DISEÑO DE UNA RED PRIVADA VIRTUAL SEGURA PARA FACILITAR LA COMUNICACIÓN, TRABAJO Y FLUJO DE INFORMACIÓN EN LA EMPRESA QOS LTDA.

Luis Alberto Perdomo Guevara

Oscar Ivan Castro Jaime

UNIVERSIDAD COOPERATIVA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

SECCIONAL BOGOTÁ D.C.

MARZO 2018

DISEÑO DE UNA RED PRIVADA VIRTUAL SEGURA PARA FACILITAR LA COMUNICACIÓN, TRABAJO Y FLUJO DE INFORMACIÓN EN LA EMPRESA QOS LTDA.

Luis Alberto Perdomo Guevara

Oscar Iván Castro Jaime

SEMINARIO CCNA

Trabajo para optar al título de Ingeniero de Telecomunicaciones

Director(a)

Oscar Fabián Corredor Camargo

UNIVERSIDAD COOPERATIVA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

SECCIONAL BOGOTÁ D.C.

MARZO 2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

PRIMER JURADO

_____

SEGUNDO JURADO

Bogota, Julio, 2018

DEDICATORIA

La implementación de este proyecto se la dedicamos a nuestros padres quienes siempre mostraron un interés por nuestro futuro, nos apoyaron emocional y económicamente, a cada uno de nuestros maestros, quienes, con su paciencia y dedicación, nos brindaron las herramientas para poder sacarlo adelante. Y finalmente, a Dios, por darnos la vida, por estar en cada paso que damos, y por poner en nuestro camino a aquellas personas que han sido un soporte y compañía durante todo el periodo de estudio.

CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

1. GLOSARIO

Ancho de banda
Capacidad de transmisión de un dispositivo o red determinado.

Dirección IP
Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Ethernet
Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

Firewall
Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

Hardware
El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

Máscara de subred
Código de dirección que determina el tamaño de la red.

Paquete
Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

Red
Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios

Router Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Servidor
Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

Switch
Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.

Tcp/ip (Transport Control Protocol / Internet Protocol)
Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

Vpn
Es una tecnología, que permite realizar el acceso de forma segura a una red corporativa a través de Internet o de una LAN. Normalmente, posibilita la entrada a la red corporativa desde el exterior mediante un ISP, creándose una segunda conexión que se comportará como si se realizara desde la propia oficina.

Wan (Wide Area Network)
Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.

2. INTRODUCCIÓN

Debido al crecimiento exponencial del mercado de las telecomunicaciones, las diferentes empresas que proporcionan servicio técnico, se ven en la obligación de orientarse hacia los avances tecnológicos para buscar ser más competitivo y poder aprovechar nuevas oportunidades en el mercado.

La competitividad a la que se está enfrentando las organizaciones que luchan para mejorar, aumentar la calidad de servicios, y de posicionarse en el mercado, genera en las compañías la necesidad de cambiar su tecnología a medida que avanza.

Por ser QOS LTDA una empresa de servicio tecnico en telefonia celular en Colombia,la cual ofrece el servicio de reparacion y mantenimiento de equipos celulares Huawey y Alcatel, debe mantenerse en búsqueda de soluciones avanzadas para satisfacer las necesidades de los clientes que cada vez son más exigentes con la calidad del servicio. Por este motivo, el tema de estudio de este trabajo, se basa en realizar un diseño y propuesta de una red VPN, que permite aQOS LTDA la posibilidad de ofrecer un servicio que podra conectar y comunicar a sus empleados fuera de la misma empresa.

3. DESCRIPCION DEL PROBLEMA

3.1. FORMULACIÓN DEL PROBLEMA

Actualmente, en la empresa QOS LTDA, los empleados no tienen una forma de poder acceder a los documentos que normalmente utilizan en su empresa, como lo son informes, software de reportes y correo corporativo, razón por la cual, la solución a el acceso a esta información y software era mediante un software de acceso remoto como, por ejemplo: Team Viewer para ingresar externamente a los dispositivos que se encuentran en la LAN. Este método de conexión no es seguro debido a que no deja un registro de cuando el usuario tuvo acceso a la red de la organización. Por lo indicado anteriormente, la empresa debe contar con un mecanismo de acceso remoto seguro como la VPN, ya que los usuarios manipulan información sensible de la organización y este método de conexión permite realizar un control de los usuarios que se conectan a través de la VPN. La VPN se encarga de establecer un túnel, es decir un canal de comunicación seguro a través de Internet para oficinas remotas, usuarios móviles y socios comerciales, disminuyendo o eliminando los costos asociados por enlaces dedicados que en tiempos pasados permitían la comunicación dedicada entre el usuario y la empresa privada. El principal objetivo del presente trabajo es el diseño e implementación de una red privada virtual utilizando el método de autenticación IPsec, que permita realizar una conexión virtual a la empresa para que los empleados puedan acceder

a la información en cualquier momento y lugar en donde se encuentren, contando solamente con un software instalado y conexión a internet.

3.2. JUSTIFICACION DEL PROBLEMA

La empresa QOS LTDA, se encarga de prestar servicios de reparación celular a diferentes usuarios en Colombia, soporte técnico en teléfonos celulares de la marca Huawey y Alcatel, con liderazgo destacado en reparación a nivel nacional. QOS LTDA ha ido integrando un grupo de profesionales con alto nivel de especialización, quienes trabajan dentro de las diferentes áreas y divisiones que componen la organización: comercial, contabilidad, soporte técnico, gerencia de proyectos y gerencia administrativa.

Debido a la evolución estructural de la empresa y el crecimiento en la demanda de información que se maneja, la red de comunicaciones existente exige tener la posibilidad de conectar y facilitar la comunicación entre las diferentes áreas que componen la compañía accediendo de forma más fácil y ágil a cualquier tipo de información deseada por el empleado a través del servidor.

Por tal motivo surge la necesidad de proponer una red privada virtual en el sistema de comunicaciones; a través de técnicas de encriptación, confidencialidad, protección de réplica y autenticación de paquetes para brindar un mayor control entre las dependencias existentes y se logre un adecuado manejo de información de la red, por lo tanto, es necesario realizar un diseño que permita mayor seguridad en el trasporte de la información y así incrementar la optimización de la red.

A través del diseño de una Red Privada virtual se puede conectar todas las oficinas de la empresa en una red corporativa ancha a través de Internet, disminuyendo los costos de largas distancias. Además, al utilizarse protocolo IPSec permite una conexión segura similar a la existente en una red privada tradicional; por lo cual representa una opción atractiva para establecer conexiones remotas en una organización. Teniendo en cuenta que compartir la información entre las diferentes áreas de la empresa también es un factor muy importante a la hora de tomar la decisión de llevar a cabo el diseño de la red para la empresa, ya que cada área necesita de la otra, siendo indispensable una de otra para el buen desarrollo de la empresa.

Por esta razón, la implementación de una red privada virtual es la más apropiada, para el manejo de la información, ajustándose a las necesidades específicas de la empresa en donde se desea ejecutar el proyecto, permitiendo un mejor desempeño en el desarrollo de sus actividades.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar una red privada virtual segura para facilitar la comunicación, trabajo y flujo de información de la empresa QOS LTDA ubicada en la ciudad de Bogotá, basados en la norma internacional seguridad ISO 27001.

4.2. OBJETIVOS ESPECIFICOS

Identificar el tipo de protocolo de túnel que se va a utilizar.
Analizar el impacto económico-técnico al implementar esta tecnología.
Mejorar la integridad, confidencialidad y seguridad de los datos.
Aplicabilidad de la norma internacional ISO 27001

5. MARCOS DE REFERENCIA.

5.1. MARCO TEÓRICO

5.1.1. ANTECEDENTES

Desde no hace mucho tiempo la empresa QOS LTDA cuenta con una red local la cual no es aprovechada al máximo para lograr una mejor comunicación y asesoría entre los mismos empleados.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación, este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que garantiza la privacidad.

Además de la comunicación entre las diferentes áreas conformadas por la empresa, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuarios pueden conectarse a la red de la empresa, pudiéndose movilizar dentro de la misma y así mismo usar los recursos disponibles dentro de la misma.

5.1.2. CONCEPTO VPN

VPN significa literalmente VIRTUAL PRIVATE NETWORK, en español RED PRIVADA VIRTUAL.

5.1.3. REQUISITOS PARA UNA VPN

5.1.3.1. CON RESPECTO AL TIPO DE CONEXIÓN

5.1.3.1.1. OFICINA CENTRAL

Corresponde a una red corporativa o la red LAN. Esta tendrá que disponer de una IP fija a través de una conexión ADSL para acceso a Internet. Debe disponer además de un dispositivo (Firewall o Router) VPN el cual administre hasta más de 5 túneles y que permita dar acceso autentificado y seguro a los usuarios y oficinas remotas.

5.1.3.1.2. USUARIOS REMOTOS

Estos utilizarán un software especial para la configuración VPN que junto con una conexión a la internet desde el ISP (proveedor de servicios de Internet) de costo local (con o sin IP fija) permite el contacto con la red privada (oficina central), como si se tratase de un puesto más de la Red Privada Central de carácter local.

5.1.3.1.3. OFICINAS REMOTAS

Tendrán que disponer de una conexión a la Internet con RDSI o ADSL (no es necesario tener IP fija) que en conjunto con un dispositivo VPN les permite ponerse en contacto con la RED Privada (oficina central) en forma confidencial.

5.1.3.2. CON RESPECTO A LAS NORMAS DE SEGURIDAD

5.1.3.2.1. COMPATIBILDAD

Para que una VPN pueda utilizar Internet, debe ser compatible con el protocolo de Internet (IP). Resulta obvia esta consideración con el fin de poder asignar y posteriormente utilizar conjuntos de direcciones IP. Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente unas pocas puedan ser empleadas en la interacción con Internet. La razón por la que sucede esto es simple, la obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un subnetting resulta imposible. Las subredes simplifican la administración de direcciones, así como la gestión de los routers y conmutadores, pero malgastan direcciones muy preciadas.

Actualmente existen varias técnicas con las que se puede obtener la compatibilidad deseada entre las redes privadas e Internet, por ejemplo, la conversión a direcciones Internet mediante NAT (Network Address Traslation) y el empleo de túneles para encapsulamiento.

En la primera de estas técnicas, las direcciones Internet oficiales coexistirán con las redes IP privadas en el interior de la infraestructura de los routers y conmutadores de las organizaciones. De este modo, un usuario con una dirección IP privada puede acceder al exterior por medio de un servidor de direcciones IP públicas mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.

5.1.3.2.2. SEGURIDAD

Debe considerarse seriamente la seguridad cuando se usa Internet. Las comunicaciones ya no van a estar confinadas a circuitos privados, sino que van a viajar a través de Internet, que es considerada una red “demasiado pública” para realizar comunicaciones privadas. Aunque puede parecer poco probable que alguien monitoreando una línea con un sniffer consiga capturar información y hacer uso de ella, ya que está encriptada, la posibilidad existe. Cuando la información está encriptada, se requieren claves para cifrar y descifrar. Los usuarios en cada extremo deben tener las claves adecuadas. Si se está configurando una conexión con una sucursal es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es y un modo de intercambiar las claves para la encriptación. Las claves públicas basadas en certificados digitales y PKI son los que más de utilizan para este propósito.

5.1.3.2.3. DISPONIBILIDAD

La disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final.

La calidad de servicio (QoS – Quality of Service), hace referencia a la capacidad que dispone una red para asegurar un cierto grado de operación de extremo a extremo. La QoS puede obtenerse como una cierta cantidad de ancho de banda o un retardo que no debe sobrepasarse, o bien como una combinación de ambas. Actualmente, la entrega de datos en Internet es realizada de acuerdo al mejor esfuerzo (best effort), lo cual no garantiza la calidad de servicio demandada. No obstante, en el futuro Internet será capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes, entre los que cabe destacar DiffServ (Differential Services), RSVP (Resource ReSerVation

Protocol) y RTP (Real Time Protocol). Pero por ahora, los proveedores sólo proporcionan la QoS de las VPNs haciendo uso del tráfico CIR (Committed Information Rate) en Frame Relay u otras técnicas (ejemplo MPLS).

5.1.3.2.4. INTEROPERABILIDAD

Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: La interoperabilidad. Los estándares sobre tunneling, autenticación, encriptación y modo de operación ya mencionados anteriormente son de reciente aparición o bien se encuentran en proceso de desarrollo. Por esta razón, previamente a la adquisición de una tecnología VPN, se debe prestar una cuidadosa atención a la interoperabilidad de extremo a extremo. Esta responsabilidad puede residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada. Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante. En el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, se deberán limitar los aspectos inter operacionales a un subconjunto que englobe aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido probado en laboratorios o bien sometido a pruebas.

5.1.4. PROTOCOLOS VPN

Una vez descrita la importancia que presentan estos cuatro elementos para las VPN, se procederá a realizar una breve descripción de los protocolos comúnmente utilizados por la marca cisco la cual fue nuestro objeto de estudio.

5.1.4.1. IPSec

El protocolo de seguridad en Internet (IPSec) proporciona las funciones de seguridad mejorada tales como algoritmos de encriptación más fuertes y de más completa autenticación. El IPSec tiene dos modos de encriptación: túnel y transporte. El modo túnel cifra el encabezado y el payload de cada paquete mientras que el modo de transporte cifra solamente el payload. Solamente los sistemas que son IPSec-obedientes pueden aprovecharse de este protocolo. También, todos los dispositivos deben utilizar una clave común o certificarla y deben tener configuración muy similar de las políticas de seguridad. Para los usuarios del VPN de acceso remoto, una cierta forma de paquete del software de tercero proporciona la conexión y el cifrado en los usuarios PC. Soportes para IPSec 56-bit (solo DES) o cifrado del 168-bit (DES triple).

5.1.4.2. PPTP/MPPE

El PPTP fue creado por el foro de PPTP, un consorcio que incluye US Robotics, Microsoft, 3COM, asciende, y ECI Telematics. El PPTP soporta el multi-protocol VPN, con 40-bit y el cifrado del 128-bit usando un protocolo llamado Microsoft Point-to-Point Encryption (MPPE). Es importante observar que el PPTP en sí mismo no proporciona la encriptación de datos.

5.1.4.3. L2TP/IPsec

El L2TP comúnmente llamado sobre el IPSec, esto proporciona la Seguridad del Protocolo IPSec sobre el tunelización del protocolo Layer 2 Tunneling Protocol (L2TP). El L2TP es el producto de una sociedad entre los miembros del foro de PPTP, Cisco, y la Fuerza de tareas de ingeniería en Internet (IETF) (IETF). Utilizado sobre todo para los VPN de accesos remotos con los sistemas operativos del Windows 2000, puesto que el Windows 2000 proporciona a un cliente de IPSec y L2TP nativo. Los Proveedores de servicios de Internet pueden también proporcionar las conexiones L2TP para los usuarios de dial in, y después cifran ese tráfico con el IPSec entre su acceso-punta y el servidor de red de la oficina remota.

5.1.5. SOFTWARE EMPLEADO

A continuación, el software empleado para la comunicación entre los diferentes sitios de trabajo.

5.1.5.1. CISCO CONFIGURATION PROFESIONAL

Cisco Configuration Professional (CCP) es una herramienta de administración de dispositivos basada en GUI para el acceso a los routers de Cisco. Esta herramienta simplifica el enrutamiento, firewall, IPS, VPN, comunicaciones unificadas, WAN, LAN y la configuración a través de interfaz gráfica de usuario basada en asistentes.

Utilizando Cisco CP, los administradores de red pueden desplegar routers con facilidad y posee la capacidad de auditoría de seguridad para revisar y recomendar cambios en la configuración del router, supervisar el estado del router, solucionar problemas de WAN y conectividad VPN.

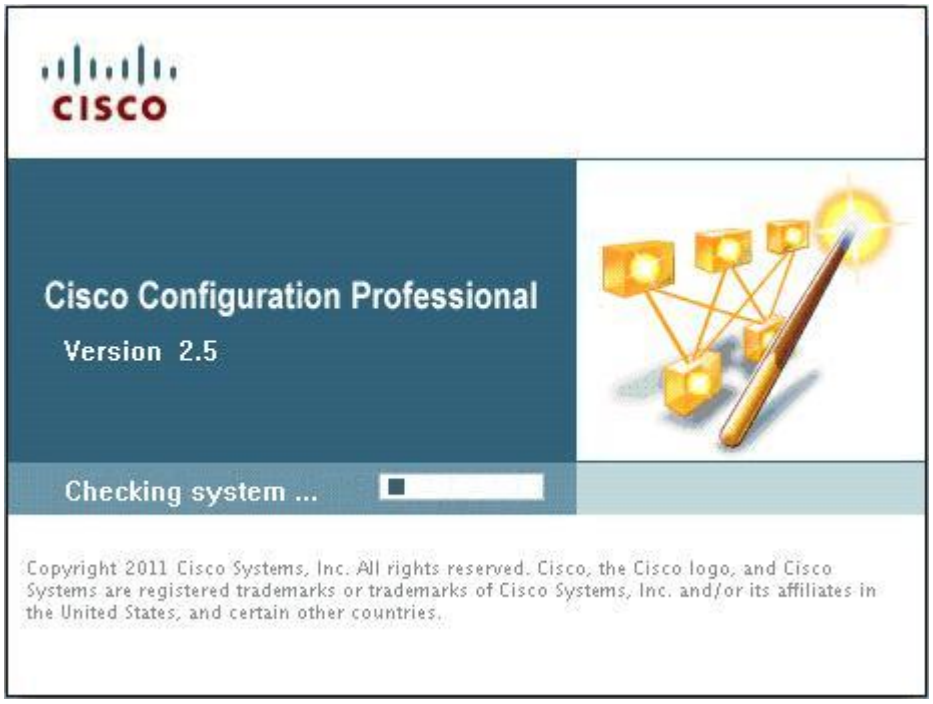


Ilustración 1. Cisco configuration profesional

5.1.6. RAZONES POR LAS CUALES ES RECOMENDABLE IMPLEMENTAR UNA VPN

5.1.6.1. REDUCCIÓN DE COSTOS

Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto) de muy alto costo que caracterizaron a muchas empresas privadas, siendo reemplazadas, por ejemplo, por acceso ADSL de un ancho de banda alto y bajo costo, disponible por lo general en la mayoría de las zonas urbanas sin mayores problemas. Los usuarios remotos móviles podrán ahorrar altos costos de llamadas telefónicas de larga distancia, bastando con que disque un proveedor de acceso local a la Internet (no IP fija). ·

5.1.6.2. ALTA SEGURIDAD

Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, dando un resultado comparable a una red punto a punto. Protocolos como 3DES (Triple data encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles

mediante software brindan un alto nivel en seguridad al sistema. Además, se utilizan varios niveles de autentificación de usuarios para el acceso a la red privada mediante llaves de ingreso, para la asegurar que el usuario es el original y no un tercero que percibe el password de autentificación. ·

5.1.6.3. ESCALABILIDAD

Para agregar usuarios a la red no es preciso realizar inversiones adicionales. La provisión de servicios se hace con dispositivos y equipos fáciles de configurar y manejar. Se usa la infraestructura de alto nivel establecida ya por los proveedores de Internet y no realizar un enlace físico que puede significar una gran inversión monetaria y de tiempo.

5.1.6.4. COMPATIBILIDAD CON TECNOLOGÍAS DE BANDA ANCHA

Una red VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red. Incluso es posible usar voz sobre IP usando la implementación VPN, y esto implica un significativo ahorro en telefonía de larga distancia.

5.1.6.5. MAYOR PRODUCTIVIDAD

Debido a un mejor nivel de acceso durante mayor tiempo se podría probar que se obtendría una mayor productividad de los usuarios de la RED. Además, se fomenta el teletrabajo con la consecutiva reducción en las necesidades de espacio físico

6. MARCO INSTITUCIONAL

6.1. MISION

Soportar de forma oportuna las necesidades de nuestros clientes brindando servicios y soluciones integrales a los requerimientos, cumpliendo con los estándares de calidad y eficiencia exigidos, y convirtiéndonos en aliados estratégicos de fabricantes, operadores y distribuidores.

6.2. VISION

QOS, soportada en talento humano responsable y profesional, y en recursos técnicos y tecnológicos del momento, será una Empresa sólida, rentable y competitiva, que, mediante la prestación de servicios y soluciones integrales

altamente calificadas, se posicionará en el mercado regional y nacional como la mejor Empresa de Servicios en calidad y eficiencia.

6.3. NUESTRA EXPERIENCIA

6.3.1. SOPORTE TÉCNICO Y REPARACIONES

Contamos con un experto recurso humano con más de 12 años de experiencia en servicio técnico de telefonía celular (AMPS, TDMA, CDMA, GSM) y certificados por las marcas más reconocidas del mercado: Nokia, Samsung, Motorola, Alcatel, etc. Adicionalmente, contamos con personal experto en soporte técnico y reparaciones de equipos telecomunicaciones de diferentes marcas y un excelente laboratorio de reparaciones que cumple con los mejores estándares de calidad.

6.3.2. ACTUALIZACIONES DE SOFTWARE Y RETRABAJOS HARDWARE

Contamos con la infraestructura necesaria y con personal experimentado en la actualización de software y hardware, que nos permiten ofrecer excelente calidad con tiempos de respuesta inmediata y garantizar cadenas de producción que trabajen turnos de 24 horas al día y los 365 días del año.

6.3.3. SERVICIO TÉCNICO CERTIFICADO

Nuestra política es realizar trabajos certificados y con respaldo; para ser consecuente con ello, QoS gestiona la certificación de su personal técnico en el mantenimiento y/o reparación de los productos de sus clientes como medio para garantizar la mejor calidad y el mejor soporte disponible.

6.4. PRINCIPIOS CORPORATIVOS

6.4.1. RESPETO POR LAS PERSONAS

Las actividades diarias se inspiran en el respeto por las personas, sus valores y creencias, respeto por los derechos y claridad en el cumplimiento, como también en las exigencias de las responsabilidades mutuas.

6.4.2. VALORES ÉTICOS

El comportamiento de los miembros de la organización se basa y ajusta a los valores y principios éticos que tradicionalmente han inspirado la vida de la organización: honestidad, integridad y justicia.

6.4.3. MEJORAMIENTO CONTINUO

Siendo ésta una manera de vivir, fundada en la conducta como un valor y un comportamiento diario y permanente, el mejoramiento continuo es un compromiso y responsabilidad de todos nuestros miembros y adscritos que hacen parte de la familia de QoS; mejoramiento en procesos, productos, procedimientos, gestión administrativa y mejoramiento en la relación humana.

6.4.4. PRODUCTIVIDAD

La productividad es la condición para la permanencia y el crecimiento de una organización, logrando así estándares de eficiencia y eficacia. QoS alcanzará niveles óptimos de productividad que aseguren el desarrollo y cumplimiento de sus acuerdos de servicio dentro de los niveles de excelencia exigidos por nuestros clientes.

6.4.5. COMPETITIVIDAD

Toda empresa se mide en su mercado. La competitividad exige el conocimiento del mercado, altos estándares de calidad, conocimientos y satisfacción oportuna de necesidades y expectativas del cliente y de un compromiso integral con la excelencia en el servicio.

6.5. ORGANIGRAMA

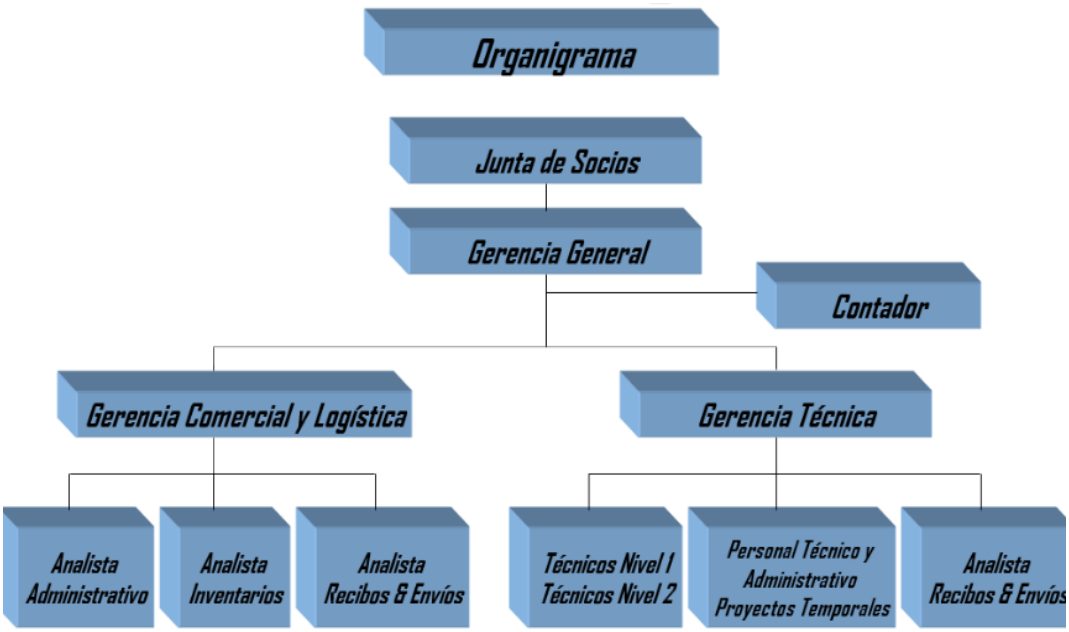


Ilustración 2. Organigrama QoS Ltda

7. METODOLOGIA EMPLEADA

A continuación, se realiza una descripción de los aspectos que se tuvieron en cuenta para el desarrollo de nuestra red privada virtual, además los pasos necesarios para su respectiva configuración. Se evidencia, de forma gráfica y escrita la topología que se implementó para el diseño de la red, las configuraciones necesarias en cada uno de los servidores que se emplean, en este caso, VPN y de archivos, y la configuración que debe realizar el cliente final que hará uso de los servicios proporcionados. Para este fin se recurrió de diversas fuentes de conocimientos evidenciadas al final del documento.

En este diseño, se permite al cliente de una red cualquiera, tener acceso a la información que alberga un servidor de archivos, el cual se encuentra en otra red. El servidor VPN será el enlace entre estas dos redes. Siendo los equipos de la marca cisco, los utilizados para lograr nuestro objetivo.

8. DISEÑO DE INGENIERIA

Para el diseño de la VPN se hizo la selección del direccionamiento IP que permite la conexión de los usuarios VPN, tal como se muestra en la siguiente figura:

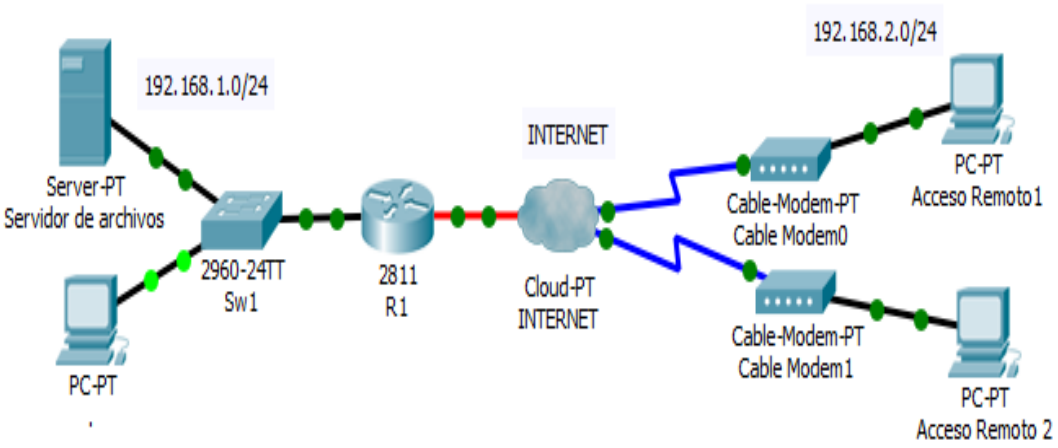


Ilustración 3. Topología de la red

Las conexiones VPN se podrán establecer a través del enlace que es propiedad del proveedor de servicios.

Inicialmente comprobamos que exista una conexión entre los equipos de acceso remoto y nuestro servidor de archivos mediante el comando de consola “ping”.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=53ms TTL=127
Reply from 192.168.1.2: bytes=32 time=5ms TTL=127
Reply from 192.168.1.2: bytes=32 time=11ms TTL=127
Reply from 192.168.1.2: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 53ms, Average = 20ms
```

Ilustración 4. Verificación de conexión con el servidor.

Se observa que el comando responde, lo que quiere decir que existe una conexión entre el servidor y el equipo remoto.

A continuación se realiza con la configuración de la VPN, para ello se utilizan los siguientes comandos:

Se crean un pool de direcciones que permite 10 conexiones simultáneas.

```
empresa(config)#ip local pool VPNPOOL 192.168.1.10 192.168.1.19
```

Se activa AAA (Autenticación, Autorización y contabilidad) en el router

```
empresa(config)#aaa new-model
```

Se define la lista de métodos de autenticación cuando un usuario se loggea

```
empresa(config)#aaa authentication login VON-USER local
```

Se Establecen los parámetros que prohíben el acceso de los usuarios a la red.

```
empresa(config)#aaa authorization network VPN_GROUP local
```

Se crea una cuenta de usuario que usarán los clientes VPN para autenticarse en el servidor.

```
empresa(config)#username vpnuser password cisco
```

Se Crea una nueva política de intercambio de claves de Internet. (1-10.000) 1 la más prioridad más alta.

```
empresa(config)#crypto isakmp policy 10
```

Se define el algoritmo de cifrado a utilizar.

```
empresa(config-isakmp)#encryption aes 192
```

Se escoge el algoritmo de hash a usar.

```
empresa(config-isakmp)#hash sha
```

Se determinar el método de autenticación: pre-shared

```
empresa(config-isakmp)#authentication pre-share
```

Se especifica el identificador de grupo Diffie-Hellman.

```
empresa(config-isakmp)#group 5
```

Se crea un grupo de intercambio de claves de internet para los clientes VPN.

```
empresa(config-isakmp)#crypto isakmp client configuration group VPN-GROUP
```

Se establece la contraseña para el grupo VPN-GROUP.

```
empresa(config-isakmp-group)#key cisco
```

Se selecciona el pool de direcciones para los clientes.

```
empresa(config-isakmp-group)#pool VPNPOOL
```

Se establece las políticas de seguridad IPSEC que se usará.

```
empresa(config-isakmp-group)#crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
```

Se crea un crypto map dinámico que se usa cuando la IP del host remoto no seconoce, como ennuestro caso que realizamos una configuración de host remoto.

```
empresa(config)#crypto dynamic-map VPN-DYNAMIC 10
```

Se asocia el transform set VPNSET al crypto map dinámico.

```
empresa(config-crypto-map)#set transform-set VPNSET
```

Se activa Reverse Route Injection (RRI).

```
empresa(config-crypto-map)#reverse-route
```

Se configura un crypto map estático que puede ser asociado a una interfaz.

Define el conjunto de usuarios con permisos de autenticación.

```
empresa(config-crypto-map)#crypto map VPN-STATIC client authentication list VPN-USERS
```

Se establece el grupo de usuarios y los parámetros de acceso a la red.

```
empresa(config)#crypto map VPN-STATIC isakmp authorization list VPN-GROUP
```

Se asocia el crypto map dinámico creado para los clientes de acceso remoto.

```
empresa(config)#crypto map VPN-STATIC 20 ipsec-isakmp dynamic VPN-DYNAMIC
```

Se Accede a la configuración de la interfaz por la que se conectarán los clientes VPN.

```
empresa(config)#interface fa1/0
```

Asociamos el crypto map a la interfaz.

```
empresa(config-if)#crypto map VPN-STATIC
```

De esta manera se finaliza la configuración de VPN remoto en el router.

Por último se configura el software (cisco configuration professional) en la PC que se encuentra fuera de la red corporativa:

Se abre la aplicación y se introduce el usuario y contraseña creada con la dirección Ip a configurar. Se pulsa la opción OK

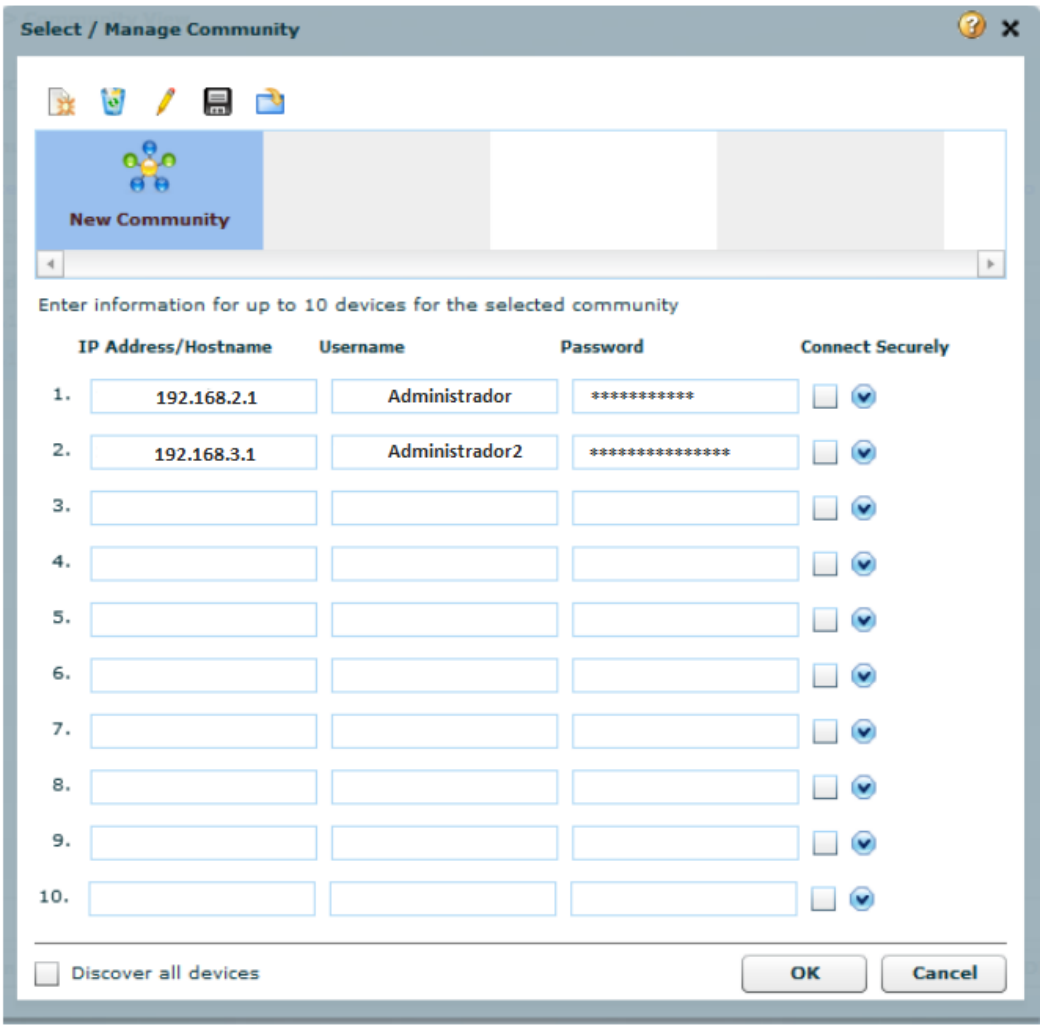


Ilustración 5. Login CCP

Se ingresa a Security > Firewall, marcamos la opción de basic firewall y damos click a launch the search task

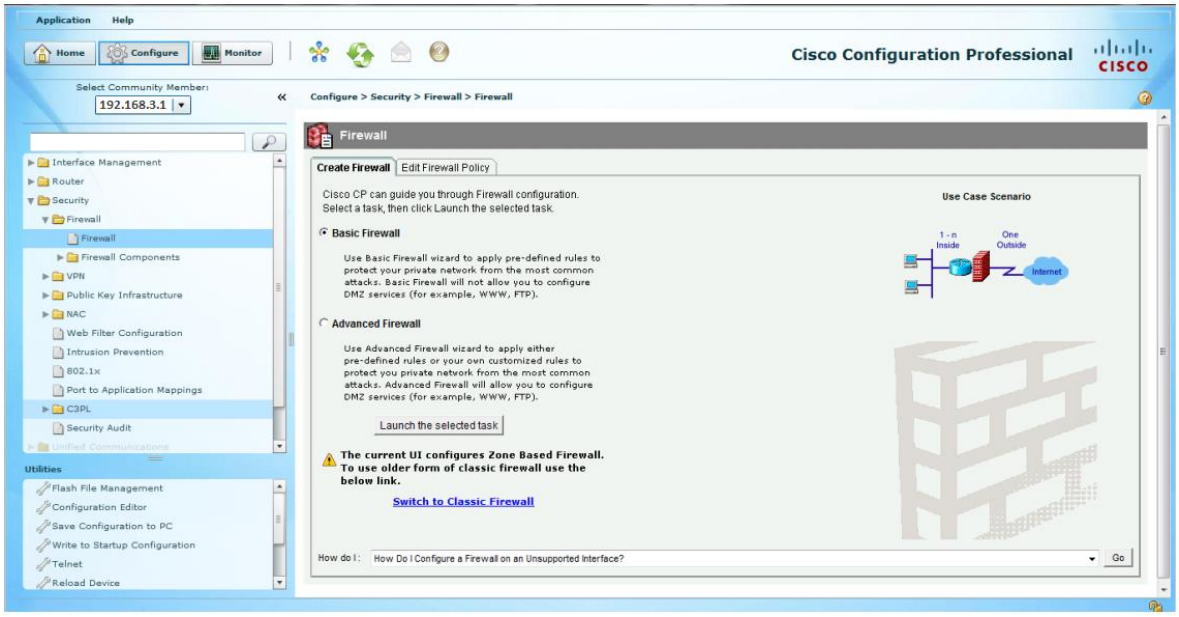


Ilustración 6. Firewall CCP

Se selecciona la interfaz que va a estar dentro y fuera del router 1 y le damos a siguiente

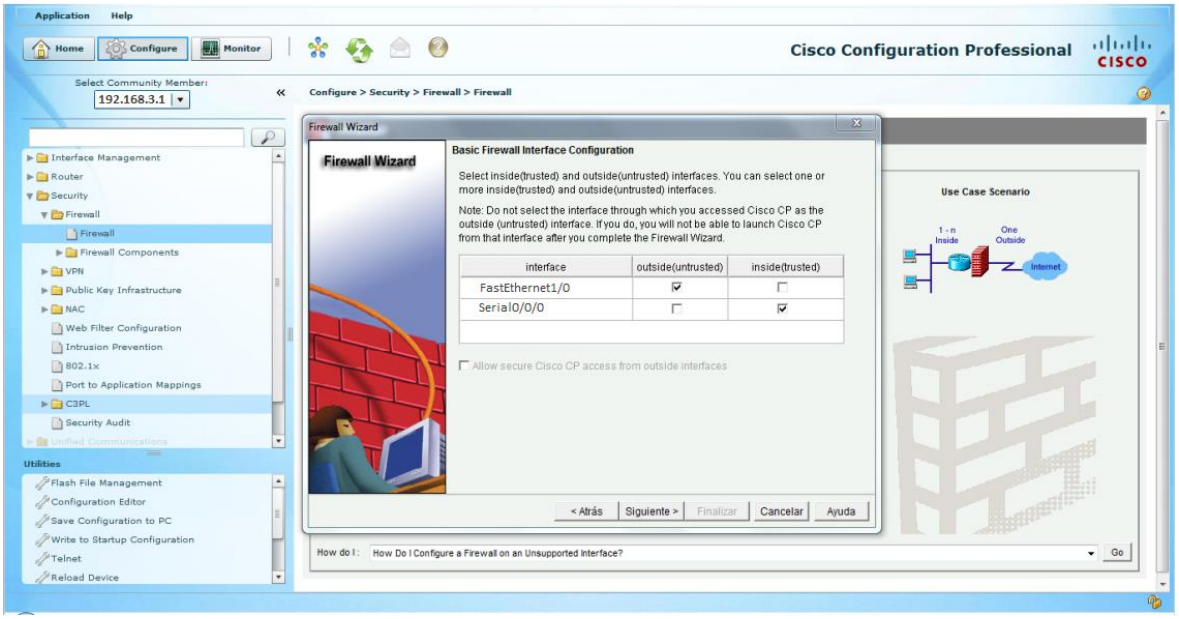


Ilustración 7. Selección interface CCP

Se coloca la seguridad a nivel bajo del firewall y le selecciona siguiente

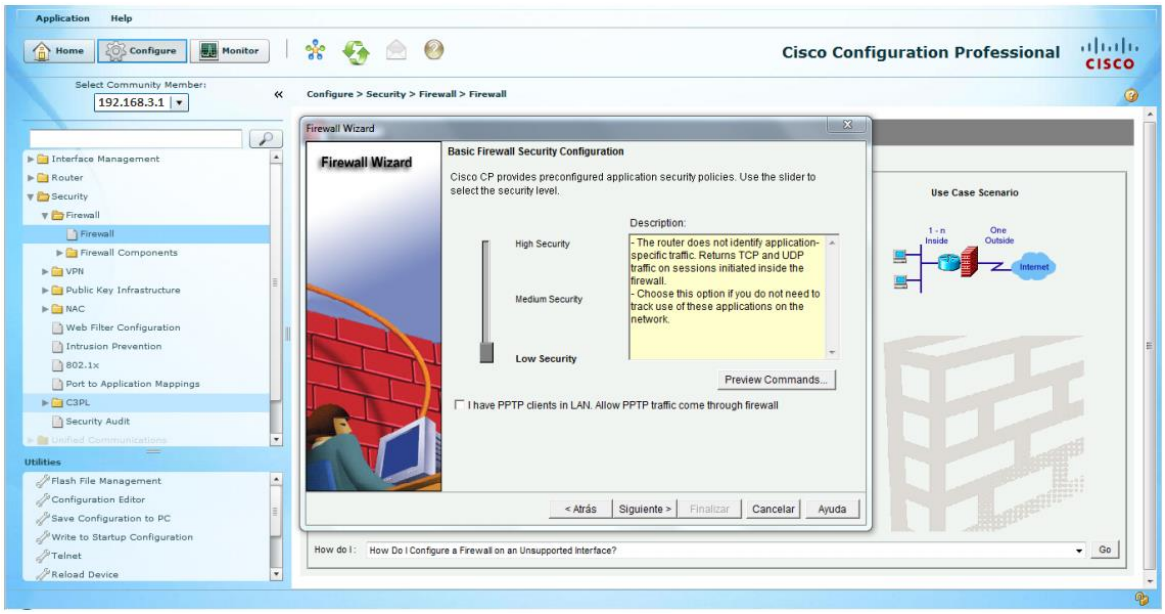


Ilustración 8. Seguridad Firewall CCP

Se permite las actualizaciones de eigrp a través del firewall y se selecciona siguiente.

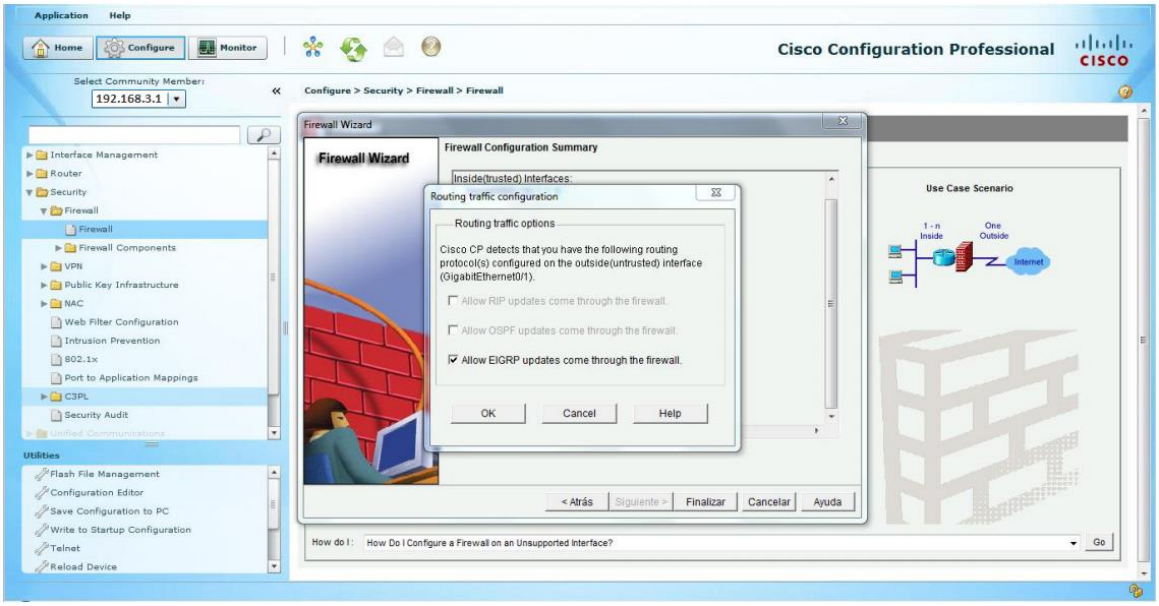


Ilustración 9. Permitir actualizaciónes CCP

Se marca la opción para que se guarden las configuraciones en el router y se selección deliver.

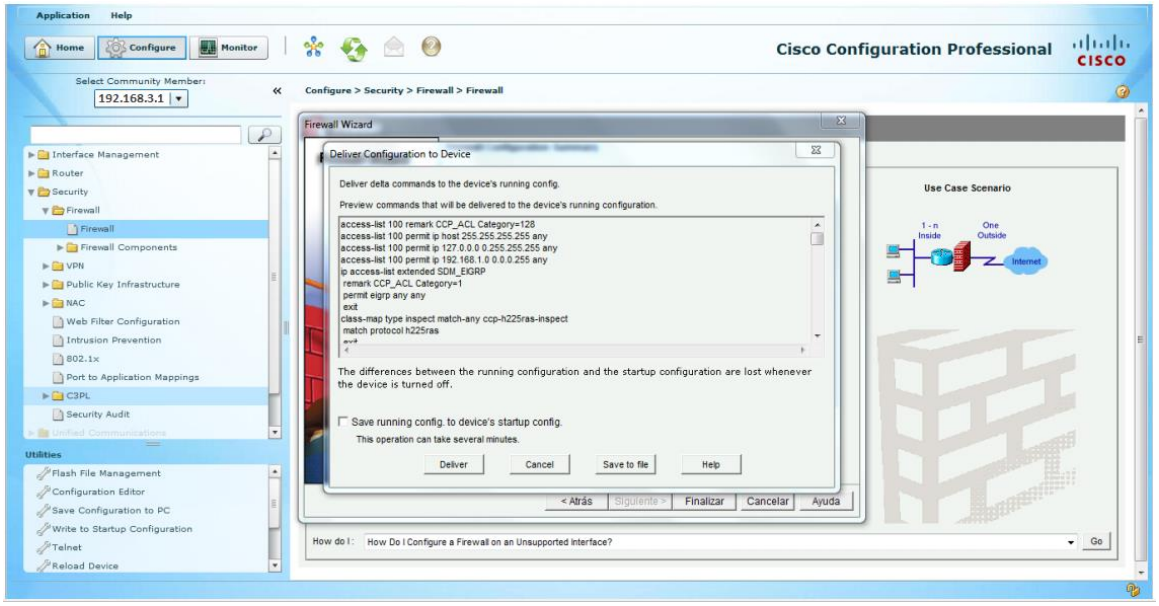


Ilustración 10. Guardar configuraciones CCP

Nos dirigimos a security > firewall >vpn> easy vpn server, enseguida se selecciona launch

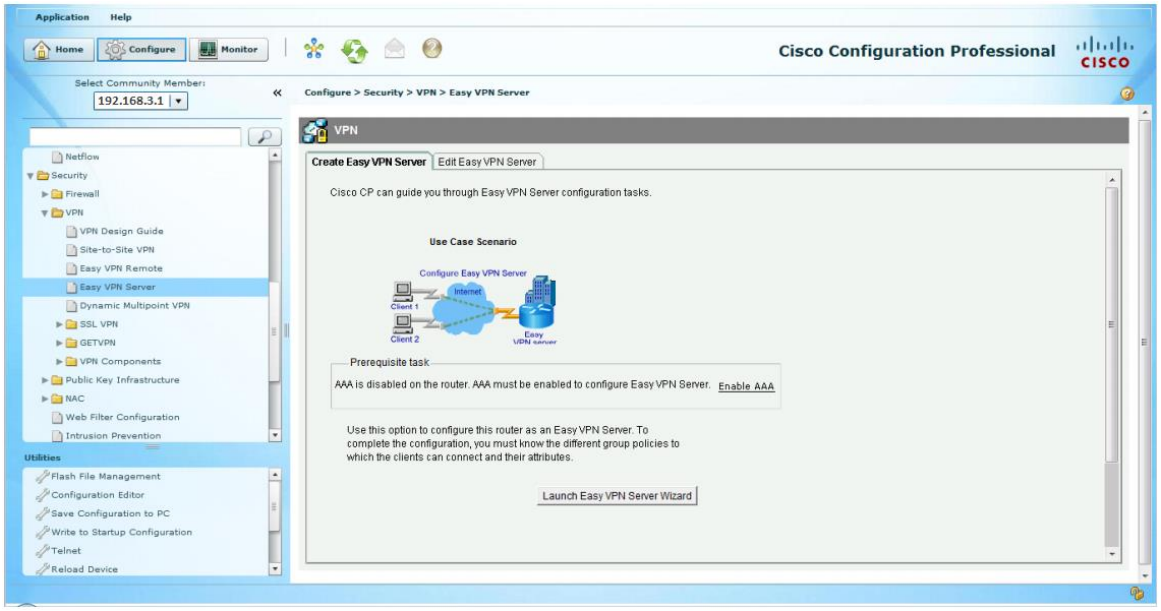


Ilustración 11. Launch easy Vpn CCP

Se pulsa la casilla de guardar la configuración en el router y se selecciona deliver para que tengan efecto los cambios

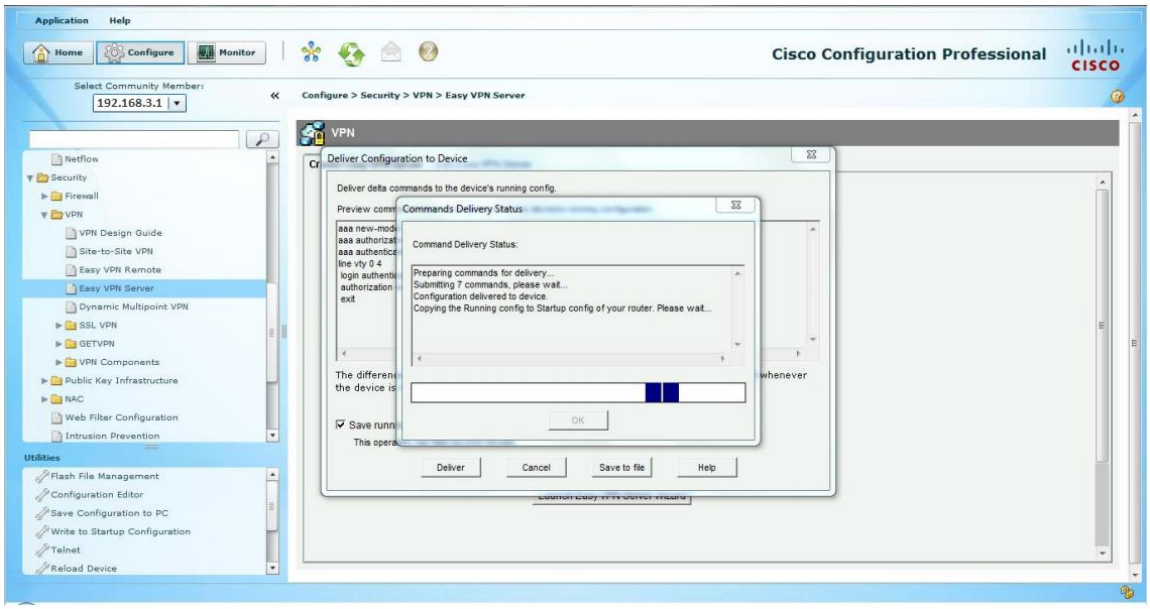


Ilustración 12. Deliver CCP

Nos saldrá esta pantalla de bienvenida, se selecciona siguiente

Ilustración 13. Pantalla de bienvenida Vpn CPP

Se marca la opción de unnumbered y seleccionamos el serial, le damos a siguiente

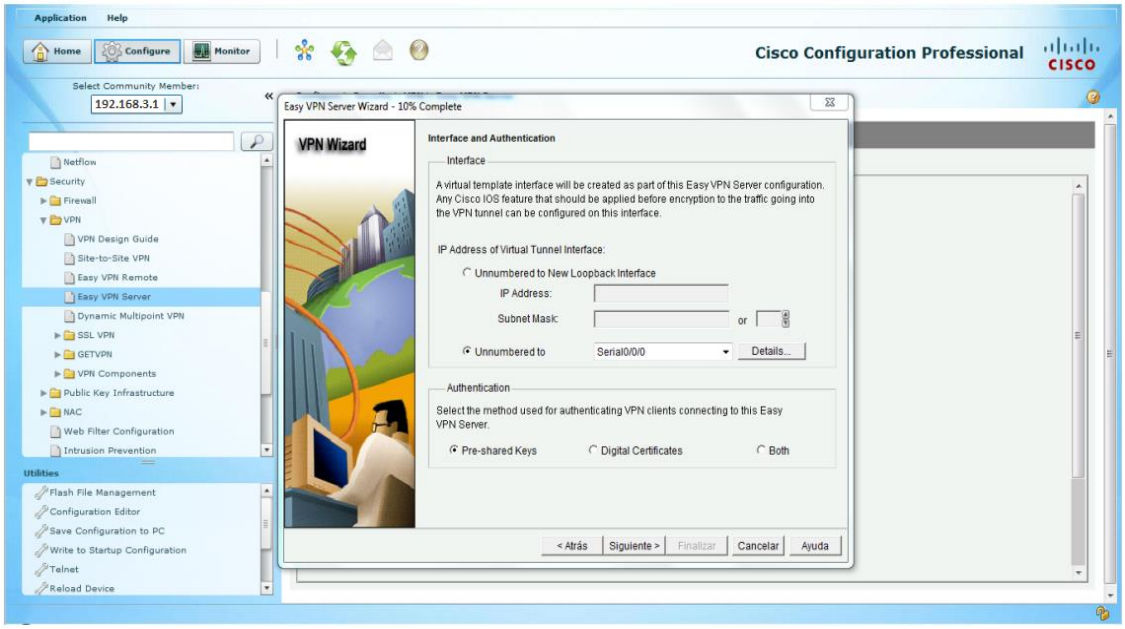


Ilustración 14. Unnumbered CCP

Se selecciona el que viene por defecto y seleccionamos siguiente

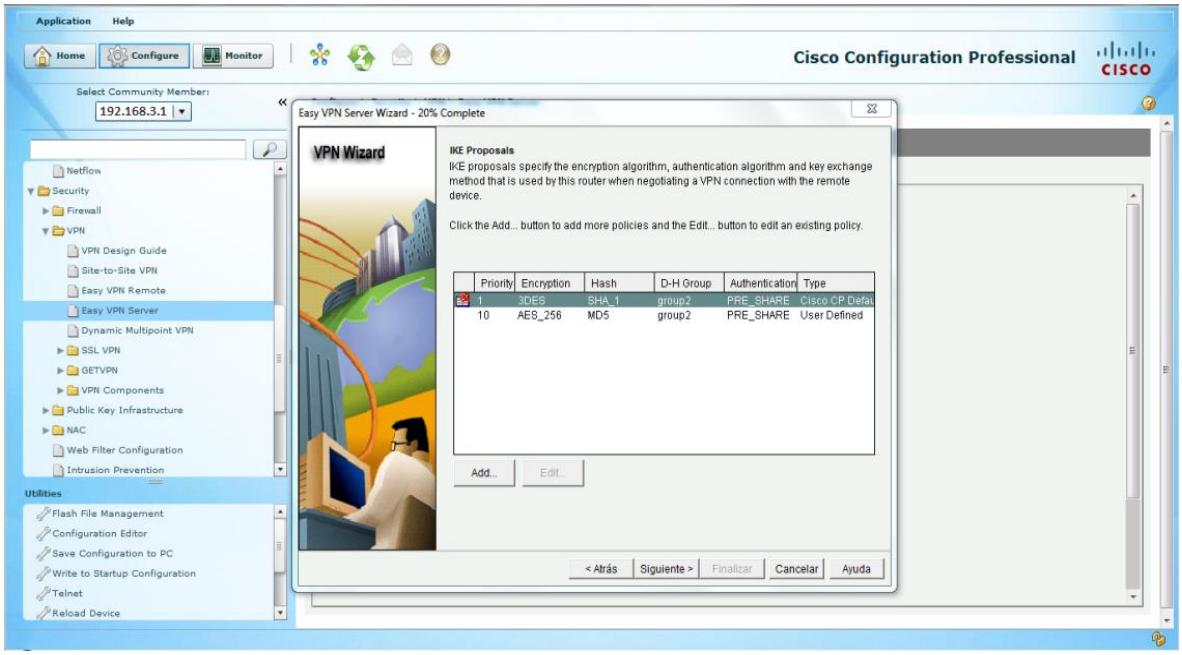


Ilustración 15. Group unnumbered CCP

Se selecciona la opción de método local y seleccionamos siguiente

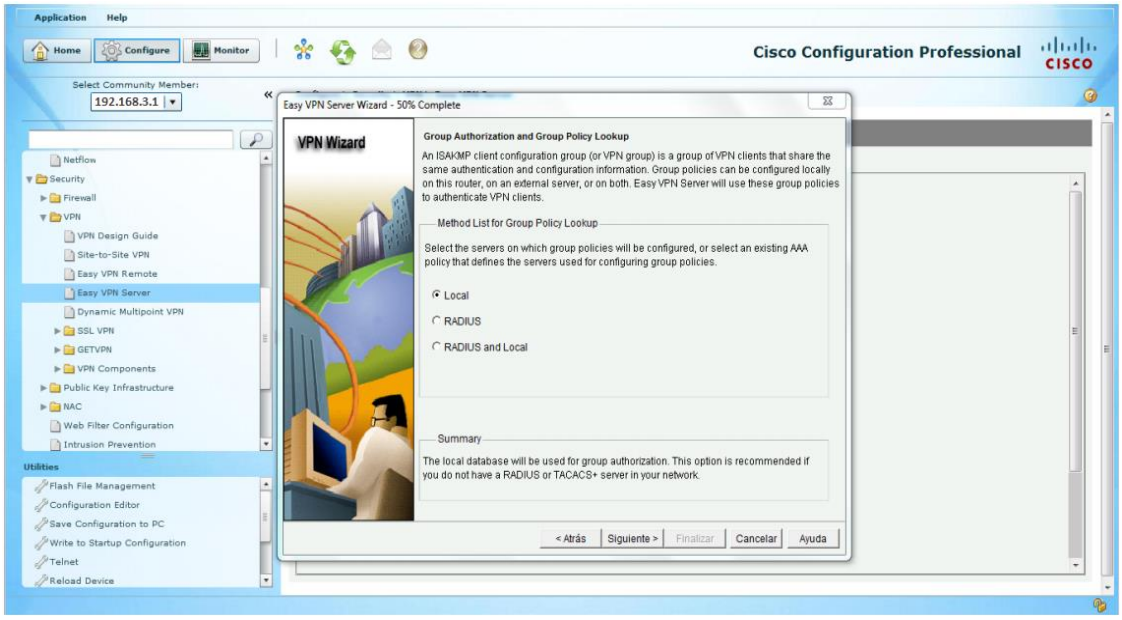


Ilustración 16. Opción método local CCP

Se habilitamos la autenticación por usuarios, luego se marca la opción de solo local.

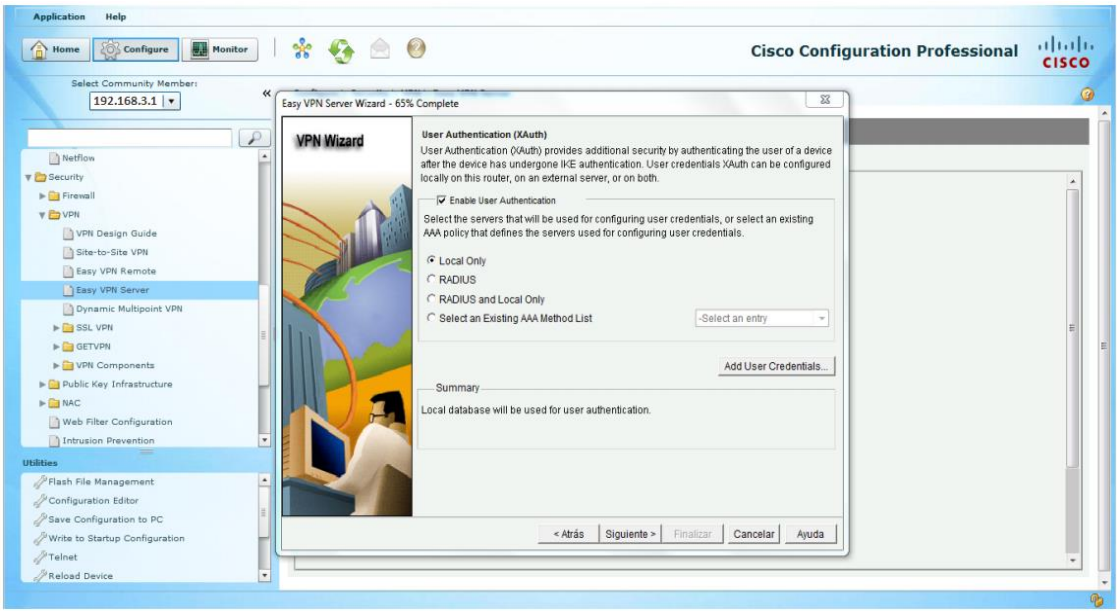


Ilustración 17. Autenticación por usuarios CCP

Se añaden los usuarios con su respectiva contraseña y se configura el nivel de privilegios en 1 y se elecciona Ok

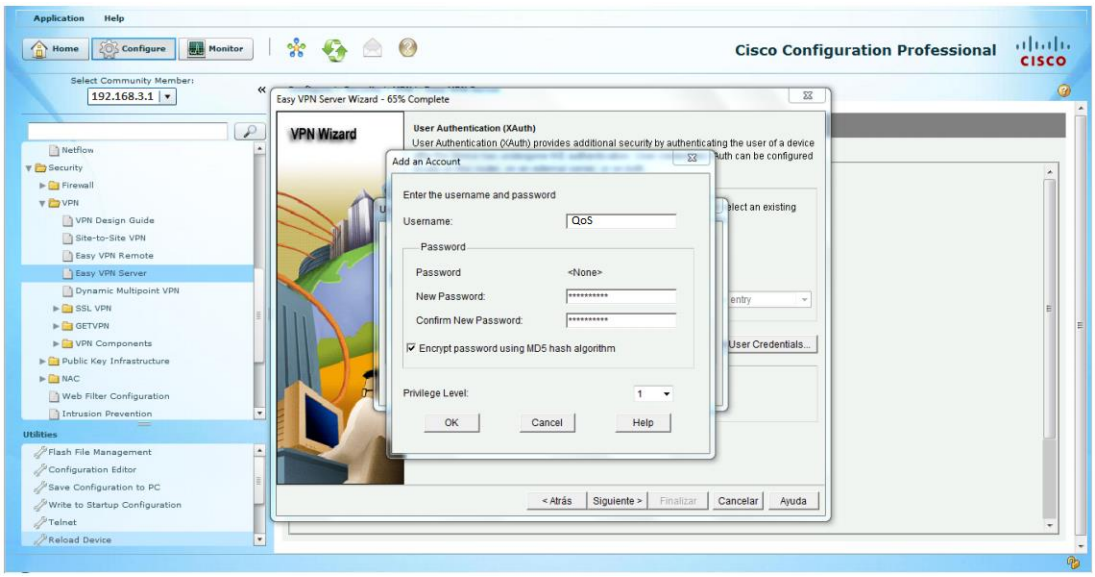


Ilustración 18. Agregación de usuarios CCP

Se crea el grupo y se configura una contraseña, y un rango de direcciones que se pueden conectar a la red a través de la vpn por acceso remoto.

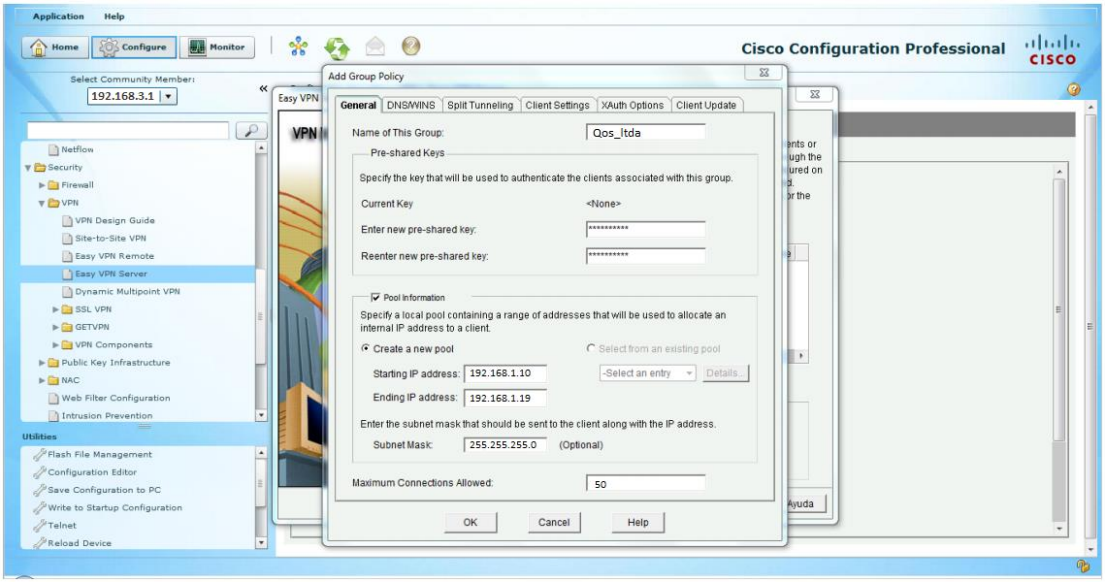


Ilustración 19. Creación de grupo CCP

En esta pantalla seleccionamos Ok.

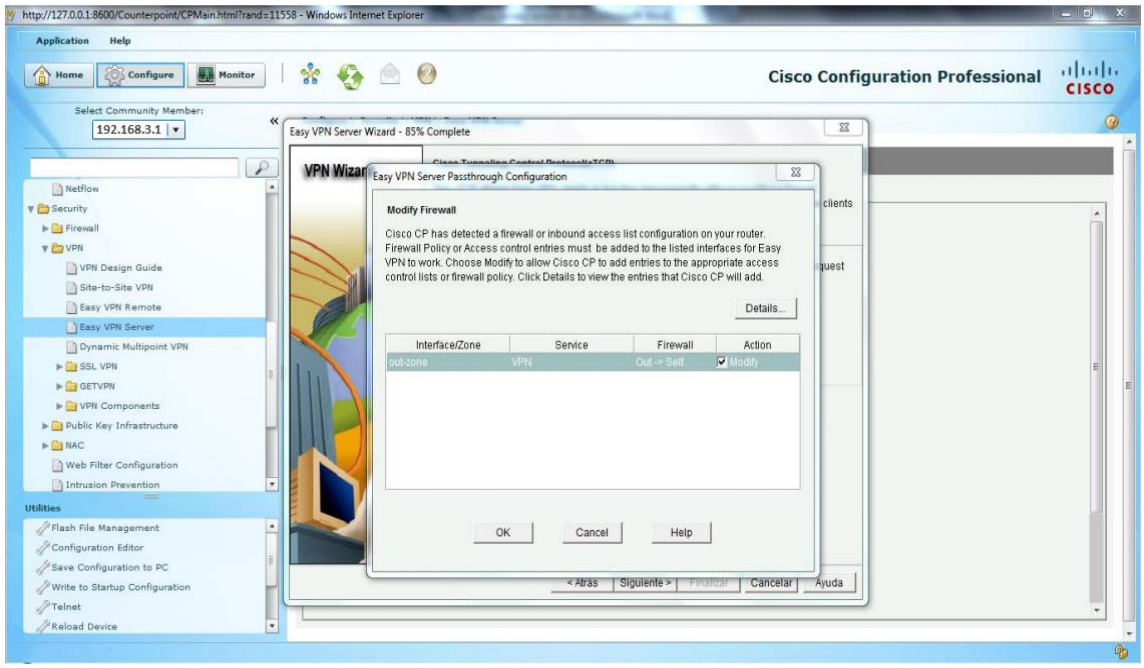


Ilustración 20. Creacion de grupo (2) CPP

Aparece un resumen y se selecciona finalizar

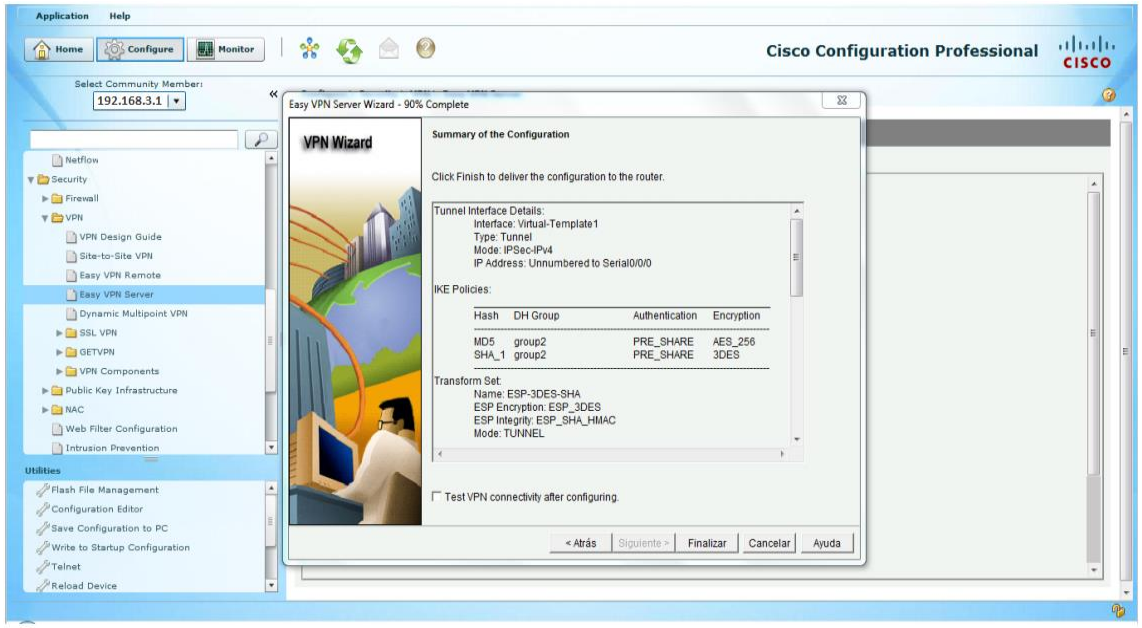


Ilustración 21. Resumen de configuración Vpn CPP

Seleccionamos la opción test tunnel y start, se espera a que termine el chequeo hasta que el túnel se encuentre en up.

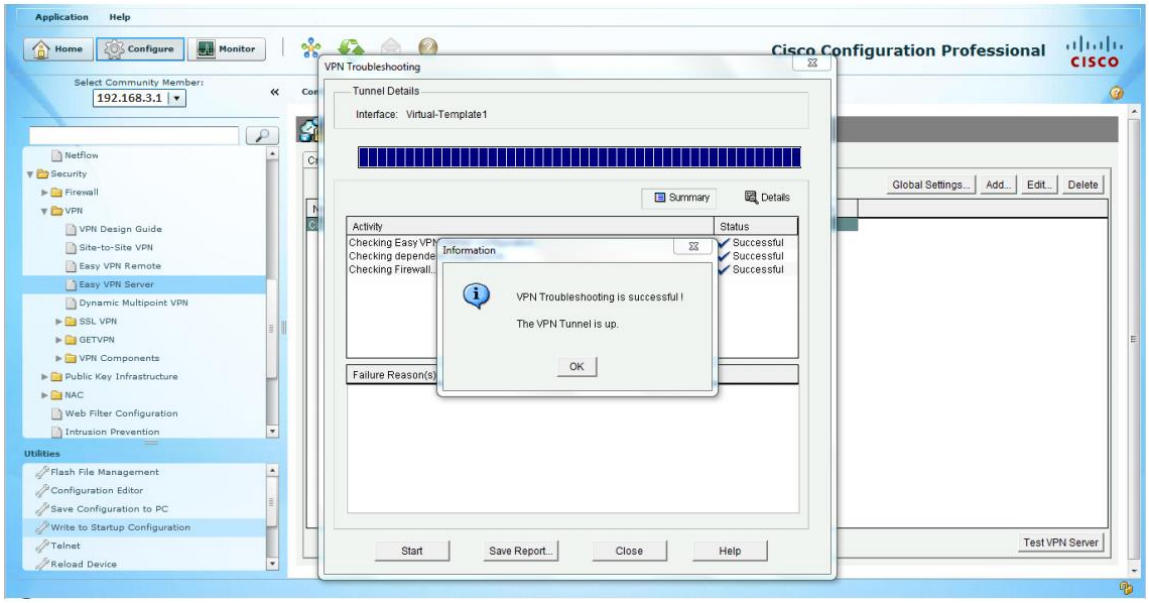


Ilustración 22. Finalizacion de la configuracion CPP

8.1. CUMPLIMIENTO DE LA NORMA ISO 27001 DE SEGURIDAD DE LA INFORMACIÓN

Hoy en día es muy importante para las empresas basarse en alguna norma internacional de seguridad con el fin de proteger su información. En esta ocasión el diseño de la red privada virtual segura en la empresa QOS LTDA. Se apoya en la norma ISO 27001 en materia de gestión de Seguridad de la Información. Desde su publicación en 2005, año en que ISO adoptó el estándar británico BS-7799-2 con la denominación ISO/IEC 27001:2005, la norma ha ido haciéndose muy importante en lo que se refiere a certificaciones en seguridad.

No obstante, ISO 27001 está muy lejos de alcanzar el grado de ajuste a nivel mundial de otros estándares de gestión, como, por ejemplo, el estándar que establece los requisitos de un sistema de Gestión de la Calidad: ISO 9001.

En Colombia, la norma ISO 27001 es de obediencia obligatoria en algunos sectores, tal como en el sector público (Decreto 1078 de 2015). Como en el caso de los operadores de información, que de acuerdo al Decreto 1931 de 2006, se hallan sujetos al cumplimiento del estándar.

Pero, el sector privado será quien con mayor fuerza pondrá a la norma ISO 27001 en un lugar más alto, debido al importante papel que puede desarrollar un sistema de gestión de la seguridad de la información (SGSI) en el ámbito del gobierno corporativo de las empresas en cuanto a gestión de riesgos se refiere.

8.1.1. CREACIÓN DE POLÍTICAS DE SEGURIDAD EN LA EMPRESA.

Para la garantizar la seguridad de la información en la empresa, es indispensable crear una política de seguridad para los usuarios que conforman la misma, se debe garantizar lo siguiente:

-No descargar música, películas u otros archivos no legales

-No abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados

-No visitar sitios web pornográficos o de contenido ilícito

-No proporcionar datos personales a desconocidos por teléfono o e-mail

-No utilizar la misma contraseña en diferentes páginas web o compartirlas.

-Descarga ilegal de software licenciado.

-Tráfico de material pornográfico.

-Uso de correo electrónico para fines personales.

-Transmisión a terceros de información confidencial.

-Identificar y priorizar los recursos informáticos de la empresa.

-Establecer condiciones de uso del correo y de navegación.

-Disponer de un plan de contingencia que contemple copias de resguardo, autenticación de usuarios, integridad de datos, confidencialidad de la información almacenada y control de acceso.

8.2. CREACIÓN DE GRUPO DE SEGURIDAD EN EL DIRECTORIO ACTIVO

Se realizará la creación de un grupo de seguridad VPN (puede ser nombrado de cualquier manera) en el directorio activo el cual ya dispone la empresa. Luego de la creación del grupo, se asociaron únicamente a los usuarios que pueden tener acceso. Esta configuración puede ser implementada en pequeñas, medianas y grandes empresas.

8.3. ESTUDIO DE FACTIBILIDAD

El proyecto es factible ya que, con este, se obtendrá un servicio estratégico para fortalecer y expandir la base de los clientes corporativos, claves para reforzar la seguridad, entre otros; brindando solución a los principales problemas de la empresa QOS LTDA. Como lo son: facilidad de comunicación entre ordenadores y usuarios de la red, seguir manteniéndose como empresa líder en el mercado y por ultimo ahorro de dinero.

IPSEC VPN es la más óptima debido a que la seguridad y la velocidad son mayores. Además, ofrece una mejor trasmisión de los paquetes; por otro lado, se cuenta con un túnel necesario para enviar y recibir datos, por su menor tiempo de ejecución, por su fácil configuración, es independiente al medio.

9. RECOMENDACIONES

A medida que se va desarrollando el tema de investigación y se le va dando mayor importancia a su utilidad, nos podemos dar cuenta que su implementación generara un gran impacto en cuanto a la organización y producción de la empresa para ello cabe desatacar que algunas aplicaciones que necesitan de procesos bastantes complejos las cuales se tienen que ejecutar en máquinas solamente dedicadas a esas operaciones ya que como son procesos bastantes pesados como cálculo de planillas, requieren ser procesadas por maquinas potentes y dedicadas a esta labor para que no se sienta algún retardo o problema en la interconexión.

Otro punto a tener en cuenta es el proveedor de servicio de Internet que se va a utilizar, si bien es cierto existen varios proveedores que nos pueden proporcionar este servicio, algunos que nos proporcionan un buen servicio son realmente muy caros para mantener en una empresa relativamente pequeña, y los que ofrecen una interconexión a Internet con precios módicos, su servicio es muy inestable y en algunos casos con interrupciones en el servicio de manera constante haciendo imposible una conexión VPN cuando se ejecutan procesos largos, es por eso necesario la constante evaluación de los proveedores de servicio de Internet.

- Verificar la calidad de los dispositivos empleados para la instalación de la red.
- Para el buen manejo de los equipos de comunicación se debe capacitar a los empleados que van a estar a cargo de estos; para que el uso de la red sea más eficiente.
- Para las personas que hacen uso de esta red, deben tener mucho cuidado en el manejo de la información para evitar la fuga de esta hacia externos.
- Para la empresa, mantenerse informada de los avances de la tecnología en lo que se refiere en materia de red, para poder mantenerse a la vanguardia de la actualidad.
- Dar mantenimiento a la Red cada cierto tiempo.

9.1. DIAGNOSTICO

La empresa QOS LTDA, por la naturaleza de su operación, tiene intercambio de datos con diversas fuentes de información, en su mayoría son en sitios de área local e internet, por lo cual se requiere tener una conexión segura, que mantenga la confidencialidad e integridad de los datos desde su origen hasta el destino de recopilación de los datos.

A medida que una empresa crece, podría ampliar a múltiples tiendas u oficinas en todo el país y alrededor del mundo. Para que todo funcione de manera eficiente, las personas que trabajan en esos lugares necesitan una forma rápida, segura y fiable de compartir información a través de redes informáticas.

Una tecnología popular para lograr estos objetivos es una VPN (red privada virtual). Una VPN es una red privada que utiliza una red pública (usualmente Internet) para conectar sitios remotos o usuarios en conjunto. El VPN usa conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa en el sitio remoto. Mediante el uso de una VPN, las empresas pueden garantizar la seguridad, quiere decir que cualquier persona que intercepte los datos cifrados no puede leerlo.

VPN, no fue la primera tecnología en hacer las conexiones remotas. Hace varios años, la forma más común de conectar equipos entre múltiples oficinas era mediante el uso de una línea arrendada. Las líneas arrendadas como la RDSI (Red Digital de Servicios Integrados, 128 Kbps), son conexiones de red privada que una empresa de telecomunicaciones puede arrendar a sus clientes. Las líneas arrendadas son una forma para la empresa de ampliar su red privada más allá de su área geográfica

inmediata. Estas conexiones forman una sola red de área amplia (WAN) para el negocio. Aunque las líneas arrendadas son fiables y seguros los contratos de arrendamiento son caros, con precios crecientes como la distancia entre oficinas aumenta.

Hoy en día, Internet es más accesible que nunca y los proveedores de servicios de Internet (ISP) siguen desarrollando servicios más rápidos y confiables a un menor costo que las líneas arrendadas. Para tomar ventaja de esto, la mayoría de las empresas han reemplazado las líneas arrendadas con las nuevas tecnologías que utilizan conexiones de Internet sin sacrificar el rendimiento y la seguridad. Las empresas comenzaron por establecer intranet, que son redes internas privadas diseñadas para uso exclusivo de los empleados de la compañía. Intranet habilita colegas distantes a trabajar juntos a través de tecnologías como el uso compartido de escritorio. Mediante la adición de una VPN, una empresa puede extender todos los recursos de la intranet para los empleados que trabajan desde oficinas remotas o en sus hogares.

10. ALCANCES Y LIMITACIONES

10.1. ALCANCES

- Se podrá autorizar la conexión de usuarios remotos hacia la LAN interna de la empresa mediante métodos de autenticación y cifrado de datos de forma segura.
- La VPN representa una gran solución para la empresa en cuanto a seguridad, confidencialidad e integridad de datos; reduciendo significativamente el costo de la transferencia de datos de un lugar a otro.

10.2. LIMITACIONES

- Al establecer las políticas de seguridad y de acceso, porque si esto no está bien definido, pueden existir consecuencias serias.
- El rendimiento y la fiabilidad dependen del ISP (proveedor de internet).
- Requiere una comprensión detallada de los conceptos de seguridad de redes.
- Se debe realizar una cuidadosa instalación y configuración.
- Problemas de compatibilidad.
- No se tienen los permisos adecuados para la implementación física por lo que se opta a realizarse en simulación packet tracer.

11. CONCLUSIONES

En la actualidad las VPN ofrecen un gran servicio para las empresas que quieran tener una comunicación segura con sus proveedores, clientes u otros, sin necesidad de implantar una red de comunicación costosa que permita lo mismo.

Los indiscutibles beneficios en infraestructura y costos a nivel empresarial que ofrece la creación de Redes Privadas Virtuales como soporte de las comunicaciones corporativas en la empresa QOS LTDA. Son el principal logro que otorga este proyecto de modalidad de grado en la interconexión de las áreas que conforman esta empresa. Esta implementación de VPN ofrece garantía de seguridad en los datos y fácil implementación, debido a que estas reemplazaran las conexiones dedicadas punto a punto por cables físicos al utilizar la Internet como su estructura y camino esencial.

Se concluye que las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que representan una excelente tecnología de acceso remoto.

Se cumplió con el objetivo principal, el cual era diseñar una red privada virtual segura para facilitar la comunicación, trabajo y flujo de información de la empresa QOS LTDA ubicada en la ciudad de Bogotá, basados en la norma internacional seguridad ISO 27001.

12. BIBLIOGRAFÍA

BROWN SMITH, Steven. Implementación De Redes Privadas Virtuales. Houston: Editorial McGraw-Hill Interamericana Editores, 2008. 594 p.

MARTINEZ HERNANDEZ, Claudio. Los Piratas Del Chip. Venezuela: Libros Digital S.A, 2002. 310 p.

KOHL PARKT, Neuman. The Kerberos Network Authentication Service. Broome: association of publishers Australia, 1993. 330 p.

POSTEL SINGHT, Brandon. Internet Control Message Protocol, Manchester: Editorial Fontana, 1981. 240 p.

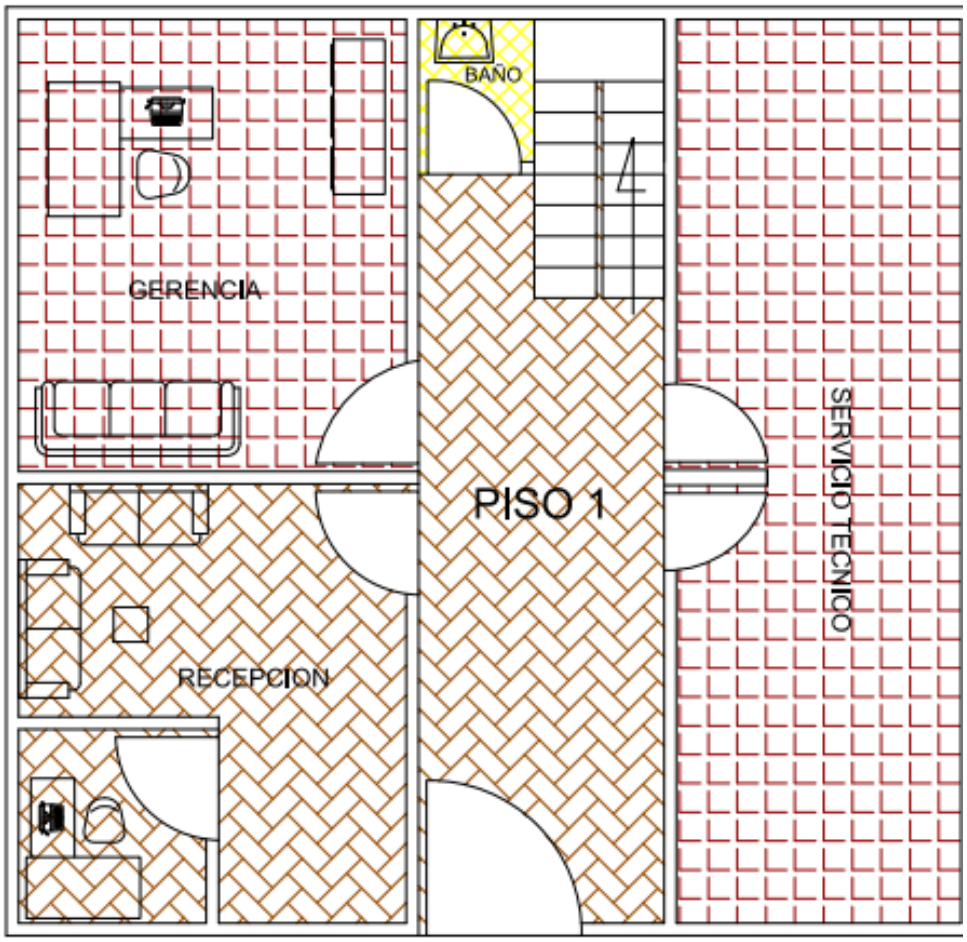
POSTEL SINGHT, Brandon. Considerations for IPv4 Internet Group Management Protocol IGMP. Manchester: Editorial Fontana, 2002. 415 p.

MENDILLO, Vicencio. Comunicaciones Seguras con Red Privada Virtual (VPN). Caracas. 2011 Universidad Central de Venezuela, Facultad de Ingeniería.

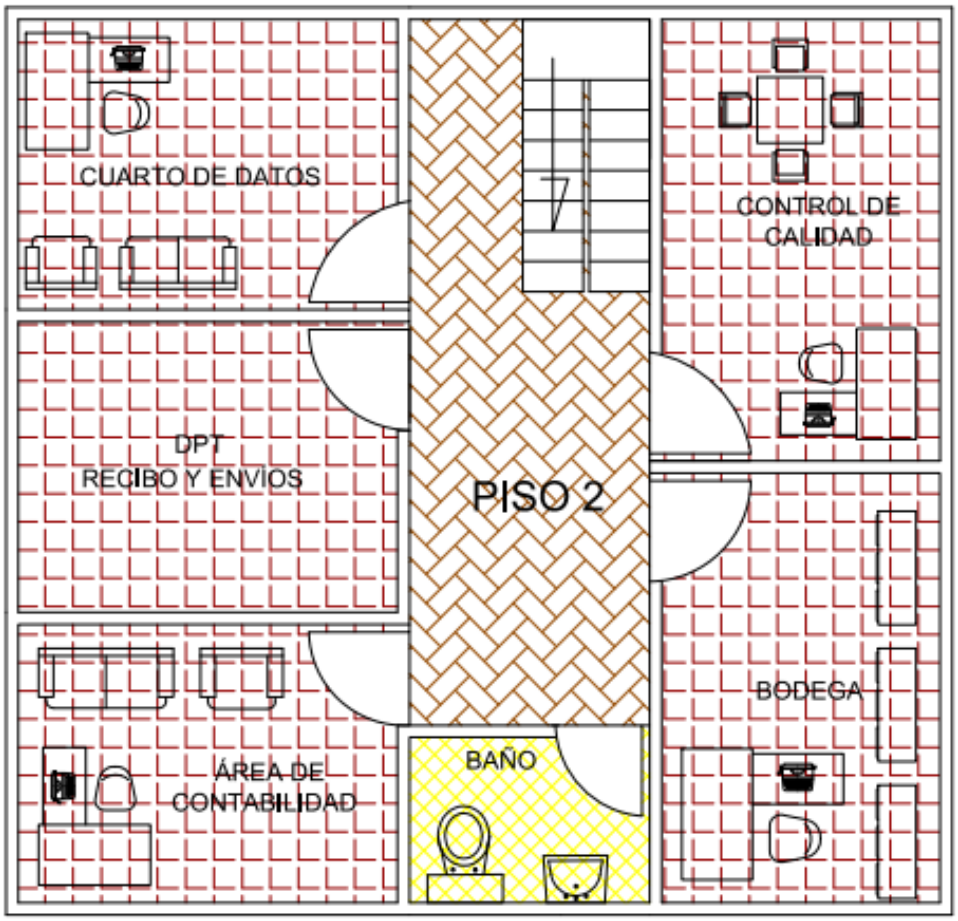
GFULLAGE, “Cómo las Redes privadas virtuales funcionan”. {13 de octubre de 2008} disponible en: (https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html).

CISCO (2010). Red privada virtual. [15/04/2018]. Disponible desde Internet en: <http://www.cisco.com/web/LA/soluciones/la/vpn/index.html>

ANEXOS



ANEXOS 1. Planta 1 QoS Ltda



ANEXOS 2. Planta 2 QoS Ltda

Bogotá, D. C., __dd___ / __mmm__ /__aaaa___

Con relación al contrato de trabajo suscrito con la **SUPERINTENDECIA DE NOTARIADO Y REGISTRO** Yo _____ Identificado con cédula de ciudadanía No. _____ de _____, estoy de acuerdo en tratar estrictamente y en forma confidencial toda la información que pueda adquirir de cualquier manera y desde cualquier fuente, mientras desempeñe las funciones propias del cargo asignado a mi nombre. Así mismo me comprometo a devolver la información confidencial a la que haya tenido acceso en el momento que termine la relación contractual, y que a pesar de dicha terminación, la obligación de confidencialidad y secreto permanecerá vigente durante un plazo de 2 años después de finalizada la relación contractual con la Entidad.

Yo entiendo que **Información Confidencial** significa: Es información que su divulgación de forma no autorizada generaría desventajas competitivas, pérdidas económicas, afectar negativamente a la Entidad, a los funcionarios y/o a los clientes (ciudadanos); pero pueden ser entregada sujeto a la normativa vigente. Incluye los nueve delitos (09) delitos tipificados en la ley 1273 de 2009 que describen los atentados contra la confidencialidad, integridad y disponibilidad de la información en Colombia.

Dentro de esta categoría se encuentran los datos e información personal semiprivada: "Datos e información personal que no es de dominio público, pero que ha sido obtenida u ofrecida por orden de una autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de administración de datos personales. Esta información puede ser o no sujeta a reserva por su titular". Así mismo también se incluyen todos los datos de los clientes, los datos personales de los funcionarios, la información de planes y proyectos estratégicos de la Entidad y toda aquella información relacionada con la operación de los servicios ofrecidos por la SNR.

Yo acepto y estoy de acuerdo que no divulgaré directa o indirectamente cualquier tipo de información confidencial, secreta ni ultra secreta a ninguna persona, a excepción de personal específico designado por la SNR, quienes tengan la necesidad de conocer esta información para cumplir con las responsabilidades de su trabajo y obligaciones del negocio, y que hayan firmado un acuerdo de confidencialidad similar.

Acepto y estoy de acuerdo que no sustraeré o removeré ningún tipo de información confidencial, secreta y/o ultra secreta de alguna de las áreas o linderos de la Entidad ni de los sistemas sin la previa autorización o permiso del Comité de Seguridad o en su defecto el Oficial de Seguridad. Adicionalmente acepto y estoy de acuerdo que no me apropiaré de ninguna información confidencial, secreta y/o ultra secreta para mi uso particular o el de otra entidad.

Acepto y estoy de acuerdo en cumplir todas las Políticas del Sistema de Gestión Integrado, Calidad y Seguridad de la Información, tanto Institucionales como de los Terceros con los cuales esté relacionada mi labor, y así ayudar a asegurar la Calidad, Confidencialidad, Integridad y Disponibilidad de la Información bajo mi cuidado. Acepto y entiendo que cualquier falta en cumplimiento de los términos de éste acuerdo podrá resultar desde una acción disciplinaria, la terminación de contrato con justa causa o la acción penal respectiva.

Éste acuerdo se hace retroactivo desde el momento de firma del contrato de trabajo respectivo, suscrito entre la **SUPERINTENDECIA DE NOTARIADO Y REGISTRO** y el Trabajador.

Firma del trabajador, Cargo,

_____ _____

LISTADO DE VERIFICACION PARA LA EVALAUACION DE LA PRESENTACION Y SOCIALIZACION DEL INFORME DE SEMINARIO DE PERFECCIONAMIENTO

DIMENSION	CRITERIOS		CUMPLE	NO CUMPLE
	ASPECTOS DE FONDO			
EVALUACION INFORME FINAL	DISEÑO DE INGENIERIA	El diseño de ingeniería responde a la solución propuesta en el problema.		
		El diseño de ingeniería propuesto se elaboró considerando en los objetivos planteados		
		La solución que sustenta el diseño de ingeniería propuesta se ha estructurado conforme a los alcances, principios, componentes de los sistemas de gestion abordados.		
		El diseño de ingeniería presenta un plan de mejoramiento, técnicamente bien elaborado.		
		Se elabora una propuesta económica consistente con la formulación del plan de mejoramiento.		
	CONCLUSIONES	Las conclusiones se encuentran asociados con los objetivos específicos.		
		Las conclusión develan de forma clara cuales fueron los logros, alances, beneficios y proyecciones futuras para el desarrollo de los procesos y áreas involucras, vistas desde los sistemas de gestión abordados.		
		Las recomendaciones garantizaban ofrecer la sostenibilidad y permanencia		

	RECOMENDACIONES	de los sistemas de gestion intervenidos, con posibilidades de mejora continua.		
		Las recomendaciones se encuentran asociadas con los alcances, componentes y principios que sustentan los sistemas de		
	ASPECTOS DE FORMA			
	PRESENTACION DEL TRABAJO	El informe se encuentra redactado de forma correcta, siguiendo normas de gramática.		
		El trabajo cumple con las normas de presentación de la norma 1486 de ICONTEC.		
		El trabajo contiene todos los capítulos requeridos.		
	TRATAMIENTO DE LA INFORMACION	Solidez y consistencia interna en el tratamiento metodológico y técnico.		
		Claridad y coherencia conceptual.		
		Originalidad y manejo de la información, frente al tema propuesto.		
		Se encuentra coherencia entre la relación de las partes del trabajo.		
		El trabajo evidencia fuerza argumentativa para presentar conclusiones.		
EVALUACION SUSTENTACION	**APORTES E INNOVACION**	Presenta aportes importantes y significativos al mejoramiento de los procesos técnicos, tecnológicos y administrativos, basados en la aplicación de los sistemas de gestion en la empresa objeto de intervención.		

	APLICACIÓN DE CONOCIMIENTOS	Se demuestra con sólidos argumentos la aplicación, transferencia e innovación de conocimientos abordados en el desarrollo del seminario..		
	DESARROLLO DEL PERFIL	Las exposiciones permiten evidenciar el desarrollo potencial de competencia profesionales, destrezas, habilidades propias del campo disciplinar.		
	CAPACIDAD PARA RESOLUCION DE PROBLEMAS	Se evidencian argumentos suficientes para resolver problemas de forma eficiente acorde a las actuaciones profesionales.		
	INTEGRACION	Se presentan una aplicación bien lograda y articulada de los sistemas de gestion aplicados.		
	RELEVANCIA	Se presentan argumentos suficientes y sustentados para demostrar que los resultados logran en alto grado satisfacer necesidades de la empresa, objeto de intervención.		
	PERTNENCIA TECNICA	Las propuestas y las recomendaciones se delimitan con un alto grado de Factibilidad técnica demostrable.		

ANEXOS 4. Listado de verificación.