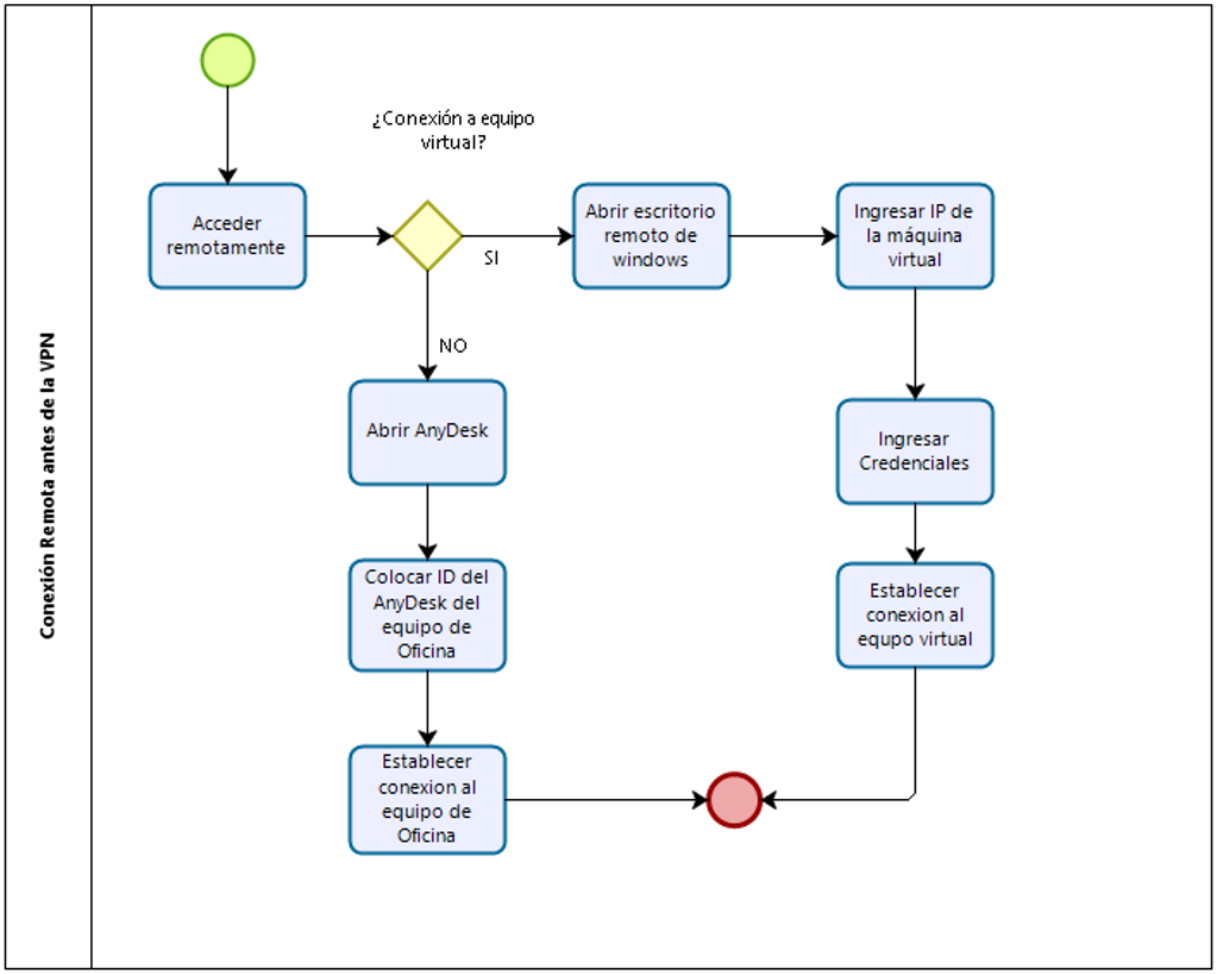


Figura 34. Diagrama de Flujo de las conexiones remotas antes de la implementación VPN

Fuente: Elaboración Propia

En la figura 34, observamos el flujo que seguían los usuarios para poder establecer conexión remota a las máquinas virtuales asignadas. Como política de la empresa no se permitía que se instale en los equipos personales de los usuarios los principales sistemas, por esa razón los usuarios se conectaban a equipos virtuales donde se encontraban instalados los principales sistemas, sin embargo, en algunos casos los usuarios necesitaban cierta información que se encontraba en los equipos de oficina, por ello, para ese tipo de acceso los usuarios se conectaban por medio del AnyDesk.

3.4.7.2.**Procedimiento de Conexión Remota después de la implementación de la VPN**

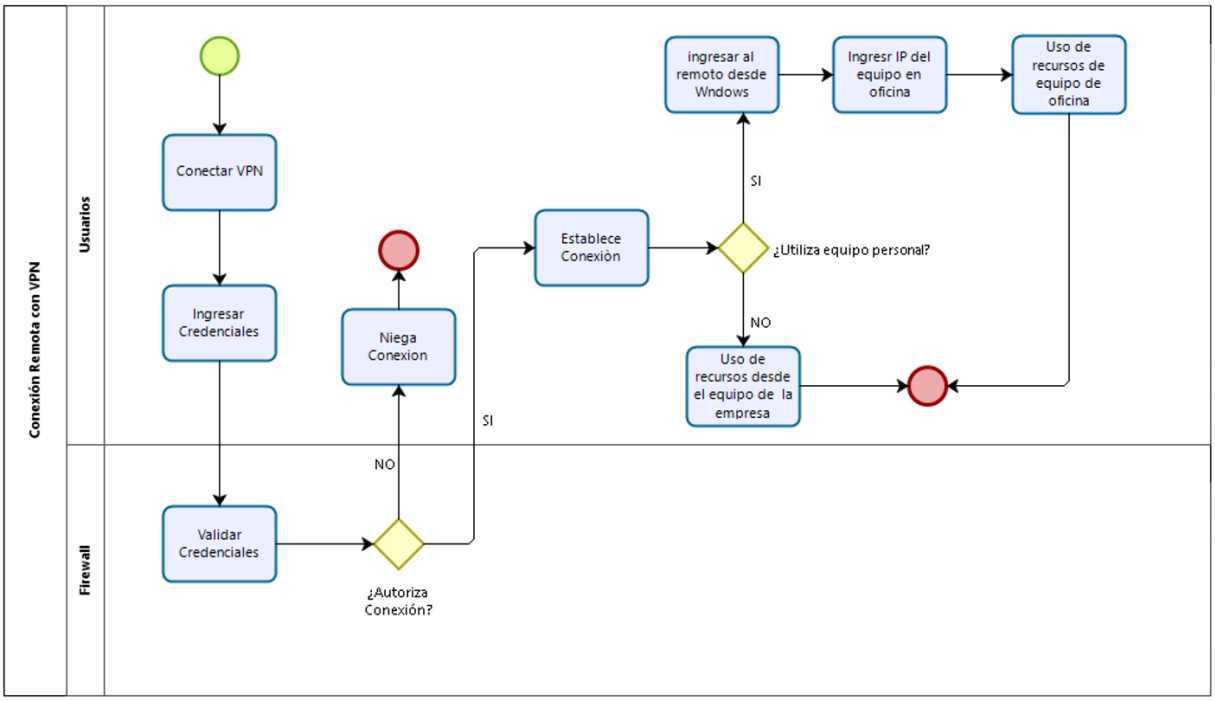


Figura 35. Diagrama de Flujo de la Conexión Remota por medio la VPN
Fuente: Elaboración Propia

En la figura 35 se observa el proceso que debe seguir un usuario para poder establecer conexión remota mediante la VPN. En el caso de los usuarios que se

encontraban dentro del grupo del personal vulnerable, quienes tenían los equipos de oficina en sus hogares, solo activaban el VPN y accedían a todos los recursos del equipo como si estuvieran en oficina. En el caso de los usuarios que iban una semana intercalada, se conectaban desde sus equipos personales o equipos prestados por la agencia hacia sus equipos de oficina por medio de conexión a escritorio remoto de Windows tras activar la VPN.

CAPÍTULO IV. RESULTADOS

4. Resultados obtenidos tras la Implementación de la VPN

4.1. Resultados de los Incidentes reportados Pre y Pos Implementación de la VPN:

Durante los meses de Julio, Agosto y Septiembre, se realizó un monitoreo de incidentes reportados para que puedan ser comparados con los incidentes obtenido el mes de mayo antes de la implementación de la VPN.

Para ello se clasifican las incidencias y se obtiene la siguiente información:

Tabla 3. Total de incidentes del trabajo remoto sin VPN en el mes de Mayo

Tipos de Incidentes	MES	# Eventos	Porcentaje de Eventos
FALTA DE ACCESO A SISTEMAS Y ARCHIVOS	MAYO	30	17%
PROBLEMAS CON LA CONEXIÓN REMOTA	MAYO	100	56%
PROBLEMAS CON EL CORREO	MAYO	27	15%
LENTITUD EN SISTEMAS	MAYO	20	11%
Total general		**177**	**100%**

Fuente: Elaboración Propia

En la tabla 3 se observa de manera resumida los constantes incidentes reportados en el mes de mayo antes de la implementación de la VPN, es decir muestra las incidencias reportadas durante el trabajo remoto mediante una IP pública la cual le daba acceso a una máquina virtual.

En las siguientes tres tablas, se observan las incidencias reportadas durante la conexión por VPN. Los usuarios se conectaban hacia sus equipos de oficina, y en el caso del personal vulnerable, quienes tenían equipos de CLI en sus hogares, accedía a los sistemas y recursos como si estuvieran en oficina estableciendo solo la conexión VPN.

Tabla 4. Total de incidentes en el trabajo remoto con VPN en el mes de Julio

Tipos de Incidentes	MES	# Eventos	Porcentaje de Eventos
FALTA DE ACCESO A SISTEMAS Y ARCHIVOS	JULIO	0	0%
PROBLEMAS CON LA CONEXIÓN REMOTA	JULIO	70	65%
PROBLEMAS CON LOS CORREO	JULIO	19	18%
LENTITUD EN SISTEMAS	JULIO	18	17%
Total general		**107**	**100%**

Fuente: Elaboración Propia

En la tabla 4 observamos el resumen de las incidencias reportadas en el mes de julio, durante el primer mes del monitoreo del trabajo remoto con la VPN.

Tabla 5. Total de incidentes en el trabajo remoto con VPN en el mes de Agosto

Tipos de Incidentes	MES	# Eventos	Porcentaje de Eventos
FALTA DE ACCESO A SISTEMAS Y ARCHIVOS	AGOSTO	0	0%
PROBLEMAS CON LA CONEXIÓN REMOTA	AGOSTO	8	19%
PROBLEMAS CON LOS CORREO	AGOSTO	10	24%
LENTITUD EN SISTEMAS	AGOSTO	10	24%
Total general		**42**	**67%**

Fuente: Elaboración Propia

En la tabla 5 observamos el resumen de las incidencias reportadas en el mes de agosto, durante el primer mes del monitoreo del trabajo remoto con la VPN.

Tabla 6. Total de incidentes en el trabajo remoto con VPN en el mes de Setiembre

Tipos de Incidentes	MES	# Eventos	Porcentaje de Eventos
FALTA DE ACCESO A SISTEMAS Y ARCHIVOS	SETIEMBRE	0	0%
PROBLEMAS CON LA CONEXIÓN REMOTA	SETIEMBRE	7	39%
PROBLEMAS CON LOS CORREO	SETIEMBRE	3	17%
LENTITUD EN SISTEMAS	SETIEMBRE	8	44%
Total general		**18**	**100%**

Fuente: Elaboración Propia

En la tabla 6 observamos el resumen de las incidencias reportadas en el mes de setiembre, durante el primer mes del monitoreo del trabajo remoto con la VPN.

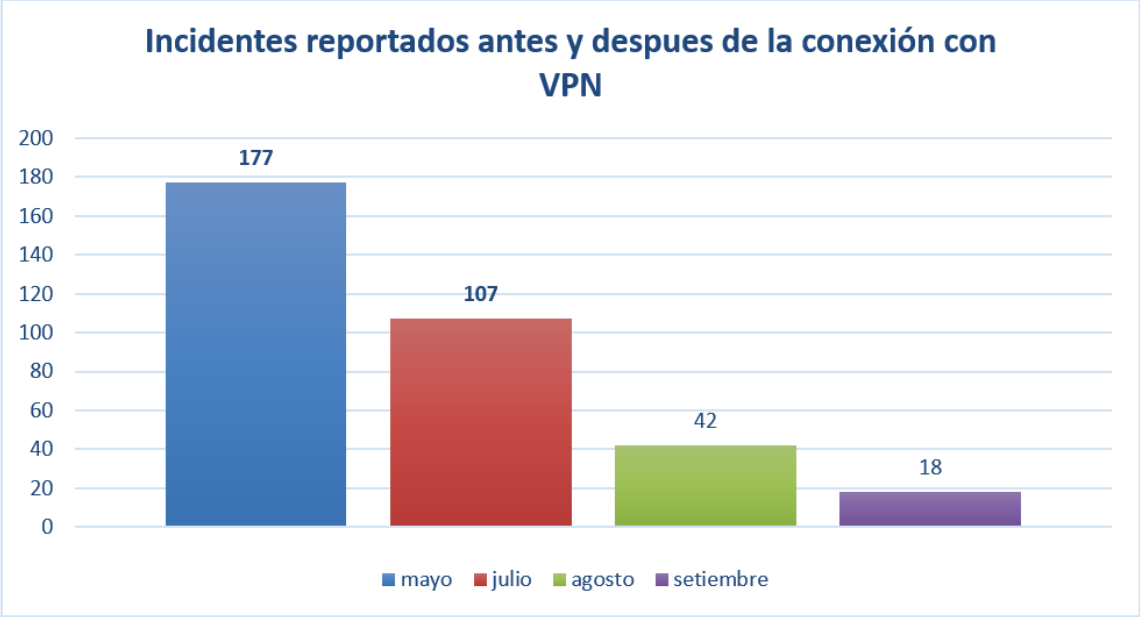


Figura 36. Incidentes reportados antes y después de la implementación de la VPN

Fuente: Elaboración Propia

En la figura 36 se observa que, en el mes de mayo, donde aún no se implementaba la VPN se reportaron 177 incidentes con la conexión remota, así mismo se observa que en el periodo de monitoreo (julio, agosto, setiembre) tras la implementación de la VPN la cantidad de incidencias reportadas fueron disminuyendo.

Durante los meses de julio a setiembre se observan las incidencias reportadas de la siguiente manera:

Figura 37. Incidentes reportados sobre la conexión remota por VPN

Fuente: Elaboración Propia

La figura 37 muestra el número de incidentes que se reportaron durante los meses de julio a setiembre asociadas a los problemas con la conexión remota, los cuales se observan que en julio se presentaron 70 inconvenientes de los cuales, en su mayoría, fueron por temas de errores en la conexión VPN hasta que los usuarios se adecuaron a la nueva modalidad de conexión, por ello en los meses de agosto y setiembre se observa que los incidentes reportados se mantienen de 7 a 8 por mes.

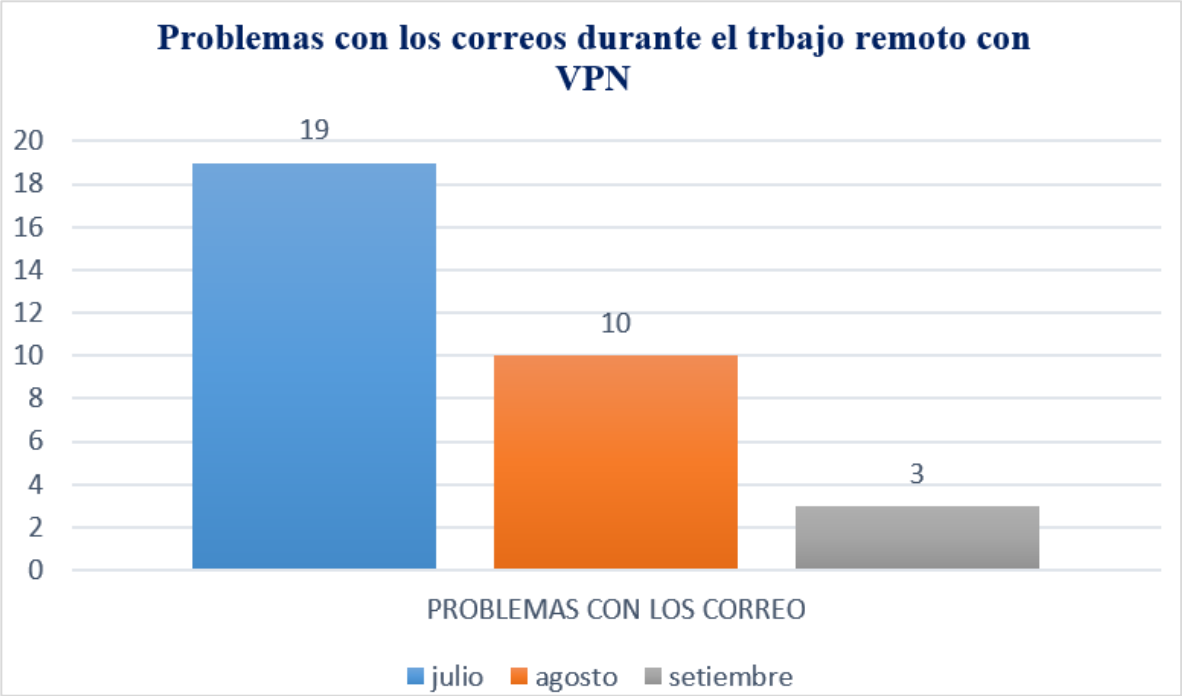


Figura 38: Problemas con los correos durante el trabajo remoto con VPN

Fuente: Elaboración Propia

En la figura 38 se observan los problemas reportados asociados a los correos, donde observamos que estos disminuyeron de julio a setiembre. En julio se observa que se presentan 19, de los cuales en su mayoría fue por lentitud en la recepción ya que el servidor se encontraba saturado, tras la liberación del espacio los incidentes disminuyeron ya que al conectarse a los equipos de oficina contaban con el Outlook el cual les permitía manejar el filtro y búsqueda de correos de forma más exacta.

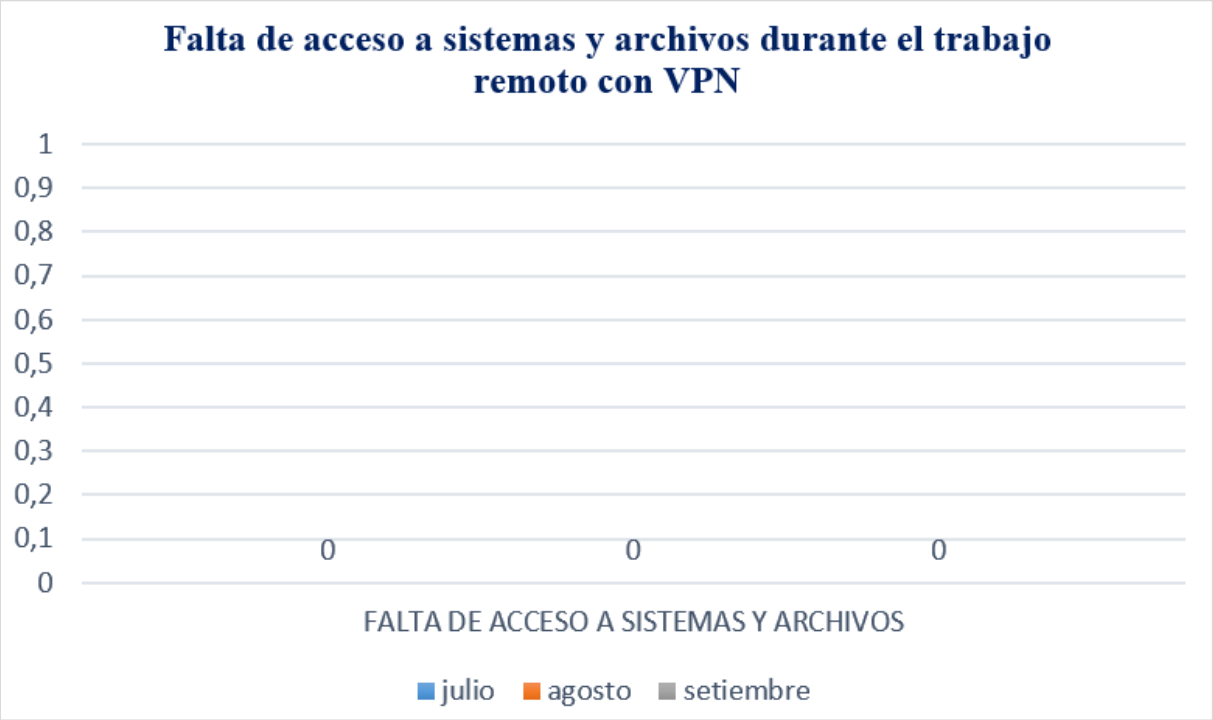


Figura 39: Falta de acceso a sistemas y archivos durante el trabajo remoto con VPN

Fuente: Elaboración Propia

En la figura 39 observamos que en cuanto se inició el trabajo remoto con VPN este inconveniente desapareció ya que los usuarios al tener accesos a sus equipos de oficina, contaban con todos los sistemas y archivos que requerían para su trabajo desempeñado en el día a día.

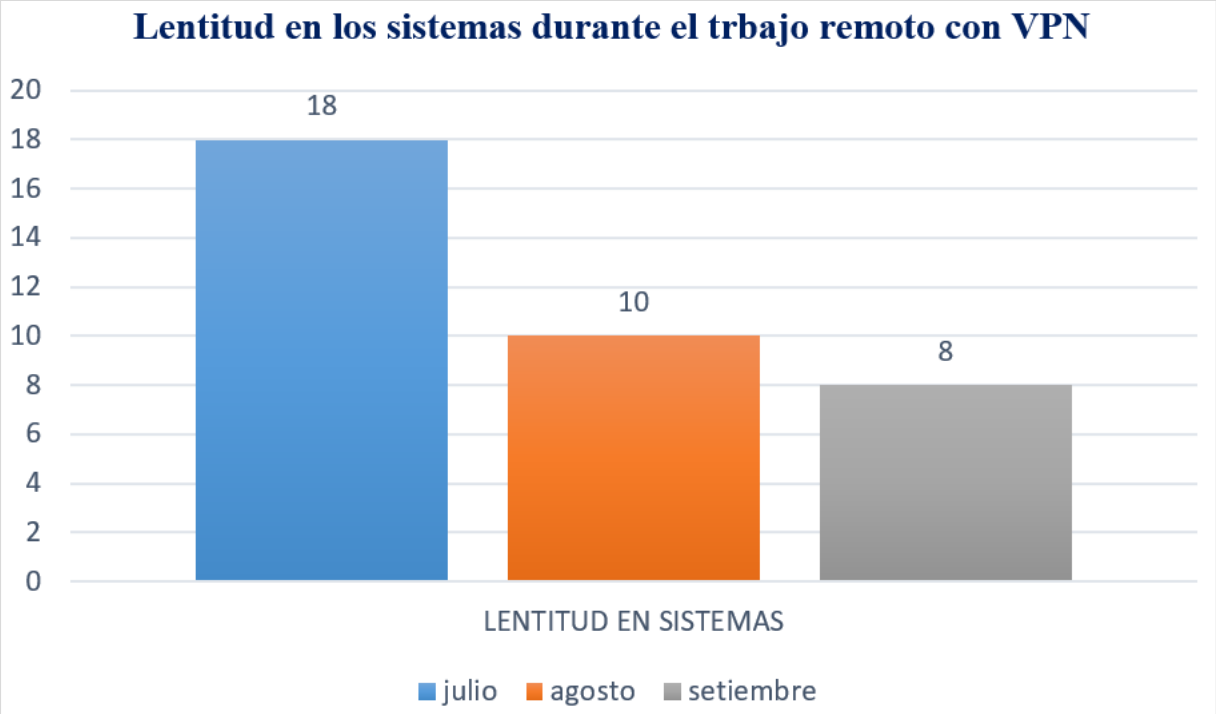


Figura 40. Incidencias reportadas sobre la lentitud de los sistemas durante el periodo de monitoreo del trabajo remoto con VPN
Fuente: Elaboración Propia

La figura 40 muestra el número de incidentes que se reportan con respecto a inconvenientes relacionados a la lentitud de los sistemas, los cuales disminuyeron al tener acceso a los sistemas dentro de la red de la empresa conectándose por VPN.

4.2.Control y monitoreo en el trabajo remoto:

El Firewall nos permite monitorear a los usuarios y sus conexiones, de esa forma se pudo mantener un control del personal para verificar que se conecten en el horario laboral correspondiente.

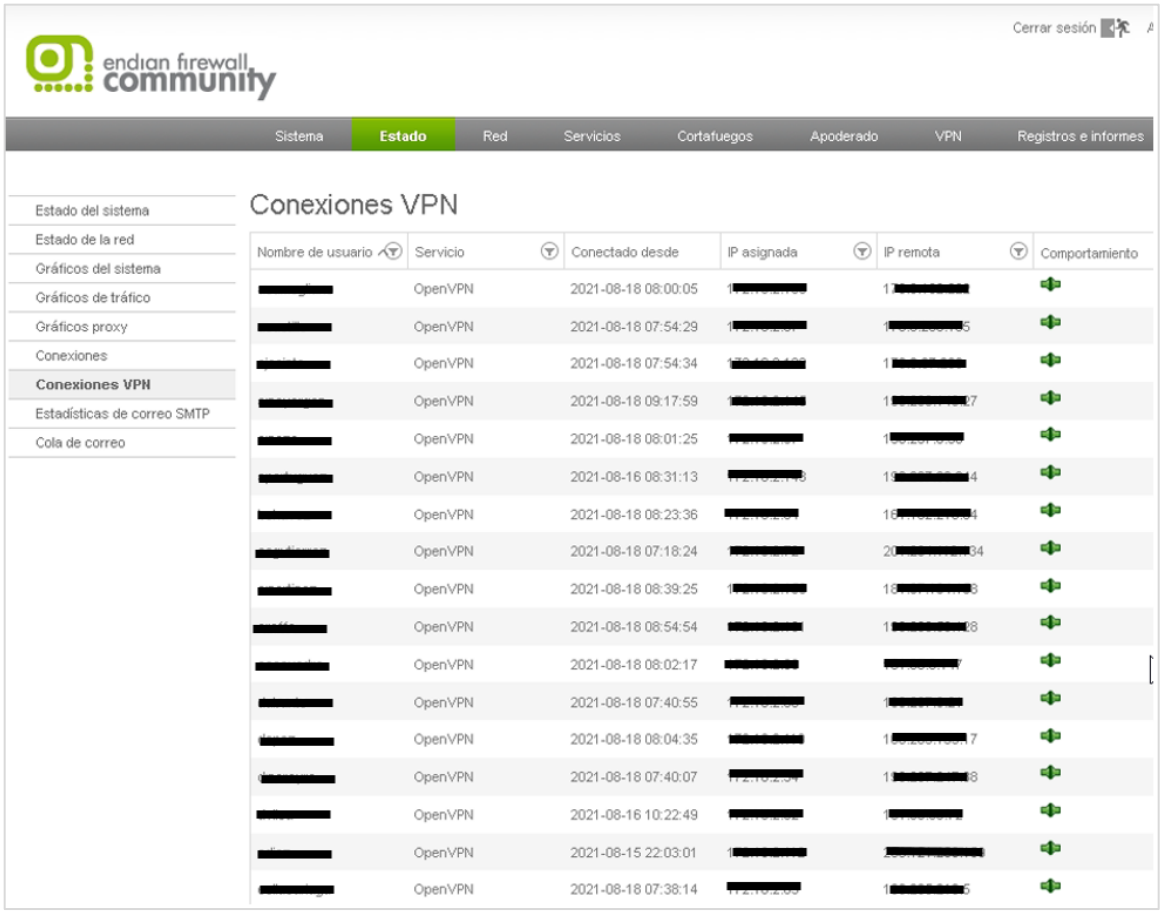


Figura 41. Monitoreo de las conexiones VPN

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

En la imagen 41 se observa las conexiones establecidas por los usuarios por medio de la VPN, donde se registra el usuario, el servicio usado, la fecha y hora de conexión, la IP asignada, la IP remota y su comportamiento.

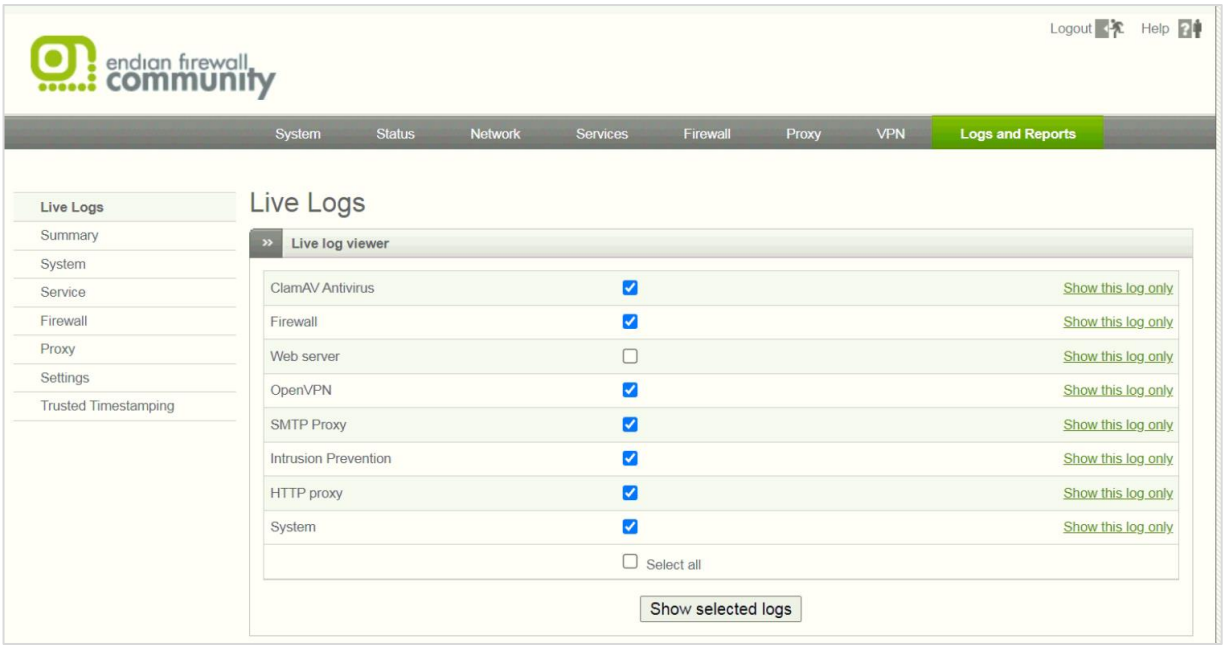


Figura 42. Logs y Reportes de Endian Firewall Comunity

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

En la figura 42 observamos que Endian Firewall Comunity tiene una sección de logs y reportes, entre ellos ubicamos los Log de las conexiones con OpenVPN.

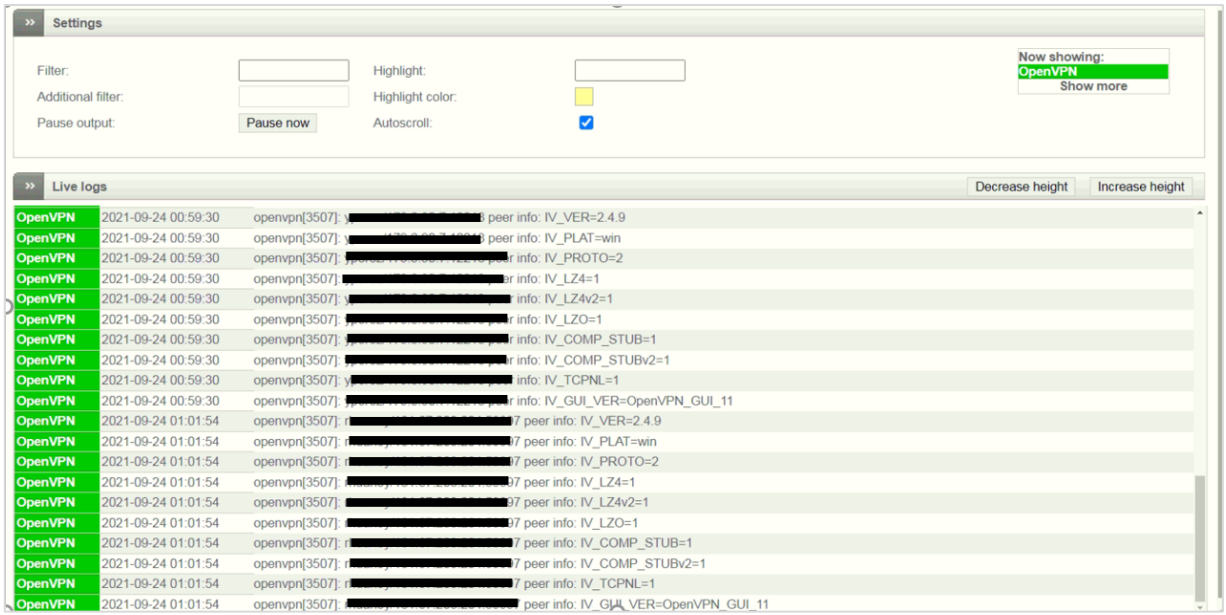


Figura 43. Live Logs Open VPN

Fuente: Firewall de CLI Gestiones Aduaneras S.A.

En la figura 43 observamos los log que guarda el Firewall con respecto a las conexiones establecidas por los usuarios mediante la VPN.

Además, estas conexiones durante el día son notificaban al correo del Supervisor de Sistemas, donde por cada conexión remota autorizada llega un correo de alerta indicando el nombre del usuario que realiza la conexión.

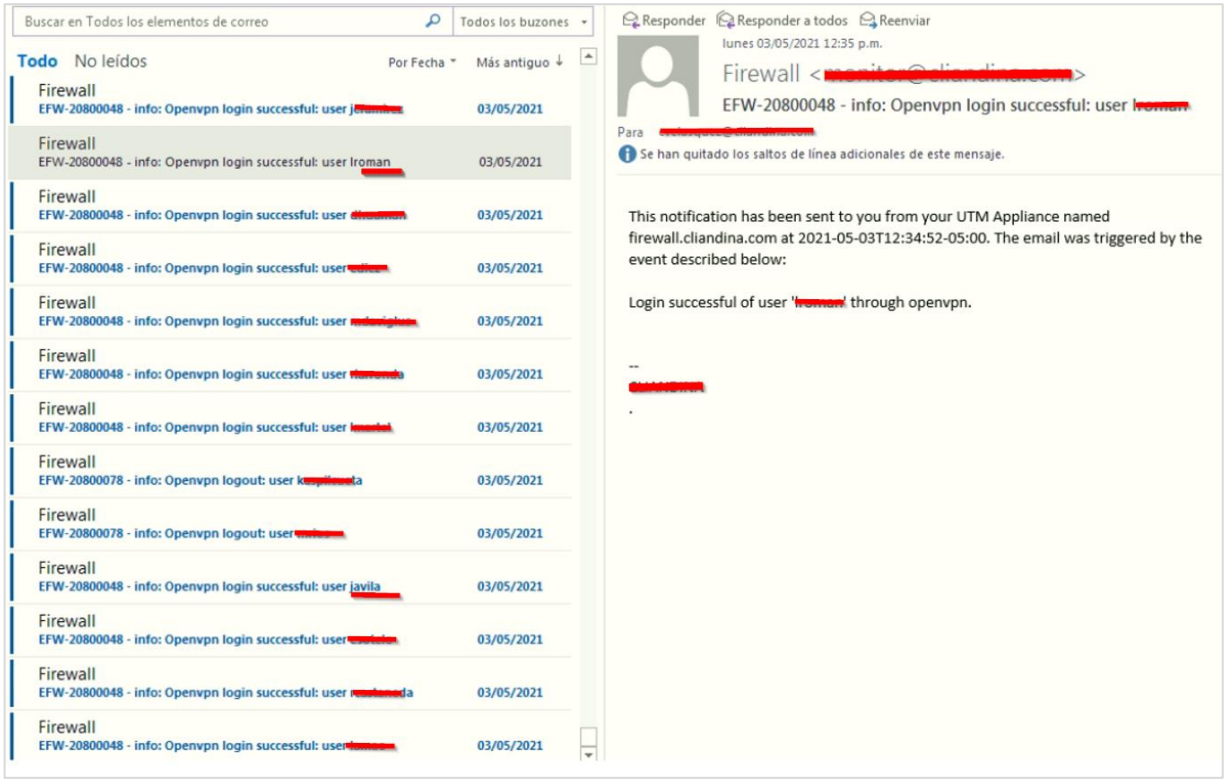


Figura 44. Notificaciones vía correo electrónico de las conexiones remotas realizadas por la VPN

Fuente: Correo electrónico del supervisor de sistemas de CLI Gestiones Aduaneras S.A.

Gracias a estos reportes se puede establecer un mejor control del acceso de los usuarios, los horarios en los que se conectan, así como las posibles pérdidas de conexión que pueden presentarse, esto con el fin de poder respaldar el trabajo remoto realizado por los usuarios.

4.3.Resultados de la productividad Pre y Pos la Implementación de la VPN:

Con respecto a la productividad de los colaboradores se obtiene un reporte del sistema SINTAD en el cual observamos lo siguiente:

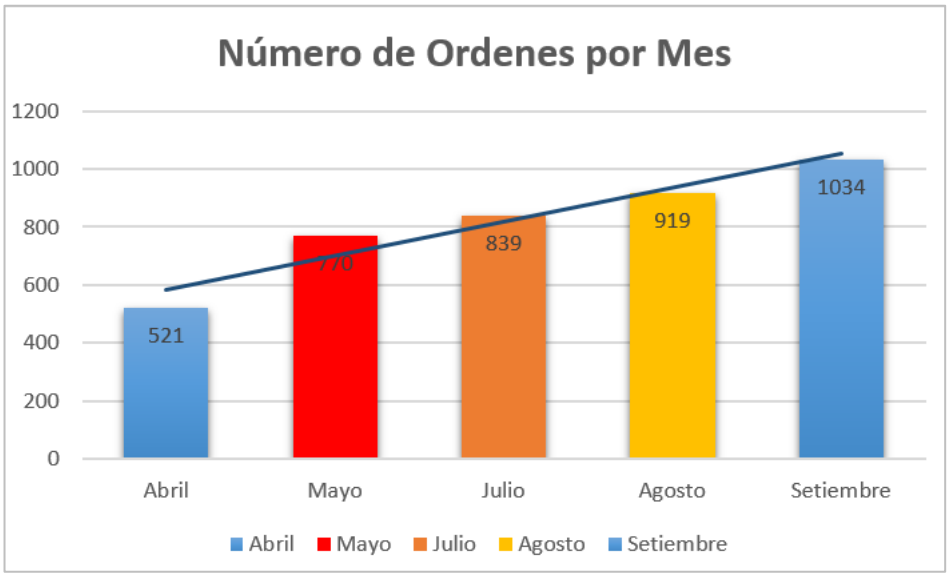


Figura 45: Número de Órdenes por mes 2020

Fuente: Elaboración Propia

En la figura 44 se observa el número de órdenes que son numeradas mensualmente por los liquidadores de la empresa CLI Gestiones Aduaneras S.A. en el gráfico observamos que durante el periodo de abril a mayo del 2020 cuando no se trabajaba con la VPN, los problemas presentados en la conexión para el trabajo remoto hacía que no se pudieran numerar ordenes de manera eficiente en el día por ello al implementar la VPN y conectándose los usuarios en especial los liquidadores de esa manera, mejoraron la productividad ya que tenían una conexión más fluida y esto logró que aumentaran la cantidad de ordenes numeradas al mes.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5. Conclusiones

5.1. Conclusiones Generales

El problema principal presentado en la organización tras el comienzo del trabajo remoto decretado por el gobierno en el Decreto de Urgencia Nº 026-2020 a causa del Covid 19, fue la deficiencia presentada en el trabajo remoto, por tal razón gracias a las competencias adquiridas en la universidad logré implementar una red VPN que brindó un mejor servicio para que los usuarios puedan conectarse de manera remota a todos los recursos de la organización y de una manera más segura, lo cual de acuerdo a los resultados obtenidos, se observa que las incidencias reportadas fueron disminuyendo de manera significativa, ya que de un total de **177** incidentes reportadas en el mes de mayo, antes de la conexión mediante VPN, éste se redujo a solo **18** incidentes reportadas usando la conexión mediante la VPN, logrando mejorar la calidad en el acceso y seguridad de los sistemas y servicios de la red en el trabajo remoto.

5.2. Conclusiones Específicas

- Los incidentes reportados por la conexión remota antes de la implementación de la VPN fueron en su mayoría debido a la cantidad de usuarios conectados a las máquinas virtuales creadas lo cual producía inestabilidad en la conexión remota, por tal razón cuando se implementó la VPN se realizaron las configuraciones necesarias en el UTM para obtener una conexión más estable ya que de **100** incidentes reportados antes de la implementación de la VPN se logró un mínimo de **7 a 8** incidentes reportados por problemas de estabilidad.

- Las sucursales de la empresa que se encontraban en Paita, Tacna, Mollendo, Ilo e Ica requerían de ciertos formatos (documentos) los cuales eran obtenidos del sistema SINTAD, por tal motivo para poder acceder a ellos eran necesario brindarles conexión a una de las máquinas virtuales, a la cual se le tenía que habilitar un puerto público, el estar abriendo y cerrando puertos constantemente hacía vulnerable la red, ya que se estaba expuesto ante posibles ataques de los ciberdelincuentes, más aún porque no siempre se informaba que ya se había culminado la operación a realizar o que ya no requerían del acceso para poder cerrar el puerto de manera inmediata. Por tal razón el implementar la VPN hizo que ya no se tenga la necesidad de abrir y cerrar puertos, ya que con solo activar la VPN en los equipos podían conectarse de manera remota al sistema de SINTAD y descargar los formatos que requerían, logrando una conexión más segura ya que permite que el tráfico de datos sea guiado hacia un túnel, lo cual es más seguro.
- Muchos de los incidentes reportados por lo cual los usuarios no lograban realizar un buen trabajo remoto era la falta de accesos a diferentes sistemas y recursos que estos tenían en los equipos de oficina ya que los usuarios se conectaban a una máquina virtual configurada de manera general, por ello una vez implementada la VPN y al establecerse la conexión a los equipos de la empresa, los usuarios lograban acceder a los sistemas y recursos de la red corporativa mediante la conexión VPN como si estuvieran en oficina, esta mejora no solo fu para el personal que se conectaba a los equipos de oficina, si no que a aquello usuarios que se les había entregado equipos corporativos, al conectarse a la VPN accedían a todos los sistemas y recursos en los equipos sin inconveniente. Por

ello gracias a la conexión VPN estos incidentes desaparecieron, ya que pasaron de **30** incidentes reportados antes de la VPN a **0** incidentes durante los meses en que se trabajó con la VPN.

- Antes de la implementación de la VPN no había forma de saber si los usuarios se conectaban durante el trabajo remoto dentro del horario laboral, pero con la implementación de la VPN esto se pudo lograr, ya que el firewall mostraba las conexiones remotas realizadas por los usuarios, registrando la fecha y hora de las conexiones, además estas conexiones llegaban al correo electrónico del supervisor de Sistemas donde podía monitorear las conexiones realizadas. Por tal razón la VPN permitió monitorear la productividad de los colaboradores durante del trabajo remoto.

5.3.Lecciones Aprendidas

- Se logró entender la importancia que tiene un firewall dentro de una organización, ya que este permite protegerla de los peligros que pueden asecharla desde el internet, además que hoy en día los firewalls ofrecen muchas más características que permitirán proteger la red de una organización.
- Se logró comprender que para conseguir una conexión eficaz y seguro en el trabajo remoto en una organización es muy importante la implementación de una VPN, ya que les permitirá a los colaboradores una mejor accesibilidad a los recursos de la empresa y seguridad en el cifrado del tráfico.
- Se logró comprender la importancia de la seguridad en las conexiones que puedan realizar los colaboradores en el trabajo remoto, ya que muchos se pueden conectar a

redes inseguras, lo cual podría vulnerar la red, sin embargo, mediante la conexión VPN ya que esta permite mantener la privacidad y seguridad en las conexiones.

- Se logra percibir que hoy en día el trabajo remoto ha incrementado mucho en las organizaciones y establecer una buena configuración permitirá mantener a todos los colaboradores conectados desde cualquier dispositivo de manera segura para la organización.
- Se logra evidenciar que debido al trabajo remoto los ataques cibernéticos han incrementado, por ello es muy importante contar con una VPN que brinde un buen cifrado y una autentificación robusta de esta manera se puede salvaguardar la información de la red VPN.

5.4.Recomendaciones.

- Se sugiere que para establecer una mejor calidad en el acceso y seguridad de los sistemas y servicios de la red en el trabajo remoto se pueda migrar o implementar el Firewall en un servidor físico, ya que la organización cuenta con todos sus servidores virtualizados en un hipervisor, esto hace que todos compartan los recursos del servidor donde están implementados, por ello los recursos que puede consumir el Firewall se ven limitados. Utilizando un Firewall de Hardware se lograría integrar en un solo elemento el hardware y el software para un dispositivo Firewall, logrando tener una protección más completa en la administración de la red, así como la velocidad y el rendimiento permanecerían intactos.
- Se sugiere se pueda considerar el obtener un firewall de Fortinet ya que de acuerdo a Gartner Magic Quadrant lo considera como el firewall líder, esto a fin de poder mejorar

la estabilidad de las conexiones remotas, ya que éste ofrece una amplia cantidad de características para la configuración y administración de una red corporativa, como se sabe actualmente se está trabajando con Endian Firewall Comunity, el cual ofrece características básicas y limitadas puesto que está asociado para operar en hogares o pequeñas empresas, hoy por hoy CLI Gestiones Aduaneras ha crecido mucho en los últimos años por ello se podría mejorar en la administración de la red, entre ellas la configuración VPN estabilizando las conexiones gracias a un soporte amplio de usuarios ya que tiene un enfoque corporativo.

- Se sugiere que para mejorar la seguridad en las conexiones remotas se establezca un nivel de protección más robusta como el doble factor de autentificación para evitar posibles ataques cibernéticos ya que el doble factor es mucho más seguro que las contraseñas puesto que garantizan que los atacantes tendrían que “trabajar más duro”, no es una solución infalible, pero es una capa extra que permitirá que no seas un blanco fácil para los atacantes. Para ello se puede implementar el acceso VPN con doble factor ya que Open VPN lo permite, se pueda evaluar la doble autentificación con miniOrange 2FA para el inicio de sesión en los equipos de los usuarios al conectarse al OpenVPN, otra opción de doble factor se encuentra en el Endian UTM.
- Se sugiere se pueda establecer un balanceo de carga y utilizando el protocolo HSRP, se permitirá redundancia en la red, en este caso para las conexiones a dos proveedores de internet distintos que se tiene en la empresa (Claro y América Móvil) y en el caso que uno de los ISP deje de funcionar por alguna falla en la conectividad el tráfico se dirigirá hacia el otro ISP de manera dinámica.

REFERENCIAS

CLI Gestiones Aduaneras. (s.f.). Nuestra Historia. Consultado el 17 de agosto del 2021. https://www.cli.com.pe/nosotros.php

CLI Gestiones Aduaneras. (s.f.). Servicios. Consultado el 19 de agosto del 2021. https://www.cli.com.pe/servicios.php

CLI Gestiones Aduaneras. (s.f.). Clientes. Consultado el 20 de agosto del 2021. https://www.cli.com.pe/clientes.php

CLI Gestiones Aduaneras. (s.f.). Clientes. Consultado el 20 de agosto del 2021. https://www.cli.com.pe/operadores.php

Diario El Peruano (2020). Decreto Supremo N° 046-2020-PCM. Consultado el 20 de agosto del 2021. https://www.gob.pe/institucion/pcm/normas-legales/462244-046-2020-pcm

Martínez, J. (2000). Administración de la producción como ventaja competitiva.70-72.

Chunga, G. (2017). El estudio y la investigación documental: estrategias metodológicas y herramientas TIC .49-50.

Koch, Richard. (2015). El principio del 80/20: El secreto de lograr más con menos. 3-11.

Tomás, Joaquín. (2009). Fundamentos de bioestadísticas y análisis de datos para enfermería. 32-39.

Endian. (2008). Manual de referencia de Endian Firewall. Consultado el 21 de agosto del 2021. http://docs.endian.com/archive/2.2/efw.vpn.html

VMWare (s.f.). ¿Qué es un hipervisor?. Consultado el 27 de agosto del 2021. https://www.vmware.com/latam/topics/glossary/content/hypervisor.html

Endian. (s.f.). Solución UTM de código abierto gratuita para redes domésticas. Consultado el 27 de agosto del 2021. https://www.endian.com/de/community/

Cisco. (s.f.). ¿Qué es una VPN? - Red privada virtual. Consultado el 28 de agosto del 2021. https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Centro Criptológico Nacional de España. (2017). Guía de Seguridad de las TIC CCN-STIC 836. 9-11.

VMWare (s.f.). VMware ESXi: el hipervisor bare metal diseñado a medida. Consultado el 01 de setiembre del 2021. https://www.vmware.com/latam/products/esxi-and-esx.html

Tanenbaum, A. y Wetherall, D. (2012). Redes de Computadoras Firewalls. Pearson Educación de Mexico. Quinta Edición.

Tanenbaum, A. y Wetherall, D. (2012). Informática Forense y software libre, Poniendo en marcha un estacón de trabajo con SLAckware13.0.

Diario El Peruano. (2020, 26 de marzo) Guía para la aplicación del Trabajo remoto. https://www.gob.pe/institucion/mtpe/normas-legales/462526-072-2020-tr

Yonan, J. (2018). Manual de referencia para OpenVPN 2.4. Consultado el 02 de Setiembre del 2021. https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

Niño, F. (2020). Diseño De Un Modelo De Virtualización Para La Implementación De Un Sistema De Servidores En Alta Disponibilidad (Trabajo para optar por el título de Ingeniero de Sistemas). UNIVERSIDAD COOPERATIVA DE COLOMBIA, Bogotá.

Gutiérrez, A. (2014). Virtualización de Servidores de la Infraestructura informática de la Universidad de Quintana Roo, Unidad Chetumal (Tesis para la obtención del grado de Ingeniero en Redes). Universidad de Quintana Roo, México.

Toala, E. (2021). Análisis De Un Software Libre De Administración Remota Para Prácticas De Los Estudiantes En El Laboratorio De Telecomunicaciones De La Universidad Estatal Del Sur De Manabí (Proyecto De Investigación previa a la obtención del Título de: Ingeniero en Computación y Redes). Universidad Estatal del Sur de Manabí, Ecuador.

Guijarro, A., Tapia, J., Viteri, X y Zambrano J. (2018). Guía de Prácticas de Endian. ISBN: 978-9942-770-36-3.

Martel, V. (2019). Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764 (Proyecto de Investigación para obtener el título profesional de Ingeniero de Redes y Comunicaciones). Universidad Pedro Ruiz Gallo, Chiclayo - Perú.

Espinoza, C. (2018). Propuesta De Una Red Privada Virtual Para Mejorar El Servicio De Comunicación En Las Tiendas Mass Para La Empresa Supermercados Peruanos S.A. (Proyecto de investigación para obtener el título de Ingeniero de Sistemas). Universidad Autónoma del Perú, Lima.

De la Cruz, S. y Vera, J. (2019). Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo (Tesis Para optar el título profesional de ingeniero en computación e informática). Universidad Pedro Ruiz Gallo, Chiclayo - Perú.

Quezada, H. (2016), Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja (Tesis previa a obtener el Título de Ingeniero en Sistemas). Universidad Nacional de Loja, Loja – Ecuador.

Cansino, D. (2012). Diseño e Implementación de una Red Privada Virtual Segura para las Oficinas de Caminosca S.A basado en plataforma Gnu/Linux (tesis previa a la obtención del título de ingeniero de sistemas). Universidad Politecnica Saleciana de Quito, Ecuador.

Almachi, P. y Chiluisa, C. (2010). Implementación de una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP FLOWERS ubicada en el cantón Latacunga (Tesis de Grado Previo a la Obtención del Título de Ingeniero en Informática y Sistemas Computacionales.). Universidad Técnica De Cotopaxi, Ecuador.

COMEXPERU, (2021). El número de mypes peruanas se redujo un 48.8% en el 2020 y la informalidad pasó al 85% como consecuencia de la Pandemia. Consultado el 24 de Setiembre del 2021. https://www.comexperu.org.pe/articulo/el-numero-de-mypes-peruanas-se-redujo-un-488-en-2020-y-la-informalidad-paso-al-85-como-consecuencia-de-la-pandemia

ANEXO n.° 1. Incidencias Reportadas en el mes de Mayo

AREA	SOLICITUD	TIPO
ESC	Pérdida en el servicio de correo	CORREO
RRHH	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Falta de Recursos en CLINET	SISTEMA
ESC	Falta de Recursos en el Servidor de Correos	CORREO
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
LIQUIDACION	Actualización de SINTAD produce alto tráfico de red	SISTEMA
LEGAL	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
SEGUIMIENTO	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Pérdida en el servicio de correo	CORREO
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
RRHH	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Falta de Recursos en el Servidor de Correos	CORREO
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
CALIDAD	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ADMINISTRACION	Pérdida en el servicio de correo	CORREO
ESC	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ESC	Falta de Recursos en el Servidor de Correos	CORREO
REVISOR	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ADMINISTRACION	Falta de Recursos en el Servidor de Correos	CORREO
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Falta de Recursos en CLINET	SISTEMA
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA

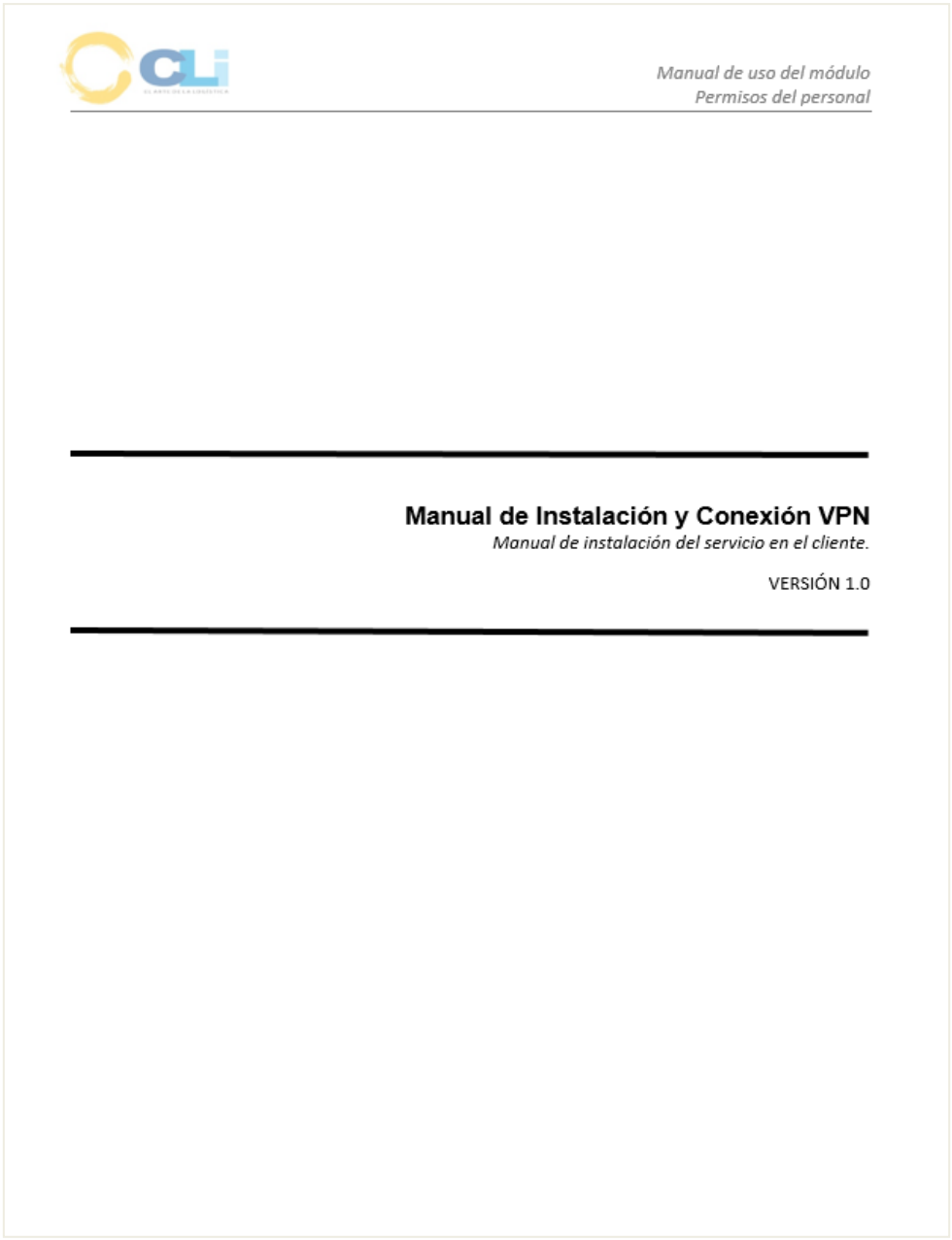
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Falta de Recursos en CLINET	SISTEMA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ADMINISTRACION	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Falta de Recursos en CLINET	SISTEMA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
RRHH	Actualización de SINTAD produce alto tráfico de red	SISTEMA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
CONTABILIDAD	Lentitud en los servidores prestados por SUNAT	SISTEMA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
CONTABILIDAD	Lentitud en los servidores prestados por SUNAT	SISTEMA
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Actualización de SINTAD produce alto tráfico de red	SISTEMA
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ESC	Interfaz poco amigable para la creación de filtros de correo	CORREO
REVISION	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Actualización de SINTAD produce alto tráfico de red	SISTEMA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Falta de Recursos en el Servidor de Correos	CORREO
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
LEGAL	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ESC	Demora en salida de correos	CORREO

ESC	Interfaz poco amigable para la creación de filtros de correo	CORREO
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Interfaz poco amigable para la creación de filtros de correo	CORREO
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Demora en salida de correos	CORREO
VISTO BUENO	Falta de Recursos en el Servidor de Correos	CORREO
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ADMINISTRACION	Lentitud en los servidores prestados por SUNAT	SISTEMA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ESC	Pérdida en el servicio de correo	CORREO
ESC	Pérdida en el servicio de correo	CORREO
RRHH	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Pérdida en el servicio de correo	CORREO
ESC	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
TRANSPORTE	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
SEGUIMIENTO	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
CALIDAD	Interfaz poco amigable para la creación de filtros de correo	CORREO
ESC	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
LIQUIDACION	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
VISTO BUENO	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
CONTABILIDAD	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA

ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
TRANSPORTE	Falta de Recursos en el Servidor de Correos	CORREO
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Exceso de multisesiones	CONEXIÓN REMOTAA
CALIDAD	Demora en salida de correos	CORREO
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
CALIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Actualización de SINTAD produce alto tráfico de red	SISTEMA
LIQUIDACION	Actualización de SINTAD produce alto tráfico de red	SISTEMA
CONTABILIDAD	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA
CARGA	Exceso de multisesiones	CONEXIÓN REMOTAA
VISTO BUENO	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
VISTO BUENO	Falta de Recursos en el Servidor de Correos	CORREO
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA
RRHH	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Demora en salida de correos	CORREO

ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ADMINISTRACION	Exceso de multisesiones	CONEXIÓN REMOTAA
REVISOR	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Interfaz poco amigable para la creación de filtros de correo	CORREO
TRANSPORTE	Exceso de multisesiones	CONEXIÓN REMOTAA
TRANSPORTE	Interfaz poco amigable para la creación de filtros de correo	CORREO
CONTABILIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
CONTABILIDAD	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ADMINISTRACION	Las máquinas virtuales no contaban con los archivos de los usuarios.	ACCESOS A LOS SISTEMAS Y ARCHIVOS
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
REVISOR	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Interfaz poco amigable para la creación de filtros de correo	CORREO
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ADMINISTRACION	Falta de Recursos en el Servidor de Correos	CORREO
LIQUIDACION	Exceso de multisesiones	CONEXIÓN REMOTAA
LIQUIDACION	Ancho de Banda Inadecuado	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
CARGA	Exceso de multisesiones	CONEXIÓN REMOTAA
ESC	Exceso de multisesiones	CONEXIÓN REMOTAA
ARCHIVO	Inconvenientes con claves de accesos	ACCESOS A LOS SISTEMAS Y ARCHIVOS
CALIDAD	Exceso de multisesiones	CONEXIÓN REMOTAA
CALIDAD	No se contaba con todos los módulos de los sistemas	ACCESOS A LOS SISTEMAS Y ARCHIVOS
ESC	Falta de Recursos en el Servidor de Correos	CORREO
SEGUIMIENTO	Exceso de multisesiones	CONEXIÓN REMOTAA

ANEXO n.° 2. Manual de instalación del PVN



Manual de uso del módulo
Permisos del personal

Manual de Instalación y Conexión VPN

Manual de instalación del servicio en el cliente.

VERSIÓN 1.0

INSTALACION DEL VPN EN UN NUEVO USUARIO

Link de descarga de los archivos para la conexión VPN y adjunto los usuarios y contraseñas de los usuarios

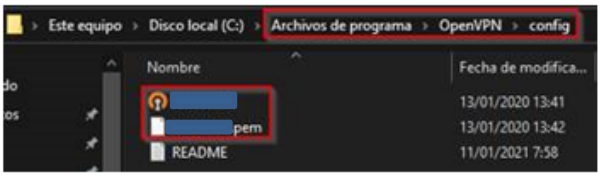
https://drive.google.com/drive/folders/1u27q7RJ1FN8WzsQsN3TnMuwOa73Rb8VO

(en este drive encontrará los archivos que se requieren para instalar)

Si la pc es de Windows 10 procede a instalar el ultimo archivo

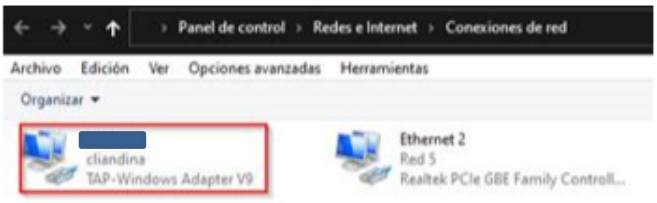
Si la pc es de Windows 7 o Windows 8 procede a instalar el otro archivo

**Los otros dos archivos de azul debe descargarlos y colocarlos en la siguiente ruta:



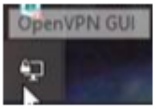
Luego debe cambiar de nombre a la tarjeta TAP del OPEN VPN a **cliandina**

Manual de uso del módulo
Permisos del personal



Luego haga doble clic en el icono de Open VPN

y en la parte inferior se va a habilitar el icono para que se conecte



Le pedirá ingresar usuario y contraseña

Una vez se conecte, se tornará color verde, luego de ello ya podrá usar los sistemas de cli

*** en el caso de los equipos que tiene Windows 7 y no se instala el TAP, debe buscar una versión anterior

Se adjuntó el link donde puede buscarlo https://build.openvpn.net/downloads/releases/

	PROCEDIMIENTO	Código: PRO-TI-006 Versión: 00 Fecha: 01/06/2020 Aprobado: GG Página 1 de 4
	Conexión VPN	

Conexión VPN

	PUESTO	NOMBRE	FECHA
ELABORADO POR:	Analista de Soporte	[redacted]	10/07/2020
REVISADO POR:	Supervisor de Sistemas	[redacted]	10/07/2020
REVISADO POR:	Jefe de Seguridad y Calidad	[redacted]	10/07/2020
APROBADO POR:	Gerente General	[redacted]	10/07/2020

	PROCEDIMIENTO	Código: PRO-TI-006 Versión: 00 Fecha: 01/06/2020 Aprobado: GG Página 2 de 4
CLI	Conexión VPN	

1. **OBJETIVO**

Describir las actividades a realizar para la creación de usuarios, y configuración para una conexión VPN para los colaboradores que se conecten de manera remota y tengan acceso a la red y a los sistemas, siguiendo una política de seguridad informática que minimice los riesgos de pérdida o robo de información.

2. **ALCANCE**

Incluye a los diferentes sistemas utilizados y la asignación de usuarios.

3. **RESPONSABILIDAD**

El Supervisor de Sistemas es el responsable de la correcta aplicación del presente procedimiento.

4. **ABREVIATURAS**

VPN: Red Privada Virtual
TAP: Tarjeta Red Virtual
Multiusuarios:

5. **REFERENCIAS**

5.1. Norma Internacional BASC Versión 05 – 2017: 7.1.3.c, 7.1.3.d, 7.1.3.e

5.2. Estándar Internacional de Seguridad BASC 5.0.2 Versión 05 – 2017: 4.2.2.c, 5.1, 5.2

5.3. Norma Internacional ISO 9001 – 2015: 7.1.3.b, 7.1.3.d

5.4. Norma Técnica Peruana NTP ISO 370001:2017 (ISO 37001:2016): 5.1.2.c, 7.1

6. **DEFINICIONES**

6.1. VPN: (Wikipedia)

6.2. Usuario: Personal de CLI

6.3. TAP: Tarjeta Red Virtual según Wifi y/o Cable

6.4. OpenVPN:

7. **CONDICIONES GENERALES**

Instalar el OpenVPN de acuerdo al Sistema Operativo que maneje el usuario.
Validar que los equipos a conectarse a la red por VPN tengan el antivirus activo y actualizado.

8. **DESCRIPCION DEL PROCEDIMIENTO**

8.1. **Creación de Usuarios**:

8.1.1. **Creación de usuarios VPN en el Firewall de CLI**

a. El Asistente y Analista de Soporte es el responsable de la creación de usuario y clave para el acceso al VPN.
b. Las credenciales a la VPN serán creadas desde el Firewall, en la pestaña VPN, en el menú Autentificación. Allí se creará y configurará a cada usuario que se va a conectar de manera remota a la red de CLI.

8.1.2. **Creación de Usuarios en las maquinas virtuales.**
8.1.2.1. Conexión a Equipos de CLI Gestiones en oficina

a. El Analista de Soporte es el responsable de la creación de usuarios y clave para el acceso a las maquinas remotas por donde los usuarios ingresarán a los sistemas de CLI.

b. La creación de los usuarios remotos se hará por grupos, cada grupo va a pertenecer a una maquina remota, los cuales ingresarán con un usuario y contraseña que se les proporcionará, todos tendrán los privilegios de usuarios estándar.

8.2. **Instalación y configuración del Cliente OpenVPN**:

a. Se debe ejecutar e instalar el OpenVPN según la versión de Windows que tengan en el equipo a conectarse, desde el siguiente enlace: https://openvpn.net/community-downloads/.
b. Luego descargaremos dos ficheros que serán copiados y ubicados en la carpeta donde se instaló el OpenVPN en la carpeta '**config**': *C:\Program Files\OpenVPN\config*

8.3. **Establecer la conexión con el Servidor OpenVPN**:

a. Se debe cambiar el adaptador de red, para ello nos ubicamos en: *Panel de control\Redes e Internet\Conexiones de red,* ubicamos el adaptador **TAP**, y cambiaremos el nombre a **cliandina,** para que pueda asociarse con los ficheros que colocamos en la carpeta de config del OpenVPN.
b. En el escritorio ubicamos el acceso directo OpenVPN, hacemos doble clic para que se habilite en la barra de tareas el icono.
c. Una vez ubicada el Icono hacemos clic derecho y seleccionamos conectar.
d. Se abrirá una ventana la cual nos pedirá ingresar el usuario y contraseña.
e. Una vez autentificado, aparecerá un aviso indicando que ya nos encontramos dentro de la red de CLI y el icono del OpenVPN se tornará de color verde.

8.4. **Acceder remotamente**:

a. Usuarios conectados desde un equipo personal a Equipos de Oficina:
   - Para poder acceder a los equipos en oficina de manera remota, debemos ingresar a **Conexión a Escritorio Remoto,** desde el equipo del usuario, y se abrirá una ventana que nos pedirá ingresar la IP del Equipo (**IP del equipo en oficina**), además ingresamos el usuario y contraseña (credenciales con las que ingresan a sus equipos en oficinas).
   - Una vez ingresadas las credenciales, seleccionaremos conectar y en automático se mostrará el escritorio del equipo correspondiente al usuario en oficina.
b. Usuarios conectados desde un equipo personal a un remoto:
   - Para poder acceder a las máquinas virtuales de manera remota, debemos ingresar a **Conexión a Escritorio Remoto,** desde el equipo del usuario, y se abrirá una ventana que nos pedirá ingresar el IP del Equipo (**IP de la maquina remota**), además el usuario y contraseña (proporcionados al usuario, previamente creadas en el equipo virtual remoto perteneciente área del usuario).
   - Una vez ingresadas las credenciales, seleccionaremos conectar y en automático se mostrará el escritorio remoto de la máquina virtual correspondiente al usuario.
c. Usuarios accediendo desde sus hogares con equipos de CLI (equipos de propiedad de CLI con todos los sistemas instalados):
   - Cuando el equipo es de propiedad de CLI, este tiene todos los sistemas instalados, así mismo tiene el Endpoint del Antivirus Bitdefende, por tal motivo solo debemos activar el VPN, una vez establecida la conexión, podrá acceder a los sistemas (SINTAD) y carpetas compartidas como si se estuviera laborando en oficina de manera presencial.
d.

Las credenciales del OpenVPN no son proporcionadas al usuario, sólo serán gestionadas por el Analista o Asistente de Soporte.
Para el personal que sale de vacaciones, se bloquearan sus accesos en todos los sistemas usados por CLI (Clinet, SINTAD, Correo).

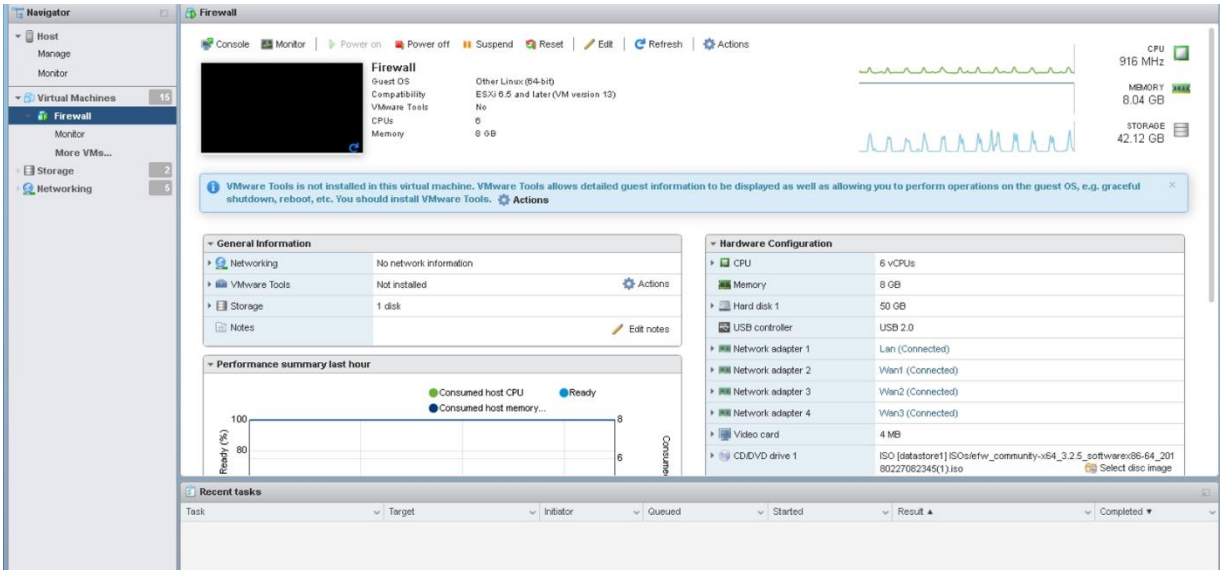
9. **CONTROL DE CAMBIOS**

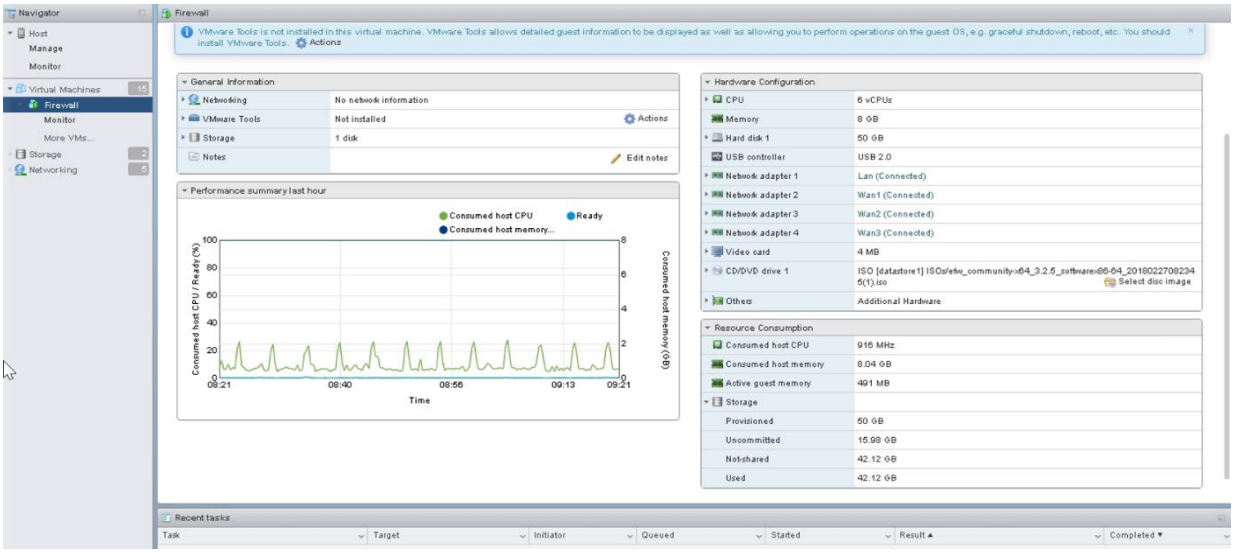
No Aplica
-Se modificó el punto **8.4 Acceder Remotamente** ya que el tipo de conexión cambió.

10. **ANEXOS**

10.1. Registro de usuarios y contraseñas VPN.

ANEXO n.° 3. Firewall Endian Comunity en VMWare





ANEXO n.° 6 Inventario de usuarios y la característica de los equipos con los que se conectan

AREA	PC'S	ESTADO	LAPTOP	ESTADO	OFICINA	OBS
ADMINISTRACION Y CONTABILIDAD					NO	la usan todos para imprimir
ADMINISTRACION Y CONTABILIDAD	1	EN CASA			NO	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			NO	se conecta desde su pc personal
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			NO	Se conecta desde su laptop personal
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			si (G2)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI	1	ALQUILADA	NO	se conecta a su pc de cli
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			NO	se conecta desde su laptop
ADMINISTRACION Y CONTABILIDAD	1	EN CLI	1	ALQUILADA	si (G1)	se conecta a su pc de cli
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			si (G2)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			si (G1)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			si (G2)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			NO	se conecta desde su pc personal a cli
ADMINISTRACION Y CONTABILIDAD	1	EN CASA			NO	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI	1	ALQUILADA	si (G1)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			si (G1)	
ADMINISTRACION Y CONTABILIDAD	1	EN CLI			NO	se conecta desde su pc personal a un remoto
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI	1	ALQUILADA	si (G2)	

SERVICIO AL CLIENTE	1	EN CLI	1	ALQUILADA	NO	se conecta a un remoto desde la laptop
SERVICIO AL CLIENTE			1	ALQUILADA	NO	se conecta al remoto
SERVICIO AL CLIENTE	1	EN CLI			NO	se conecta de su laptop personal a cli
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI	1	ALQUILADA	si (G1)	
SERVICIO AL CLIENTE	1	EN CLI			NO	se conecta a la pc de cli
SERVICIO AL CLIENTE	1	EN CLI			si (G2)	
SERVICIO AL CLIENTE	1	EN CLI			si (G2)	
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI			si (G1)	
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI			si (G1)	
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI	1	ALQUILADA	si (G2)	
SERVICIO AL CLIENTE	1	EN CLI			si (G2)	
SERVICIO AL CLIENTE	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CLI			si(G2)	
SERVICIO AL CLIENTE	1	EN CLI			si (G1)	
SERVICIO AL CLIENTE	1	EN CLI	1	ALQUILADA	NO	se conecta de la laptop a cli
SERVICIO AL CLIENTE	1	EN CLI			si (G2)	
SERVICIO AL CLIENTES	1	EN CASA			NO	
SERVICIO AL CLIENTE	1	EN CASA			NO	

SERVICIO AL CLIENTE		EN CASA	1	PROPIO	NO	tiene laptop de cli
SERVICIO AL CLIENTE					NO	se conecta de su laptop personal a un remoto
SERVICIO AL CLIENTE			1	ALQUILADA	NO	
SERVICIO AL CLIENTE					NO	Se conecta de su laptop a un remoto
SERVICIO AL CLIENTE					NO	se conecta de su laptop personal a un remoto
TRANSPORTE	1	EN CLI			si (G1)	
TRANSPORTE	1	EN CASA			NO	
TRANSPORTE	1	EN CLI			si (G1)	
TRANSPORTE	1	EN CLI			NO	
TRANSPORTE	1	EN CLI			si (G2)	
TRANSPORTE	1	EN CASA			NO	
VISTO BUENO	1	EN CLI	1	ALQUILADA	si (G1)	se conecta a un remoto desde la laptop
VISTO BUENO	1	EN CLI			si (G1)	
VISTO BUENO					si (G2)	usa pc de mensajería
VISTO BUENO	1	EN CLI			si (G2)	
VISTO BUENO	1	EN CLI	1	ALQUILADA	si (G2)	se conecta a la pc de cli
ARCHIVO	1	EN CLI			si (G1)	
ARCHIVO	1	EN CLI			si (G2)	
ARCHIVO	1	EN CLI			si (G1 - G)	
REVISORES	1	EN CASA			NO	
REVISORES	1	EN CASA			NO	
REVISORES	1	EN CASA			NO	
REVISORES					NO	se conecta de su pc personal a un remoto
RRHH	1	EN CLI			si (G1)	
RRHH	1	EN CLI	1	PROPIO	Si (G2)	se conecta a su pc de cli
LEGAL					NO	se conecta de su laptop personal a un remoto
LEGAL	1	EN CLI			NO	se conecta de su laptop personal a cli
CALIDAD			1	PROPIO	NO	
CALIDAD	1	EN CLI			NO	se conectan a su pc de CLI
CALIDAD	1	EN CLI			si (G1)	vienen cuando se requiere / se conecta de su laptop personal
CALIDAD	1	EN CLI			si (G2)	vienen cuando se requiere / se conecta de su laptop personal

LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CLI			NO	
LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CASA			NO	se conecta de su pc personal a un remoto
LIQUIDADORES	1	EN CASA			NO	
	1	EN CASA			NO	
LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CASA			NO	
LIQUIDADORES	1	EN CLI	1	ALQUILADA	SI	Turno noche
JEFATURA			1	PROPIO	NO	
JEFATURA			1	PROPIO	NO	
JEFATURA			1	PROPIO	NO	
JEFATURA	1	EN CLI	1	ALQUILADA	si (G1)	
SEGUIMIENTO	1	EN CLI	1	ALQUILADA	si (G2)	se conecta a la pc de cli
SEGUIMIENTO	1	EN CLI	1	ALQUILADA	si (G2)	se conecta a la pc de cli
SEGUIMIENTO	1	EN CLI			si (G1)	se conecta de su laptop personal a cli
BACKUP			1	ALQUILADA	NO	se conecta a un remoto desde la laptop
CARGA	1	EN CLI			NO	se conecta a su pc de cli
CARGA	1	EN CLI			NO	se conecta desde du laptop personal
CARGA	1	EN CLI	1	ALQUILADA	NO	vienen cuando se requiere / se conecta a la pc de cli
CARGA					NO	Se conecta de su laptop a un remoto
CARGA			1	PROPIO	No	
COMERCIAL	1	EN CASA			NO	
COMERCIAL	1	EN CLI			NO	se conecta de su pc personal
INHOUSE			1	ALQUILADA		
INHOUSE						
INHOUSE						
INHOUSE	1	EN CASA				
INHOUSE		EN CASA	1	PROPIO		
INHOUSE						

INHOUSE						
INHOUSE			1	ALQUILADA		
INHOUSE	1	EN CASA				
INHOUSE	1	EN CLI				
INHOUSE	2	OFICINA				
INHOUSE	2	OFICINA				
INHOUSE			1	PROPIO	NO	
INHOUSE			1	PROPIO		
IN HOUSE	1	EN CASA				
IN HOUSE			1	PROPIO		
GERENCIA	2	EN CLI EN CASA			NO	
GERENCIA		EN CASA	1	PROPIO	NO	
SISTEMAS	1	EN CLI			NO	
SISTEMAS	1	EN CLI			NO	
SISTEMAS					NO	no la está usando / remoto
	1	EN CLI			NO	se conecta a su pc de cli
SISTEMAS	1	EN CLI			si (G1)	
SISTEMAS	1	EN CLI			NO	
SISTEMAS					NO	
SISTEMAS					si (G2)	
ARMADO	1	EN CLI			si (G1 - G2)	
ARMADO	1	EN CLI			si (G1 - G2)	
ARMADO	1	EN CLI			si (G1 - G2)	
OPERACIONES	1	EN CLI				los despachadores se contactan para descargar su información
OPERACIONES	1	EN CLI	1	ALQUILADA	si (G2)	se conecta a aun remoto
Secretaria	1					
DIRECTORIO	1	EN CLI				
DIRECTORIO	1	EN CLI				para inducciones /despachadores
DIRECTORIO	1	EN CLI				para inducciones /despachadores
ALMACEN	3	EN CLI				por recuperar
ALMACEN	4	EN CLI				
ALMACEN			1	ALQUILADA		
ALMACEN SALA DE SERVIDORES	4					

TOTAL	**116**	**34**