ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE RIESGOS DE LA RED IP/MPLS DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES, BASADO EN LA NORMA ISO/IEC 27005 Y PROPUESTA DE MEJORAMIENTO DEL CONTROL DE ACCESO A LA ADMINISTRACIÓN DE SUS DISPOSITIVOS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

FALCONÍ NORIEGA MARCO FABRICIO
fafaltg@hotmail.com

RODRIGUEZ GARCIA LUCIA SILVERIA
lu5_8@hotmail.com

DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO
phidalgo@ieee.org

Quito, Enero 2012

DECLARACIÓN

Nosotros, Marco Fabricio Falconí Noriega y Lucia Silveria Rodríguez García, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Marco F. Falconí N. Lucia S. Rodríguez G.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Marco Falconí y Lucia Rodríguez, bajo mi supervisión.

_____

Ing. Pablo Hidalgo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Al Ingeniero Pablo Hidalgo, por su valiosa guía y honrosa colaboración para el desarrollo y culminación del presente Proyecto de Titulación.

A los ingenieros del Área O&M Plataforma IP/MPLS de la Corporación Nacional de Telecomunicaciones E.P., por las facilidades brindadas durante el desarrollo del presente proyecto, de manera especial al Ingeniero Andrés Almeida por su gratificante predisposición, orientación y colaboración.

A nuestros maestros, por compartirnos sus conocimientos a lo largo de nuestra estadía en esta prestigiosa institución del saber.

Lucia Rodríguez

Fabricio Falconí

DEDICATORIA

A mis padres y hermanos pues la etapa que estoy concluyendo en mi vida es fruto de su sacrificio y comprensión, de sus palabras de aliento y motivación, de su estímulo y apoyo constante, mi triunfo es también el de ustedes. ¡Los amo!

A mis amigos por estar conmigo en los momentos buenos y malos, por su cariño y compañía, y por ser al igual que mi familia el empuje diario para culminar con éxito una más de mis metas.

Va por ustedes, pues fueron quienes se constituyeron en la mayor motivación para día a día, escalón tras escalón, lograr alcanzar este objetivo, se los dedico, pues es un logro más en mi vida y ustedes forman parte de ella.

Fabricio Falconí

DEDICATORIA

A Dios por ser la luz que guía mi camino.

A mis padres, María y Virgilio las personas que más quiero y admiro, y quienes son mi fuente de inspiración; a mis hermanos José, Paola y Diego por su esfuerzo y apoyo incondicional, lo que ha hecho posible poder cumplir una meta más en mi vida profesional.

Y a todos quienes creyeron en mí.

Lucia Rodríguez

ÍNDICE DE CONTENIDOS

CONTENIDO

CAPÍTULO 1
MARCO TEÓRICO

1.1 RED IP/MPLS

CAPÍTULO 2
SITUACIÓN ACTUAL DE LA RED IP/MPLS DE LA CNT E.P.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANEXOS

RESUMEN

Se realiza un análisis de riesgos de la red IP/MPLS de la Corporación Nacional de Telecomunicaciones, en base a la norma ISO/IEC 27005, y un estudio del control de acceso a la administración de los dispositivos de la red IP/MPLS. Producto de este trabajo, se proponen controles, normas y procedimientos para corregir las falencias encontradas, con el fin de garantizar que la red esté siempre operativa.

En el capítulo 1, se realiza una introducción a las redes IP/MPLS, su arquitectura, elementos, funcionamiento y aplicaciones; se incluye un enfoque sobre la seguridad de la información, elementos de la seguridad, vulnerabilidades, amenazas, ataques, atacantes y se describe la norma ISO/IEC 27005.

En el capítulo 2, se estudia la evolución de la red IP/MPLS de la CNT E.P., su plataforma tecnológica, su proyección a corto plazo y el ACS v3.2 utilizado actualmente en la administración de sus dispositivos, las políticas y atributos que rigen su funcionamiento y se determinan las falencias presentes.

En el capítulo 3, se lleva a cabo el desarrollo del análisis de riesgos, se identifican los activos, amenazas y vulnerabilidades presentes; se determina el impacto y el nivel de riesgo ante la ocurrencia de un evento no deseado y se proponen los controles a aplicar para mitigar dichos riesgos.

En el capítulo 4, se proponen normas y procedimientos para mejorar el control de acceso a la administración de los dispositivos de la red IP/MPLS, se redefinen los atributos en los cuales se basa el funcionamiento del Sistema de Control de Acceso y se propone su actualización, además de una guía de configuración.

En el capítulo 5, se establecen las conclusiones y recomendaciones del proyecto.

Como anexo, se presenta el Protocolo de Pruebas de Aceptación realizado para demostrar las ventajas de actualizar el Sistema de Control de Acceso.

PRESENTACIÓN

El presente Proyecto de Titulación tiene como finalidad analizar los riesgos de la red IP/MPLS de la CNT E.P. en base a la norma ISO/IEC 27005 y proponer medidas para mejorar el control de acceso a la administración de sus dispositivos. Puesto que la CNT E.P. es una de las empresas más sólidas del país en el campo de las telecomunicaciones, es imprescindible garantizar su correcta operatividad.

La seguridad de la información es parte integral de las redes informáticas; es necesario disponer de tecnología, dispositivos, herramientas y técnicas que aseguren los activos de información: la información contenida y la infraestructura computacional a nivel de hardware y software, más aún cuando los ataques informáticos van en aumento.

Es de mucha importancia la realización del presente Proyecto de Titulación, pues permite determinar las vulnerabilidades y amenazas a las que está expuesta la seguridad informática de una organización y el impacto que ocasionarían en el negocio, para inmediatamente evaluar el riesgo de probables eventos no deseados y poder así establecer e implementar los controles necesarios para mitigar dichos riesgos.

De igual forma este trabajo refleja la importancia de contar con un Sistema de Control de Acceso de buenas características y configurado adecuadamente, al momento de evitar accesos no autorizados, no controlados o no deseados a la administración de los dispositivos de una red, que pudiesen afectar su correcta operatividad.

Aquellas organizaciones que estén interesadas en mejorar su seguridad informática, pueden considerar el presente proyecto, como una guía al momento de desarrollar un análisis de riesgos u optimizar el control de acceso a sus activos.

CAPÍTULO 1

MARCO TEÓRICO

1.1 RED IP/MPLS

1.1.1 INTRODUCCIÓN [1]

Internet considerada como la red de redes, es el medio de comunicación más utilizado hoy en día, interconecta redes pequeñas ampliando su cobertura y dando la posibilidad de intercambiar información entre ordenadores ubicados en cualquier parte del mundo.

Millones de personas utilizan Internet para realizar algún de tipo de actividad, sea ésta de conocimiento, de pasatiempo o de motivo laboral. Se puede acceder a una página web de forma instantánea y obtener información de diferente índole; de hecho, la mayoría de las empresas ofrecen sus servicios a través de una página web en Internet, en busca de obtener mayor competitividad.

Uno de los protocolos de comunicaciones[1] con el cual empezó a funcionar Internet y permitir la comunicación entre las máquinas que integran esta red, fue el protocolo IP (*Internet Protocol*) o Protocolo de Internet. IP proporciona un servicio de transporte de paquetes no fiable, por lo que se le conoce también como el protocolo del mejor esfuerzo; es decir, hace lo mejor posible pero garantizando poco.

IP es el protocolo mayormente utilizado por los ordenadores conectados a Internet, es compatible con cualquier sistema operativo y tipo de hardware. El incremento acelerado del Internet ha convertido al protocolo IP en la base de las

[1] Protocolos de comunicaciones: conjunto de reglas normalizadas que facilitan el intercambio de información y hacen que un sistema de comunicaciones funcione apropiadamente.

redes de telecomunicaciones; IP de acuerdo al modelo de referencia OSI[2] es el protocolo de capa de red[3]. Cabe recalcar que Internet fue inicialmente diseñado para transportar aplicaciones tolerantes en el tiempo, por ejemplo *e-mail*, FTP[4], Telnet[5], etc.

Entre las desventajas del protocolo IP se tienen: [2]

- IP es un protocolo no orientado a conexión, no existe previo acuerdo entre origen y destino antes de enviar información, por lo que no garantiza la entrega de los paquetes enviados.

- IP es ineficiente ante situaciones de congestión, al aumentar el nivel de tráfico en la red la entrega de los paquetes se vuelve un proceso lento. Si la congestión llega a ser crítica, se empiezan a descartar paquetes para reducir los niveles de congestión, sin realizar ningún tipo de distinción en el nivel de importancia que pudiera tener cada paquete.

- IP no maneja QoS (*Quality of Service*). La calidad de servicio hace referencia a conseguir el ancho de banda y la latencia[6] necesaria para una aplicación determinada, especialmente importante para aplicaciones denominadas “Tiempo Real” como la voz o video.

- Realiza un enrutamiento basado en software a nivel de capa de red, más lento que la conmutación a nivel de capa de enlace[7] del modelo OSI.

El crecimiento exponencial de usuarios en la red con gran volumen de tráfico y la aparición de nuevas aplicaciones en tiempo real: VoIP[8], telefonía móvil con

[2]OSI: *Open System Interconnection*, modelo utilizado como referencia para entender cómo funciona un sistema de comunicaciones, para ello define 7 capas.
[3]Capa de red: tercera capa del modelo OSI, se definen tres características principales: direccionamiento lógico, enrutamiento y ruteo.
[4]FTP: *File Transfer Protocol*, protocolo para la transferencia de archivos, basado en la arquitectura cliente-servidor.
[5] Telnet: acrónimo de *Telecommunications Network*, es un protocolo que permite acceder a través de una red a otra máquina remotamente.
[6] Latencia: suma de retardos temporales dentro de una red. El retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.
[7] Capa de enlace: segunda capa del modelo OSI, define los protocolos que determinan cuando un dispositivo puede enviar datos por un medio en particular.
[8] VoIP: *Voice over IP*, grupo de recursos (normas, dispositivos, protocolos) que hacen posible que la señal de voz viaje sobre el protocolo IP.

acceso a Internet, juegos en línea, videoconferencias, etc., que son tolerantes a pérdida pero no a retardo, han impulsado a desarrollar nuevas arquitecturas o tecnologías de red con la finalidad de asegurar que Internet pueda ofrecer calidad de servicio y satisfacer las necesidades de los usuarios, que cada vez son mayores.

Es así, que a mediados de los años 90 surgió una tecnología para satisfacer la gran demanda de ancho de banda y calidad de servicio requerida por los usuarios para aplicaciones multimedia; esta tecnología estaba preparada para ofrecer cualquier tipo de servicio que en su momento el usuario deseaba, se trataba de la tecnología ATM (*Asynchronous Transfer Mode*).

ATM o Modo de Transferencia Asincrónica, es la tecnología de capa enlace que transmite la información en pequeños paquetes de longitud fija denominados celdas. Una celda está formada por 53 bytes, 5 bytes de cabecera y 48 de datos. ATM está considerada como una tecnología de conmutación de celdas a altas velocidades.

ATM ofrece un servicio orientado a conexión, es decir, se establece una conexión previa al intercambio de información. Se utilizan canales o circuitos virtuales[9] (VC o *Virtual Circuit*) y caminos o rutas virtuales[10] (VP o *Virtual Path*), los cuales indican el camino fijo que la celda debe seguir evitando un desorden de las celdas al llegar a su destino.

En la figura 1.1, se tiene un ejemplo de una red IP sobre ATM, se puede observar la presencia de dos tipos de nodos: conmutadores ATM[11] y *routers* IP[12].

El modelo de IP sobre ATM fue ganando rápidamente su espacio ya que se

[9] Circuitos Virtuales: conexión unidireccional entre dos dispositivos a través de la cual se transmiten datos entre sí directamente, proporcionando la misma función que una línea alquilada física, pero sin un circuito físico.
[10] Rutas Virtuales: conjunto de circuitos virtuales, conectan tramos enteros de una red ATM, facilitan la conmutación de los circuitos virtuales.
[11] Conmutador ATM: responsable del tráfico de celdas en la red ATM, lee y actualiza la información en la cabecera de la celda y es conmutada rápidamente a una interfaz de salida a su destino.
[12] *Router* IP: dispositivo de capa 3 del modelo OSI, permite asegurar el direccionamiento de paquetes de datos, seleccionando la mejor ruta para ello.

lograba cubrir los requerimientos de ancho de banda requerido por los usuarios y con el establecimiento de rutas virtuales se podían ofrecer ciertos parámetros de calidad de servicio.

Sin embargo, el funcionamiento de IP sobre ATM implica la superposición de una topología virtual de *routers* IP sobre una topología real de conmutadores ATM, como se lo representa en la figura 1.1.

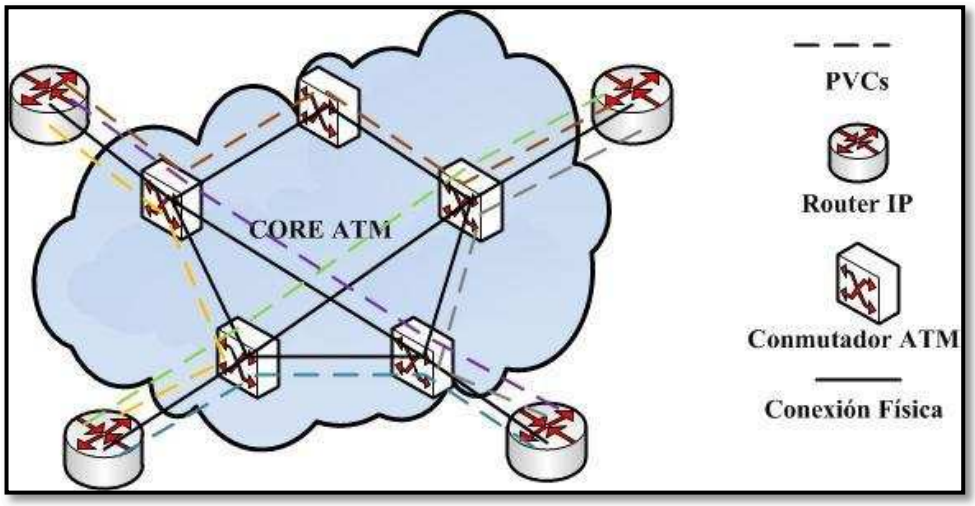


Figura 1.1: Red IP sobre ATM [2]

El *backbone*[13] ATM se presenta como una nube central rodeada por los *routers* IP de la periferia. Cada *router* se comunica con el resto mediante PVCs (Circuitos Virtuales Permanentes) que se establecen sobre la topología física de la red ATM.

Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los *routers* de la periferia. Los *routers* IP desconocen la topología real de la infraestructura ATM que sustentan los PVCs, los cuales son vistos como enlaces punto a punto entre cada par de *routers*.

A pesar de los beneficios que ofrece el modelo de red IP sobre ATM, se presentan ciertos inconvenientes: [2]

[13] *Backbone:* principales conexiones troncales y equipos en una red.

- Gestionar dos redes diferentes: una infraestructura ATM y una red lógica IP superpuesta, ocasionan a los proveedores de servicio mayores costes de gestión global de sus redes.

- Existe lo que se llama la "tasa impuesta por la celda", que es un desperdicio de ancho de banda (aproximadamente 20%) ocasionado por información adicional que viaja además de los datos en cada celda y que reduce en ese mismo porcentaje el ancho de banda disponible.

- La solución IP sobre ATM presenta problemas de crecimiento exponencial, ya que para n nodos IP se necesitan n * (n-1) circuitos virtuales para obtener una topología lógica completamente mallada. Por ejemplo, en una red con 5 nodos IP con una topología virtual totalmente mallada sobre una red ATM, se necesitarían 5 x 4 = 20 PVCs (uno en cada sentido de transmisión).

Es así que, con el afán de superar los inconvenientes que se presentan en el modelo de red IP sobre ATM, se buscó tener un tipo de tecnología que pudiera realizar un transporte mucho más eficiente del tráfico IP predominante en las redes.

Por esta razón, en 1997, el IETF (*Internet Engineering Task Force*) crea el grupo de trabajo MPLS (*MultiProtocol Label Switching*) para promover la creación de un estándar emergente encaminado a superar los retos del envío de paquetes IP.

La nueva tecnología debía tomar lo bueno de ATM y llevarlo al mundo IP, el resultado fue la creación del protocolo MPLS en 1998, establecido en la RFC[14] 3031.

Una red IP/MPLS se constituye de equipos que manejan el protocolo IP y MPLS.

[14] RFC: *Request for Comments*, documentos que sirven de referencia para la comunidad de Internet, en los que se especifican los estándares, tecnologías y protocolos relacionados con Internet y redes en general.

1.1.2 MPLS (*MULTIPROTOCOL LABEL SWITCHING*)

1.1.2.1 Concepto de MPLS

MPLS, Conmutación de Etiquetas Multiprotocolo, es una solución híbrida de última generación que toma lo positivo de las redes orientadas a conexión y lo integra con las redes no orientadas a conexión. Se le considera como la evolución de la arquitectura de red IP sobre ATM.

1.1.2.2 Características de MPLS

- Utiliza direcciones IP, como direccionamiento de capa de red del modelo OSI.
- Multi-protocolo, diseñado para soportar varios protocolos no solamente IP.
- Utiliza trayectos virtuales a través de los cuales viajan los paquetes; estos trayectos son negociados y establecidos según el estado de la red y las necesidades de la conexión.
- Utiliza etiquetas (ver sección 1.1.3.1) para el envío de paquetes, que están relacionadas con las redes IP de destino.
- MPLS acelera y simplifica el proceso de envío de paquetes.
- Opera entre la capa de enlace y capa de red del modelo OSI, por lo cual, es considerada como tecnología de capa 2.5.
- MPLS integra la conmutación de capa de enlace con el enrutamiento IP de la capa de red.

1.1.2.3 Arquitectura MPLS [1], [3], [4]

La arquitectura MPLS está conformada por dos planos, en cada uno de los cuales

se llevan a cabo tareas diferentes.

1.1.2.3.1 Plano de Control

En el plano de control se realiza básicamente un intercambio de información de enrutamiento y etiquetas.

Entre los protocolos de enrutamiento que utiliza MPLS para elaborar y mantener actualizadas las tablas de enrutamiento de los nodos de la red están: OSPF(*Open Shortest Path First*) protocolo de estado-enlace[15]; EIGRP (*Enhanced Interior Gateway Routing Protocol*) protocolo híbrido propietario de Cisco que combina lo mejor de los algoritmos de vector distancia[16] y de estado-enlace, IS-IS (*Intermediate System To Intermediate System*) protocolo de estado-enlace, BGP (*Border Gateway Protocol*) protocolo que intercambia información de enrutamiento entre sistemas autónomos[17].

Para intercambiar información de etiquetas se lo hace mediante los protocolos TDP (*Tag Distribution Protocol*), LDP (*Label Distribution Protocol*) y RSVP (*Resource Reservation Protocol*) utilizado para realizar ingeniería de tráfico (ver sección 1.1.5.1).

El plano de control contiene dos tablas que almacenan la información de enrutamiento y etiquetas, éstas son:

- **RIB** (*Routing Information Base*): en esta tabla están todas las rutas aprendidas por cada uno de los nodos de la red.
- **LIB** (*Label Information Base*): en esta tabla se almacenan todas las

[15] Estado-enlace: método de enrutamiento en el que cada *router* llega a conocer la topología de la red, ya que informa a los demás nodos de la red sus distancias con sus enlaces vecinos. La clave y dificultad de este método es la difusión y el consumo elevado de memoria. Entre sus ventajas está la convergencia rápida de la red.
[16] Vector distancia: método de enrutamiento en el que cada *router* informa sólo a sus nodos vecinos de todas las distancias conocidas por él, mediante vectores de distancias (de longitud variable según los nodos conocidos); es así que, cada nodo conoce sólo la distancia hacia los distintos nodos de la red pero no la topología. Un *router* envía actualizaciones periódicamente y cada vez que varíen sus vectores de distancias.
[17] Sistema autónomo: conjunto de redes y equipos de red, que se encuentran bajo una misma administración.

etiquetas asignadas por el nodo y las etiquetas que han sido recibidas de los nodos vecinos.

1.1.2.3.2 Plano de Datos

Al igual que en el plano de control, contiene dos tablas en las cuales se basa para realizar un simple envió de paquetes basado en etiquetas, estas tablas son:

- **LFIB** (*Label Forwarding Information Base*): esta tabla se construye en base a la información de enrutamiento y etiquetas que provee el plano de control. La LFIB mantiene un mapeo entre la interfaz y etiqueta de entrada con la interfaz y etiqueta de salida correspondiente; se utiliza durante el proceso de envío de paquetes.

- **FIB** (*Forwarding Information Base*): esta tabla es similar a la RIB del plano de control, con la diferencia que en ésta se especifica el siguiente salto para alcanzar una ruta determinada.

En la figura 1.2 se presentan los componentes de la arquitectura MPLS. En el plano de control el protocolo OSPF aprende y anuncia la ruta 10.0.0.0/8, mediante el protocolo LDP recibe la etiqueta 17 para ser usada en paquetes cuyo destino sea la red con dirección 10.x.x.x y genera una etiqueta local 24 que es enviada a los vecinos, de forma tal que ellos puedan etiquetar los paquetes con la etiqueta apropiada para la red 10.x.x.x.

En el plano de datos el protocolo LDP realiza un ingreso en la LFIB estableciendo que la etiqueta 24 deber ser cambiada con la etiqueta 17 y se envían todos los paquetes realizando el cambio de etiquetas indicado.

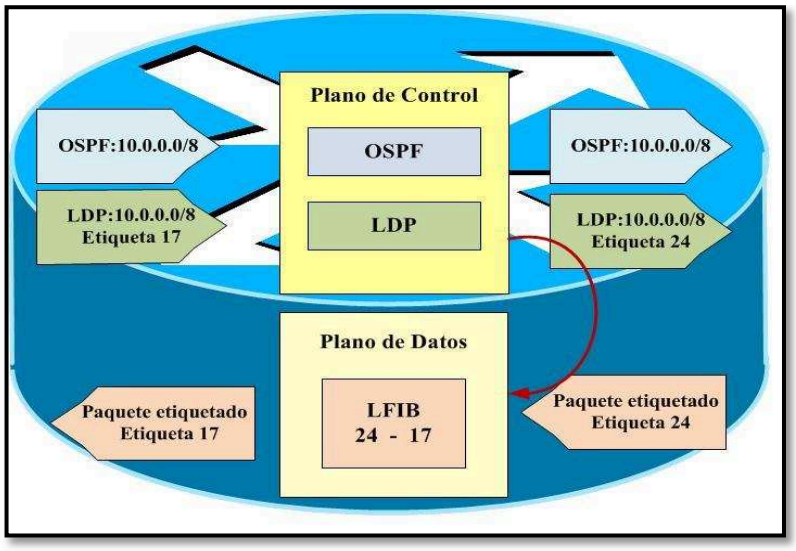


Figura 1.2: Arquitectura MPLS [3]

1.1.3 ELEMENTOS DE UNA RED IP/MPLS [1]

1.1.3.1 Etiqueta

Una etiqueta es un identificador pequeño de longitud fija que va en la cabecera MPLS; se utiliza para identificar un FEC (ver sección 1.1.3.2). Las etiquetas tienen significado local, es decir, se puede repetir el número de etiqueta en dos o más *routers*.

El formato de una etiqueta está definido de tal forma que ayude a la toma de decisión al momento que un paquete vaya a ser enviado. En la figura 1.3 se representa la ubicación que tiene la cabecera MPLS respecto a las cabeceras de los otros niveles; además se indica cómo se reparten los 32 bits correspondientes a la cabecera MPLS de la que forma parte la etiqueta.

- Etiqueta: 20 bits que identifican el LSP (ver sección 1.1.3.3) que recorrerá el paquete a lo largo de un dominio MPLS.
- EXP: 3 bits que son utilizados para definir servicios diferenciados, es decir clases de servicio (ver sección 1.1.5.2).

- S: 1 bit utilizado para indicar el final de la pila de cabeceras. Si su valor es 1 indica que esta cabecera es la última de la pila.

- TTL: siglas de *Time To Live*, ocupa 8 bits y sirve para establecer un límite en el número de saltos que puede realizar un paquete en su recorrido por la red.

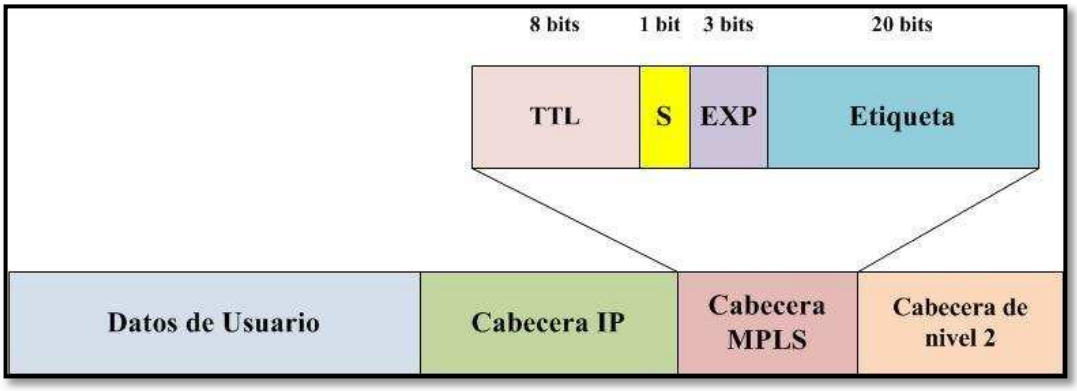


Figura 1.3: Ubicación y estructura de la cabecera MPLS [4]

Un paquete etiquetado viajará a través del *backbone* en un dominio MPLS mediante la conmutación de etiquetas.

1.1.3.2 FEC *(Forwarding Equivalence Class)*

FEC o clase equivalente de envío, es la representación de un grupo de paquetes que comparten los mismos atributos o requerimientos para su transporte.

La asignación de un paquete a una determinada FEC se hace una sola vez, cuando el paquete ingresa a la red.

1.1.3.3 LSPs *(Label Switched Paths)*

El intercambio de etiquetas permite la creación de “caminos virtuales” conocidos como LSPs, son vistos como túneles entre los extremos de una red IP/MPLS;

funcionalmente equivalentes a los PVCs en ATM.

Un LSP o ruta establecida en una red IP/MPLS, es un trayecto unidireccional definido con QoS entre dos puntos extremos de la red, a través del cual se dirigen todos los paquetes asignados a la misma FEC. Si se requiere una transmisión de información full dúplex se deberá establecer dos LSPs, uno en cada sentido.

Es así que, previo a la transferencia de información, se establece una conexión origen destino; los nodos intermedios que formarían parte de la ruta son identificados e informados de la intención de establecer la citada conexión.

1.1.3.4 LSRs *(Label Switching Routers)*

Los LSRs o *routers* de conmutación de etiquetas son los nodos centrales en una red IP/MPLS. Su función es reenviar paquetes luego de realizar un intercambio de etiquetas basándose en su tabla FIB, todas sus interfaces están habilitadas para manejar tráfico MPLS. Se les conoce también como P *Routers* (*Provider Routers*) ya que son de propiedad del proveedor de servicios.

1.1.3.5 LERs *(Label Edge Routers)*

Los LERs o *routers* de etiqueta de borde, son los nodos ubicados en la frontera de una red IP/MPLS. Realizan funciones tradicionales de enrutamiento y son capaces de proporcionar compatibilidad con diferentes tipos redes: ATM, *Frame Relay*[18], Ethernet[19], etc.

Un LER maneja el tráfico que ingresa o sale de una red IP/MPLS. A la entrada clasifica los paquetes y los etiqueta, y a la salida extrae la etiqueta del paquete y lo enruta según la capa 3 del modelo OSI.

[18] *Frame Relay*: tecnología de red orientada a conexión, utilizada para el servicio de transmisión de voz y datos a altas velocidades.
[19] Ethernet: estándar para la transmisión de datos para redes de área local.

A los LERs se les conoce también como PE *Routers* o (*Provider Edge Routers*); no todas sus interfaces están habilitadas para el manejo de tráfico MPLS. EL primer LER que interviene en un LSP se le denomina de entrada y al último se le denomina de salida.

En la figura 1.4, se representa un esquema con los equipos LSRs y LERs que forman parte de la red IP/MPLS y el establecimiento de un LSP entre el equipo LER de entrada y el LER de salida.

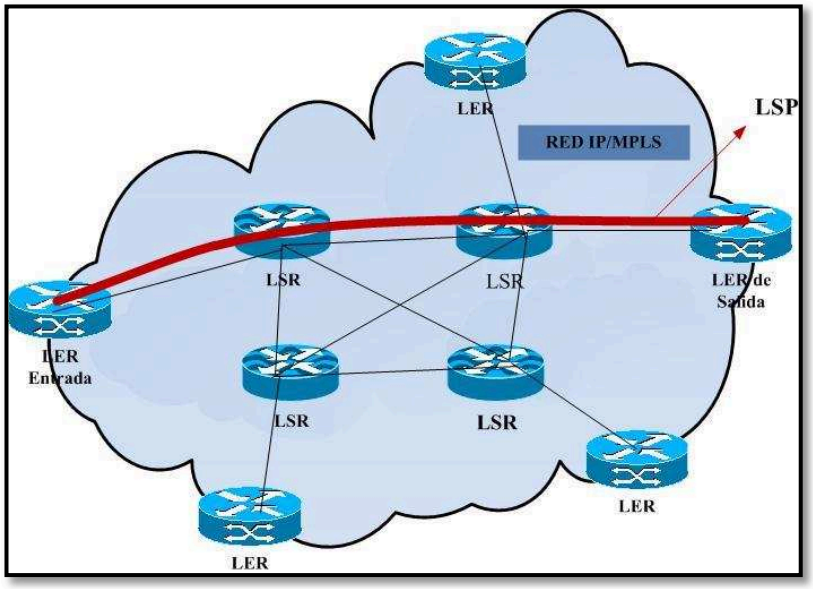


Figura 1.4: Equipos LSRs y LERs en una red IP/MPLS

1.1.4 FUNCIONAMIENTO DE UNA RED IP/MPLS [1], [5]

El proceso para el envío de información a través de una red IP/MPLS, considera los siguientes pasos:

- Intercambio de información de enrutamiento.
- Asignación y distribución de etiquetas.
- Creación de tablas.

- Construcción de LSPs.
- Conmutación de etiquetas.

1.1.4.1 Intercambio de información de enrutamiento

Antes que el tráfico empiece a viajar por la red IP/MPLS, los *routers* intercambian información de la topología de la red a través de los protocolos de enrutamiento (OSPF, IS-IS, EIGRP).

En la figura 1.5 se puede apreciar como cada uno de los nodos de la red, empiezan a intercambiar información con sus vecinos, anunciando su entorno topológico, así como los recursos disponibles en sus enlaces.

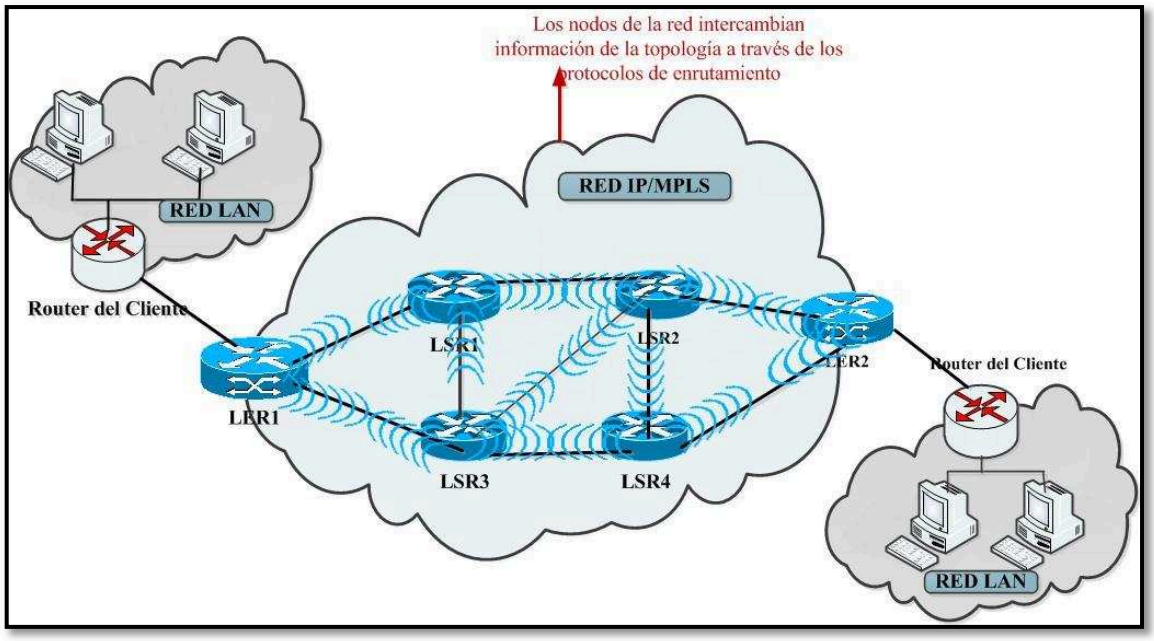


Figura 1.5: Intercambio de información de enrutamiento en la red IP/MPLS

1.1.4.2 Asignación y distribución de etiquetas

Una vez que los protocolos de enrutamiento intercambian información y se construyen las tablas de enrutamiento en cada nodo de la red IP/MPLS, se realiza

una asignación y distribución de etiquetas para proceder a crear las tablas correspondientes y poder dirigir el tráfico que llegue posteriormente.

Cada nodo de la red IP/MPLS asigna una etiqueta local para cada destino de la tabla de enrutamiento.

En una red IP/MPLS se denomina nodo *upstream* (ascendente) a aquél que envía un paquete por un puerto dado a otro nodo de la red, y a aquél nodo que recibe dicho paquete se le llama nodo *downstream* (descendente). La decisión de asociar una etiqueta a un FEC se realiza de un nodo *downstream* a un nodo *upstream*.

La distribución de etiquetas se realiza mediante los protocolo LDP, TDP o RSVP, los cuales permiten que los nodos LERs y LSRs se informen de la asignación de etiquetas que han realizado los vecinos.

Existen dos formas de realizar una distribución de etiquetas, éstas son:

- **Distribución no solicitada**: se realiza cuando un nodo de la red IP/MPLS informa a sus nodos vecinos de forma independiente, de las asignaciones de etiquetas que éste ha realizado. En este caso no solo asigna las etiquetas sino que además informa de las asociaciones a los nodos vecinos.

- **Distribución bajo demanda:** solo se informa de la asignación de etiquetas a otros nodos previa solicitud.

En la figura 1.6 se presenta una distribución de etiquetas bajo demanda. El nodo LER2 de salida directamente conectado con la Red X, realiza una asignación de etiqueta local 60 hacia dicha red; el nodo LSR (nodo *Upstream*) solicita al nodo LER2 (nodo *Downstream*) una etiqueta hacia la misma red, el cual le envía la etiqueta asignada. El nodo LER1 de igual forma solicita a su vecino una etiqueta

hacia la Red X, el cual le responderá una vez que haya recibido la etiqueta del LER2 y tras haber asignado una etiqueta local 50 hacia dicha red; para este caso el nodo LSR actuará como nodo *Downstream*.

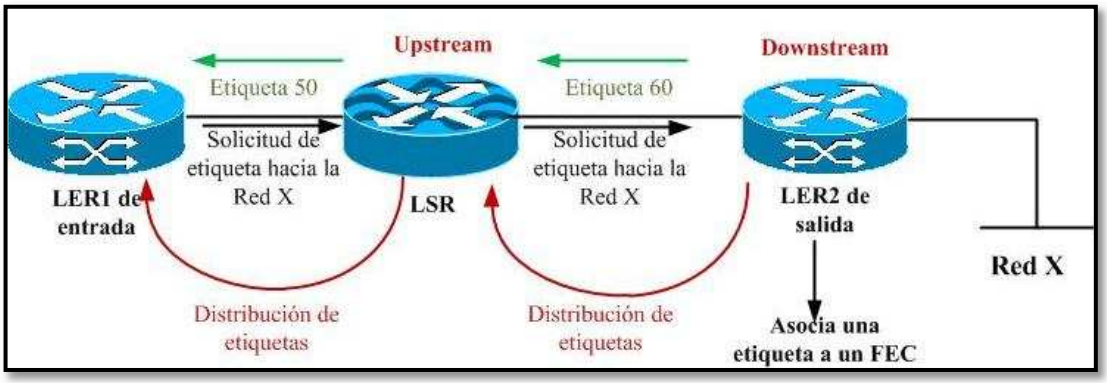


Figura 1.6: Distribución de etiquetas bajo demanda

1.1.4.3 Creación de tablas

Producto de la asignación y distribución de etiquetas, se crean las tablas respectivas en cada nodo de la red IP/MPLS para poder reenviar los paquetes entrantes.

En la figura 1.7, se tiene un ejemplo sobre la asignación y distribución de etiquetas, y la creación de las tablas LIB, FIB y LFIB en uno de los nodos de la red IP/MPLS. Los protocolos de distribución de etiquetas son los encargados de agregar las etiquetas en las tablas FIB, LIB y LFIB y distribuirlas a sus nodos vecinos. En esta figura se sigue el siguiente proceso:

1.- El nodo LSR2 asigna una etiqueta local 34 con destino a la red 10.0.0.0/8 y realiza una distribución no solicitada a cada uno de sus vecinos.

2.- El LSR3 de igual forma asigna una etiqueta local 70 con destino a la red 10.0.0.0/8 y la almacena en su tabla LIB, a la vez que ingresa una entrada en la misma tabla de la etiqueta 34 que recibe del nodo LSR2.

3.- El LSR3 ingresa en su tabla FIB el próximo salto para llegar a la red 10.0.0.0/8, que es el nodo LSR2 del cual recibió la etiqueta 34.

4.- Finalmente el LSR3 define una entrada en su tabla LFIB, indicando que el paquete que llegue con la etiqueta 70, será cambiada por la etiqueta 34 para ser enviado al próximo salto.

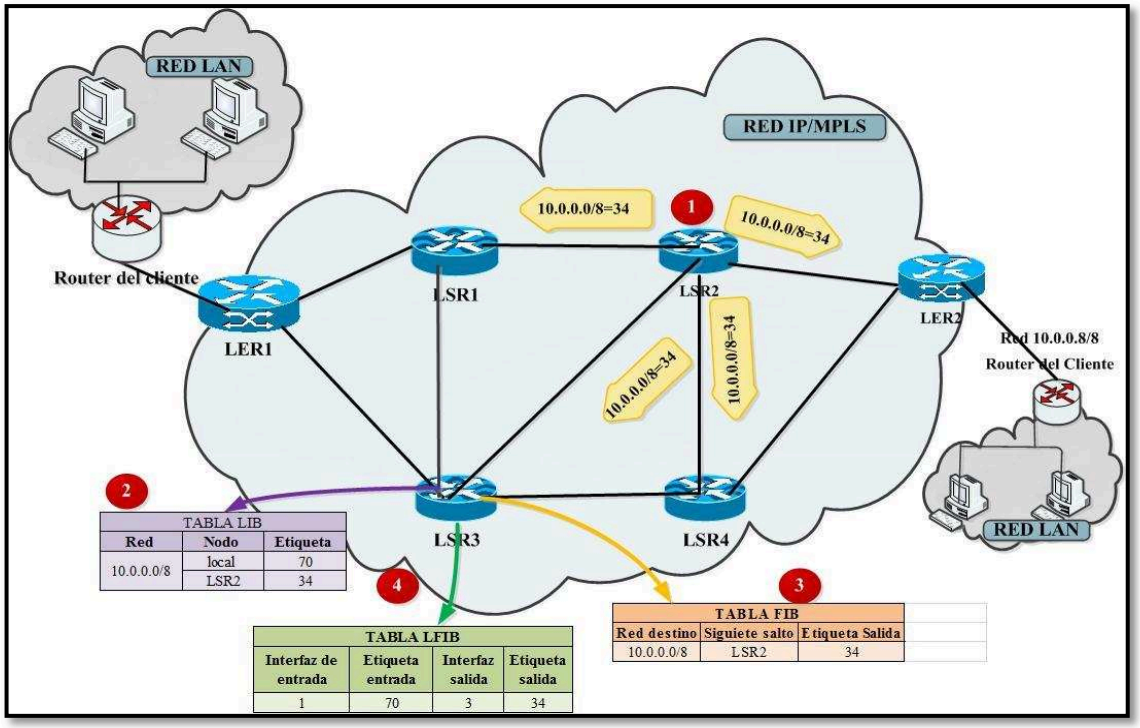


Figura 1.7: Creación de tablas LIB, FIB, LFIB

1.1.4.4 Construcción de un LSP

Un LSP es una secuencia de nodos MPLS que reenvían paquetes etiquetados basándose en un determinado FEC; se forma entre el equipo de entrada y el equipo de salida de la red IP/MPLS. El LER de entrada inicia una cadena de mensajes de petición de etiquetas para crear un LSP, el LER de salida responde con mensajes de asociación de etiquetas formando el LSP correspondiente.

La ventaja de establecer un LSP es la negociación de una ruta óptima. En la

figura 1.8, se tiene un ejemplo del proceso para la creación de un LSP. El flujo de datos de origen al destino está marcado por las líneas entrecortadas de color morado; el equipo de borde de la red IP/MPLS, LER1 (LER de entrada) empieza a realizar la solicitud de etiquetas para así poder establecer el camino para el envío de los datos (línea entrecortada de color verde).

El equipo del otro extremo, LER2 (LER de salida) responde a dicha solicitud y empieza la distribución de las etiquetas (línea entrecortada de color rojo), quedando establecido el LSP correspondiente.

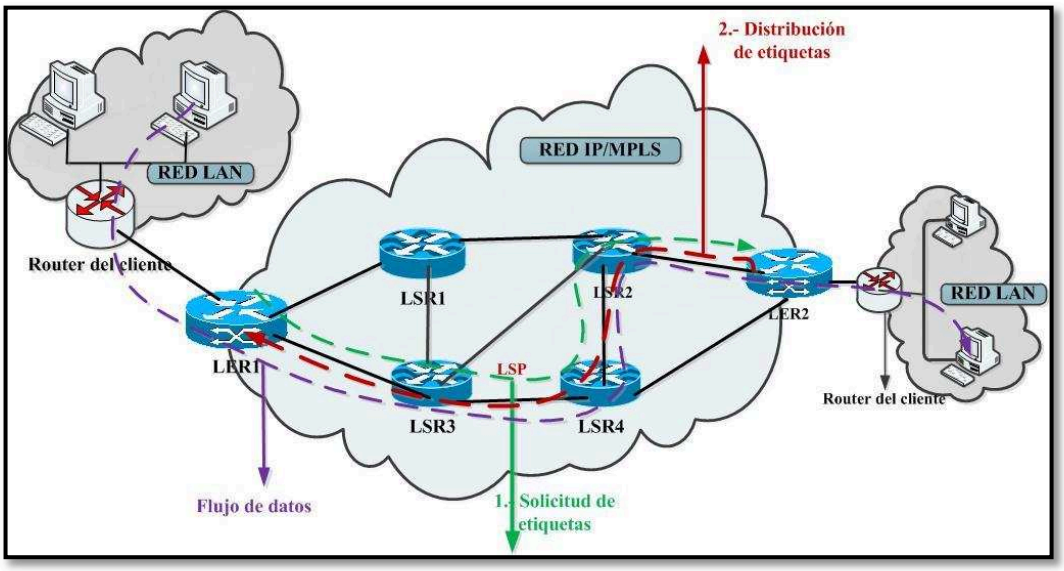


Figura 1.8: Construcción de un LSP

1.1.4.5 Conmutación de etiquetas

Los equipos LER de entrada ubicados en la frontera de la red IP/MPLS, al recibir el tráfico entrante analizan y clasifican los paquetes en base a la dirección IP de destino y la QoS que el paquete demande en un nuevo FEC o en uno ya existente.

Se inserta la etiqueta MPLS que identifique el LSP correspondiente por el cual será enviado el paquete entrante. Un *router* IP normal lo que haría es seleccionar

el próximo salto para el envío del paquete, no así un equipo LER, lo que hace es seleccionar el camino entero (LSP) que el paquete deberá seguir a través de la red IP/MPLS para llegar a su destino.

Una vez que una etiqueta MPLS ha sido insertada en un paquete, el LER se encarga de enviar dicho paquete al siguiente nodo, el cual realiza una consulta en su tabla FIB para determinar el próximo salto y en su tabla LFIB para hacer un cambio de etiqueta, es decir una simple conmutación de etiquetas. Finalmente el equipo LER de salida se encarga de remover la etiqueta y enrutar el paquete recibido según capa 3 del modelo OSI.

En la figura 1.9 se detallan todos los pasos que se realizan en el proceso de conmutación de etiquetas.

1.- De la red del cliente se originan dos paquetes IP representados de color amarillo y celeste.

2.- Al llegar los paquetes al equipo de borde de la red IP/MPLS (LER1), éste los etiqueta clasificándoles en una determinada FEC, a y b respectivamente. Al paquete de color amarillo lo envía por la interfaz 2 asignándole la etiqueta 70 y el otro paquete lo envía por la misma interfaz pero con la etiqueta 23.

3.- Al llegar al siguiente nodo de la red (LSR3), éste consulta en la tabla LFIB, en base a la cual se realiza la conmutación de etiquetas; en el paquete amarillo se cambia la etiqueta 70 por la 34 y se lo envía por la interfaz 3 y en el paquete celeste se cambia la etiqueta 23 por la 80 y se lo envía por la interfaz 4. Este proceso se realiza de forma similar en cada nodo LSR de la red IP/MPLS.

4.- Finalmente al llegar los paquetes al nodo LER de salida de la red IP/MPLS (LER2), se extraen las etiquetas MPLS de cada uno de los paquetes y se los enruta según capa 3 del modelo OSI.

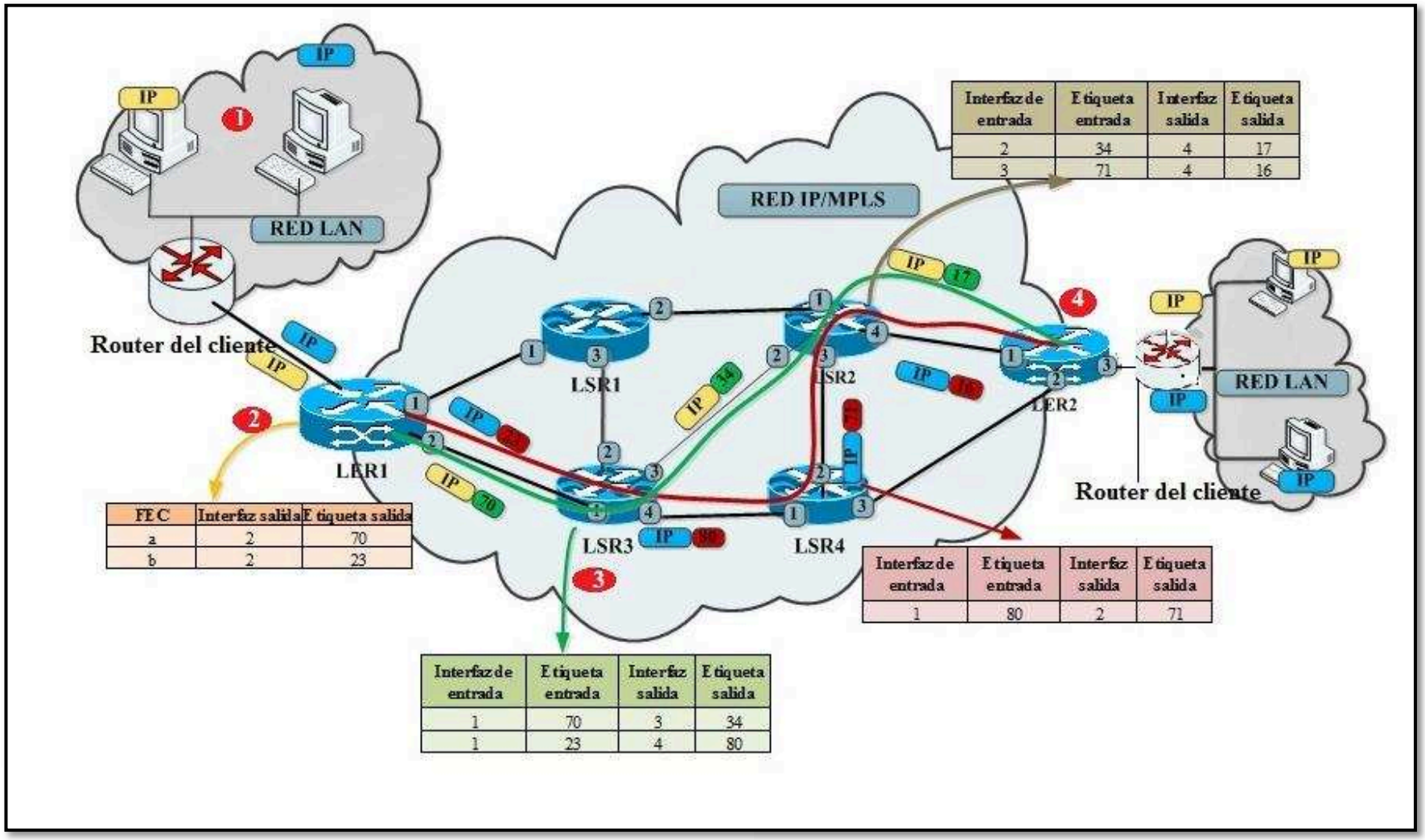


Figura 1.9: Principio de conmutación de etiquetas MPLS

1.1.5 SERVICIOS EN UNA RED IP/MPLS [6], [7]

1.1.5.1 MPLS TE (*Traffic Engineering*)

TE o ingeniería de tráfico consiste en utilizar de manera óptima la infraestructura de red, para lo cual se debe adecuar de mejor manera el tráfico presente haciendo uso de enlaces que estén siendo subutilizados, ya que no se encuentran dentro del camino más corto calculado por la métrica del IGP[20].

La ingeniería de tráfico lo que hace es prever la posibilidad de dirigir el tráfico a través de la red por caminos diferentes de la ruta preferida, que sería el camino más corto calculado por el protocolo de enrutamiento IGP. El resultado de aplicar la ingeniería de tráfico en la red IP/MPLS, es la distribución del tráfico de una manera uniforme sobre enlaces disponibles y hacer un mayor uso de los enlaces que estén siendo subutilizados. La red IP/MPLS ofrece ingeniería de tráfico haciendo uso del protocolo RSVP, el cual implementa una señalización antes que el flujo de datos sea enviado a la red, construyendo un canal virtual a lo largo del cual se reservan los recursos necesarios.

Establecer un LSP que cumpla con los requisitos de ingeniería de tráfico, requiere las siguientes acciones:

- Especificación de requisitos que se desean en cuanto a prestaciones para el LSP (direcciones de los LER de frontera, ancho de banda necesario, etc.).
- Determinar la ruta más adecuada para el LSP en la red IP/MPLS; se entiende por ruta adecuada aquella formada por los enlaces y nodos que puedan acomodar los requisitos requeridos por el LSP.
- Establecimiento de las correspondencias de etiquetas entre los nodos de salida y entrada así como los nodos intermedios.

[20] IGP: *Interior Gateway Protocol*, protocolos de enrutamiento utilizados dentro de un mismo sistema autónomo.

En la figura 1.10 se observa que el camino para ir de A hacia B, escogido por el protocolo de enrutamiento, sin tener en cuenta si este enlace está congestionado o no, es el camino superior (está a tres saltos de A), representado por las líneas entrecortadas de color verde; lo que hace la ingeniería de tráfico es decidir el camino, no por el número de saltos o costo de los enlaces, como normalmente se escogería con un IGP, sino el menos utilizado o congestionado (camino inferior, color rojo), aunque esté a 4 saltos de A.

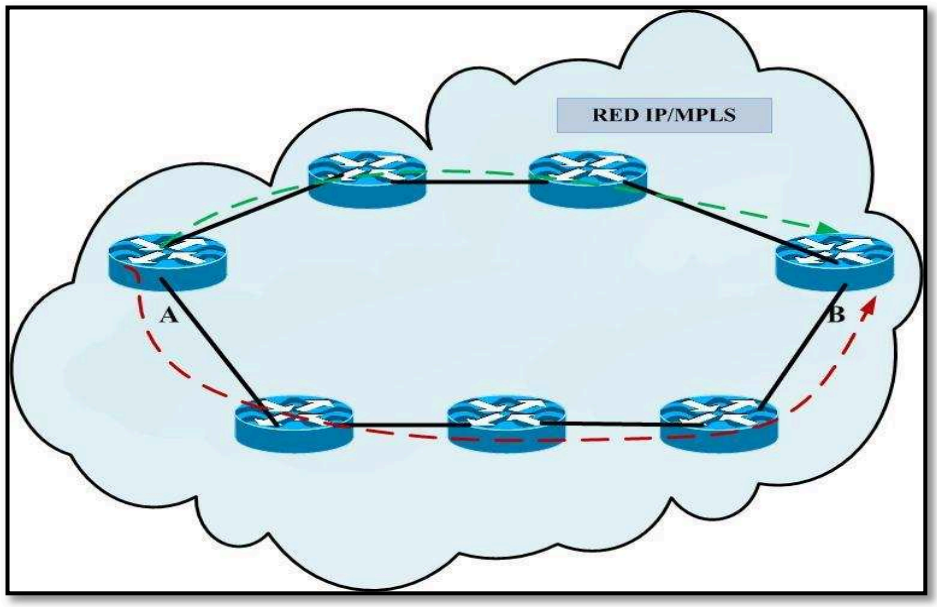


Figura 1.10: Ingeniería de tráfico en la red IP/MPLS

1.1.5.2 CoS (*Class of Service*)

Ofrecer calidad de servicio hace referencia a clase de servicio. La clase de servicio es un esquema de clasificación con que son agrupados los tráficos que tienen requerimientos de rendimiento similares, de tal manera de poder diferenciar diferentes tipos de tráfico y por ende poder priorizarlos. Cada nivel de prioridad está diseñado para soportar tipos específicos de tráfico.

El campo EXP definido en la cabecera MPLS, permite que una red IP/MPLS propague la clase de servicio con el correspondiente LSP, es decir, permite

ofrecer servicios diferenciados. Entre cada par de nodos de la red, se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

MPLS define 5 clases de servicio, estas clases son: [8]

Video: clase de servicio para transportar video, tiene un nivel de prioridad más alto que las clases de servicio para datos.

Voz: la clase de servicio para transportar voz tiene un nivel de prioridad equivalente al de video, es decir, más alto que las clases de servicio para datos.

Datos de alta prioridad (D1): ésta es la clase de servicio con el nivel de prioridad más alto para datos. Se utiliza particularmente para aplicaciones que son críticas en cuanto a necesidad de rendimiento, disponibilidad y ancho de banda.

Datos de prioridad (D2): esta clase de servicio se relaciona con aplicaciones que no son críticas y que tienen requisitos particulares en cuanto a ancho de banda.

Los datos no prioritarios (D3): representan la clase de servicio de prioridad más baja.

1.1.5.3 VPNs (*Virtual Private Networks*) [9], [10], [11]

Actualmente las empresas tienen la necesidad de que las redes de área local superen las barreras de la comunicación local, es decir, permitir la comunicación entre el personal y oficinas que se encuentren geográficamente distantes. Esto es posible estableciendo una VPN o Red Privada Virtual.

Una VPN es un tipo de tecnología de red que permite la extensión de una red privada sobre una infraestructura compartida, con funcionalidades de red y seguridad similares a las que se tiene en una red privada. Las VPNs son una

solución para el soporte intra/extranet integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

La aceptación que ha tenido la tecnología MPLS como una tecnología de convergencia de red a elegir, ha llevado a poner una gran atención en las VPN basadas en MPLS.

Para establecer una VPN en una red IP/MPLS se requieren de tres elementos, éstos son:

Dispositivo CE (*Customer Edge*): *router* o conmutador situado en las instalaciones del cliente, puede pertenecer y ser gestionado por el cliente o por el proveedor de servicios.

Dispositivo PE: equipo de borde de la red IP/MPLS, es donde reside toda la inteligencia de VPNs, donde empieza y termina una VPN y donde se establecen todos los túneles (LSPs) necesarios para conectar con todos los otros PEs.

Dispositivo P: equipo central en la red IP/MPLS, los cuales interconectan los diferentes equipos PEs, no participan realmente en la funcionalidad de una VPN, se encargan de simplemente conmutar el tráfico en base a las etiquetas MPLS.

Los tipos de VPNs que se pueden implementar sobre una red IP/MPLS se detallan a continuación.

1.1.5.3.1 VPNs capa 2

La característica principal de las VPNs capa 2, es que ofrecen independencia entre la red del proveedor y la red del cliente. Dan la posibilidad de transportar servicios emulados de un lugar a otro, esto se lo hace de una manera transparente para los equipos CEs ubicados en el borde de la red del cliente.

El enfoque que realizan las VPNs a nivel de capa dos, aborda dos tipos de conectividad, los mismos que se detallan a continuación.

Conectividad punto a punto: el transporte de tramas capa 2 a través de la nube IP/MPLS se lo hace por medio de los LSPs, los cuales a su vez transportan múltiples circuitos virtuales. Un circuito virtual es como un LSP dentro del túnel LSP original.

Un circuito virtual es utilizado para transportar información de un único cliente, mientras que un LSP contiene varios circuitos virtuales, por lo que estaría transportando información de varios clientes. Los circuitos virtuales, al igual que los LSPs, son unidireccionales, así que al necesitar una comunicación bidireccional se requiere establecer uno en cada sentido.

El *router* de borde de entrada de la red IP/MPLS encapsula la trama capa 2 del cliente y es asociada a una doble etiqueta, una que identifica al circuito virtual conocida como “etiqueta VC” y otra que identifique el LSP conocida como “etiqueta LSP”.

En la figura 1.11, se presenta un esquema del establecimiento de una VPN de capa 2 sobre una red IP/MPLS entre dos sitios de un cliente, punto-punto.

Conectividad multipunto: la solución que MPLS ha desarrollado para este escenario se denomina VPLS (*Virtual Private* LAN[21] *Service*). El cliente puede tener varias sucursales geográficamente distantes con las cuales desea establecer comunicación, para lo cual necesitaría una conectividad multipunto.

La red IP/MPLS frente a este tipo de escenario emula un *switch* o un puente para conectar todas las redes de área local del cliente creando una red LAN en puente único, ver la figura 1.12.

[21] LAN: *Local Area Network*, sistema de comunicación entre computadoras, con la característica que las distancia entre estos equipos es pequeña.

Los *routers* PEs realizan un aprendizaje de direcciones MAC como un simple *switch*. Un PE mantiene una tabla de envío de capa dos independiente, conocida como VFI (*Virtual Forwarding Instance*) para cada VPN establecida. En la figura 1.13 se observa que el cliente tiene configuradas VLANs[22] en cada una de sus sucursales, lo que implica una VPN por cada comunicación entre VLANs correspondientes.

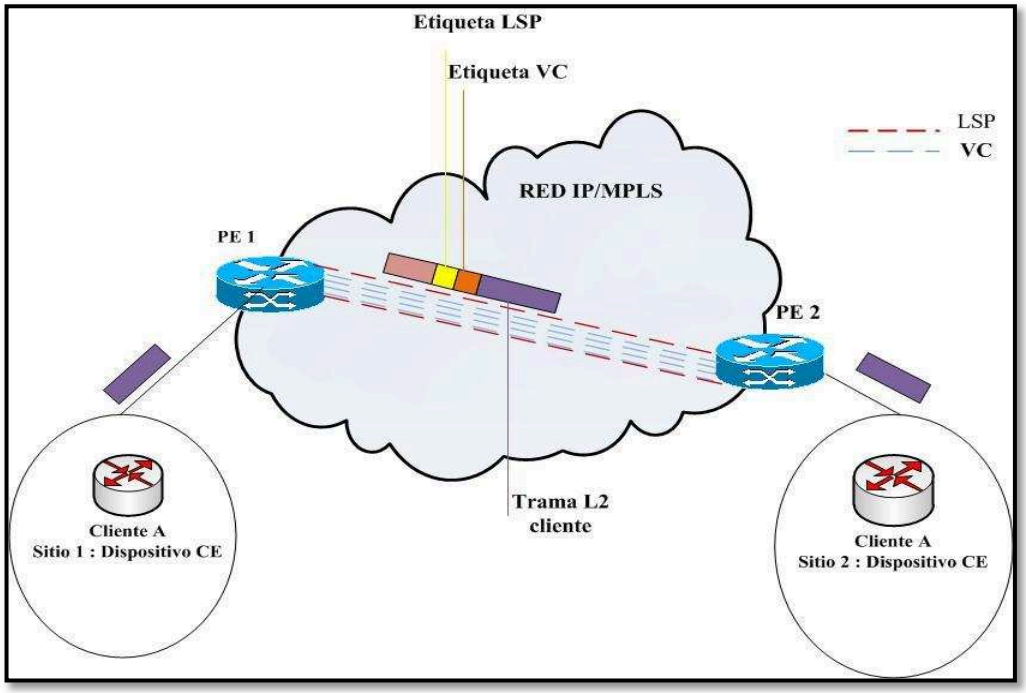


Figura 1.11: VPN capa 2 sobre una red IP/MPLS [10]

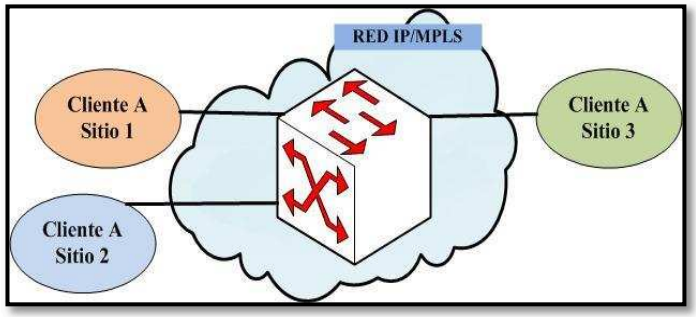


Figura 1.12: VPLS sobre una red IP/MPLS, puente único [11]

[22] VLAN: *Virtual* LAN, método para crear varias redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un mismo conmutador físico o en una única red física.

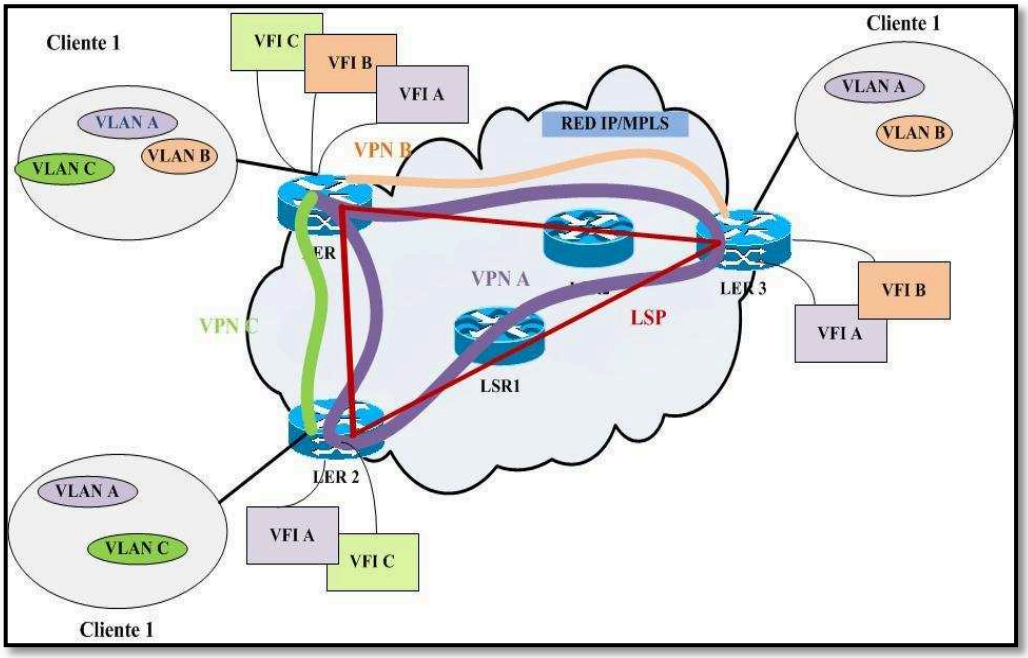


Figura 1.13: VPLS sobre una red IP/MPLS [11]

1.1.5.3.2 VPNs capa 3

Se basa en el manejo de datagramas IP de los clientes. Un PE de la red al recibir un paquete de un cliente busca la dirección IP de destino al cual va dirigido dicho paquete, en una tabla de envío de paquetes IP para ser encaminado a través de la red IP/MPLS utilizando un LSP. Para llevar a cabo este proceso los *routers* de borde de la red IP/MPLS necesitan intercambiar información de enrutamiento con los equipos de borde del cliente. Los PEs intercambian las rutas aprendidas con otros PEs utilizando el protocolo de enrutamiento BGP (*Border Gateway Protocol*) protocolo que intercambia información entre sistemas autónomos, por lo que se les conoce también como BGP/VPNs MPLS.

Un *router* de borde de la red IP/MPLS puede tener múltiples VPNs de capa 3; para cada VPN mantiene una tabla de enrutamiento independiente conocida con el nombre de VRF (*Virtual Routing and Forwarding*). VRF es una tecnología que permite tener múltiples tablas de rutas separadas, las cuales pueden coexistir en el mismo *router* y al mismo tiempo.

Para un PE una VRF puede contener múltiples interfaces físicas, lógicas o subinterfaces, si los sitios que se conectan a estas interfaces pueden compartir la misma información de enrutamiento. Las tablas de rutas se mantienen independientes unas de otras, lo que hace posible tener direcciones IP iguales sin que se presente ningún tipo de conflicto.

En la figura 1.14 se tiene un esquema que representa el establecimiento de VPNs capa 3 sobre una red IP/MPLS. Similar al ejemplo anterior de VPLS sobre la red IP/MPLS, pero en este caso se manejan VRFs para enrutamiento de capa 3.

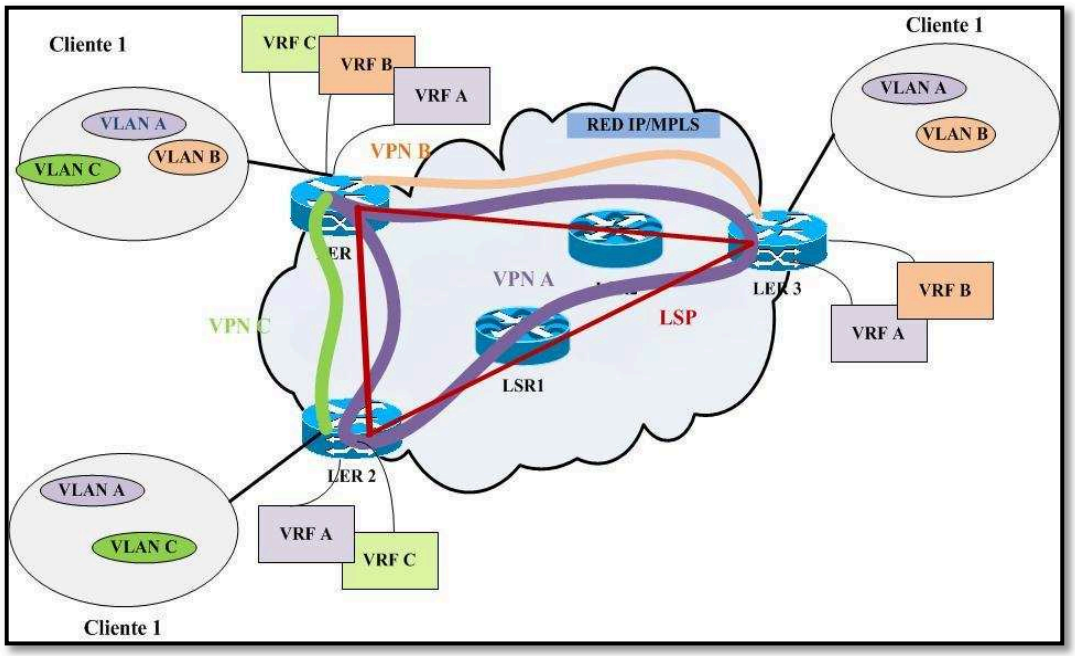


Figura 1.14: BGP/VPNs sobre una red IP/MPLS [11]

1.2 SEGURIDAD DE LA INFORMACIÓN [12], [13]

1.2.1 INTRODUCCIÓN

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas.

1.2.2 CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN [14]

La seguridad de la información se define como el conjunto de medidas, estándares, procesos, procedimientos, estrategias, recursos educativos, recursos informáticos y recurso humano integrado, para mantener bajo protección y libre de riesgos la información de una empresa.

La información es uno de los elementos más valiosos e importantes para una empresa, evitar que ésta sea divulgada, mal utilizada, robada, borrada o saboteada por personas no autorizadas juega un papel importante en el éxito de la empresa. La información puede estar presente en diferentes formas o medios: impresa, escrita en un papel, guardada o transmitida haciendo uso de algún medio electrónico; cualquiera sea su forma en la que se encuentre debe ser debidamente protegida.

Los controles con los que cuente la empresa u organización para garantizar la seguridad de la información deben ser supervisados, revisados y mejorados periódicamente, para asegurase que están cumpliendo con los objetivos para los cuales fueron establecidos e implementados.

1.2.3 ELEMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

1.2.3.1 Confidencialidad

Consiste en evitar que la información sea divulgada o accedida por personal no autorizado, garantizando la privacidad en la información.

1.2.3.2 Integridad

Es mantener la información libre de modificaciones no autorizadas, no controladas o accidentales; la información debe permanecer inalterada, a menos que las modificaciones sean autorizadas y registradas para garantizar su validez y consistencia.

1.2.3.3 Disponibilidad

La información debe estar siempre disponible cuando los procesos o personal autorizado requieran hacer uso de ella, garantizando así la continuidad de acceso a los elementos de información.

1.2.3.4 Autenticación

Se determina la identidad del usuario utilizando algún método para el efecto, el más utilizado es usar un nombre de usuario y una contraseña aunque en la actualidad existen métodos más seguros. Solo un usuario autenticado correctamente debe acceder a la información.

1.2.3.5 Autorización

Una vez que el usuario haya sido autenticado correctamente se determina lo que le está permitido realizar.

1.2.3.6 Auditoría

Contar con reportes de las actividades realizadas en la administración de la red, que permitan tomar acciones frente a problemas de seguridad suscitados.

1.2.3.7 No Repudio

Impedir que personas o entidades nieguen que la información, datos, archivos o algún otro recurso de la empresa hayan sido accedidos o alterados por ellos cuando en efecto así hubiese sucedido.

1.2.3.8 Control de Acceso

Es la capacidad de controlar el nivel de acceso que individuos o entidades tienen a los recursos de la red o información en general.

1.2.4 ACTIVOS DE INFORMACIÓN

El término hace referencia a todos los elementos que contienen, mantienen o guardan la información. Son estos activos los que se debe proteger evitando su pérdida, modificación o su uso inadecuado, garantizando la estabilidad y buena imagen de la empresa. A estos activos se les ha clasificado dentro de tres grupos.

1.2.4.1 Información Contenida

Constituye la información misma de la empresa, la que debe mantenerse siempre confiable, íntegra y disponible. Se debe tomar en cuenta que los ataques generados para apoderarse de este activo no solo se dan del exterior, inclusive personal de la misma empresa puede hacer uso de ella con fines maliciosos.

1.2.4.2 Infraestructura Computacional

Son los elementos o equipos en los cuales se almacena, transmite o procesa la información; se debe garantizar siempre su normal funcionamiento. Para ello, es necesario contar con medidas preventivas ante posibles accidentes como: fallas eléctricas, robos, daños, desastres naturales, etc.

1.2.4.3 Los usuarios

Constituye el personal autorizado que administra la información contenida y la infraestructura computacional de la empresa. Es uno de los activos más difícil de proteger porque su estabilidad laboral no está garantizada. Además es esencial que sean ellos mismos, quienes adquieran un compromiso de responsabilidad y estén conscientes de la importancia de tener una actitud ética con la empresa.

1.2.5 VULNERABILIDADES, AMENAZAS, ATAQUES Y ATACANTES

1.2.5.1 Vulnerabilidades

Son debilidades presentes en una red o sistema de información, incluyen la entidad que maneja o administra dicho sistema que lo vuelven susceptible o idóneo para que las amenazas puedan materializarse, con el resultado de sufrir daños o perjuicios que no necesariamente pueden ser materiales.

1.2.5.2 Amenazas

Tipos de eventos o acciones que pueden afectar o causar daño a los activos de información, afectando su seguridad.

Las vulnerabilidades tienen una relación estrecha con las amenazas, las amenazas no pueden concretarse si no existen vulnerabilidades y las vulnerabilidades no pueden ser explotadas sin amenazas.

1.2.5.2.1 Clasificación de las amenazas

Las amenazas pueden ser internas o externas al sistema o empresa que lo administra, se clasifican en tres grupos:

a) Criminalidad

Son todas las acciones que son ejecutadas por el ser humano que violan la ley y están penadas por ella.

b) Sucesos de origen físico

Son desastres naturales o eventos técnicos así como los causados indirectamente por el ser humano.

c) Negligencias y decisiones institucionales

Constituyen las acciones, decisiones u omisiones de los responsables de la administración de la red o del sistema de información.

1.2.5.3 Ataques [15]

Son métodos y/o mecanismos utilizado por un atacante para desestabilizar o causar daños en una red o sistema de información. Los ataques que se pueden generar pueden ser activos, los que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos que se limitan a registrar el uso de los recursos y/o acceder a la información guardada o transmitida por la red o sistema.

En la figura 1.15 se pueden apreciar los diferentes tipos de ataques de los que puede ser víctima la información.

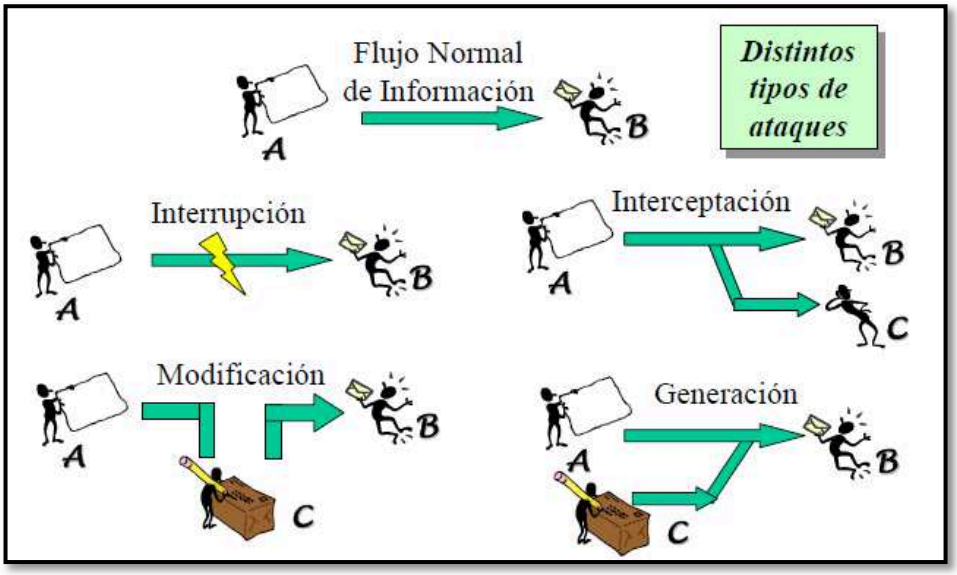


Figura 1.15: Tipos de ataques en una red o sistema de información [15]

1.2.5.3.1 Tipos de ataques

a) Actividades de reconocimiento de sistemas

Considerado como un ataque pasivo ya que no genera daño alguno, se limitan a obtener información sobre la organización, sus redes y sistemas informáticos. Se suelen realizar actividades como escaneo de puertos para determinar qué servicios están activos, reconocimiento de versiones de sistemas operativos, etc.

b) Detección de vulnerabilidades en los sistemas

Se trata de detectar y documentar las posibles vulnerabilidades en la red o en los sistemas informáticos, para de acuerdo a ello, desarrollar o utilizar herramientas que permitan explotar dichas vulnerabilidades, este tipo de herramientas son conocidos como "*exploits*".

c) Robo de información mediante la interceptación de mensajes

Trata de interceptar mensajes o documentos que son enviados a través de la red,

vulnerando la confidencialidad y privacidad de los usuarios. En este tipo de ataque está el conocido "*Man in the middle*", que es la ubicación de un usuario o programa ilegal en medio de una sesión, adueñándose de ella y haciendo que los usuarios legítimos piensen que están conectados directamente con sus recursos y/o servicios.

d) Modificación del contenido y secuencia de los mensajes transmitidos

Es un ataque activo, en el que el intruso reenvía mensajes y documentos que ya fueron previamente transmitidos a través de la red, tras modificarlos de forma maliciosa, conocidos como ataques de repetición.

e) Análisis de tráfico

Ataque pasivo, que trata de observar los datos y el tipo de tráfico que está siendo transmitido a través de la red, utilizando para ello herramientas conocidas como "sniffers".

f) Ataques de suplantación de identidad

En este tipo de ataques existen varias posibilidades, siendo la más conocida como "IP *Spoofing*" (enmascaramiento de dirección IP); un atacante consigue modificar la cabecera de los paquetes enviados a un determinado destino, para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así por ejemplo el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado.

Otra de las posibilidades dentro de este tipo de ataque es el secuestro de sesiones ya establecidas, conocido como "*hijacking* ", donde el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir. Con el secuestro de sesiones se podrían

llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático, por ejemplo, transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.

g) DNS *Spoofing*

Ataques de falsificación de DNS[23], en los que se pretende tratar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea en los nombres de dominio de las direcciones IP, provocando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas web falsas o bien la interceptación de sus mensajes que estén siendo enviados a través de la red.

h) Capturas de cuentas de usuario y contraseñas

Se puede suplantar la identidad de los usuarios haciendo uso de herramientas que permitan capturar sus contraseñas como programas de software espías o dispositivos de hardware que permiten registrar todas las pulsaciones en el teclado de un ordenador.

Además se pude obtener información de cuentas de usuario y contraseñas recurriendo a lo que se conoce con el nombre de ingeniería social, en la que un usuario podría ser engañado por una persona ajena a la organización para que le facilite sus contraseñas o claves de acceso.

i) Modificación del tráfico y tablas de enrutamiento

Este tipo de ataque consiste en desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o

[23] DNS: *Domain Name System*, sistema de nombres de dominio. Protocolo de la capa aplicación que se utiliza en una red para convertir los nombres de host en sus direcciones IP asociadas.

medios antes de que éstos lleguen a su destino legítimo para facilitar los ataques de interceptación de datos.

j) Conexión no autorizada a equipos y servidores

Existen varias formas de establecer conexiones no autorizadas a otros equipos y servidores, algunas de ellas son: violación de sistemas de control de acceso, explotación de agujeros de seguridad, utilizar puertas traseras o "*backdoors*"[24] y "*rookits*"[25].

k) Introducción en el sistema a través de códigos maliciosos

Se entiende por código malicioso o dañino (*malware*), cualquier programa documento o mensaje susceptible que cause daño a las redes o sistemas de información. Dentro de esta definición estarían incluidos:

- Virus: aplicaciones diseñadas para alterar el normal funcionamiento de un sistema informático, no tienen la facultad de replicarse a sí mismos. Pueden llegar a alterar datos almacenados en un computador, causando daños importantes en los sistemas inclusive bloqueando las redes informáticas.

- Gusanos: aplicaciones con características similares a la de los virus con la particularidad de que son capaces de replicarse por sí mismos. Aunque su objetivo no sea alterar o dañar archivos contenidos en un computador, sino más bien causar molestias consumiendo recursos.

- Troyanos: programas maliciosos que aparentan ser aplicaciones legítimas, pero al ser ejecutados traen consigo funciones ocultas diseñadas para violar los sistemas de seguridad.

---

[24] *Backdoors:* conjunto de instrucciones no documentadas dentro de un programa o sistema operativo legítimo, que permiten acceder o tomar control del equipo saltándose los controles de seguridad.

[25] *Rootkits*: programas que se instalan en un equipo reemplazando a una herramienta o servicio legitimo del sistema operativo, que además de reemplazar incorpora otras funciones ocultas que facilitan entre otras cosas, el control remoto del equipo comprometido.

Uno de los objetivos más comunes de estos códigos maliciosos es dejar habilitado un *backdoor*, para que un usuario no autorizado pueda administrar remotamente el dispositivo en el cual fueron ejecutados dichos programas.

l) Ataques contra sistemas criptográficos[26]

Consiste en atacar los sistemas criptográficos descubriendo las claves utilizadas para cifrar determinados mensajes o documentos almacenados en un sistema u obtener información sobre el algoritmo criptográfico utilizado.

Las técnicas principales en este tipo de ataque son:

- Ataques de fuerza bruta: que trata de romper las claves de acceso en base a un ensayo de prueba y error. Es decir, intenta las veces que sean necesarias con n posibilidades de combinación de claves hasta lograr romper el sistema criptográfico.
- Ataques de diccionario: se utiliza una lista de posibles contraseñas, palabras de diccionario en uno o varios idiomas, nombres comunes, nombres de localidades, fechas de calendario, etc.

m) Fraudes, engaños y extorsiones

- *Phishing*: ataque en el que se trata de conseguir números de cuentas, claves de acceso o demás información confidencial para realizar con ello operaciones fraudulentas que perjudiquen a los usuarios, legítimos propietarios.
- *Pharming*: es una variable del "*phishing*", los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a páginas falsas, en lugar de las legítimas para sustraer sus datos.

[26] Sistema Criptográfico: sistema de encriptación de información.

- *Spamming*: consiste en el envío indiscriminado de correos electrónicos no deseados, con la difusión de ofertas falsas o engañosas.

n) Ataques de Denegación de Servicio (DoS)

Consisten en el uso de diferentes técnicas que tiene como objetivo colapsar determinados equipos o redes informáticas para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Existen las siguientes formas de hacerlo:

- Ejecutar actividades que produzcan un elevado consumo de recursos de las máquinas afectadas (procesador, memoria y/o disco duro), provocando una caída en su rendimiento. Por ejemplo el establecimiento de múltiples conexiones simultáneas, o ataques que son generados contra los puertos de configuración de los *routers.*
- Provocar el colapso de redes de ordenadores, mediante la generación de grandes cantidades de tráfico generalmente desde múltiples sitios.
- Transmisión de paquetes mal formados o que incumplan la regla de un protocolo, provocando la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.

o) Ataques de Denegación de Servicio Distribuido (DDoS)

Se llevan a cabo mediante equipos “zombis”, los cuales son infectados por virus o troyanos, sin que sus propietarios lo hubiesen notado, abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque.

1.2.5.4 Atacantes [15]

Son personas que en su mayoría tienen conocimientos de programación, protocolos, redes, sistemas, etc., y los utilizan para analizar y/o explotar vulnerabilidades en redes o sistemas de información.

1.2.5.4.1 Clasificación de Atacantes

Existen diferentes tipos de atacantes. Se los puede clasificar en varios grupos, de acuerdo a sus conocimientos, experiencias o motivaciones como: atracción por lo prohibido, intereses financieros, políticos, éticos, venganza o simplemente por curiosidad. A continuación se citan los diferentes tipos de atacantes.

a) *Lammer*

Son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan.

A pesar de sus limitados conocimientos, son responsables de varios de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de Internet, y que pueden ser utilizadas por personas sin conocimientos técnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

b) *Hacker*

Intrusos que se dedican a atacar los sistemas informáticos como pasatiempo y como reto técnico; entran en estos sistemas para demostrar y poner a prueba su inteligencia y conocimientos, pero no pretenden provocar daños en ellos.

Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como ilegal en algunos países. El perfil típico de un *hacker* es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etc.), que invierte un importante número de horas a la semana a su afición.

En la actualidad muchos *hackers* defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que sólo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que aunque no se produzca ningún daño, se podría revelar información confidencial afectando a su privacidad.

c) *Cracker*

Individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivada por intereses económicos, políticos, entre otros. Es decir es un verdadero pirata informático.

d) *Phreaker*

Son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Hoy en día como la telefonía ha tenido un desarrollo importante utilizando sistemas digitales más avanzados, estas personas hacen uso de varias herramientas de un *hacker* o *cracker* que les permite monitorear y/o tomar control de los sistemas telefónicos.

1.2.6 HERRAMIENTAS UTILIZADAS EN LA SEGURIDAD DE LA INFORMACIÓN [16]

A continuación se describen las tecnologías y herramientas más utilizadas y aplicadas en el área de seguridad de la información.

1.2.6.1 ACLs (*Access Control Lists*) [17]

Son utilizadas como un método para otorgar un nivel básico de seguridad para el acceso a la red. Constituyen una lista de instrucciones que se aplican a la interfaz de un dispositivo de red. Se realiza una administración del tráfico de la red, ya que indican al dispositivo en el cual se encuentren configuradas qué tipo de paquetes aceptar o rechazar basándose en condiciones específicas, como tipo de protocolo, dirección origen, de destino o puerto. La figura 1.16 detalla el proceso que sigue una ACL para analizar el tráfico que entra o sale por una interfaz del dispositivo en el cual ha sido configurada.

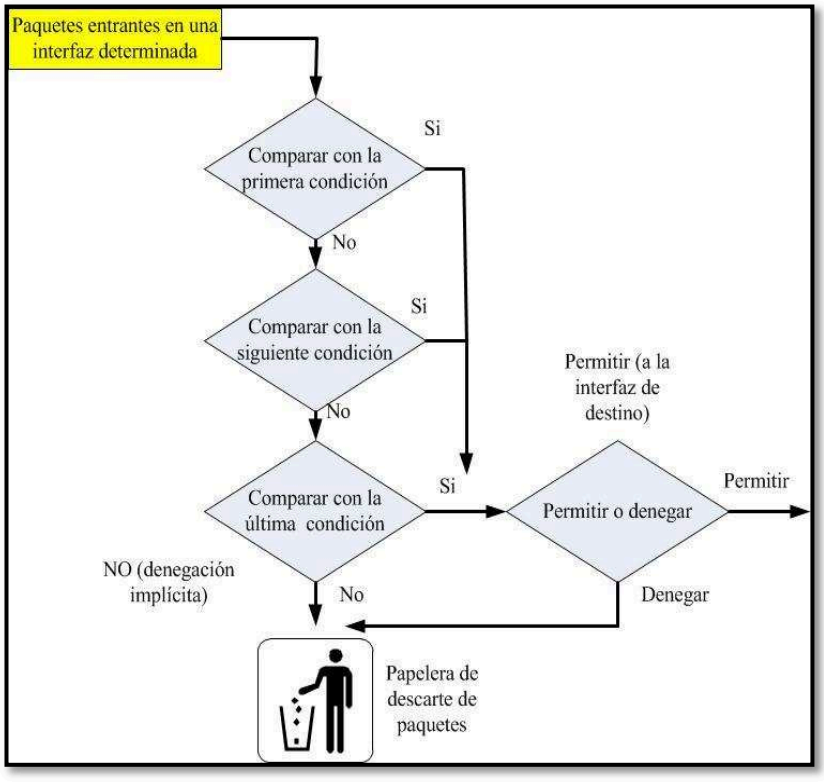


Figura 1.16: Funcionamiento de una ACL

Los paquetes entrantes o salientes por una interfaz específica, son evaluados uno por uno en función de las condiciones establecidas en la ACL; la ACL puede estar configurada para permitir o denegar el paso de los paquetes, aunque, al no cumplir alguna o algunas de las condiciones establecidas tiene un no implícito que hará que los paquetes sean rechazados.

1.2.6.2 Sistema de Control de Acceso [18]

Un sistema de control de acceso ACS por sus siglas en inglés, es un sistema que ofrece el servicio AAA (Autenticación, Autorización, Auditoría) con la finalidad de controlar el acceso remoto a una red o a la administración de sus dispositivos.

El servicio AAA puede ser configurado de forma local en cada uno de los dispositivos de la red, pero al tratarse de una red con gran cantidad de equipos es recomendable tener un sistema centralizado para optimizar dicho servicio.

1.2.6.2.1 Conceptos y Funciones

a) Cliente AAA

Se denomina como cliente AAA al software que soporte los servicios de seguridad AAA y esté corriendo sobre un dispositivo de red; por lo general, se le llama directamente Cliente AAA al dispositivo de red. Cuando alguien desee tener acceso a la red, los dispositivos de la red deben estar configurados para enviar las peticiones de acceso y autorización al ACS, el cual se encargará de otorgar o denegar el acceso de acuerdo a ciertas políticas que estén previamente configuradas en éste. Si la respuesta devuelta por el ACS es positiva se dice que se ha realizado una autenticación satisfactoria y quedará establecida la sesión.

b) Cliente Usuario Final

Cliente usuario final es aquel que desea acceder a la red o a la administración de

los dispositivos de la red, quien deberá identificarse para acceder de forma autorizada.

c) TACACS (*Terminal Access Controller Access Control System*)

Protocolo AAA que se encarga gestionar el acceso a la administración de los dispositivos de red, otorgando servicios separados de autenticación, autorización y auditoría. Utiliza un puerto TCP *(Transmission Control Protocol)* para establecer las conexiones.

TACACS+ es la versión mejorada de este protocolo.

d) RADIUS (*Remote Authentication Dial-In User Server*)

Protocolo AAA que se encarga de gestionar el acceso a los servicios que ofrece la red, otorgando servicios combinados de autenticación y autorización, y de forma independiente auditoría. Autentica y autoriza al usuario que accede a la red, permitiéndole acceder únicamente a los servicios autorizados y registra las peticiones realizadas por dicho usuario. Utiliza un puerto UDP *(User Datagram Protocol)* para realizar las conexiones.

e) Diferencias de los protocolos TACACS+ y RADIUS

En la tabla 1.1 se detallan las diferencias entre los protocolos TACACS+ y RADIUS.

1.2.6.2.2 Escenario AAA para un ACS

Un escenario AAA está conformado básicamente por un cliente AAA, un cliente usuario final y el ACS. En la figura 1.17 se tiene un usuario final que desea establecer una sesión con un cliente AAA, el cual antes de responder a dicha solicitud envía las peticiones de acceso y autorización al ACS, que a su vez

puede trabajar con una base de datos de usuarios externa para verificar los datos del usuario final y dependiendo del resultado otorgará o no el permiso solicitado.

Punto de Comparación	TACACS+	RADIUS
Protocolo Transmisión	TCP Protocolo de capa de transporte orientado a conexión. Confiable, transmisión de datos full dúplex.	UDP Protocolo de capa de transporte no orientado a conexión. Intercambio de datagramas sin acuse de recibo ni entrega garantizada.
Puerto Utilizado	49	Autenticación y Autorización: 1645 y 1812 Auditoría 1646 y 1813
Encripción	Cifrado completo de paquetes.	Encripción de *password* solo de hasta 16 bytes.
Arquitectura AAA	Control independiente de cada uno de los servicios: autenticación, autorización, auditoría.	Autenticación y autorización se combinan como un solo servicio.
Propósito	Administración de dispositivos de la red.	Control de acceso a los usuarios a la red.

Tabla 1.1: Diferencias entre los protocolos TACACS+ y RADIUS [18]

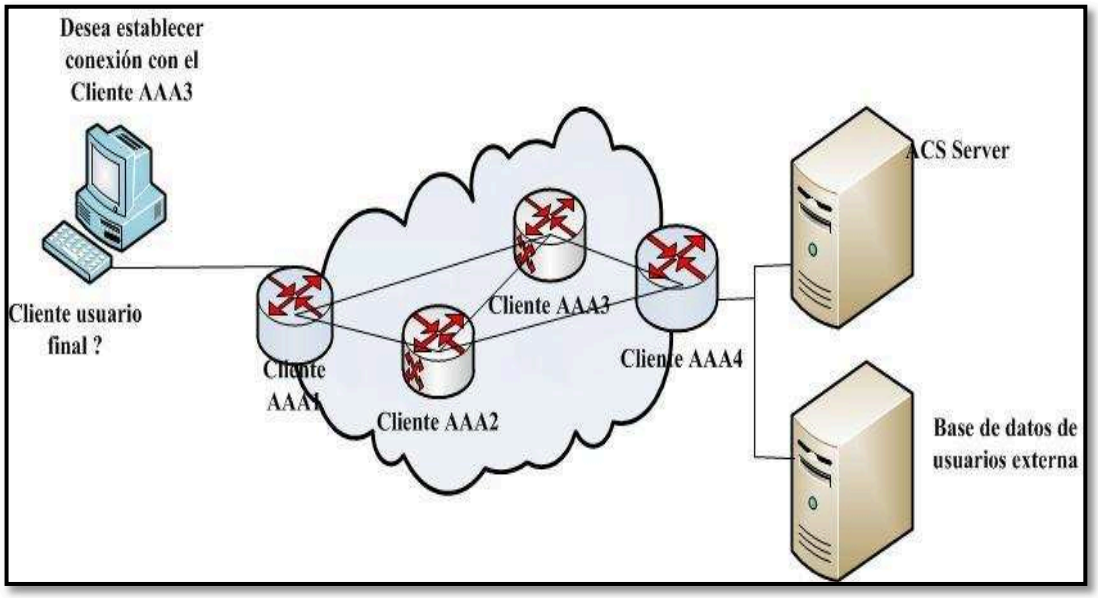


Figura 1.17: Escenario AAA

1.2.6.3 *Firewall* [19]

Sistema diseñado para mantener a las personas o sistemas no autorizados fuera de una red privada (Intranet). Todo el tráfico que entra o sale de la red privada pasa a través del *Firewall*, lo que le permite diferenciar cuál es el tráfico autorizado para permitir su paso y/o utilización, y cuál es el tráfico no autorizado para que éste sea bloqueado.

Un *Firewall* puede ser implementado mediante hardware, software o una combinación de los dos, evitando que los usuarios no autorizados de una red externa como Internet tengan acceso a las redes privadas.

En la figura 1.18 se presenta un esquema de un *Firewall* que protege a una red privada. Todo el tráfico que entra a la intranet pasa a través del *Firewall*, el cual analizará qué tipo de tráfico está autorizado para permitir o no su paso.

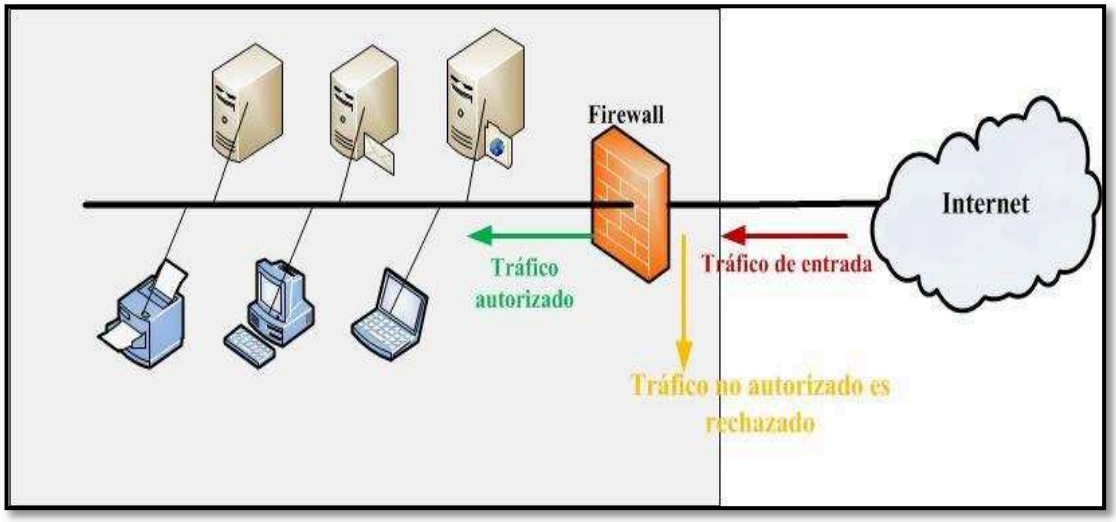


Figura 1.18: Esquema de un *Firewall* que protege una Intranet [19]

Los *firewalls* han tenido una evolución constante, mejorando el tipo de servicios que ofrecen; a continuación se describe los diferentes tipos de *firewalls* según las capacidades de bloqueo que éstos tienen.

1.2.6.3.1 Firewalls de filtrado de paquetes

Actúan mediante la inspección de paquetes, si un paquete coincide con el conjunto de reglas del filtro[27], el paquete será aceptado de lo contrario será rechazado enviando una respuesta de error al emisor. Este tipo de filtrado de paquetes no examina si el paquete forma parte de una secuencia de tráfico ya existente; es examinado en función de la información contenida en los encabezados de los paquetes, por ejemplo, dirección IP origen, dirección IP destino, tipo de paquete TCP o UDP, número de puerto.

Las direcciones IP origen y destino, permiten identificar el ordenador que originó el paquete y hacia dónde está dirigido, mientras que el tipo de paquete y el número de puerto especifican el tipo de servicio que se utiliza. Un *Firewall* de filtrado de paquetes trabaja principalmente en la capa 3 del modelo OSI, sin embargo permite y deniega tráfico en información de capa 4 como protocolo y número de puerto de origen y destino.

1.2.6.3.2 Firewalls de control de paquetes a nivel de capa aplicación

Actúan sobre la capa de aplicación[28] del modelo OSI. La clave está en que el utilizar un *Firewall* de capa aplicación implica el conocimiento de protocolos utilizados en cada aplicación; este tipo de *firewalls* es más seguro que un *Firewall* de filtrado de paquetes, ya que realizan una evaluación completa del contenido de los paquetes intercambiados.

El análisis detallado de los datos requiere una gran capacidad de procesamiento, lo que provoca una ralentización de las comunicaciones, ya que cada paquete es analizado minuciosamente. Debe interpretar una gran variedad de protocolos y las vulnerabilidades asociadas a ellos para funcionar de forma efectiva.

---

[27] Filtro: se refiere a un conjunto de reglas que contienen las condiciones necesarias que deben cumplirse para determinar si un paquete es o no dañino.

[28] Capa de aplicación: proporciona una interfaz entre el software de comunicaciones y las aplicaciones que necesitan comunicarse fuera de las computadoras en las que residen. Capa 7 del modelo OSI.

1.2.6.3.3 Firewalls de inspección de estado

Este tipo de *firewalls* tienen en cuenta también la colocación de cada paquete individual dentro de una serie de paquetes. Se le conoce también como la inspección de estado de paquetes, ya que mantienen registros de todas las conexiones que pasan a través del *Firewall,* siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente o es un paquete erróneo.

Ayudan a prevenir ataques contra conexiones ya establecidas o ataques de denegación de servicio.

1.2.6.4 IDS (*Intrusion Detection System*)

Un IDS o sistema de detección de intrusos, es un sistema desarrollado para detectar accesos no autorizados a una red. Los IDSs suelen disponer de una base de datos de “firmas” de ataques conocidos.

Se encarga de analizar detenidamente el tráfico de la red comparándolo con sus bases de datos de firmas y determinar si existe algún tipo de actividad o comportamiento anormal o sospechoso como: escaneo de puertos, paquetes mal formados, entre otros y alertar si el resultado fuese positivo.

Un IDS trabaja en conjunto con un *Firewall* ya que no tiene la capacidad de bloquear un ataque, simplemente lo detecta y alerta.

Existen dos tipos de IDSs, éstos son:

1.2.6.4.1 HIDS (HostIDS)

Se encarga de buscar rastros dejados por los atacantes en un equipo de la red interna cuando intentaron tomar control sobre éste; realizan una evaluación de

toda la información obtenida y llegan a una conclusión como resultado.

1.2.6.4.2 NIDS (NetworkIDS)

Su función es detectar ataques en toda la red, capturando todo el tráfico que transita por ella.

1.2.6.5 IPS (*Intrusion Prevention System*)

IPS o sistema de prevención de intrusión, es un mecanismo mucho más completo que un IDS, controla el acceso de usuarios ilegítimos adicionando la posibilidad de bloquear los ataques y no simplemente monitorearlos. El objetivo del IPS es detectar, analizar y bloquear ataques.

Los IPSs se agrupan según el modo en que detecten el tráfico malicioso, de la siguiente forma:

- Basado en firmas: compara el tráfico con la lista de firmas de ataques conocidos, para ello debe mantener la lista de firmas actualizadas.
- Basado en políticas: se definen políticas de seguridad estrictas, de acuerdo a ellas se permite o bloquea el tráfico.
- Detección en anomalías: se generan gran variedad de falsos positivos[29], debido a que es difícil establecer lo normal o estándar. Aquí se encuentran dos tipos de detección:
  - ✓ Detección estadística de anormalidades: todo el tráfico de la red es analizado durante un tiempo determinado, luego de lo cual se crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a dicha línea, se genera una alarma.

[29] Falsos positivos: son alarmas generadas sin que se haya realizado ningún tipo de intrusión, constituyen un problema grave aunque son prácticamente inevitables.

- ✓ Detección no estadística de anormalidades: el administrador es quien define la línea de lo que considere un patrón normal de tráfico, que es la base para la comparación del tráfico.

1.2.7 CISCO ACS (*ACCESS CONTROL SYSTEM*)

El Cisco ACS es un sistema de control de acceso que permite aplicar políticas de control de acceso en un punto centralizado de la red, para garantizar un acceso remoto seguro a la red o la administración de sus dispositivos mediante los protocolos RADIUS y TACACS+.

1.2.7.1 Cisco ACS para Sistemas Windows [18]

El Cisco ACS al ser instalado sobre un Servidor Windows pasa a operar los siguientes servicios:

- CSAdmin: el Cisco ACS dispone de una interfaz web que facilita su administración.
- CSAuth: maneja servicios de autenticación.
- CSDBSync: proporciona sincronización para trabajar con bases de datos externas de usuarios, mediante la aplicación RDBMS[30].
- CSLog: maneja registros de autenticación y contabilidad.
- CSMon: maneja actividades de monitorización, grabación y notificación sobre el rendimiento del Cisco ACS.
- CSTacacs: permite la comunicación entre los clientes AAA Tacacs+ y el servicio de autenticación.

[30] RDBMS: *Relational Database Management System* o Sistema de Gestión de Bases de Datos Relacionales, es un sistema cuyo propósito general es el de manejar de manera clara, sencilla y ordenada un conjunto de datos que posteriormente se convertirán en información relevante.

- CSRadius: permite la comunicación entre los clientes AAA Radius y el servicio de autenticación.

1.2.7.1.1 Autenticación en un Cisco ACS

La autenticación determina la identidad del usuario final que desea acceder a la red y la verifica. Un método tradicional de autenticación es mediante el uso de un nombre de usuario y contraseña. Pero hoy en día existen métodos más seguros que utilizan tecnologías como CHAP[31] y OTP[32]. Cisco ACS soporta el uso de tarjetas *token*, las cuales son consideradas uno de los métodos de autenticación OTP más seguros.

El proceso de autenticación en un escenario AAA se realiza entre el cliente AAA y el Servidor AAA, quedando desprotegido en el trayecto entre el usuario final y el cliente AAA; es por ello, que el usuario final debe utilizar un modo seguro para establecer una conexión hacia el cliente AAA, por ejemplo SSH[33], de lo contrario las credenciales enviadas por el usuario final pueden ser fácilmente capturadas utilizando algún tipo de programa espía.

1.2.7.1.2 Bases de Datos de Usuarios para Autenticación

El Cisco ACS puede realizar el proceso de autenticación utilizando una variedad de bases de datos de usuarios. Se citan a continuación los diferentes tipos de bases de datos soportados por el Cisco ACS:

- **Base de Datos Cisco ACS**: constituye la base de datos interna del sistema; las peticiones de autenticación y autorización del cliente AAA se comparan con la información contenida en esta base de datos, dependiendo del resultado se autorizará o no el acceso.

[31] CHAP: *Challenge Handshake Authentication Protocol*, verifica la identidad del cliente remoto utilizando un intercambio de información en tres etapas, esta verificación se basa en un secreto compartido como una contraseña.
[32] OTP: *One Time Password* o contraseña de un solo uso, la cual debe ser validada previo inicio de una sesión, éste tipo de método evitan los ataques por fuerza bruta.
[33] SSH: *Secure Shell,* protocolo que permite acceder remotamente a los dispositivos de una red de forma segura, utiliza técnicas de cifrado evitando que la información viaje en texto plano.

- **Base de Datos Windows:** constituye la base de datos almacenada en el servidor Windows. El Cisco ACS al recibir los datos del usuario final para realizar la autenticación y/o autorización los envía a la base de datos de Windows para validarlos y así permitir o denegar el acceso.

- **Bases de Datos Externa:** constituyen bases de datos alojadas en servidores externos, esto es posible gracias al RDBMS que permite tener una correcta sincronización.

1.2.7.1.3 Autorización en un Cisco ACS

El Cisco ACS puede enviar las políticas de un perfil de usuario al cliente AAA para determinar los servicios de red a los cuales puede acceder o los privilegios asignados para realizar actividades de administración en los clientes AAA. Además puede proporcionar información al cliente AAA para configurar un túnel seguro a un usuario específico a través de una red pública como Internet.

1.2.7.1.4 Auditoría en un Cisco ACS

El Cisco ACS hace uso de funciones de contabilidad proporcionadas por los protocolos TACACS+ y RADIUS que permiten grabar datos relevantes para cada sesión de usuario cuando éste desea acceder o accede a la red o la administración de sus dispositivos.

Los datos son grabados en bases de datos ODBC[34] que pueden ser exportados para realizar auditorías de seguridad o elaboración de informes.

1.2.7.1.5 Administración del Cisco ACS

Cisco ACS cuenta con un esquema de administración flexible. Todas las tareas de administración referentes al sistema se las puede realizar a través de una

[34] ODBC: *Open Database Connectivity*, estándar de base de datos que hace posible el acceder a cualquier dato de cualquier aplicación, sin importar que sistema de gestión de base de datos almacene los datos.

interfaz HTML[35], lo que permite una administración remota del sistema. Se sugiere seguir el siguiente orden para una correcta administración.

- **Configurar Administradores:** se debe configurar los usuarios con privilegios de administración para acceder al Cisco ACS; se debe contar con reglas bien definidas sobre el control de acceso, para el establecimiento y mantenimiento de una correcta política administrativa.

- **Configurar la interfaz HTML:** se tiene la posibilidad de configurar la interfaz HTML del Cisco ACS habilitando solo los controles y características que se fueran a utilizar, y evitar así, lidiar con parámetros desconocidos que nunca se los utilizaría. Para ello, se debe tener un conocimiento preciso de lo que sí sería útil y necesario para evitar inconvenientes en el futuro.

- **Configurar Clientes AAA:** se configuran los grupos de clientes AAA y en cada uno de ellos se ingresan los clientes correspondientes; se asigna el nombre del dispositivo, la dirección IP, la clave secreta compartida (clave que se utiliza para validar al cliente AAA), el grupo de dispositivos del que forma parte y finalmente se especifica el protocolo AAA que maneja el dispositivo de red para poder realizar las actividades de autenticación, autorización y auditoría RADIUS o TACACS+.

- **Configurar Bases de Datos Externas**: en esta fase de implementación se decide si se va o no a utilizar una base de datos externa para mantener y establecer cuentas de usuario para realizar el proceso de autenticación, que por lo general depende de la administración de la red existente. Si se decidiera utilizar una base de datos externa se deben especificar los requisitos que debería manejar el Cisco ACS para la replicación de base de datos, *backups* y sincronización.

- **Configurar Perfiles de Autorización:** se configuran las restricciones de acceso a la red y la autorización de comandos para las actividades de

[35] HTML: *HyperText Markup Language*, lenguaje utilizado en la elaboración de páginas web, en el que se describe la escritura y el contenido en forma de texto, además se complementa el texto con objetos tales como imágenes.

administración en los dispositivos de la red que se desean administrar, clientes AAA.

- **Configurar Grupos de Usuarios:** se configuran los grupos de usuarios en los que se especifican parámetros con los cuales el Cisco ACS manejará el proceso de autenticación y autorización. Además se debe tomar en cuenta que al utilizar bases de datos de usuarios externas debe existir una relación con estas bases.

- **Configurar Usuarios**: una vez establecidos los grupos de usuarios se pueden crear las cuentas de usuario; se debe tener en cuenta que un usuario puede pertenecer solo a un grupo de usuarios.

- **Configurar Auditoria:** configurar el cómo se presentarán los informes y actividades entre ellos: reportes de autenticación, autorización y auditoria para sesiones ya sea mediante el protocolo TACACS+ o RADIUS.

1.2.7.2 Cisco ACS para Sistemas Linux [20]

Es una solución basada en el sistema operativo Linux, que utiliza un concepto diferente para controlar el acceso a la red. Ofrece una monitorización avanzada, mediante alarmas, informes mucho más personalizados e incorpora herramientas para identificar problemas de conectividad hacia los diferentes clientes AAA, como *ping, traceroute, nslookup.*

Con respecto al Cisco ACS para sistemas Windows tiene algunas similitudes, tales como:

- Trabaja con los protocolos RADIUS y TACACS+.

- Maneja la base de datos de usuarios interna, así como también, trabaja con bases de datos externas.

El Cisco ACS para sistemas Linux a diferencia del Cisco ACS para sistemas

Windows se compone de varios elementos que lo convierten en un sistema de control de acceso a la red más seguro, rápido y confiable.

1.2.7.2.1 Componentes del Cisco ACS Linux

- **Sistema operativo ADE-OS:** *Application Deployment Engine- Operating System* o aplicación para la implementación del motor del sistema operativo basado en Linux.

- **Software ACS*:*** solución de última generación para controlar el acceso a la red. El control de acceso lo maneja en base a políticas que cumplen con los estándares de autenticación, autorización y auditoría. Un modelo de políticas consiste de un conjunto de condiciones y atributos que permiten establecer reglas para el acceso dinámicas y personalizadas.

- **Hardware ACS:** hardware sobre el cual pasan a funcionar el ADE-OS y el software Cisco ACS. Cisco ofrece un dispositivo de la serie 1121 enfocado al Cisco ACS para sistemas Linux. Existe una solución alternativa, mediante virtualización, utilizando VMware[36] Server; las versiones admitidas son VMware ESX[37] 3.5 y 4.0. Para ello se debe configurar el ambiente de la máquina virtual para cumplir con los requerimientos mínimos del sistema.

1.2.7.2.2 Interfaces de Administración del Cisco ACS

Se dispone de tres tipos de interfaces para administrar el sistema.

a) Interfaz basada en web

Las tareas de configuración se presentan en un orden lógico, independientemente

[36] VMware: Aplicación utilizada para virtualización.
[37] VMware ESX: *VMware Elastic Sky X*, sistema operativo de VMware basado en linux, corre como un sistema operativo dedicado al manejo y administración de máquinas virtuales ya que no necesita un sistema operativo host sobre el cual sea necesario instalarlo.

del área en particular que se esté configurando. Se refleja un nuevo modelo de políticas, en la que los atributos necesarios para la configuración de grupos de usuarios, grupos de dispositivos, filtros de acceso a la red, entre otros, se mantienen de forma independiente. Presenta la posibilidad de ordenar y filtrar ciertos elementos de una lista determinada.

b) Interfaz de línea de comando

Es una interfaz basada en texto, para llevar a cabo algunas tareas de configuración y monitoreo, para ello se debe contar con permisos de administrador.

EL software ADE-OS, en el que basa la interfaz de línea de comandos, soporta tres modos de comandos:

- **EXEC:** para realizar tareas de operación a nivel del sistema, tales como instalar, iniciar, detener la aplicación, copiar archivos, restaurar copias de seguridad, desplegar algún tipo de información.
- **ACS *Configuration*:** permite establecer el nivel de depuración de los registros, para la gestión del Cisco ACS, componentes de ejecución y mostrar la configuración del sistema.
- ***Configuration***: se realizan tareas adicionales de configuración para la aplicación del servidor en un entorno ADE-OS.

c) Interfaz de programación

Consiste de un servicio web y una interfaz de línea de comandos proporcionada por Cisco, que permiten a los desarrolladores de software mediante programación mejorar algunas características y funciones del sistema. Se puede tener acceso a la base de datos de monitorización y reportes del Cisco ACS, de acuerdo a ello desarrollar aplicaciones personalizadas o resolver posibles problemas del mismo.

Además mediante la interfaz de línea de comandos que ofrece el Cisco ACS se tiene la posibilidad de crear, leer, actualizar, eliminar objetos del Cisco ACS, o desarrollar un *script* automatizado para efectuar algún tipo de actividad de forma masiva.

1.2.7.2.3 Modelo de Políticas

El Cisco ACS Linux es un sistema de control de acceso basado en un modelo de políticas. Una política puede ser simple o compleja.

Una política simple aplica un solo resultado a todas las solicitudes de acceso sin ningún tipo de condiciones; una política compleja se trata de un conjunto de reglas que ponen a prueba varias condiciones para evaluar la petición de acceso.

Se pueden crear servicios de acceso múltiples para procesar diferentes tipos de solicitudes de acceso, por ejemplo para la administración de dispositivos o para acceder a la red.

Terminología en una política

- **Política:** conjunto de reglas para llegar a tomar una decisión sobre si se permite o no el acceso. Se debe establecer una regla por defecto, ya que puede darse el caso de que una petición de acceso no coincida con ninguna de las reglas establecidas.
- **Servicio de acceso:** conjunto de políticas para evaluar la solicitud de acceso. Hay dos servicios de acceso por defecto, uno para la administración de dispositivos mediante el protocolo TACACS+ y otro para acceder a la red mediante el protocolo RADIUS.
- **Elementos de la política:** objetos que definen las condiciones de la política de acceso, por ejemplo hora, fecha, condiciones personalizadas basadas en atributos o los permisos de autorización. Los elementos de

política hacen referencia a la creación de reglas para la política de acceso.

- **Perfil de autorización:** permisos otorgados para un servicio de acceso a la red basado en RADIUS; se definen los permisos de acceso que serán concedidos al momento de acceder a la red.

- ***Shell profile*:** permisos otorgados para un servicio de acceso a la administración de los clientes AAA basado en TACACS+. Por ejemplo, nivel de privilegio en el Cisco IOS[38], tiempo de espera para inhabilitar una sesión, etc.

- **Conjunto de comandos:** se definen los comandos que se podrán o no ejecutar en el *shell* del IOS de los clientes AAA que manejen TACACS+.

- **Política de identidad:** se puede elegir la forma de autenticar, la base de datos que se utilizará y el protocolo para el proceso de autenticación.

- **Política de autorización:** es el resultado de la regla aplicada.

- **Política de excepción:** es un tipo de política especial que permite configurar cierto tipo de excepciones para una política de autorización determinada.

1.2.7.2.4 Políticas basadas en reglas

Este tipo de políticas han sido desarrolladas con la finalidad de superar los retos de políticas basadas únicamente en la identidad. En el Cisco ACS para sistemas Windows, un usuario estaba asociado a un grupo de usuario, por lo tanto todos los usuarios asociados a un grupo de usuarios tenían las mismas restricciones de acceso en todo momento; ya que la autorización está asociada al grupo de usuarios, para usuarios que necesiten permisos diferentes en condiciones diferentes este tipo de políticas no funciona.

El Cisco ACS para sistemas Linux crea reglas basadas en varias condiciones

[38] IOS: *Internetwork Operating System*, sistema operativo utilizado por los equipos de red marca Cisco.

además de la identidad, tales como ubicación, hora y fecha, tipo de acceso entre otras, dependiendo de ello se determina qué permisos de acceso se otorga. Las condiciones principales para establecer una política basada en reglas se detallan a continuación.

a) Condiciones de Identidad

Existen dos métodos principales para definir el mecanismo y la fuente de la solicitud de autenticación: basado en contraseñas, que consiste en comparar el nombre de usuario y contraseña con la base de datos de usuarios que se maneje y basada en certificados. Si se realiza una autenticación basada en certificados, el Cisco ACS debe seleccionar un perfil de certificado de autenticación único y si se lo hace mediante una base de datos de identidad, se debe definir una lista de bases de datos para acceder en secuencia hasta que la autenticación tenga éxito.

b) Condiciones de Restricción

Un tipo de política puede ser para la selección de servicios basada en un conjunto de reglas, el Cisco ACS decide qué servicios de acceso autorizar basado en varias opciones configuradas, protocolo AAA usado para la solicitud, la fecha y hora en que el Cisco ACS recibe la solicitud, el grupo de dispositivos de red al que pertenece el cliente AAA, el cliente AAA que envía la solicitud.

1.3 ANÁLISIS DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN [12]

La seguridad de la información en cualquier organización o empresa está directamente relacionada con los riesgos a los que está expuesta. El proceso para establecer medidas de seguridad para proteger la información, es por lo general un proceso engorroso y complejo, un análisis de riesgos optimiza este proceso.

El análisis de riesgos es crucial para el desarrollo y operación de un plan de

seguridad de la información. En esta etapa, la organización debe construir lo que será su “modelo de seguridad”, esto es, una representación de todos sus activos y sus dependencias jerárquicas, así como la identificación de amenazas (todo aquello que pudiera ocurrir y que tuviera un impacto para la organización). Posteriormente se realiza la estimación de impactos (probabilidad de que se materialice la amenaza) y se calcula el riesgo al que está sometida la organización.

Sin embargo, este diagnóstico es válido sólo para ese momento puntual en el tiempo. No es algo estático sino que va a cambiar a lo largo del tiempo: nuevos activos, nuevas amenazas, modificación en la ocurrencia de las amenazas, etc. Por tanto, continuamente la organización debe replantearse su diagnóstico y cuestionarse si tiene nuevos síntomas o si los síntomas detectados en análisis anteriores han sido ya mitigados y poder tratar otras carencias de menor importancia. [21]

1.3.1 CONCEPTO

Es un estudio para identificar amenazas, las que se pueden concretar a través de fallas de seguridad conocidas como vulnerabilidades, su probabilidad de ocurrencia en diferentes tipos de escenarios y el impacto que ocasionarían, con el fin de establecer los controles idóneos para aceptar, disminuir, eliminar o transferir el riesgo.

1.3.2 METODOLOGÍAS PARA LA ESTIMACIÓN DEL RIESGO

El análisis de riesgos puede llevarse a cabo con diferentes grados de detalle, dependiendo de la criticidad de los elementos involucrados en el proceso, tipo de vulnerabilidades presentes en el sistema de información, incidentes detectados anteriormente en la organización, etc. Por lo que, la metodología para llevar a cabo la estimación del riesgo puede ser cualitativa o cuantitativa o una combinación de ambas dependiendo de las circunstancias.

1.3.2.1 Metodología cualitativa

Es una de las metodologías más utilizadas y difundidas para realizar una estimación del riesgo, ya que se trata de un proceso dinámico e intuitivo. Esta metodología se basa en una escala de atributos calificativos, los cuales describen la magnitud de las consecuencias potenciales, por ejemplo: crítica, alta, media, baja.

Una de las ventajas de la estimación cualitativa, es la facilidad de comprensión por el personal involucrado en el proceso, y su desventaja es la dependencia en la selección subjetiva dentro de la escala establecida.

En el desarrollo de esta metodología se toman en cuenta cuatro parámetros principales: amenazas, vulnerabilidades que siempre están presentes en una red o sistema de información, el impacto asociado a una amenaza si ésta llegara a materializarse y las medidas o controles preventivos o correctivos.

1.3.2.2 Metodología cuantitativa

Implica realizar una recolección de datos, cálculos complejos, técnicas de modelamiento[39], etc. Se utiliza una escala con valores numéricos, a diferencia de la anterior que utilizaba una escala descriptiva, tanto para la evaluación de probabilidades de ocurrencia como para sus consecuencias basándose en datos provenientes de varias fuentes.

El éxito de esta metodología depende de lo completos y exactos que sean los valores numéricos y de la validez que tengan los modelos utilizados. Utiliza dos parámetros para la estimación del riesgo, la probabilidad de que el evento ocurra y una estimación del costo o las pérdidas en caso de que el evento sea positivo.

[39] Las técnicas de modelamiento recogen aspectos relevantes de acuerdo a las intenciones que tenga el modelador, de las que se pretende extraer conclusiones de tipo predictivo. Se modela para comprender mejor o explicar mejor un proceso o unas observaciones.

Una estimación cuantitativa del riesgo puede realizarse después de haber realizado una estimación cualitativa, sin embargo, cada tipo de metodología puede ser ejecutada por separado o combinarse y ser ejecutadas de forma simultánea.

1.3.3 NORMA ISO/IEC[40] 27005:2008 [22]

ISO/IEC es un comité técnico en el campo de la tecnología de la información, formado por una organización especializada en el desarrollo y difusión de estándares a nivel mundial (ISO) y por una comisión que prepara y publica estándares en el campo de la electrotecnología (IEC).

La norma ISO/IEC 27005: 2008, forma parte de la serie 27000 de las normas ISO/IEC, estas normas son aplicables a cualquier tipo de organización, sea ésta pública, privada, grande o pequeña. La norma ISO/IEC 27005: 2008 titulada "Tecnología de Información – Técnicas de seguridad – Gestión de Riesgos de Seguridad de Información" fue publicada en junio del 2008; esta norma proporciona una guía para la gestión del riesgo en un Sistema de Seguridad de la Información y permite definir nuestro propio enfoque para estimar el riesgo.

1.3.3.1 Objeto y campo de aplicación de la norma ISO/IEC 27005:2008

Establece directrices para la gestión del riesgo en la seguridad de la información. Diseñada para facilitar la implementación satisfactoria de la seguridad de la información, tomando como referencia la gestión del riesgo.

Esta norma es aplicable a todos los tipos de organizaciones que pretenden gestionar el riesgo que podría comprometer la seguridad de la información de la organización.

El alcance para la gestión del riesgo puede ser: una aplicación de tecnología de la

[40] ISO/IEC: *International Organization for Standardization / International Electrotechnical Commission*.

información, infraestructura de tecnología de la información, un proceso de negocio, servicios ofrecidos por la entidad o una parte definida de la organización.

1.3.3.2 Estructura de la norma ISO/IEC 27005:2008

Para una mejor comprensión de las actividades a desarrollar durante el proceso de la gestión del riesgo en la seguridad de la información, la norma ISO/IEC 27005:2008 estructura cada actividad de la siguiente forma:

Referencia: se especifica la información que se utilizará como base para poder desarrollar la actividad.

Acción: se describe en qué consiste la actividad que se realizará.

Guía de desarrollo: proporciona información guía, dando una orientación de cómo llevar a cabo la acción a quién o quienes la desarrollen.

Resultado: se establece la información que se tendrá como respuesta, una vez que la actividad haya sido desarrollada.

1.3.3.3 Visión general del proceso de gestión del riesgo en la seguridad de la información

La norma ISO/IEC 27005 para la gestión del riesgo en la seguridad de la información establece 6 actividades: establecimiento del contexto, valoración (análisis y evaluación) del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo. En cada una de estas actividades se describe el proceso que se debe realizar, otorgando ciertas directrices para que los resultados obtenidos sean los óptimos y apegados a la realidad.

En el proceso de gestión del riesgo debe existir un intercambio continuo de

información entre los directivos y el personal operativo de la organización; el informar sobre los riesgos identificados permitirá reducir el daño potencial que éstos podrían ocasionar. La predisposición o colaboración prestada por los directivos y el personal responsable de la mitigación de los riesgos facilitará el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz.

1.3.3.4 Análisis de Riesgos según la NORMA ISO/IEC 27005:2008

1.3.3.4.1 Establecimiento del contexto

Referencia: información relevante de la organización, que ayude a establecer el contexto de la gestión del riesgo en la seguridad de la información.

Acción: establecer el contexto para la gestión del riesgo en la seguridad de la información: criterios básicos, definición del alcance y los límites, y establecer una organización que opere la gestión del riesgo en la seguridad de la información.

Guía para el desarrollo: es esencial determinar el propósito de la gestión del riesgo en la seguridad de la información, de esto dependerá el establecimiento del contexto. El propósito puede ser:

- Dar soporte a un Sistema de Gestión de la Información.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan para la continuidad del negocio.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.

Los criterios básicos a considerar pueden ser:

- Criterios para la evaluación del riesgo en la seguridad de la información, por ejemplo: la importancia de la integridad, disponibilidad y confidencialidad para las operaciones y la organización o la criticidad de los activos involucrados.
- Criterios de impacto del riesgo expresándolo en términos del grado de daño o coste para la organización, por ejemplo: daños para la reputación, pérdida del negocio y del valor financiero, incumplimiento de requisitos legales.
- Criterios de aceptación del riesgo, que en lo general dependen de la frecuencia de las políticas metas y objetivos de la organización. Sin embargo, cada organización debería fijar sus propias escalas del nivel de aceptación del riesgo que podrían ser, en función del beneficio estimado y el riesgo estimado.

Al definir el alcance y los limites se debe considerar que todos los activos relevantes a la organización sean tomados en cuenta al realizar la valoración del riesgo, activos como: de información, funciones y estructuras de la organización, política de seguridad de información de la organización, ubicación de la organización y sus características geográficas, etc.

En cuanto a la organización, se deben establecer responsabilidades para el desarrollo del proceso de gestión de riesgos, por ejemplo: identificar y analizar las partes interesadas, definir las funciones y las responsabilidades de todas las partes, tanto internas como externas de la organización y esencialmente establecer las rutas para escalar decisiones.

Resultado: criterios básicos definidos, alcance y límites, y organización del proceso de gestión del riesgo en la seguridad de la información.

1.3.3.4.2 Valoración del riesgo en la seguridad de la información

Referencia: información definida en el establecimiento del contexto, tales como criterios básicos, el alcance, los límites y la organización establecida para el proceso de la gestión del riesgo en la seguridad de la información.

Acción:

Analizar el riesgo: identificar y estimar el riesgo, lo que incluye:

- Identificar los activos dentro del alcance establecido.
- Identificar las amenazas y sus orígenes.
- Identificar los controles existentes y los planificados.
- Identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o la organización.
- Identificar las consecuencias que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad de los activos.
- Evaluar el impacto en el negocio de la organización que pueda resultar de incidentes posibles o reales en la seguridad de la información.
- Evaluar la probabilidad de los escenarios de incidente.
- Estimar el nivel de riesgo para todos los escenarios de incidente pertinentes.

Evaluar el riesgo:

- Comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

Guía para el desarrollo: un riesgo es la combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo.

a) Análisis de riesgos

Los siguientes puntos constituyen la identificación del riesgo en la organización:

- **Identificación de los activos:** se entiende por activo todo aquello que tiene valor para la organización y por lo tanto requiere protección. Se debe identificar todos los activos de la organización de acuerdo al alcance y los límites establecidos; es esencial localizar al propietario de cada activo, ya que es la persona más indicada para proporcionar información sobre dicho activo. El propietario de cada activo no necesariamente tiene derechos de propiedad del activo, es la persona que se encarga del mantenimiento, funcionamiento, etc.

- **Identificación de amenazas**: una amenaza tiene el potencial de causar daños a activos tales como: información, procesos, sistemas y por consiguiente a la organización. Si una amenaza se llegara a efectuar, puede causar perjuicios a más de un activo, en tal caso, el impacto ocasionado dependería de los activos que se verían afectados. Las amenazas y su probabilidad de ocurrencia serán identificadas de acuerdo a la información proporcionada por el propietario de cada activo.

- **Identificación de los controles existentes**: se debe comprobar si existen controles para el tratamiento de los riesgos, con el fin de evitar tener controles repetidos. De existir, éstos deben ser verificados para garantizar que funcionan correctamente, ya que pueden ser la causa para la presencia de vulnerabilidades. La forma de comprobar la efectividad de tales controles es ver la manera en que reducen la probabilidad de ocurrencia de la amenaza y la dificultad de explotar la vulnerabilidad o el

impacto del incidente. Un control existente o planificado, puede ser calificado como ineficaz, insuficiente o injustificado. Si es injustificado o insuficiente, debería ser revisado para ver si es eliminado, remplazado o permanece.

- **Identificación de vulnerabilidades:** esta actividad se basará en la información de los puntos anteriores, es decir, identificación de activos, identificación de amenazas y la identificación de los controles existentes. Las vulnerabilidades pueden ser identificadas en áreas como: organización, procesos y procedimientos, personal, ambiente físico, hardware, software o equipos de comunicaciones, rutinas de gestión, entre otras. La vulnerabilidad para causar daño necesita la presencia de una amenaza y viceversa, por si solas constituyen solo un riesgo latente.

  Identificación de consecuencias: pueden ser, pérdida de reputación de la organización, daño a la imagen de la organización, problemas con la continuidad del negocio, etc. Las consecuencias pueden ser de naturaleza temporal o permanente como la destrucción de un activo. Se deben tener en cuenta los activos de la organización, sus amenazas y vulnerabilidades. La organización podría identificar sus consecuencias operativas en función de pérdida de tiempo, tiempo de investigación y reparación, pérdida de oportunidad, imagen, reputación y buen nombre, costo financiero de las habilidades específicas para reparar el daño, entre otras.

Los siguientes puntos constituyen la estimación del riesgo en la organización:

- **Valoración de las consecuencias:** se deberá evaluar el impacto ocasionado en la organización, resultado de la explotación de una amenaza a través de una vulnerabilidad. La valoración de activos es un factor clave en la valoración del impacto de un escenario de incidente, porque el incidente puede afectar a más de un activo o únicamente una parte de un activo. Diferentes amenazas y vulnerabilidades tendrán impactos diferentes en los activos, por ejemplo la pérdida de

confidencialidad, integridad o disponibilidad. La valoración de las consecuencias, por tanto, se relaciona con la valoración de activos con base en el análisis del impacto en el negocio.

Las consecuencias se pueden expresar en términos financieros, técnicos, del impacto humano u otros criterios pertinentes para la organización. En algunos casos, se requiere más que un valor numérico para especificar las consecuencias para diferentes tiempos, lugares, grupos o situaciones.

Al finalizar esta actividad se debería tener los riesgos identificados con su respectiva valoración y prioridad de acuerdo a los criterios establecidos para la evaluación del riesgo.

- **Valoración de los incidentes:** al haber identificado los diferentes escenarios de incidentes, es menester establecer la probabilidad de cada incidente y el impacto que ocasionarían cuando éstos ocurran. Se debe considerar la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas. Se toma como base la información de los escenarios de incidentes, que incluye la identificación de las amenazas, los activos afectados, las vulnerabilidades explotadas y las consecuencias para los activos y los procesos del negocio. Se obtendrá la probabilidad de los diferentes escenarios de incidente.

- **Nivel de estimación del riesgo:** se deberá estimar el nivel de riesgo para todos los escenarios de incidente, para ello se utiliza la lista de los escenarios de incidente con sus consecuencias relacionadas con los activos, los procesos del negocio y su probabilidad de ocurrencia. La estimación del riesgo asigna valores cualitativos o cuantitativos a la probabilidad y las consecuencias de un riesgo. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias.

b) Evaluación del riesgo

Consiste en tomar las decisiones pertinentes de acuerdo a los criterios definidos en el establecimiento del contexto para evaluar el riesgo. Los criterios de evaluación del riesgo deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna. Se deberían tomar en cuenta los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones a tomar para la evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo.

Resultado: lista de los riesgos que amenazan a la organización, identificados, analizados y evaluados.

1.3.3.4.3 Tratamiento del riesgo en la seguridad de la información

Referencia lista de los riesgos que amenazan a la organización, identificados, analizados y evaluados.

Acción: seleccionar controles para reducir, retener, o evitar los riesgos y definir un plan para tratamiento del riesgo.

Guía para el desarrollo: para el tratamiento del riesgo existen cuatro opciones a elegir: reducción del riesgo, retención del riesgo, evitación del riesgo y transferencia del riesgo.

Las opciones para el tratamiento del riesgo deberían ser seleccionadas de acuerdo al resultado de la valoración del riesgo, el costo que involucre su implementación y los beneficios que se tendrían como resultado de tales opciones.

a) Reducir el riesgo

Implica la selección de controles adecuados de acuerdo a los requerimientos identificados en la valoración y tratamiento del riesgo. Se deben tomar en cuenta los criterios de aceptación del riesgo, requisitos legales, reglamentarios y contractuales. Las acciones de control para reducir el riesgo puede tratarse de: corrección, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y toma de conciencia. Al seleccionar el tipo de control es importante considerar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles en comparación con el valor de los activos que se protegen, es decir relación costo-beneficio.

Existen cierto tipo de restricciones que se deben considerar al momento de seleccionar los controles, algunas de éstas son: restricciones de tiempo, restricciones financieras, restricciones operativas, restricciones legales, facilidad de uso, restricciones de personal, etc.

b) Retener el riesgo

Si el nivel del riesgo de acuerdo a la evaluación del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se lo puede retener.

c) Evitar el riesgo

Si los riesgos identificados son demasiado altos, y el costo que implica tratar dicho riesgo sobrepasa los beneficios que se obtendrán se opta por una decisión de evitar por completo el riesgo, mediante el retiro de una actividad o conjunto de actividades planificadas o existentes. Por ejemplo, riesgos causados por la naturaleza se opta por transferir físicamente las instalaciones que estén en peligro a otro lugar donde no exista tal riesgo o esté al menos bajo control.

d) Transferir el riesgo

Involucra la decisión de compartir el tratamiento de algún o algunos riesgos con partes externas, mediante seguros que darán soporte a las consecuencias o subcontrataciones de un asociado cuya función será monitorear el sistema de información y tomar medidas inmediatas para detener un ataque antes de que éste produzca un nivel definido de daño.

Éste puede generar la creación de nuevos riesgos o modificar los riesgos identificados existentes. Cabe recalcar que se puede transferir la responsabilidad para el tratamiento del riesgo, pero no se puede transferir la responsabilidad del impacto, los clientes que se vieran afectados ante eventos adversos atribuirán las fallas a la organización.

Resultado: definición del plan para el tratamiento de los riesgos. Realizado este proceso se debe determinar los riesgos residuales, lo que implica una actualización o iteración de la valoración del riesgo, considerando los resultados esperados del tratamiento propuesto para tal riesgo. Si el riesgo residual aún no satisface los criterios de aceptación del riesgo de la organización, puede ser necesaria otra iteración del tratamiento del riesgo antes de proceder con la aceptación del riesgo.

CAPÍTULO 2

SITUACIÓN ACTUAL DE LA RED IP/MPLS DE LA CNT E.P.

2.1 RED IP/MPLS [1]

En busca de poder ofrecer una mayor variedad de servicios y costos reducidos para los usuarios finales, ampliar la cobertura para llegar a diferentes poblaciones y aprovechando el *backbone* Nacional de Fibra Óptica[41], nace la idea de una red de última generación basada en la tecnología MPLS. Sobre esta red se podrían ofrecer los servicios ya existentes, de telefonía fija alámbrica e inalámbrica, datos e Internet (estos servicios se detallan más adelante en la sección 2.4), y poder sumar nuevos servicios como IP-TV[42], cumpliendo así con las metas del Plan Nacional de Conectividad[43].

Tras una serie de pruebas y procedimientos que se ejecutaron para efectuar la demostración de capacidades y puesta a punto para su funcionamiento, a inicios del 2009 la red IP/MPLS empezó a operar con equipos en las provincias de Pichincha y Tungurahua y se extendió rápidamente a otros puntos del país.

2.1.1 EVOLUCIÓN DE LA RED IP/MPLS

2.1.1.1 Fase Inicial

La red IP/MPLS se implementó para optimizar el transporte de servicios de voz, datos, video e Internet, con una cobertura casi total a lo largo de la Provincia de

[41] *Backbone* Nacional de Fibra Óptica: la red de fibra óptica más grande a nivel nacional, instalada en todo el territorio ecuatoriano.
[42] IPTV: *Internet Protocol Television*, denominación comúnmente utilizada para los sistemas de distribución por subscripción de señales de televisión o vídeo usando conexiones de banda ancha sobre el protocolo IP.
[43] PNC o Plan Nacional de Conectividad: fue creado para mejorar los indicadores de cuatro servicios: telefonía fija, Internet banda ancha, inclusión social y atención al ciudadano.

Pichincha y parcial en la provincia de Tungurahua.

La fase inicial de la red IP/MPLS nace como una red jerárquica con equipos de *core*, distribución y acceso. Los equipos identificados como *core* representan a los equipos tipo P o LSR, *routers* que realizan la conmutación de paquetes basados en una simple revisión y conmutación de etiquetas. Los equipos identificados como distribución y acceso que están a uno y dos saltos de los equipos de *core* respectivamente representan a los equipos tipo PE, que vendrían a ser los *routers* extremos que realizan la revisión de enrutamiento.

La fase inicial de la red IP/MPLS se conformó por 3 equipos P y 32 equipos PE ubicados en la Provincia de Pichincha y 2 equipos PE ubicados en la Provincia de Tungurahua.

2.1.1.2 Fase 1

La implementación de la red IP/MPLS en la fase inicial en la CNT E.P. cubrió rápidamente las expectativas deseadas, teniendo con ella una mejora en la calidad de los servicios de red y un abaratamiento de costos, por lo que su expansión se veía necesaria e inmediata.

Poco tiempo después de la puesta en funcionamiento de la fase inicial, ésta se extendió agregando equipos PE en las Provincias de Carchi, Guayas, Santo Domingo, Orellana, Imbabura, Esmeraldas, Napo, Pastaza, Cotopaxi y Chimborazo. Al igual que en la fase inicial se tenían 3 equipos P.

En resumen esta fase estuvo conformada por 3 equipos P y 57 equipos PE.

2.1.1.3 Fase 2

El objetivo en esta segunda fase fue fortalecer el *backbone* nacional de la red IP/MPLS, lo que permitiría ampliar la gama de servicios a sus clientes, mejorar los

niveles de servicios y contribuir con el desarrollo social de la población ecuatoriana, promoviendo el acceso a las tecnologías de información y telecomunicaciones. La red IP/MPLS fase 2 es la que se tiene implementada actualmente.

En esta fase se tienen 11 equipos P, 8 más que en la fase 1, ampliando así la cobertura a nivel de *backbone* en las provincias de Tungurahua, Esmeraldas, Pastaza, Guayas, Manabí y Azuay. Se cuenta con 73 equipos PE ubicados en las diferentes provincias del país. Adicionalmente, en esta fase se agregaron 3 equipos denominados *Route Reflectors*[44] con la finalidad de mejorar el rendimiento y administración de la red.

2.1.2 INFRAESTRUCTURA DE LA RED IP/MPLS DE LA CNT E.P.

2.1.2.1 Equipos de la red IP/MPLS de la CNT E.P. [1]

La red IP/MPLS de la CNT E.P está compuesta por equipos de marca Cisco. En la tabla 2.1 se listan los equipos que la componen y en la figura 2.1 se aprecia la topología de la red.

	#	PROVINCIA	NODO	HOSTNAME	MARCA	MODELO
Route Reflector	1	GUAYAS	BELLAVISTA	GYEBLLX01	CISCO	ASR1006
	2	PICHINCHA	IÑAQUITO	UIOINQX01	CISCO	ASR1006
	3	TUNGURAHUA	AMBATO SUR	AMBSURX01	CISCO	ASR1006
Equipos P	1	AZUAY	CUENCA CENTRO	CCACNTP01	CISCO	GSR 12816
	2	ESMERALDAS	LAS PALMAS	ESMPALP01	CISCO	GSR 12810
	3	GUAYAS	CORREOS GUAYAQUIL	GYECNTP01	CISCO	CRS-8/S
	4	GUAYAS	BELLAVISTA	GYEBLLP01	CISCO	CRS-8/S
	5	MANABÍ	MANTA	PVJMNTP01	CISCO	GSR 12810
	6	PASTAZA	PUYO CENTRO	PUYCNTP01	CISCO	GSR 12810
	7	PICHINCHA	IÑAQUITO	UIOINQP01	CISCO	CRS-8/S

Tabla 2.1: Equipos de la red IP/MPLS de la CNT E.P. (Página1 de 3)

[44] *Route Reflector* o RR, es un componente de enrutamiento dentro de una red que se comporta básicamente como un espejo, que refleja las actualizaciones que recibe a sus vecinos, evitando tener una red totalmente mallada.

	#	PROVINCIA	NODO	HOSTNAME	MARCA	MODELO
Equipos P	8	PICHINCHA	MARISCAL	UIOMSCP01	CISCO	CRS-8/S
	9	PICHINCHA	QUITO CENTRO	UIOQCNP01	CISCO	GSR 12810
	10	TUNGURAHUA	AMBATO CENTRO	AMBCNTP01	CISCO	CRS-8/S
	11	TUNGURAHUA	AMBATO SUR	AMBSURP01	CISCO	CRS-8/S
Equipos PE	1	AZUAY	CUENCA CENTRO	CCACNTE01	CISCO	7609-S
	2	BOLÍVAR	GUARANDA	GRDCNTE01	CISCO	7609-S
	3	CAÑAR	AZOGUEZ	AZGCNTE01	CISCO	7609-S
	4	CARCHI	TULCÁN	TLCCNTE01	CISCO	7609-S
	5	CARCHI	TULCÁN	TLCCNTE02	CISCO	ME 6524
	6	CHIMBORAZO	RIOBAMBA CENTRO	RBBCNTE01	CISCO	7609-S
	7	COTOPAXI	LATACUNGA CENTRO	LTCCNTE01	CISCO	7609-S
	8	COTOPAXI	LATACUNGA CENTRO	LTCCNTE02	CISCO	ME 6524
	9	EL ORO	MACHALA CENTRO	MCHCNTE01	CISCO	7609-S
	10	ESMERALDAS	LAS PALMAS	ESMPALE01	CISCO	7609-S
	11	ESMERALDAS	LAS PALMAS	ESMPALE02	CISCO	ME 6524
	12	GUAYAS	CORREOS GUAYAQUIL	GYECNTE01	CISCO	7606-s
	13	GUAYAS	FINANSUR	GYEFNSE01	CISCO	7613
	14	GUAYAS	CORREOS DEL ECUADOR	GYECNTE02	CISCO	ME 6524
	15	GUAYAS	FINANSUR	GYEFNSE02	CISCO	ME 6524
	16	IMBABURA	IBARRA	IBRCNTE01	CISCO	7609-S
	17	IMBABURA	IBARRA	IBRCNTE02	CISCO	7609-S
	18	LOJA	LOJA CENTRO	LOJCNTE01	CISCO	7609-S
	19	LOS RÍOS	BABAHOYO	BBHCNTE01	CISCO	7609-S
	20	LOS RÍOS	QUEVEDO	BBHQVDE01	CISCO	ME 6524
	21	MANABÍ	MANTA	PVJMNTE01	CISCO	7606-s
	22	MANABÍ	PORTOVIEJO CENTRO	PVJCNTE01	CISCO	7606-s
	23	MORONA SANTIAGO	MACAS	MCSCNTE01	CISCO	7609-S
	24	NAPO	TENA CENTRO	TENCNTE01	CISCO	7609-S
	25	ORELLANA	ORELLANA CENTRO	PFOCNTE01	CISCO	7609-S
	26	ORELLANA	ORELLANA CENTRO	PFOCNTE02	CISCO	ME 6524
	27	PASTAZA	PUYO CENTRO	PUYCNTE01	CISCO	7609-S
	28	PASTAZA	PUYO CENTRO	PUYCNTE02	CISCO	ME 6524
	29	PICHINCHA	CARCELÉN	UIOCCLE01	CISCO	7609-S
	30	PICHINCHA	CONDADO	UIOCNDE01	CISCO	7609-S
	31	PICHINCHA	COTOCOLLAO	UIOCTCE01	CISCO	7609-S
	32	PICHINCHA	CUMBAYÁ	UIOCBYE01	CISCO	7609-S
	33	PICHINCHA	ESCUELA ESPEJO	UIOEEPE01	CISCO	7606-s
	34	PICHINCHA	IÑAQUITO	UIOINQE01	CISCO	7613
	35	PICHINCHA	IÑAQUITO	UIOINQE02	CISCO	ME 6524

Tabla 2.1: Equipos de la red IP/MPLS de la CNT E.P. (Página 2 de 3)

	#	PROVINCIA	NODO	HOSTNAME	MARCA	MODELO
Equipos PE	36	PICHINCHA	LA FLORIDA	UIOLFLE01	CISCO	7606-s
	37	PICHINCHA	LA PAZ	UIOLPZE01	CISCO	7606-s
	38	PICHINCHA	LAS CASAS	UIOLCSE01	CISCO	7606-s
	39	PICHINCHA	MARISCAL	UIOMSCE01	CISCO	7613
	40	PICHINCHA	MARISCAL	UIOMSCE04	CISCO	7606-s
	41	PICHINCHA	MONTESERRÍN	UIOMSRE01	CISCO	7606-s
	42	PICHINCHA	QUITO CENTRO	UIOQCNE01	CISCO	7613
	43	PICHINCHA	VILLAFLORA	UIOVLFE01	CISCO	7609-S
	44	PICHINCHA	CALDERÓN	UIOCLDE01	CISCO	7609-S
	45	PICHINCHA	CARAPUNGO	UIOCRPE01	CISCO	ME 6524
	46	PICHINCHA	CARONDELET	UIOCRDE01	CISCO	7606-s
	47	PICHINCHA	CAYAMBE	UIOCAYE01	CISCO	7609-S
	48	PICHINCHA	COLLALOMA	UIOCLME01	CISCO	7606-s
	49	PICHINCHA	GUAJALÓ	UIOGJLE01	CISCO	7609-S
	50	PICHINCHA	GUAMANÍ	UIOGMNE01	CISCO	7609-S
	51	PICHINCHA	LA BOTA	UIOLBTE01	CISCO	7606-s
	52	PICHINCHA	LA CAROLINA	UIOLCLE01	CISCO	7606-s
	53	PICHINCHA	LA LUZ	UIOLLZE01	CISCO	7609-S
	54	PICHINCHA	LA LUZ	UIOLLZE02	CISCO	ME 6524
	55	PICHINCHA	LOS NEVADOS	UIOLNVE01	CISCO	7606-s
	56	PICHINCHA	MACHACHI	UIOMCHE01	CISCO	7609-S
	57	PICHINCHA	MARISCAL	UIOMSCE02	CISCO	ME 6524
	58	PICHINCHA	MARISCAL	UIOMSCE03	CISCO	ME 6524
	59	PICHINCHA	MONJAS	UIOMNJE01	CISCO	7609-S
	60	PICHINCHA	PINTADO	UIOPTDE01	CISCO	7609-S
	61	PICHINCHA	QUINCHE	UIOQCHE01	CISCO	7609-S
	62	PICHINCHA	QUITO CENTRO	UIOQCNE02	CISCO	ME 6524
	63	PICHINCHA	SAN ISIDRO DEL INCA	UIOSNIE01	CISCO	7606-s
	64	PICHINCHA	SANGOLQUÍ	UIOSGQE01	CISCO	7609-S
	65	PICHINCHA	TUMBACO	UIOTBCE01	CISCO	7606-s
	66	PICHINCHA	ESTACIÓN TERRENA	UIOETTE01	CISCO	7609-S
	67	SANTA ELENA	SALINAS	LBTSLNE01	CISCO	7609-S
	68	STO. DOMINGO	STO. DOMINGO	STDCNTE01	CISCO	7609-S
	69	SUCUMBÍOS	NUEVA LOJA CENTRO	NVLCNTE01	CISCO	7609-S
	70	SUCUMBÍOS	LAGO AGRIO	NVLCNTE02	CISCO	ME 6524
	71	TUNGURAHUA	AMBATO CENTRO	AMBCNTE01	CISCO	7609-S
	72	TUNGURAHUA	AMBATO SUR	AMBSURE01	CISCO	7606-s
	73	ZAMORA	ZAMORA	ZMRCNTE01	CISCO	7609-S

Tabla 2.1: Equipos de la red IP/MPLS de la CNT E.P. (Página 3 de 3)

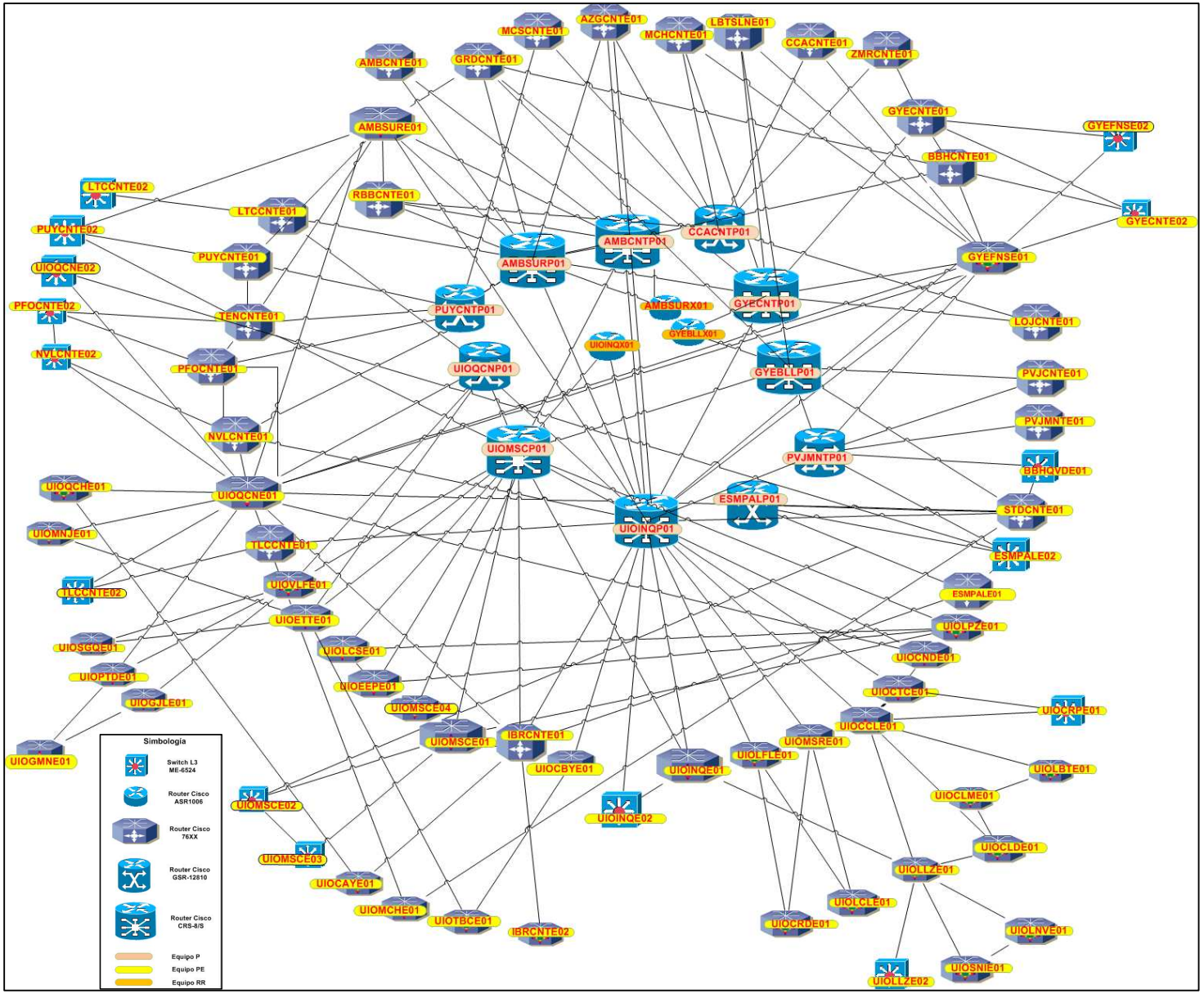


Figura 2.1: Red IP/MPLS de la CNT E.P. [1]

2.1.2.2 Características Técnicas [2]

En la tabla 2.2 se tienen las principales características técnicas de los distintos modelos que conforman la red IP/MPLS.

Marca y modelo	**Cisco ASR 1006.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere de 6 unidades de *rack* para su montaje.	
	12 *slot* para tarjetas SPA (*Shared Port Adapters*).	
	2 *slot* para tarjetas ESP (*Embedded Services Processor*).	
	Soporta hasta 3 tarjetas SIP (*SPA Interface Processors*).	
	2 *slot* para procesador de *router.*	
	Incopora dos fuentes de alimentación AC o DC.	
	Trae un ventilador incorporado.	
Características del sistema	Capacidad máxima de conmutación : 20 Gbps.	
	Consumo de energía máximo de 590 W DC o 560 W AC.	
	Funciona con el Sistema Operativo Cisco IOS XE.	
Protocolos	MPLS, SNMP, Telnet, SSH, IPv4,IPv6,BGPv4 (*Border Gateway Protocol Version 4*),OSPF (*Open Shortest Path First),* IS-IS (*Intermediate System-to-Intermediate System*).	
Descripción	Ofrece características de calidad de servicio para la prestación de servicios de primera calidad, para ello Cisco combina las tarjetas SPA y SIP habilitando la priorización de servicios de voz, video y datos para redes inteligentes, flexibles y seguras. Su sistema operativo permite realizar actualizaciones de software sin impacto mientras el equipo está en servicio (ISSU con sus siglas en inglés *In Service Software Upgrade*).	
Marca y modelo	**Cisco GSR 12816.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Una unidad por *rack* para su montaje.	
	Dispone de 16 *slot.*	
	3 *slot* para tarjetas SFCs (*Switch Fabric Cards*).	
	2 *slot* para tarjetas CSCs (*Clock Scheduler Cards*).	
	2 *slot* para tarjetas de alarma.	
	Incorpora 4 fuentes de alimentación DC o 3 AC.	
	Dispone uno o dos procesadores de *router.*	
	Posee dos ventiladores.	
	Dos bandejas para cables de alimentación.	
Características del sistema	Capacidad máxima de conmutación : 1.28 Tbps.	
	Potencia máxima entrada AC 4651 W y DC 4212 W.	
	Funciona con el sistema Operativo Cisco IOS XR o Cisco IOS.	
Protocolos	IPv4, MPLS, BGPv4, IS-IS, OSPF, RIPv2 (*Routing Information Protocol Version 2*), IGMP (*Internet Group Management Protocol*), DVMRP (*Distance Vector Multicast Routing Protocol*) , PIM DX/SX (*Protocol Independent ulticast dense mode/sparse mode*).	
Descripción	Representan la gama más inteligente en la industria de soluciones de enrutamiento ya que es el primer sistema Terabit disponible para proveedores de servicios en redes IP/MPLS. Maneja QoS, alta disponibilidad, transporte ATM/Frame Relay, garantiza un núcleo integrado combinando características de punta.	

Tabla 2.2: Características Técnicas, equipos de la Red IP/MPLS (Página 1 de 3)

Marca y modelo	**Cisco GSR 12810.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Dos unidades por *rack* para su montaje.	
	Dispone de 10 *slot.*	
	5 *slot* para tarjetas SFCs(*Switch Fabric Cards*).	
	2 *slot* para tarjetas CSCs (*Clock Scheduler Cards*).	
	2 *slot* para tarjetas de alarma.	
	Incorpora 2 fuentes de alimentación DC o AC.	
	Dispone uno o dos procesadores de *router.*	
	Posee un ventilador.	
	Una bandeja para cables de alimentación.	
Características del sistema	Capacidad máxima de conmutación : 800 Gbps.	
	Potencia máxima entrada AC 2790 W y DC 2430 W.	
	Funciona con el sistema Operativo Cisco IOS XR o Cisco IOS.	
Protocolos	IPv4, MPLS, BGPv4 *(Border Gateway Protocol Version 4*), IS-IS *(Intermediate System-to-Intermediate System*), OSPFv2.0 (*Open Shortest Path First Version 2.0*), RIPv2 (*Routing Information Protocol Version 2)* , IGMP (*Internet Group Management Protocol*), DVMRP (*Distance Vector Multicast Routing Protocol)* , PIM DX/SX (*Protocol Independent ulticast dense mode/sparse mode*).	
Descripción	Equipo de la serie Cisco 12000 que representan la gama más inteligente de soluciones de enrutamiento ofreciendo una capacidad máxima de envío de 40 Gbps por slot. Enfocado a los proveedores de servicios sobre redes IP/MPLS.	
Modelo	**CRS 1-8/S.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Dos unidades por *rack*.	
	Dispone de 8 *slot* para tarjetas MSCs *(Modular Services Cards)* .	
	4 *slot* para tarjetas *Fabric Cards.*	
	8 *slot* para tarjetas PLIMs (*Physical Layer Interface Modules)* .	
	Incopora 2 fuentes de alimentación DC o AC.	
	2 *slot* para procesadores de *router.*	
	2 ventiladores.	
Características del sistema	Capacidad máxima de conmutación : 640 Gbps.	
	Potencia máxima entrada AC 2790 W y DC 2430 W.	
	Funciona con el sistema Operativo Cisco IOS XR.	
Protocolos	CDP(*Cisco Discovery Protocol)* , IPv4, IPv6, ICMP, BGPv4 *(Border Gateway Protocol Version 4)* , OSPFv2,OSPFv3,IS-IS, MBGP (*Multiprotocol* BGP), MSDP (*Multicast Source Discovery Protocol*), MPLS, LDP, RSVP, RPL (*Route Policy Language*), SNMP (*Simple Network Management Protocol)* , MD5 (*Message Digest Algorithm*), SSHv2 *(Secure Shell Version 2)* , SFTP (*Secure* FTP), SSL (*Secure Sockets Layer)* .	
Descripción	Sistema de enrutamiento de alta escalabilidad que integra múltiples funciones POP (*Post Office Protocol*) proporcionando flexibilidad en el servicio, es un sistema continuo de operación.	
Marca y modelo	**Cisco 7609-S.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere de 21 unidades de *rack* para su montaje.	
	Cuenta con 9 *slot.*	
	2 *slot* para procesadores de router.	
	2 ventiladores.	
	Equipo calificado de nivel 3 según NEBS(*Network Equipment Building Standards*).	
Características del sistema	Capacidad máxima de conmutación : 720 Gbps.	
	Potencia máxima entrada AC 4000 W y DC 6000 W.	
	Funciona con el sistema Operativo Cisco IOS.	
Protocolos	OSPF, RIP, BGPv4, IS-IS, IGMP, PIM-SM, PIM-DM, MPLS.	
Descripción	Conmutación capa 3, conmutación capa 2, asignación dirección dinámica IP, soporte de DHCP, soporte de MPLS, soporte VLAN, limitación de tráfico, soporte de ACL, QoS, MPLS VPN.	

Tabla 2.2: Características Técnicas, equipos de la Red IP/MPLS (Página 2 de 3)

Marca y modelo	Cisco 7606-S.	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere de 7 unidades de *rack* para su montaje.	
	Dispone de 6 *slot.*	
	Incorpora dos fuentes de alimentación AC o DC.	
	Dispone de dos tarjetas de procesamiento.	
	Posee rejillas de ventilación a los lados del chasis.	
	Equipo calificado de nivel 3 según NEBS(*Network Equipment Building Standards*).	
Características del sistema	Capacidad máxima de conmutación : 480 Gbps.	
	Potencia máxima entrada 2700 W AC o 2700 W DC.	
	Memoria RAM de 3 GB instalada, expandible a 6 GB.	
	Funciona con el sistema Operativo Cisco IOS.	
Protocolos	OSPF, RIP, BGPv4, IS-IS, IGMP, PIM-SM (*Protocol Independent Multicast- Sparse Mode*), PIM-DM, MPLS.	
Descripción	Permite a los proveedores de servicios sobre redes IP/MPLS ofrecer una gran variedad de aplicaciones de voz,datos y video con gran rendimiento. Soporta Conmutación a nivel de capa 3 y capa 2, asignación dirección dinámica IP, soporte de DHCP,limitación de tráfico, soporte de ACL, QoS.	
Marca y modelo	**Cisco ME 6524 Ethernet Switch.**	
Unidades de rack	1.5 unidades de *rack* para su montaje.	
Potencia máxima entrada AC	400 W.	
Potencia máxima entrada DC	400 W.	
Puertos	24 Ethernet 10/100/1000 Mbps downlinks y 8 SFP uplinks Gigabit Ethernet.	
Tamaño de tablas de direcciones MAC	96000 entradas.	
Protocolos	OSPF, EIGRP,IS-IS,BGPv4,HSRP *(Hot Standby Router Protoco*),VRRP (*Virtual Router Redundancy Protoco* l),GLBP (*Gateway Load Balancing Protocol*), MPLS , LDP.	
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1t.	
Componentes de software	Cisco IOS.	
Capacidad de conmutación	32 Gbps.	
Memoria Flash	192 MB.	
Memoria DRAM	512 MB.	
Memoria RAM	768 MB.	
Características principales	Soporta MPLS e IPv6 y la integración de servicios sobre VPN capa 2 y capa 3.	
Marca y modelo	**Cisco 7613.**	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere 18 unidades de *rack* para su montaje.	
	Cuenta con 13 *slot.*	
	2 *slot* para procesadores de *router.*	
	2 ventiladores.	
	Equipo calificado de nivel 3 según NEBS(*Network Equipment Building Standards).*	
	2 fuentes de alimentación AC o DC.	
Características del sistema	Capacidad máxima de conmutación : 720 Gbps.	
	Potencia máxima entrada AC 4000 W y DC 6000 W.	
	Funciona con el sistema Operativo Cisco IOS.	
Protocolos	LDP,MPLS,IGMP,ATM, DHCP, Frame Relay, HDLC, ICMP, IP, PPP, PPPoA, PPPoE, MLPPP, IPSec	
Descripción	Cisco reune las mejores cualidades de un router convecional en el modelo 7613. A medida que Internet continúa su expansión y evolución, los proveedores de servicios están demandando una mayor cantidad y calidad de ancho de banda para apoyar el crecimiento de los ingresos al mismo tiempo controlar los costos para seguir siendo rentables y competitivas. El Cisco 7613 ofrece configuraciones flexibles y modulares , arquitectura distribuida, reducción de costos y la protección de las inversiones.	

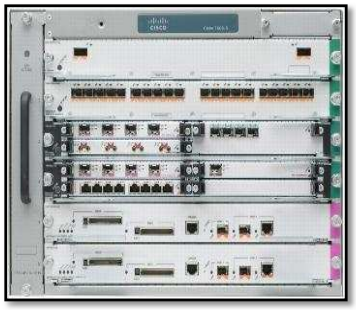


Tabla 2.2: Características Técnicas, equipos de la Red IP/MPLS (Página 3 de 3)

2.1.3 PROYECCIÓN DE LA RED A CORTO PLAZO

La CNT E.P. tiene como meta la ampliación de la red IP/MPLS para brindar servicios de telefonía, datos e Internet a sus clientes en sectores en donde actualmente no tiene acceso, se tiene prevista la adquisición de equipos Cisco, Huawei y Alcatel. Además el Área O&M[45] Plataforma IP/MPLS pasará a administrar también la ex red metro de Pacifictel conocida como red IP/MPLS del Pacífico, la cual está compuesta por 45 equipos tipo PE marca Huawei y 3 equipos tipo P marca Cisco.

Metas Propuestas:

- Incrementar el acceso IP en localidades no contempladas en la ampliación de la red IP/MPLS fase 2.
- Reemplazar equipamiento IP tecnológicamente obsoleto.
- Ofertar nuevos puntos de presencia IP en cantones y principales parroquias en donde existan dependencias y/o sucursales de clientes Corporativos y de Gobierno.
- Unificar la administración de la red IP/MPLS con la red IP/MPLS de la extinta Pacifictel.

2.2 ÁREA DE OPERACIONES Y MANTENIMIENTO PLATAFORMA IP/MPLS [1]

De acuerdo a la estructura actual de la CNT E.P., el área O&M Plataforma IP/MPLS forma parte de la Gerencia Nacional Técnica. Esta área es la encargada de administrar la red IP/MPLS a nivel nacional, por lo que se presentará una descripción de su estructura y las principales actividades que realiza respeto a la red.

[45] O&M: acrónimo de Operaciones y Mantenimiento.

2.2.1 OBJETIVO

"Mantener, gestionar, operar y aprovisionar la red a nivel nacional, para garantizar la disponibilidad en los servicios, incrementar la optimización y efectividad de la red."

2.2.2 ESTRUCTURA Y ACTIVIDADES DEL ÁREA

El área está determinada por 2 niveles de escalamiento dirigidos y supervisados por el jefe del área; para el personal de cada nivel se asigna las actividades y responsabilidades correspondientes.

2.2.2.1 Nivel 1: Soporte Red IP/MPLS

El personal de trabajo que forma parte del nivel 1 se encarga de realizar todas las actividades relacionadas a la atención de clientes, aprovisionamiento y solución de problemas, soporte de la red, determinación y solución de fallas, mantenimiento preventivo y correctivo de la red y atención de órdenes de trabajo generadas por el área de Ingeniería[46].

2.2.2.2 Nivel 2: Responsables Red IP/MPLS

En el nivel 2 en cambio se realizan todas las actividades que están relacionadas a la administración de la red, crecimiento, rediseño, contacto con áreas de *marketing*, relación con proveedores y resolución de fallas mayores que no pueden ser atendidas por el nivel 1.

El nivel 1 escala la resolución de problemas al siguiente nivel si la complejidad así lo amerita.

[46] Área de Ingeniería: otra área de la CNT E.P. que forma parte de la Gerencia Nacional Técnica. Ver sección 2.3.1.

El jefe del Área se encarga de supervisar que todas las actividades del nivel 1 y nivel 2 sean cumplidas a cabalidad.

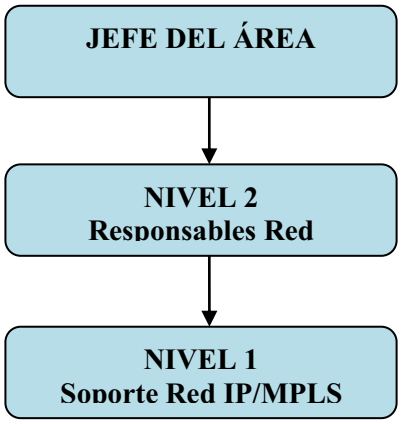


Figura 2.2: Estructura del Área O&M Plataforma IP/MPLS

2.3 OTRAS ÁREAS DE LA CNT E.P. RELACIONADAS CON LA RED IP/MPLS

Además del Área O&M Plataforma IP/MPLS, existen otras áreas dentro de la CNT E.P. que por sus funciones requieren acceso a la administración de los dispositivos que componen la red IP/MPLS. Estas áreas son descritas a continuación.

2.3.1 *CALL CENTER*

La CNT E.P. cuenta con un centro de administración de servicio al cliente nivel 1, con cobertura nacional denominado *Call Center*; en él se reciben y registran las fallas reportadas por los clientes en la entrega de servicios, voz, datos o Internet. Se verifican los datos del cliente (número de contrato, estado de pago), se obtienen síntomas de la falla y se realizan pruebas y resolución de problemas de nivel 1.[47]

[47] Resolución de problemas de nivel 1: verificación de mora en los pagos, conectividad.

2.3.2 NOC

Cuando la revisión de nivel 1 no es suficiente para resolver el problema, el *Call Center* contacta inmediatamente con el *Network Operation Center* (NOC), centro de administración de servicio al cliente nivel 2, el cual efectúa la revisión extremo a extremo sobre la red y determina la causa real del problema, para así asignarlo al área posterior correspondiente si el problema requiere un tratamiento más meticuloso.

2.3.3 INGENIERÍA

Verifican la disponibilidad para el ingreso de un nuevo cliente, coordinan con personal encargado de la administración de DSLAM[48] para la instalación de nuevos equipos, diseños o mejoras en la red o cambios en sistemas operativos. Además son los encargados de coordinar, planificar y entregar servicios.

2.3.4 GESTIÓN DE RED

Monitorean el estado de la red con la finalidad de generar reportes de incidentes, estadísticas de los servicios y disponibilidad de la plataforma IP/MPLS.

2.3.5 GESTIÓN XDSL

Se encargan del direccionamiento IP de Clientes Corporativos y de la administración de los DSLAM.

2.3.6 MULTISERVICIOS

A este grupo pertenece el personal encargado de monitorear la red para verificar disponibilidad para la provisión de servicio a nuevos usuarios.

[48] DSLAM*: Digital Subscriber Line Access Multiplexer*, Es un multiplexor localizado en la central telefónica que proporciona a los abonados acceso a los servicios DSL sobre cable de par trenzado de cobre. El dispositivo separa la voz y los datos de las líneas de abonado.[3]

2.3.7 DESCA[49]

La empresa DESCA ha sido quien ha provisto los equipos Cisco que conforman la red IP/MPLS y puesto que en el contrato de compra, una de las cláusulas tipifica que además de los equipos se adquiere también el soporte correspondiente; personal de esta empresa tendrá acceso a la administración de los dispositivos.

2.4 SERVICIOS QUE OFRECE LA CNT E.P. QUE DEPENDEN DE LA RED IP/MPLS [1]

La CNT E.P. ofrece una variedad de servicios que utilizan la red IP/MPLS para su provisión, lo que le ha permitido que se constituya en una de las empresas más sólidas en el campo de la telecomunicaciones a nivel nacional.

2.4.1 INTERNET

2.4.1.1 Internet Corporativo Premium

Este servicio está orientado hacia clientes que requieren:

- Alta capacidad
- Alta disponibilidad
- Alta redundancia

Esto se logra ya que la CNT E.P. cuenta con enlaces redundantes de Fibra Óptica en el núcleo de la red IP/MPLS y en la capa de transmisión; dispone de redundancia en la salida internacional hacia Internet y ofrece servicio técnico las 24 horas del día, 365 días al año.

[49] DESCA: es una empresa proveedora de Soluciones de Infraestructura y Telecomunicaciones basada en Mejores Prácticas que apoya a sus clientes en: Planificación, Diseño, Implementación, Migración, Operaciones y Optimización.

2.4.1.1.1 Características Técnicas

- Servicio de Internet simétrico con una compartición de 1:1.
- *Pool* de 5 direcciones IP LAN.
- Dirección IP pública fija en la WAN.
- Incluye Asesor técnico exclusivo de Nivel 2.
- Reporte de *Up Time* detallado por WEB.
- Disponibilidad del 99.8% *Up Time*.

2.4.1.2 Banda Ancha PYMES[50]

Este servicio está enfocado a pequeñas y medianas empresas dándoles la posibilidad de poder ser cada vez más competitivas. Se ofrece un servicio técnico las 24 horas al día, los 365 días al año.

2.4.1.2.1 Características Técnicas

- Compartición del servicio 4:1.
- Conexión de Internet mediante última milla de cobre o fibra.
- Conexión a través de una dirección IP pública fija en la WAN.
- Instalación incluye entrega y configuración equipo terminal CPE[51], Wi-Fi; incluye 4 puertos LAN.
- Disponibilidad del servicio 99% *Up time*.

[50] PYMES: pequeñas y medianas empresas.
[51] CPE: Equipo terminal de abonado, proporcionado por el proveedor del servicio al cliente.

2.4.1.3 FastBoy

Es un servicio asimétrico[52] de datos ADSL (*Asymetric Digital Susbcriber Line*) que se realiza a través del par de cobre de la línea telefónica, sin que esto implique ocupar la línea telefónica para estar conectado a Internet.

2.4.1.3.1 Características Técnicas

- Compartición del servicio 8:1.
- Conexión a través de una dirección IP pública dinámica, si el cliente desea puede contratar adicionalmente una IP Fija.
- Instalación incluye modem inalámbrico WI-FI configurado.
- Atención técnica *Call Center*.
- Velocidades disponibles desde los 600 Kbps hasta los 4100 Kbps.
- No subcontrata servicios, proporcionando mayor y mejor mantenimiento.

2.4.1.4 *Web Hosting*

Este servicio provee a los usuarios un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web; de esta forma la CNT E.P. fomenta el contenido nacional, que es fundamental para el crecimiento del sector de Internet. Como complemento a este servicio la CNT E.P. puede proveer dominios de primer y segundo nivel[53].

[52] Servicio asimétrico: Mayor ancho de banda de bajada y menor ancho de banda de subida.
[53] Dominios de primer y segundo Nivel: los dominios de primer nivel constituyen la finalidad del uso de una página web (.com, .net, .org, etc.) y los de segundo nivel, los que cualquier persona puede registrar en cualquier momento (.cnt.com, .dominios.org, etc.)

2.4.1.4.1 Beneficios

- **Integral:** Se puede conseguir descuentos al momento de integrar demás servicios que brinda la CNT E.P.
- **Accesible:** La CNT E.P. cuenta con una extensa gama de paquetes de *hosting* que se adecuarán a diversas necesidades y presupuestos.
- **Rapidez:** Los visitantes verán un veloz despliegue de sus páginas Web.
- **Monitoreo continuo**: Modernos sistemas de alerta que monitorean la red constantemente para prevenir y corregir fallas.
- **Soporte técnico calificado**: Atención personalizada en caso de contingencias o dudas.

2.4.1.5 *Streaming*

El objetivo de este servicio es ofrecer un valor agregado a sus clientes por medio del cual puedan difundir su contenido o programación multimedia por Internet a una cobertura mundial en formato en vivo o pregrabado. El contenido puede ser información, imágenes, vídeo, aplicaciones flash o cualquier contenido accesible vía Web.

2.4.1.5.1 Beneficios

- Calidad y volumen de procesamiento del servidor de difusión provisto y que brindará la conectividad a Internet.
- El servicio es publicado al cliente por medio de un *streaming unicast*[54] en formato WMV[55].

[54] *Streaming unicast:* es una conexión cliente-servidor donde el video es recibido solo por el cliente que lo solicita. [3]
[55] Formato WMV: *Windows Media Video*, formato de video desarrollado por Microsoft. [4]

- Se entregará al cliente un *link* para conexión de la señal a difundir para que sea añadida en su página web o como desee publicarla.
- La CNT E.P. documentará las estadísticas de ancho de banda y de cantidad de clientes conectados.
- Se generará un control para restringir las conexiones a usuarios no registrados en caso que el cliente lo solicite.

2.4.2 TELEFONÍA FIJA

El cliente podrá acceder al servicio ya sea de manera residencial o comercial, sin restricción a ningún tipo de llamadas, sin embargo se podrá solicitar su restricción. Además el cliente podrá solicitar los servicios de llamada en espera e identificador de llamadas.

Cuando un cliente solicita más de 4 líneas telefónicas para un mismo domicilio o unidad habitacional, a partir de la cuarta línea pasará a categoría comercial. Las categorías residencial y comercial difieren en su costo por llamada.

2.4.2.1 Telefonía fija Alámbrica

Es un servicio de telecomunicaciones que permite el intercambio bi-direccional de tráfico de voz en tiempo real a través de un aparato telefónico fijo hacia cualquier lugar con acceso telefónico sea local, nacional, celular o internacional a través de la infraestructura tecnológica de la empresa.

2.4.2.2 Telefonía fija Inalámbrica

Tecnología que permite brindar servicios de telefonía a sectores en donde las redes convencionales no tienen acceso.

2.4.3 TELEFONÍA PÚBLICA

La conforman terminales de comunicación instalados en las vías públicas, en centros de concentración y tráfico de personas, colegios, universidades, con los cuales la CNT E.P. proporciona a sus clientes una gran facilidad de acceso a comunicación urgente, con calidad de voz hacia cualquier destino del mundo (llamadas locales, regionales, nacionales, celulares e internacionales). Los beneficios que tiene este servicio son:

- Es una opción importante de comunicación en la vía pública.
- Permite llamar a cualquier destino.
- Está disponible las 24 horas del día.
- Calidad de voz.

2.4.4 TELEFONÍA IP

Es el servicio telefónico que toma como base la tecnología de VoIP (voz sobre protocolo de internet), la cual posibilita la conversión de la señal de voz en paquetes de datos para que pueda ser transmitida a través de la red.

2.4.5 DATOS

2.4.5.1 Servicio de transmisión de datos internacionales

Transmisión de datos entre dos puntos que se encuentran en diferentes países a través del establecimiento de un enlace de transmisión de datos. El enlace de transmisión es independiente de las tecnologías y medios físicos utilizados por la CNT E.P. o del proveedor del tramo internacional, sean éstas cobre, fibra, o microonda (se excluyen enlaces satelitales). Ofrece velocidades desde 128 Kbps hasta 1 Gbps.

2.4.5.1.1 Características Técnicas

- *Delay*[56] de enlaces locales: 120 ms.
- Disponibilidad del servicio: 99.6 % mensual.
- Pérdida de paquetes: 0% en canales sin carga.
- Seguridad: circuitos virtuales privados.

2.4.5.2 Servicio de transmisión de datos locales

Servicio que consiste en el establecimiento de un enlace de transmisión de datos para conectividad entre dos puntos que se encuentran dentro de una misma provincia. El enlace de transmisión es independiente de las tecnologías y medios físicos utilizados por la CNT E.P., sean éstas cobre, fibra, o microonda (se excluyen enlaces satelitales). Ofrece velocidades desde 128 Kbps hasta 1 Gbps.

2.4.5.2.1 Características Técnicas

- *Delay* de enlaces locales: 15 ms.
- Disponibilidad del servicio: 99.6% mensual.
- Disponibilidad del *Backbone*: 99.999% mensual.
- Pérdida de paquetes: 0% en canales sin carga.
- Seguridad: circuitos virtuales privados.

2.4.5.3 Servicio de transmisión de datos interurbano

Servicio que consiste en el establecimiento de un enlace de transmisión de datos para conectividad entre dos puntos que se encuentran en diferentes provincias. El

[56] Delay: demora que se produce entre la emisión y la recepción de los datos. [5]

enlace de transmisión es independiente de las tecnologías y medios físicos utilizados por la CNT E.P., sean éstas cobre, fibra, o microonda (se excluyen enlaces satelitales). Ofrece velocidades desde 128 Kbps hasta 1 Gbps.

2.4.5.3.1 Características Técnicas

- *Delay* de enlaces locales: 50 ms.
- Disponibilidad del servicio: 99.6 % mensual.
- Disponibilidad del *backbone*: 99.999% mensual.
- Pérdida de paquetes: 0% en canales sin carga.
- Seguridad: circuitos virtuales privados.

2.5 CONTROL DE ACCESO A LA ADMINISTRACIÓN DE LOS DISPOSITIVOS DE LA RED IP/MPLS DE LA CNT E.P.

2.5.1 POLÍTICAS DE CONTROL DE ACCESO [1]

El área O&M Plataforma IP/MPLS no cuenta con una estructura de políticas formales en cuanto al control de acceso a la administración de los equipos de su red, pero se toman en cuenta ciertos lineamientos, los cuales se manejan mediante un sistema de control de acceso, bajo la dirección del responsable de la red IP/MPLS.

A continuación se describen los lineamientos manejados por el área, que fueron provistos por el responsable de la red.

2.5.1.1 De los Administradores

- Se denomina Administrador a la persona encargada de establecer,

implementar y controlar los lineamientos en el sistema de control de acceso, esto es, asignar usuarios, crear grupos de usuarios, administrar contraseñas, manejar *logs* y todo lo demás concerniente a este sistema.

- El responsable de la red IP/MPLS de la CNT E.P será el Administrador Principal del sistema de control de acceso.
- El Administrador Principal podrá designar administradores secundarios que le ayudarán en su cometido.
- El Administrador Principal establecerá las capacidades y restricciones que tendrán los administradores secundarios.
- El Administrador Principal se encargará de revisar los *logs* de acceso en busca de anomalías.

2.5.1.2 De los Grupos de Usuarios

- Se denomina grupo de usuario al conjunto de usuarios que dentro de la CNT E.P. realizan las mismas actividades y tendrán los mismos permisos y restricciones de acceso a la administración de los dispositivos de la Red IP/MPLS de la CNT E.P.
- O&M Plataforma IP/MPLS comparte con otras áreas de la CNT E.P. la misión de mantener los servicios ofertados al cliente operando de manera correcta (como se detalló en la sección 2.3).
- Se dispondrá además de un grupo llamado SISTEMAS DE GESTIÓN, en el cual se encuentran los sistemas de gestión utilizados para el monitoreo y gestión de la red, Cisco ANA[57] y Cisco ISC[58].
- El personal del área O&M Plataforma IP/MPLS que se encarga de resolver problemas en la red IP/MPLS que no los pueden cubrir el *Call Center* y el NOC conforma el grupo llamado ADMINISTRADORES.

[57] Cisco ANA: Cisco *Active Network Abstraction*, software de gestión y monitoreo de red.
[58] Cisco ISC: Cisco IP *Solution Center*, provee una administración inteligente de la red.

2.5.1.3 De la Asignación de Usuarios

- Se denomina usuario, a las persona que requiere acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. ya sea para monitorizarlos, configurarlos o resolver problemas.
- Se asignará a cada usuario un nombre de inicio de sesión y contraseña para que acceda a la administración de los dispositivos de la red IP/MPLS de la CNT E.P.
- La asignación de un nuevo usuario se realiza previa solicitud al Administrador del sistema de control de acceso, el cual después de aprobar dicha solicitud asignará y configurará en el sistema de control de acceso, un nombre de usuario con la letra del primer nombre seguido del apellido:

  Interesado: Jorge Villagrán

  Usuario: jvillagran

2.5.1.4 De la Asignación de Contraseñas

La contraseña es también asignada por el Administrador del sistema de control de acceso, quien solicita al usuario que la cambie tras el primer uso. La contraseña deberá ser alfanumérica.

2.5.1.5 De los Grupos de Dispositivos

Los dispositivos se agruparán de acuerdo a la función que desempeñan en la red IP/MPLS de la CNT E.P. Así entonces se agrupará a los dispositivos en Equipos P, Equipos PE y Equipos de Capa 2.

2.5.1.6 De la Gestión de Privilegios

- Gestionar los privilegios y restricciones que regirán el actuar de los

usuarios que accedan a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. Estos privilegios y restricciones serán designados por el Administrador del sistema de control de acceso.

- El Administrador asigna un perfil de acceso a cada uno de los grupos de usuarios de acuerdo a las funciones competentes, evitando que realicen funciones que no les corresponden o que afecten al correcto funcionamiento de la red.

- El perfil de acceso, conocido también como perfil de autorización, contempla los comandos del IOS Cisco que permite o niega al grupo de usuarios ejecutar en un equipo.

La tabla 2.3 muestra los comandos permitidos y no permitidos, y el grupo de usuarios al cual se aplican.

PERFILES DE AUTORIZACIÓN			
PERFIL	**Comandos**		**GRUPO DE USUARIOS**
	permitidos	**denegados**	
MULTISERVICIOS	exit	se deniega todos los demás comandos que no se especifican	MULTISERVICIOS GESTIÓN XDSL GESTIÓN DE RED NOC
	ping		
	show		
	ssh		
	telnet		
	traceroute		
MONITOREO	se permiten todos los demás comandos excepto de los denegados	clear-line	CALL CENTER SISTEMAS DE GESTIÓN
		configure	
		debug	
		show startup-config	
		show users	
		shutdown	
		who	

Tabla 2.3: Perfiles de autorización (Página 1 de 2)

PERFILES DE AUTORIZACIÓN			
PERFIL	**Comandos**		**GRUPO DE USUARIOS**
	permitidos	**denegados**	
CONFIGURAR	cdp	se deniega todos los demás comandos que no se especifican	INGENIERíA DESCA
	clear		
	configure terminal		
	copy running-config		
	description		
	encapsulation		
	end		
	exit		
	interface		
	no **excepto** (no username,no router,no enable password, no ip vrf)		
	ip		
	ping		
	service instance		
	show		
	snmp-server		
	ssh		
	switchport		
	telnet		
	traceroute		
	write memory		
ADMINISTRACIÓN	TODOS	NINGUNO	ADMINISTRACIÓN

Tabla 2.3: Perfiles de autorización (Página 2 de 2)

2.5.2 SISTEMA DE CONTROL DE ACCESO PARA LA ADMINISTRACIÓN DE LOS DISPOSITIVOS DE LA RED IP/MPLS DE LA CNT E.P.

La plataforma que maneja la Jefatura O&M Plataforma IP/MPLS actualmente para el control de acceso a los dispositivos de la red IP/MPLS, es un *Cisco Access Control System* ACS v3.2, que entró en funcionamiento con la implementación de la primera fase de la red IP/MPLS, en la que se tienen ingresados la mayor parte de los dispositivos de la red IP/MPLS.

2.5.2.1 Función del Cisco ACS v3.2

Es imprescindible la utilización de un sistema de control de acceso puesto que la resolución de problemas se realiza mediante escalamiento. Muchas personas tienen acceso a los dispositivos y es necesario controlar, registrar y monitorear el acceso de usuarios a los mismos y las actividades por ellos realizadas, con la finalidad de detectar problemas en cuanto al mal uso o malas prácticas en la configuración de los equipos, logrando de esta manera identificar el origen del problema mediante la revisión de reportes. Si bien los equipos manejan *logs*, éstos poseen poco espacio en memoria, y son fácilmente accesibles.

2.5.2.2 Componentes de Servidor para el Cisco Secure ACS v3.2

Software

El sistema Cisco *Secure Access Control System* v3.2 se encuentra instalado sobre un Sistema Operativo Windows Server 2003 de 64 bits.

Hardware

Las características de hardware del Servidor se puede observar en la tabla 2.4.

Marca	Dell PowerEdge 1800
Disco Duro	73GB SCSI Ultra320 | 10000pm
Memoria RAM	1GB (2x512MB) DDR2
Procesador	Intel® Xeon CPU 2.80 GHz, 64 bits
Tarjeta de Red	Intel Gigabit NIC 10/100/1000Mbps integrada
Unidad CD/DVD	Lector DVD IDE 16x | LG-Samsung-Toshiba
Tarjeta gráfica	ATI Radeon 7000-M integrada 16MB SDRAM
Dimensiones | peso	Alto: 45cm, ancho: 21,8cm, profundidad: 57,4cm | 34,5KG

Tabla 2.4: Características de Hardware del Sistema de Control de Acceso

2.5.2.3 Ubicación y Seguridad Física del Cisco ACS v3.2

La topología mostrada en la Figura 2.3 muestra la ubicación lógica del ACS Cisco v3.2.

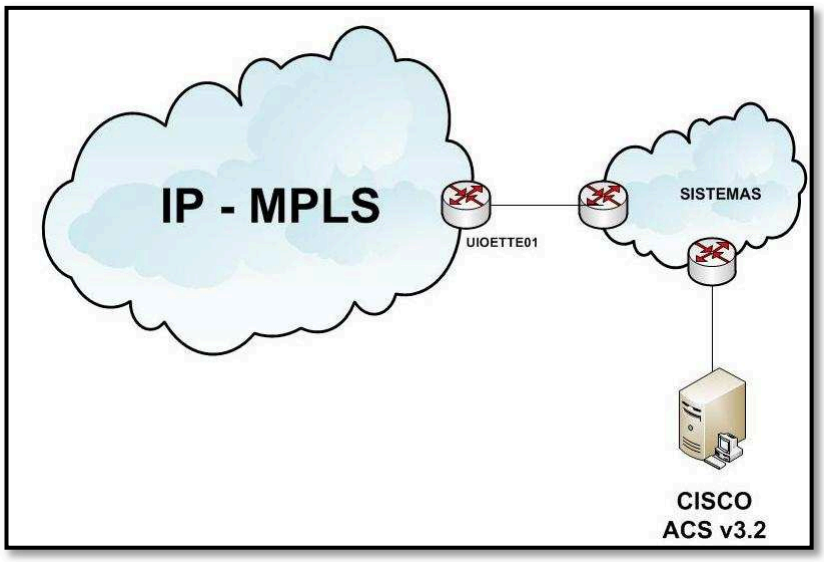


Figura 2.3: Ubicación lógica del cisco ACS v3.2

Como se aprecia, el Cisco ACS v3.2, utilizado para la administración de los dispositivos de la red IP/MPLS de la CNT E.P., está conectado a la red del Departamento de Sistemas de la CNT E.P.

Físicamente el servidor sobre el cual está instalado el Cisco ACS v3.2, está ubicado en el laboratorio del área O&M Plataforma IP/MPLS. En la Tabla 2.5 se indican los componentes de seguridad física para el Cisco ACS v3.2.

Componente	SI	NO
Cámaras		X
Equipo contra incendios		X
Climatización	X	
Control de acceso físico		X

Tabla 2.5: Componentes de seguridad física del Cisco ACS v3.2

2.5.2.4 Implementación de Políticas en el Sistema de Control de Acceso

2.5.2.4.1 Administración

En la figura 2.4 se puede observar los usuarios administradores configurados en el Cisco ACS v3.2.

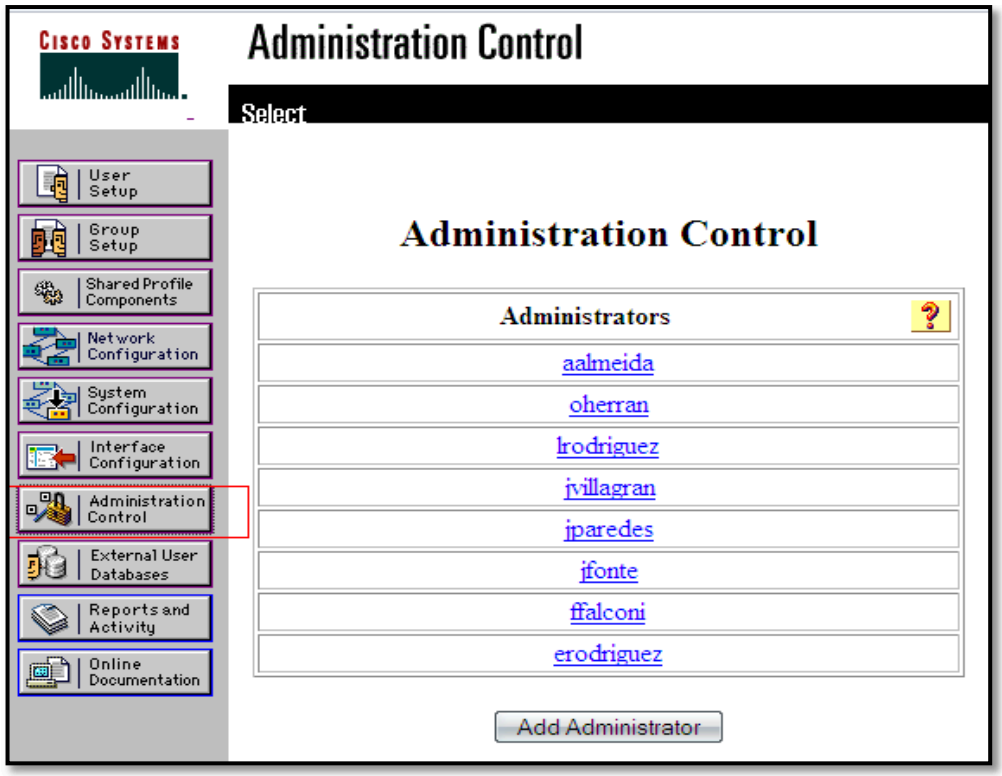


Figura 2.4: Cisco ACSv3.2: Administradores

En esta figura se puede observar que se crearon los administradores lrodriguez y ffalconi, correspondientes a los autores del presente proyecto de titulación para poder así acceder a la administración del Cisco ACS v3.2.

2.5.2.4.2 Grupos de Usuarios

De acuerdo a las áreas de trabajo, se tienen configurados grupos de usuarios para manejar el control de acceso a los dispositivos de la red IP/MPLS en función

de las actividades que cada una de ellas realizan. En la figura 2.5 se puede observar los grupos creados; adicionalmente se encuentran otros grupos que en algún momento se configuraron a modo de prueba y no han sido eliminados como CISCO WORKS, Multiservicios_Conf, Huawei, PRUEBANEO.

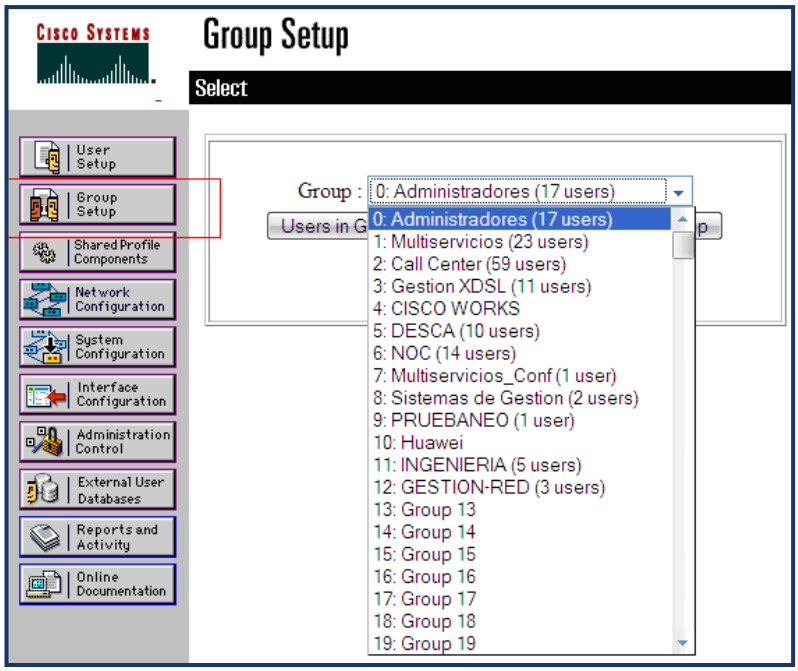


Figura 2.5: Cisco ACS v3.2: Grupos de Usuarios

2.5.2.4.3 Usuarios

En la figura 2.6 se puede observar un ejemplo de usuarios configurados en el Cisco ACS v.3.2 que forman parte de los diferentes grupos de usuarios.

User	Status	Group
ralmeida	Enabled	INGENIERIA (5 users)
bsanchez	Enabled	GESTION-RED (3 users)
ltorres	Enabled	Administradores (17 users)
jcamacho	Enabled	INGENIERIA (5 users)
jvillagran	Enabled	Administradores (17 users)
aalmeida	Enabled	Administradores (17 users)

Figura 2.6: Cisco ACS v3.2: Usuarios Configurados

2.5.2.4.4 Grupos de Dispositivos

Los dispositivos, clientes AAA manejados actualmente por el ACS, se encuentran agrupados de acuerdo a la función que desempeñan dentro de la red IP/MPLS de la CNT E.P. y a su correspondiente fase de implementación. Se tiene así, la siguiente clasificación:

a) Equipos_P

Grupo de dispositivos que forman parte del *core* de la red IP/MPLS, que realizan las función de los equipos tipo P.

b) Equipos_Sin_ISC

Se los considera como equipos de agregación, es decir permiten la integración de la red en general a la red IP/MPLS, puesto que dichos equipos solo hablan IP. Se denominan sin ISC, porque no son administrados vía *IP Solution Center*, que es la plataforma utilizada para administrar equipos Cisco.

c) Equipos_Con_ISC

Son los encargados de proporcionar los servicios de la red IP/MPLS, constituyen los equipos PE. Estos equipos se administran mediante el Cisco ISC.

d) Equipos MPLS Fase 2

Constituyen todos los equipos que se agregaron en la implementación de la red IP/MPLS fase 2, revisados en la sección 2.1.1.3.

2.5.2.4.5 Gestión de Privilegios

Se refiere a gestionar lo que se le permite al usuario hacer una vez que tiene

acceso a algún dispositivo de la red IP/MPLS.

En la figura 2.7 se muestran los perfiles de autorización configurados en el Cisco ACS v3.2.

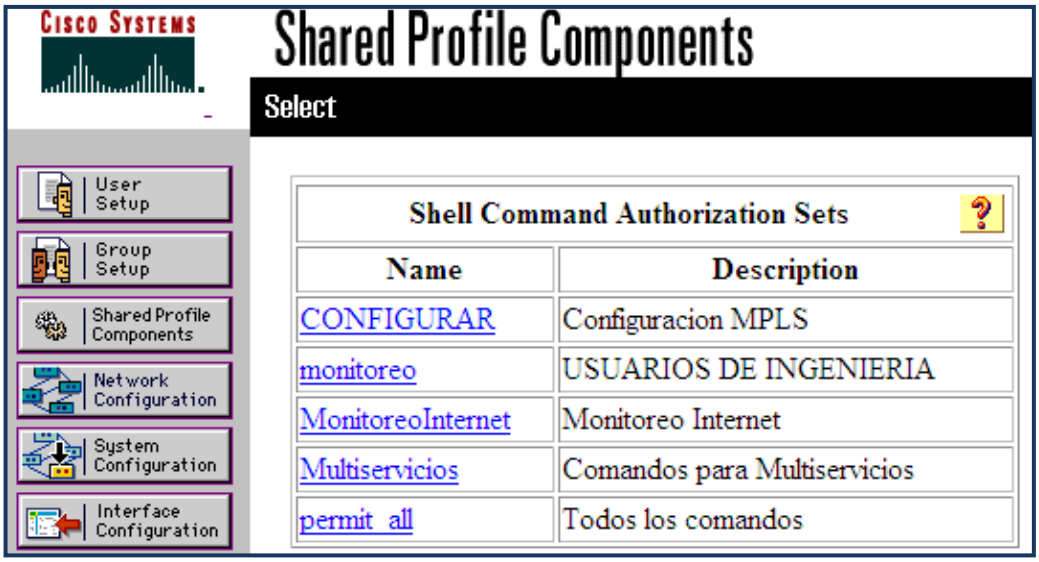


Figura 2.7: Cisco ACS v3.2, Perfiles de Autorización

2.5.3 FALENCIAS EN EL CONTROL DE ACCESO A LA ADMINISTRACIÓN DE LOS DISPOSITIVOS DE LA RED IP/MPLS

Al no contar con un correcto control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P., no se podrán atender adecuadamente órdenes de trabajo, solicitudes de clientes y cualquier otra configuración general que se requiera.

A continuación se listan las falencias encontradas, que podrían llevar a perder el control de acceso a la administración de los dispositivos de la red.

2.5.3.1 Falencias en las Políticas de Control de Acceso

- Actualmente el Área O&M Plataforma IP/MPLS no cuenta con un

documento formal referente a las políticas de control de acceso, que establezcan las responsabilidades del personal y las medidas que se deberían tomar ante cualquier eventualidad que comprometa la confidencialidad, integridad y disponibilidad de la información y el correcto aprovisionamiento de servicios a los clientes. Lo cual lleva a poner en riesgo el correcto funcionamiento de la red IP/MPLS y por consiguiente el nombre de la institución.

- Los administradores secundarios del sistema de control de acceso asignados por el Administrador Principal tienen los mismos permisos que este último.

- No existe un registro de grupos de usuarios, cuentas de usuarios, dispositivos de red o clientes AAA, grupos de dispositivos que hayan sido configurados en el sistema de control de acceso Cisco ACS v3.2.

- A pesar de la recomendación dada por el Administrador del sistema de control de acceso del uso de contraseñas alfanuméricas, se permite la utilización de contraseñas simples cuando éstas son cambiadas en el primer uso por el usuario respectivo.

- No se define fecha de caducidad de las contraseñas configuradas en los dispositivos de red o en el Cisco ACS v3.2.

- La agrupación de los dispositivos de la red IP/MPLS no toma en cuenta la ubicación geográfica de los mismos.

- No se cumple con la recomendación del Administrador del sistema de control de acceso de agrupar los dispositivos por su función dentro de la red, ya que se ha creado un grupo de Equipos MPLS Fase 2.

- No se realiza una revisión periódica de los usuarios a los que se les ha habilitado una cuenta en el Cisco ACS v3.2, es así que existen varios usuarios que ya han dejado de pertenecer a determinadas áreas o a toda la Corporación y no se les ha deshabilitado su cuenta, inclusive hay muchas cuentas que han expirado y no se han eliminado.

- No se contemplan otras marcas de dispositivos de red para su administración, la gestión de privilegios basada en comandos está diseñada únicamente para equipos Cisco. Como se vio en la sección 2.1.3 la red IP/MPLS constará a futuro con equipos de otras marcas (Huawei y Alcatel).

2.5.3.2 Falencias en la Administración de los Dispositivos de la Red IP/MPLS

- No existen acciones adecuadas para garantizar el acceso autorizado a la administración de los dispositivos de la red. Solo un porcentaje de los equipos que integran la red IP/MPLS, se encuentran anexados al sistema de control de acceso Cisco ACS v3.2.

- Los equipos que no están anexados al Cisco ACS v3.2 se administran mediante usuarios locales configurados en cada uno de los equipos, para ser específicos un usuario local por área, a los que se les ha asignado diferentes niveles de privilegios de acuerdo al área.

- Esta asignación de privilegios por nivel constituye una gran falencia para la seguridad de la red, pues el acceso a ciertos equipos importantes no está controlado de manera correcta y un mal uso de los mismos podría ocasionar la baja de servicio a muchos clientes desde masivos a corporativos.

- Al utilizar únicamente usuarios locales, no se estaría cumpliendo a cabalidad los objetivos para los cuales se adquirió el Cisco ACS v3.2, como son el control del no repudio, controlar el acceso a todos los equipos de la red IP/MPLS, llevar un registro de los cambios en las configuraciones que se realicen en cada uno de los equipos y de los usuario que acceden a dichos equipos, optimizar la aplicación de diferentes niveles de privilegios para quienes acceden a los equipos, etc.

- Además algunos equipos no anexados en el Cisco ACS v3.2 tampoco cuentan con la configuración de usuarios locales, simplemente tienen

configurada la clave de acceso al modo privilegiado (clave *enable*), la cual es conocida por todas las personas de las diferentes áreas que acceden a la gestión de dichos equipos. Esto se convierte en un riesgo de seguridad ya que al realizar un cambio erróneo en la configuración, no se podría determinar un responsable y se abre la posibilidad de reincidencia.

- El que el Cisco ACS v3.2 esté en la red del Departamento de Sistemas de la CNT E.P. hace que el control de acceso a la administración de los dispositivos dependa de la correcta operatividad de dicha red, a la cual no se tiene acceso; si se pierde la conectividad a la red de Sistemas, se perderá el control de acceso a los dispositivos de la red IP/MPLS de la CNT E.P.

2.5.3.3 Falencias en el Sistema de Control de Acceso Cisco ACS v3.2

- Para ingresar al Sistema operativo Windows Server 2003, sobre el cual está instalado el Cisco ACS v3.2, no se tiene configurada ninguna contraseña de seguridad.

- En cuanto a la seguridad lógica del ACS v3.2 no se tiene instalado algún antivirus, que ayude a proteger el servidor en el cual está instalado el Cisco ACS v3.2.

- El Cisco ACS v3.2 no cuenta con redundancia que garantice la disponibilidad del servicio, así que si llegare a fallar dicho sistema, como ha pasado en varias ocasiones, se dejaría sin control de acceso a la administración de los equipos de la red IP/MPLS.

- Si la caída del servicio es crítica y se necesita acceso inmediato se tendría que ingresar a los equipos de la red mediante los usuarios locales configurados en cada uno de ellos, perdiendo así el control de auditoria y autorización.

- El Cisco ACS v3.2 se encuentra conectado a la red del Departamento de Sistemas de la CNT E.P y no directamente a la red IP/MPLS, lo que hace

que el control de acceso dependa del correcto funcionamiento de una red ajena a la administrada.

- Al ingresar a la interfaz web utilizada para administrar el Cisco ACS v3.2 se utiliza el protocolo HTTP, por lo que las credenciales que envía el usuario viajan en texto plano, esto es sin seguridad.

Con respecto a la seguridad física para el servidor sobre el que está instalado el Cisco ACS v3.2:

- No se cuenta con un *rack* específico y protegido en el laboratorio.
- Al laboratorio accede personal encargado de la climatización, soporte de DESCA, pasantes, personal de limpieza entre otros; sin ningún tipo de control alguno. Cualquier ataque intencional, como apagar el equipo, o accidental, como tropezar con un cable, podría dejar sin control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P.

A lo largo del estudio del Cisco ACS v3.2 se han detectado los siguientes defectos de software (*bugs* de programación):

- Repentinamente el Sistema registra nombres de usuarios repetidos o no permite la creación de nuevos usuarios, determinando que ya han sido utilizados, cuando no ha sido así. Lo que implica seleccionar otro nombre de usuario, entonces la modalidad de asignación de nombres de usuario se ve alterada.
- Ocasionalmente no se cumplen los perfiles de autorización para el control de acceso a los equipos de la red IP/MPLS, unas veces restringiendo comandos permitidos (limitando el trabajo del personal autorizado) y otras, aún más grave, permitiendo comandos restringidos a personal no autorizado o sin los suficientes conocimientos, pudiendo afectar los servicios que utilizan la red IP/MPLS.

- En los registros que se generan de los usuarios que se autentican para acceder a los equipos de la red IP/MPLS, se visualizan usuarios inexistentes, sin ningún tipo de atributos o que tengan relación con los usuarios que se tiene ingresados en el Cisco ACS v3.2, ocasionando confusión cuando se requiere verificar dichos registros.

2.5.4 REQUERIMIENTOS DEL ÁREA O&M PLATAFORMA IP/MPLS

- Se requiere contar con un documento formal que establezca las políticas que se deben seguir y ejecutar, para garantizar la seguridad en el control de acceso a la administración de los dispositivos de la red.

- Las políticas establecidas deberán ser de conocimiento de todo el personal que forme parte de la Corporación y esté vinculado con la administración y manejo de los equipos de la red IP/MPLS, de tal manera que conozcan sus responsabilidades y sanciones ante el incumplimiento de las mismas.

- El área O&M Plataforma IP/MPLS tiene planificado la ampliación de la red IP/MPLS incluyendo equipos de las marcas Huawei y Alcatel, por lo consiguiente, se requiere de un sistema de control de acceso robusto y que brinde el servicio AAA para diferentes marcas, garantizando de mejor manera los permisos de accesibilidad para el acceso a la administración de los equipos de la red IP/MPLS de la CNT E.P.

- Se requiere de un sistema de control de acceso redundante, para evitar, caídas del servicio de control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P.

- Se requiere que el sistema de control de acceso posea más seguridad tanto física como lógica.

- Se requiere que el sistema de control de acceso dependa únicamente de la red IP/MPLS y no de otras redes como de la red del Departamento de Sistemas de la CNT E.P.

- Se requiere de alertas cuando se produzcan eventos como: múltiples intentos de ingreso fallidos, ingreso de comando no autorizados, sobre procesamiento o caída del sistema de control de acceso.

- Se requiere una redefinición de los perfiles de autorización para los grupos de usuarios que necesiten acceder a los equipos de la red de acuerdo al área de la que forman parte.

- Se requiere que se permita el acceso solo a personal autorizado al cuarto de equipos en el que se encuentra el sistema de control de acceso, y éste cuente con clave de acceso al sistema operativo.

- Se requiere disponer de planes de contingencia ante cualquier tipo de eventualidad que afecte el normal funcionamiento del control de acceso a la administración de los equipos de la red IP/MPLS, que permitan dar respuestas en tiempos mínimos.

- Se requiere revisar periódicamente la configuración de cuentas de usuario en el sistema de control de acceso con la finalidad de verificar cuentas expiradas o bloqueadas, eliminar cuentas de usuarios de personal que haya dejado de pertenecer a la Corporación o que ya no requiera acceso a la administración de los dispositivos de la red y monitorizar el uso adecuado o modificar los perfiles de autorización asignados.

- Se requiere que el acceso a la administración a todos los equipos de la red IP/MPLS de la CNT E.P. se realice mediante el sistema de control de acceso, además de llevar un inventario de estos equipos. El Área requiere administrar además de los equipos mencionados, todos los equipos utilizados para acceder a la misma y aquellos conocidos como *Route Reflectors*.

CAPÍTULO 3

ANÁLISIS DE RIESGOS DE LA RED IP/MPLS DE LA CNT E.P.

Como se revisó en el primer capítulo del presente proyecto de titulación, el propósito de realizar un análisis de riesgos es identificar: los activos que aportan un valor al objeto de nuestro estudio, las amenazas que pueden causar algún tipo de daño alterando el normal funcionamiento de la red, la entrega de servicios o desempeño de tales activos, determinar el nivel de impacto que puede tener en caso de que llegara a efectuarse un evento, y las medidas que se deberían tomar o ejecutar para eliminar o minimizar el impacto de los posibles riesgos.

El análisis de riesgos se realizará tomando como referencia la Norma ISO/IEC 27005:2008 que se revisó en el capítulo 1, sección 1.3.3.

El análisis y evaluación de riesgos dentro de la norma ISO/IEC 27005:2008, es visto en conjunto y se define como “Valoración de riesgo”; en la figura 3.1 se indican los pasos a seguir durante el proceso de análisis y evaluación de riesgos.

3.1 ESTABLECIMIENTO DEL CONTEXTO

3.1.1 ALCANCE Y LÍMITES

La CNT E.P. es considerada la empresa líder en la prestación de servicios de telecomunicaciones a nivel nacional a través de su red IP/MPLS; es fundamental entonces asegurar su correcto funcionamiento mediante lineamientos que se deberían implementar para corregir o actuar ante un evento, que podría poner en riesgo la entrega de servicios y con ello la honorabilidad y buen nombre de la empresa.

Figura 3.1: Procedimiento del análisis de riesgos según la norma ISO/IEC 27005:2008

El presente análisis de riesgos cubre los equipos tipo P y PE de la red IP/MPLS de la CNT E.P. en la provincia de Pichincha, con la finalidad de preservar la entrega de servicios a los clientes en esta provincia.

Su objetivo es identificar los activos que contribuyen a la entrega de servicios a los clientes, las vulnerabilidades y amenazas a las que están expuestos estos activos y evaluar el riesgo de una incorrecta entrega de servicios, de acuerdo a los clientes de la provincia de Pichincha que se verían afectados.

Se establecerán recomendaciones para minimizar incidentes en la red IP/MPLS de la CNT E.P. que afecten a la entrega de servicios en la provincia de Pichincha. Se cuenta con la colaboración de la jefatura y personal del área O&M Plataforma IP/MPLS proporcionando toda la información necesaria para poder llevar con éxito este proceso.

3.1.2 CRITERIOS BÁSICOS

Es aconsejable seleccionar o desarrollar un enfoque adecuado para el análisis de riesgos que aborde los siguientes criterios: criterios de valoración de activos, criterios de probabilidad de ocurrencia de amenazas, criterios de impacto, criterios

de evaluación del riesgo.

Los criterios básicos se establecen de acuerdo a una escala de atributos calificativos, como lo define la metodología cualitativa, acompañados de una valoración numérica que no precisamente consiste en aplicar la metodología cuantitativa, ya que ésta consiste en realizar cálculos matemáticos complejos. La asignación de valores numéricos a cada uno de los atributos calificativos es con el objetivo de llegar a una estimación del riesgo lo más exacta posible.

3.1.2.1 Criterios de valoración de los activos

Los criterios para valorar los activos que afecten a la entrega de servicios en la red IP/MPLS se realizan teniendo en cuenta la importancia o dependencia respecto a otros activos, sus funcionalidades dentro de la red para la entrega de servicios y la integridad, disponibilidad y confidencialidad de la información que rige su funcionamiento.

La tabla 3.1 contiene los criterios calificativos y los valores numéricos correspondientes que serán utilizados para la evaluación de cada uno de los activos. El producto de los valores asignados de cada parámetro se evaluará de acuerdo al rango de valores establecidos en la tabla 3.2, obteniendo como resultado final el nivel de importancia (NI) de cada activo para la entrega de servicios.

3.1.2.2 Criterios de probabilidad de ocurrencia de amenazas

En la tabla 3.3 se muestran criterios calificativos y los valores numéricos correspondientes que serán utilizados para la valoración de probabilidad (Pbdd) de ocurrencia de amenazas.

PARÁMETROS / VALORACIÓN		DEPENDENCIA	FUNCIONALIDAD	CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD
1	bajo	Ningún otro activo depende de éste para la entrega de servicios.	Activo con capacidades tecnológicas muy limitadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración puede afectar de forma insignificante la entrega de servicios.
2	moderado	Pocos activos dependen de éste para la entrega de servicios.	Activo con capacidades tecnológicas limitadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar en parte la entrega de servicios.
3	alto	Una gran cantidad de activos dependen de éste para la entrega de servicios.	Activo con capacidades tecnológicas avanzadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar significativamente la entrega de servicios.
4	muy alto	Un número considerable de activos dependen de éste para la entrega de servicios.	Activo con capacidades tecnológicas muy avanzadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar gravemente la entrega de servicios.
5	crítico	Todos los activos dependen de éste para la entrega de servicios.	Activo con capacidades tecnológicas de última generación.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar totalmente la entrega de servicios.

Tabla 3.1: Criterios para la valoración de activos

NIVEL IMPORTANCIA= DEPENDENCIA*FUNCIONALIDAD*
(CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD)

VALORACIÓN		DESCRIPCIÓN
1 - 6	no es importante	El activo es insignificante para la entrega de servicios a través de la red, de acuerdo a los criterios de dependencia, funcionalidad y la confidencialidad, integridad y disponibilidad de su archivo de configuración.
7 - 16	poco importante	El activo tiene poca importancia para la entrega de servicios a través de la red, de acuerdo a los criterios de dependencia, funcionalidad y la confidencialidad, integridad y disponibilidad de su archivo de configuración.
17 - 30	importante	El activo es importante para la entrega de servicio a través de la red, de acuerdo a los criterios de dependencia, funcionalidad y la confidencialidad, integridad y disponibilidad de su archivo de configuración.
31 - 50	muy importante	El activo es muy importante para la entrega de servicio a través de la red, de acuerdo a los criterios de dependencia, funcionalidad y a la confidencialidad, integridad y disponibilidad de su archivo de configuración.
51 - 125	crítico	El activo es vital para la entrega de servicios a través de la red, de acuerdo a los criterios de dependencia, funcionalidad y a la confidencialidad, integridad y disponibilidad de su archivo de configuración.

Tabla 3.2: Rango de valores para determinar el nivel de importancia de los activos

VALORACIÓN		DESCRIPCIÓN
1 (0 - 25) %	muy improbable	Amenazas cuya probabilidad de explotar vulnerabilidades es muy baja.
2 (26 - 50) %	medianamente probable	Amenazas que con poca frecuencia explotan vulnerabilidades.
3 (51 - 75) %	altamente probable	Amenazas que frecuentemente explotan vulnerabilidades.
4 (76 - 100)%	muy probable	Amenazas que en la mayoría de los casos explotan vulnerabilidades.

Tabla 3.3: Criterios de probabilidad de ocurrencia de amenazas

3.1.2.3 Criterios de valoración de las consecuencias

La valoración de las consecuencias, en otras palabras, el impacto que ocasionaría una amenaza si llegara a concretarse, se hará considerando dos puntos de vista, el primero considerando el número de clientes que se verían afectados y el segundo considerando el impacto ocasionado en la entrega de servicios y el tiempo de recuperación de los mismos.

En la tabla 3.4 se establecen los criterios calificativos y los valores numéricos para determinar el impacto desde el punto de vista del número de clientes que se verían afectados.

VALORACIÓN		DESCRIPCIÓN
1	insignificante	Ante la ocurrencia de una amenaza, un número muy pequeño de clientes dejarían de recibir el servicio, menor a 19 clientes.
2	pequeño	Ante la ocurrencia de una amenaza, un número pequeño de clientes dejarían de recibir el servicio, entre 20 y 100 clientes.
3	moderado	Ante la ocurrencia de una amenaza, un número moderado de clientes dejarían de recibir el servicio, entre 101 y 500 clientes.
4	grave	Ante la ocurrencia de una amenaza, un número significativo de clientes dejarían de recibir el servicio, entre 501 y 1000 clientes.
5	catastrófico	Ante la ocurrencia de una amenaza, un gran número de clientes dejarían de recibir el servicio, mayor a 1000 clientes.

Tabla 3.4: Criterios de valoración del impacto (Imp 1)

En la tabla 3.5 se establecen los criterios para valorar el impacto desde el punto de vista de la pérdida en la entrega de servicios y su tiempo de recuperación.

VALORACIÓN		DESCRIPCIÓN
1	insignificante	El tiempo de recuperación es inmediato, el cliente no percibe pérdida del servicio.
2	pequeño	El tiempo de recuperación es casi inmediato, el cliente apenas percibe pérdida del servicio.
3	moderado	El tiempo de recuperación es considerable, el cliente percibe pérdida del servicio.
4	grave	El tiempo de recuperación es amplio, el cliente percibe una pérdida del servicio considerable y reclama su reposición.
5	catastrófico	El tiempo de recuperación es muy amplio, el cliente percibe la pérdida del servicio y exige su reposición inmediata.

Tabla 3.5: Criterios de valoración del impacto (Imp 2)

3.1.2.4 Criterios de evaluación del riesgo

El producto de la probabilidad de ocurrencia asignada a cada amenaza por el impacto que éstas llegarían a ocasionar, será evaluado de acuerdo al rango de valores establecidos en la tabla 3.6, obteniendo el nivel de riesgo en cada activo.

Nivel del Riesgo (NR)= Pbdd * Imp 1 * Imp 2

VALORACIÓN		DESCRIPCIÓN
1 - 6	bajo	El riesgo es bajo, considerando el número de clientes que se verían afectados y el tiempo que le tomaría a la empresa reactivar los servicios. La pérdida del servicio para los clientes sería muy leve.
7 - 16	moderado	El riesgo es moderado, considerando el número de clientes que se verían afectados y el tiempo que le tomaría a la empresa reactivar los servicios. La pérdida del servicio para los clientes sería moderada.
17 - 30	alto	El riesgo es alto considerando el número de clientes que se verían afectados y el tiempo que le tomaría a la empresa reactivar los servicios. La pérdida del servicio para los clientes sería alta.
31 - 50	muy alto	El riesgo es muy alto considerando el número de clientes que se verían afectados y el tiempo que le tomaría a la empresa reactivar los servicios. La pérdida del servicio para los clientes sería muy alta.
51 - 100	critico	El riesgo es crítico considerando el número de clientes que se verían afectados y el tiempo que le tomaría a la empresa reactivar los servicios. La pérdida del servicio para los clientes sería crítica.

Tabla 3.6: Criterios de evaluación del riesgo

3.1.2.5 Criterios para el tratamiento del riesgo

Una vez que se obtenga una lista de todos los riesgos evaluados, pese a que se tienen cuatro opciones para tratar el riesgo (retener, reducir, evitar, transferir), se escogerán dos de ellas de acuerdo a los criterios establecidos en la tabla 3.7. Los riesgos a ser transferidos se indicarán de darse el caso.

VALORACIÓN DEL RIESGO	TRATAMIENTO DEL RIESGO
Bajo	Retención del riesgo
Moderado	
Alto	Reducción del riesgo
muy alto	
Crítico	

Tabla 3.7: Criterios de tratamiento del riesgo

- **Reducir el riesgo:** Los controles a aplicar implican corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y toma de conciencia. De existir riesgos para los cuales su reducción implique costos excesivamente elevados se optará por transferirlos.

- **Retener el riesgo:** No se requiere la implementación de controles adicionales y el riesgo se puede aceptar o retener.

3.1.2.6 Criterios de prioridad en la aplicación de controles

Una vez identificados los riesgos a reducir y determinados los controles, se debe considerar la prioridad con la que estos controles serán implementados. Esta prioridad se calcula en base al nivel de riesgo obtenido y al nivel de importancia del activo, para lo cual estos valores han sido ponderados como se indica en la tabla 3.8, donde NRp y NIp corresponden a los valores ponderados del nivel de riesgo e importancia del activo, respectivamente.

NIVEL DE RIESGO			NIVEL DE IMPORTANCIA		
VALORACIÓN		NRp	VALORACIÓN		NIp
1 - 6	bajo	1	1 - 6	no es importante	1
7 - 16	moderado	2	7 - 16	poco importante	2
17 - 30	alto	3	17 - 30	importante	3
31 - 50	muy alto	4	31 - 50	muy importante	4
51 - 100	critico	5	51 - 125	crítico	5

Tabla 3.8: Ponderación de los valores del nivel del riesgo y nivel de importancia

Prioridad = NRp * NIp

En la tabla 3.9 se muestran los criterios de prioridad en la aplicación de controles.

VALORACIÓN		DESCRIPCIÓN
1 - 6	Baja	Los controles en estos equipos pueden esperar, pero deberán implementarse una vez que los controles en los equipos con prioridades alta y media hayan sido implementados.
7- 13	Media	Los controles en estos equipos deberán implementarse a la brevedad, pero se puede esperar hasta que los controles en los equipos con prioridad alta se hayan implementado.
14 -25	Alta	Los controles en estos equipos deberán implementarse lo más pronto posible.

Tabla 3.9: Criterios de prioridad en la aplicación de controles

3.2 VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades que existen, así como los controles existentes y sus falencias, determinan las consecuencias potenciales, y finalmente prioriza los

riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo el cual consiste en:
    - ✓ Identificación del riesgo
    - ✓ Estimación del riesgo
- Evaluación del riesgo

3.2.1 ANÁLISIS DE RIESGOS

3.2.1.1 Identificación de riesgos

El propósito de la identificación de riesgos es determinar los activos que contribuyen en la entrega de los servicios que brinda la CNT E.P a través de la red IP/MPLS en la provincia de Pichincha, las amenazas a las que están expuestos estos activos, las vulnerabilidades que podrían ser explotadas por las amenazas y las consecuencias de no contar con los controles necesarios.

3.2.1.1.1 Identificación de activos

a) Activos primarios

Los servicios entregados por la CNT E.P. a través de la red IP/MPLS, detallados en la sección 2.4, constituyen los activos primarios.

b) Activos de soporte

Se denominan activos de soporte, a aquellos de los cuales dependen los activos primarios (los servicios que se entregan).

b.1) Activos de soporte físico [1]

Los activos de soporte físico constituyen los dispositivos P (3 equipos) y PE (38 equipos) de la red IP/MPLS de la provincia de Pichincha, los cuales se listan en la tabla 3.10.

La figura 3.2 muestra la topología de la red IP/MPLS de la CNT E.P. correspondiente a la provincia de Pichincha. Estos equipos constituyen los activos físicos.

	#	NODO	HOSTNAME	MARCA	MODELO
Equipos P	**1**	IÑAQUITO	UIOINQP01	CISCO	CRS 1-8/S
	2	MARISCAL	UIOMSCP01	CISCO	CRS 1-8/S
	3	QUITO CENTRO	UOQCNP01	CISCO	GSR 12810
Equipos PE	**1**	CAYAMBE	UIOCAYE01	CISCO	7609-S
	2	CUMBAYÁ	UIOCBYE01	CISCO	7609-S
	3	CARCELÉN	UIOCCLE01	CISCO	7609-S
	4	CALDERÓN	UIOCLDE01	CISCO	7609-S
	5	COLLALOMA	UIOCLME01	CISCO	7606-s
	6	CONDADO	UIOCNDE01	CISCO	7609-S
	7	CARONDELET	UIOCRDE01	CISCO	7606-s
	8	CARAPUNGO	UIOCRPE01	CISCO	ME 6524
	9	COTOCOLLAO	UIOCTCE01	CISCO	7609-S
	10	ESCUELA ESPEJO	UIOEEPE01	CISCO	7606-s
	11	ESTACIÓN TERRENA	UIOETTE01	CISCO	7609-S
	12	GUAJALÓ	UIOGJLE01	CISCO	7609-S
	13	GUAMANÍ	UIOGMNE01	CISCO	7609-S
	14	IÑAQUITO	UIOINQE01	CISCO	7613

Tabla 3.10: Activos de soporte físico (Página 1 de 2)

	#	NODO	HOSTNAME	MARCA	MODELO
Equipos PE	15	IÑAQUITO	UIOINQE02	CISCO	ME 6524
	16	LA BOTA	UIOLBTE01	CISCO	7606-s
	17	LA CAROLINA	UIOLCLE01	CISCO	7606-s
	18	LAS CASAS	UIOLCSE01	CISCO	7606-s
	19	LA FLORIDA	UIOLFLE01	CISCO	7606-s
	20	LA LUZ	UIOLLZE01	CISCO	7609-S
	21	LA LUZ	UIOLLZE02	CISCO	ME 6524
	22	LOS NEVADOS	UIOLNVE01	CISCO	7606-s
	23	LA PAZ	UIOLPZE01	CISCO	7606-s
	24	MACHACHI	UIOMCHE01	CISCO	7609-S
	25	MONJAS	UIOMNJE01	CISCO	7609-S
	26	MARISCAL	UIOMSCE01	CISCO	7613
	27	MARISCAL	UIOMSCE02	CISCO	ME 6524
	28	MARISCAL	UIOMSCE03	CISCO	ME 6524
	29	MARISCAL	UIOMSCE04	CISCO	7606-s
	30	MONTESERRÍN	UIOMSRE01	CISCO	7606-s
	31	PINTADO	UIOPTDE01	CISCO	7609-S
	32	QUINCHE	UIOQCHE01	CISCO	7609-S
	33	QUITO CENTRO	UIOQCNE01	CISCO	7613
	34	QUITOCENTRO	UIOQCNE02	CISCO	ME 6524
	35	SANGOLQUÍ	UIOSGQE01	CISCO	7609-S
	36	SAN ISIDRO DEL INCA	UIOSNIE01	CISCO	7606-s
	37	TUMBACO	UIOTBCE01	CISCO	7606-s
	38	VILLAFLORA	UIOVLFE01	CISCO	7609-S

Tabla 3.10: Activos de soporte físico (Página 2 de 2)

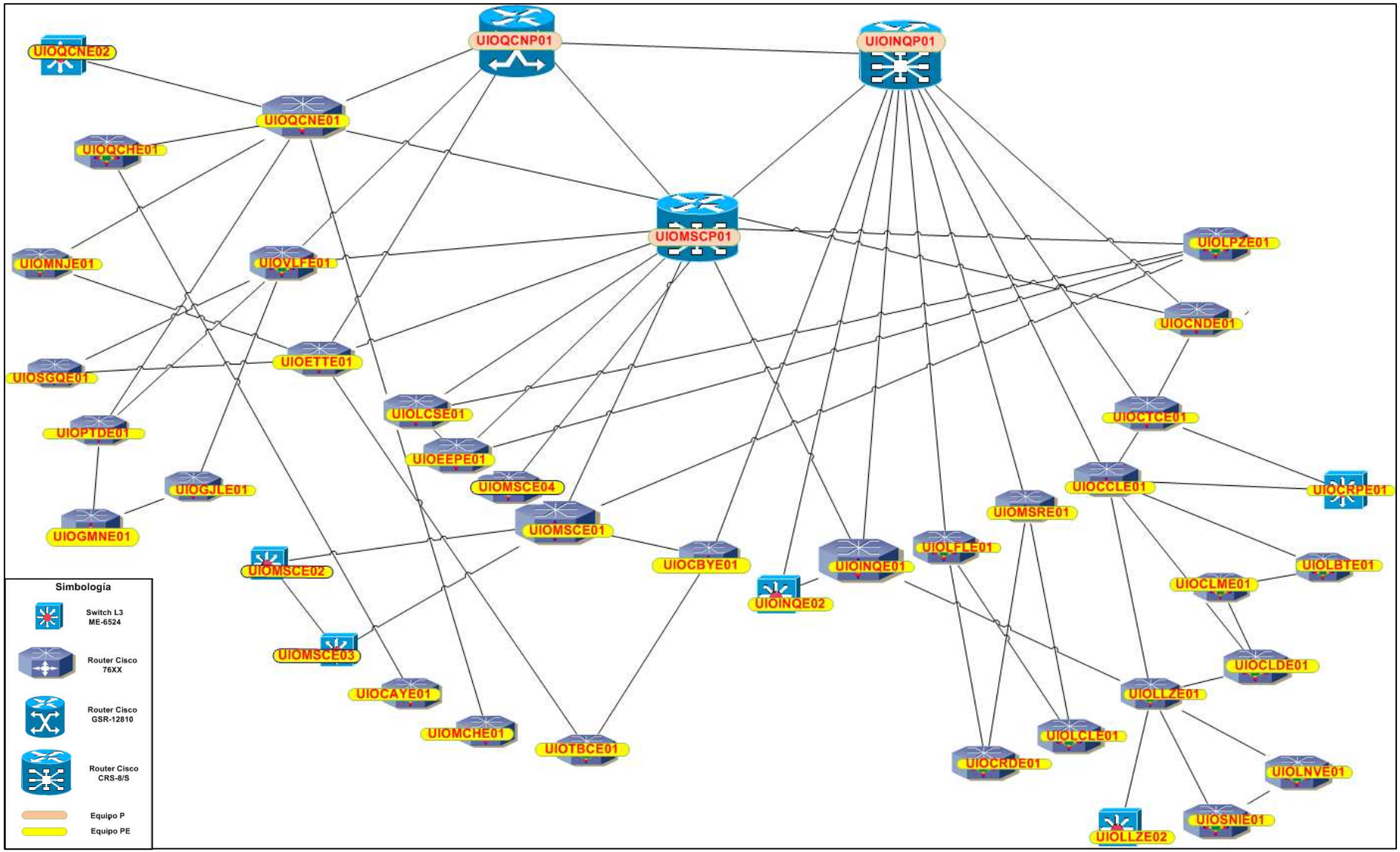


Figura 3.2: Topología de la red IP/MPLS de la CNT E.P. (Pichincha) [1]

b.2) Activos de soporte humano

- Personal del Área O&M Plataformas IP/MPLS.
- Personal de las demás áreas de la CNT E.P. que por sus funciones requieren acceso a la red IP/MPLS de la CNT E.P.
- Personal de la empresa DESCA, que contribuye en el soporte a la red IP/MPLS de la CNT E.P.

La tabla 3.11 muestra los activos de soporte humano identificados en la CNT E.P.

	CARGO	#
O&M Plataforma IP/MPLS	ANALISTA DE OPERACIONES	1
	ANALISTA DE TELECOMUNICACIONES JUNIOR	11
	ARQUITECTO DE RED	1
	JEFE DE ÁREA	1
	PROFESIONAL	1
CALL CENTER	ASESOR DE SERVICIO AL CLIENTE CONTAC CENTER	30
NOC	ASISTENTE DE SOPORTE NOC	16
INGENIERÍA	ANALISTA DE TELECOMUNICACIONES	4
	ANALISTA DE TELECOMUNICACIONES SENIOR	1
GESTIÓN DE RED	ANALISTA DE TELECOMUNICACIONES JUNIOR	1
	AUXILIAR OPERATIVO	2
GESTIÓN XDSL	ANALISTA DE TELECOMUNICACIONES	3
	ANALISTA DE TELECOMUNICACIONES JUNIOR	12
	ANALISTA DE TELECOMUNICACIONES SENIOR	1
	ASISTENTE DE TELECOMUNICACIONES	2
MULTISERVICIOS	ANALISTA DE TELECOMUNICACIONES	1
	ANALISTA DE TELECOMUNICACIONES JUNIOR	8
	ANALISTA DE TELECOMUNICACIONES SENIOR	2
	ASISTENTE DE TELECOMUNICACIONES	2
	ESPECIALISTA TÉCNICO	2
	TÉCNICO SUPERVISOR	12
DESCA	INGENIEROS DE SOPORTE DESCA	4
SISTEMAS DE GESTIÓN	USUARIOS	2

Tabla 3.11: Activos de soporte humano

3.2.1.1.2 Valoración de activos

Se utiliza la escala definida en la sección 3.1.2.1, criterios de valoración de los activos, para valorarlos. En la tabla 3.12 se muestra el resultado.

PROPIETARIOS DE LOS ACTIVOS: ANALISTAS DE TELECOMUNICACIONES JUNIOR O&M PLATAFORMA IP/MPLS						
#	NODO	EQUIPO	CRITERIOS DE VALORACIÓN DE ACTIVOS			VALOR DEL ACTIVO
			Dependencia	Funcio-nalidad	Disponibilidad Integridad Confidencialidad	
1	CALDERÓN	UIOCLDE01	1	4	4	16
2	CARAPUNGO	UIOCRPE01	1	3	4	12
3	CARCELÉN	UIOCCLE01	3	4	4	48
4	CARONDELET	UIOCRDE01	1	4	4	16
5	CAYAMBE	UIOCAYE01	1	4	4	16
6	COLLALOMA	UIOCLME01	1	4	4	16
7	CONDADO	UIOCNDE01	2	4	4	32
8	COTOCOLLAO	UIOCTCE01	2	4	4	32
9	CUMBAYÁ	UIOCBYE01	2	4	4	32
10	ESCUELA ESPEJO	UIOEEPE01	2	4	4	32
11	ESTACIÓN TERRENA	UIOETTE01	2	4	3	24
12	GUAJALÓ	UIOGJLE01	2	4	4	32
13	GUAMANÍ	UIOGMNE01	1	4	4	16
14	IÑAQUITO	UIOINQP01	5	5	5	125
15	IÑAQUITO	UIOINQE01	5	4	4	80
16	IÑAQUITO	UIOINQE02	2	3	4	24
17	LA BOTA	UIOLBTE01	1	4	4	16
18	LA CAROLINA	UIOLCLE01	1	4	4	16
19	LA FLORIDA	UIOLFLE01	2	4	4	32
20	LA LUZ	UIOLLZE01	2	4	4	32
21	LA LUZ	UIOLLZE02	1	3	4	12
22	LA PAZ	UIOLPZE01	2	4	4	32
23	LAS CASAS	UIOLCSE01	2	4	4	32
24	LOS NEVADOS	UIOLNVE01	1	4	4	16
25	MACHACHI	UIOMCHE01	1	4	4	16
26	MARISCAL	UIOMSCP01	5	5	5	125
27	MARISCAL	UIOMSCE01	2	4	4	32
28	MARISCAL	UIOMSCE04	2	4	4	32
29	MARISCAL	UIOMSCE02	1	3	4	12
30	MARISCAL	UIOMSCE03	1	3	4	12
31	MONJAS	UIOMNJE01	1	4	4	16
32	MONTESERRÍN	UIOMSRE01	2	4	4	32
33	PINTADO	UIOPTDE01	2	4	4	32
34	QUINCHE	UIOQCHE01	1	4	4	16
35	QUITO CENTRO	UOQCNP01	5	5	5	125
36	QUITO CENTRO	UIOQCNE01	3	4	4	48
37	QUITO CENTRO	UIOQCNE02	1	3	4	12
38	SAN ISIDRO DEL INCA	UIOSNIE01	1	4	4	16
39	SANGOLQUÍ	UIOSGQE01	1	4	4	16
40	TUMBACO	UIOTBCE01	1	4	4	16
41	VILLAFLORA	UIOVLFE01	2	4	4	32

Tabla 3.12: Valoración de activos

A continuación se exponen ejemplos, para la asignación de valores a los respectivos criterios de evaluación y su correspondiente cálculo.

1.- Nodo: Iñaquito; Equipo: UIOINQE02

Dependencia: se le ha asignado el valor “2”, puesto que, según la topología mostrada en la figura 3.2, pocos activos dependen de éste.

Funcionalidad: Se le ha asignado el valor “3”, puesto que se trata de un modelo ME 6524 cuyas capacidades tecnológicas son inferiores en comparación con los otros modelos.

Confidencialidad, Integridad y Disponibilidad: se le ha asignado el valor “4”, puesto que la divulgación, modificación o no disponibilidad de la información que rige el funcionamiento del equipo podría afectar gravemente la entrega de los servicios a través del mismo.

2.- Nodo: Mariscal; Equipo: UIOMSCP01

Dependencia: se le ha asignado el valor “5”, ya que al tratarse de un equipo P, todos los demás equipos dependerán de este activo para una correcta entrega de servicios.

Funcionalidad: se le ha asignado el valor “5”, puesto que se trata de un equipo cuyas capacidades tecnológicas son las mejores presentes en la red IP/MPLS.

Confidencialidad, Integridad y Disponibilidad: se le ha asignado el valor “5”, puesto que la divulgación, modificación o no disponibilidad de la información que rige el funcionamiento del equipo podría afectar totalmente la entrega de los servicios a través del mismo y de otros.

Al equipo PE de Iñaquito (UIOINQE01), a pesar que, según la topología (figura 3.2) de él no dependen muchos activos, se le ha asignado el nivel de dependencia más alto ya que a este equipo se conectan otras plataformas de

telecomunicaciones de la CNT E.P.; entre las más importantes están la PSTN (*Public Switched Telephone Network*), ATM, GPON (*Gigabit-capable Passive Optical Network*), ISP (*Internet Service Provider*), BRAS (*Broadband Remote Access Server).*

De acuerdo a los resultados obtenidos se tienen como equipos críticos de la red a los equipos P de Iñaquito, Mariscal y Quito Centro; además un equipo PE de Iñaquito; estos equipos se encuentran identificados de color rojo con el fin de resaltar su nivel de importancia, puesto que constituyen la base fundamental para el funcionamiento de la red IP/MPLS no solamente en la provincia de Pichincha sino a nivel Nacional.

Uno de los puntos de vista para la valoración del impacto es el número de clientes que se verían afectados; es así que en la tabla 3.13 se presenta una lista de los activos de soporte físico con el número de clientes en cada uno de ellos. Como se aprecia, se tienen los valores únicamente para los equipos PE, puesto que se considera que de los equipos P dependen todos los clientes.

3.2.1.1.3 Identificación de amenazas

La tabla 3.14 presenta una lista de amenazas que podrían convertirse en un verdadero peligro en el caso que llegaran a concretarse afectando la entrega de servicios que se hace a través de la red IP/MPLS de la CNT E.P. Estas amenazas pueden ser deliberadas, accidentales o ambientales (naturales).

Se utiliza la letra D para todas las acciones deliberadas o mal intencionadas que tienen como objetivo causar daño a los activos de la información, la letra A se utiliza para identificar las acciones humanas que pueden dañar accidentalmente los activos de información y la letra E se utiliza para todos los incidentes que no se basa en las acciones humanas sino más bien son producto de eventos naturales.

#	EQUIPO	MASIVOS	MASIVOS/10	CORPORATIVOS	TOTAL CLIENTES
1	UIOCCLE01	8016	802	81	882
2	UIOCNDE01	4284	428	71	499
3	UIOCTCE01	9056	906	70	975
4	UIOCBYE01	6112	611	80	691
5	UIOEEPE01	428	43	59	101
6	UIOETTE01	960	96	47	143
7	UIQINQE01	24324	2432	578	3011
8	UIOINQE02	0	0	186	186
9	UIOLFLE01	1300	130	56	186
10	UIOLPZE01	552	55	92	147
11	UIOLCSE01	756	76	122	197
12	UIOMSCE01	17276	1728	255	1982
13	UIOMSCE02	0	0	128	128
14	UIOMSCE03	0	0	116	116
15	UIOMSCE04	0	0	180	180
16	UIOMSRE01	1308	131	46	177
17	UIOQCNE01	12448	1245	244	1488
18	UIOVLFE01	9100	910	77	987
19	UIOCLDE01	5712	571	56	627
20	UIOCRPE01	0	0	29	29
21	UIOCRDE01	544	54	123	177
22	UIOCAYE01	1744	174	45	219
23	UIOCLME01	684	68	42	111
24	UIOGJLE01	7008	701	74	774
25	UIOGMNE01	4880	488	55	543
26	UIOLBTE01	1084	108	25	133
27	UIOLCLE01	4352	435	219	655
28	UIOLLZE01	6636	664	66	729
29	UIOLLZE02	0	0	20	20
30	UIOLNVE01	1580	158	53	211
31	UIOMCHE01	2072	207	51	258
32	UIOMNJE01	5192	519	43	562
33	UIOPTDE01	10752	1075	54	1129
34	UIOQCHE01	1468	147	34	180
35	UIOQCNE02	0	0	153	153
36	UIOSNIE01	1516	152	27	179
37	UIOSGQE01	12056	1206	127	1332
38	UIOTMBE01	2848	285	40	324

Tabla 3.13: Número de clientes por activo [1]

Se considera como clientes masivos aquellos que tienen contratado únicamente el servicio de Internet FastBoy y clientes Corporativos aquellos que tienen varios servicios de los que ofrece la CNT E.P. contratados, como: Internet Corporativo Premium, Banda Ancha PYMES, enlaces de transmisión de datos. Estos servicios fueron descritos en el Capítulo 2, sección 2.4. Por lo que para el cálculo total de clientes se realiza la relación de que 1 cliente corporativo equivale a 10 clientes masivos.

TIPO	AMENAZAS	ORIGEN		
Daño físico	Incendio	A	D	E
	Filtraciones de agua	A	D	E
	Polvo y sobrecalentamiento			E
Eventos naturales	Fenómenos sísmicos			E
Pérdida de los servicios escenciales	Pérdida de suministro de energía	A	D	E
Compromiso de la información	Espionaje remoto		D	
	Escucha encubierta		D	
	Hurto de medios o documentos		D	
	Hurto de equipos		D	
	Recuperación de medios reciclados o desechados		D	
Fallas técnicas	Falla del equipo	A		
	Mal funcionamiento del equipo	A		
	Saturación de la red	A	D	
Acciones no autorizadas	Uso no autorizado del equipo		D	
	Desconexión de puertos	A	D	
	Ataques informáticos		D	
	Corrupción de los datos		D	
	Copia mal intencionada del archivo de configuración		D	
Compromiso de las funciones	Divulgación de la información	A	D	
	Error en el uso	A		
	Abuso de derechos		D	
	Falsificación de derechos		D	
	Negación de acciones		D	
	Incumplimiento en la disponibilidad del personal	A		

Tabla 3.14: Identificación de amenazas

3.2.1.1.4 Identificación de los controles existentes

El área O&M Plataforma IP/MPLS a pesar de no contar con un documento formal de políticas, en cuanto a la administración de la red IP/MPLS, lleva a cabo ciertos

controles que de alguna forma permiten minimizar la probabilidad de que ciertas amenazas puedan concretarse. En la tabla 3.15 se listan los controles implementados y las observaciones correspondientes.

3.2.1.1.5 Identificación de las vulnerabilidades

En la tabla 3.16 se presentan las vulnerabilidades identificadas en cada uno de los nodos de la red IP/MPLS, que harían posible que las amenazas llegaran a concretarse.

TIPO DE AMENAZA	CONTROLES EXISTENTES	OBSERVACIONES
Daño físico	Sistema anti-incendios.	El control no está implementado en todos los nodos. En los nodos donde se cuenta no se realiza una revisión periódica de su estado.
	Sistema enfriamiento (ventilación, acondicionador).	El control no está implementado en todos los nodos. En algunos nodos su implementación no es adecuada. No se realiza mantenimiento periódico del mismo.
Eventos naturales	*Backups.*	No todos los equipos de la red cuentan con respaldos del archivo de configuración.
Pérdida de los servicios esenciales	Sistema ininterrumpible de energía (UPS).	El control no está implementado en todos los nodos. En los nodos que tienen este control no se realiza una revisión periódica de su estado.
Compromiso de la información	Seguridad física.	La seguridad física en sus nodos es insuficiente.
Fallas técnicas	Enlaces redundantes.	No todos los dispositivos de la red IP/MPLS cuentan con enlaces redundantes.
	Se dispone con los siguientes sistemas de gestión y monitoreo de la red, Cacti, Cisco ANA y Cisco ISC.	No todos los equipos de la red se encuentran ingresados en los sistemas de gestión para su monitorización.
	El área dispone de personal capacitado para la resolución de problemas en la red.	Ocasionalmente el personal no es suficiente para cubrir la demanda de configuración de nuevos servicios o resolución de problemas en la red.
Acciones no autorizadas	*Rack* cerrado.	No todos los equipos disponen de *rack* cerrado.
	Se cuenta con un Sistema de Control de Acceso Cisco ACS para la administración de los dispositivos de la red.	Existen falencias en la administración y configuración del ACS. Falta de políticas para la administración de los equipos de la red.
Compromiso de las funciones	Se cuenta con un sistema de control de acceso Cisco ACS para la administración de los dispositivos de la red.	Existen falencias en la administración y configuración del ACS. Falta de políticas para la administración de los equipos de la red.

Tabla 3.15: Identificación de controles existentes

3.2.1.1.6 Identificación de las consecuencias

Las consecuencias se definen como el impacto que podrían ocasionar las amenazas si éstas llegaran a explotar las vulnerabilidades presentes en cada uno de los nodos de la red.

En la tabla 3.16 se describe de forma general el impacto que ocasionaría cada amenaza identificada.

3.2.1.2 Estimación del riesgo

3.2.1.2.1 Valoración de las consecuencias

La valoración de las consecuencias de cada amenaza en cada activo se lo presenta en la tabla 3.16, para ello se utilizan los criterios de valoración de impacto establecidos en las tablas 3.4 y 3.5.

3.2.1.2.2 Valoración de los incidentes

Consiste en valorar la probabilidad (Pbdd) de ocurrencia de cada amenaza, tomando en cuenta los controles existentes y acontecimientos de incidentes suscitados anteriormente respecto a la red. Para ello se utilizan los criterios de probabilidad de ocurrencia de amenazas establecidos en la tabla 3.3. La valoración de los incidentes en cada activo se presenta en la tabla 3.16.

3.2.2 EVALUACIÓN DEL RIESGO

Se analizan en cada equipo las vulnerabilidades que posee y las amenazas que pudieren explotar dichas vulnerabilidades con la finalidad de valorar la probabilidad de ocurrencia de amenazas y el impacto que pudieren ocasionar para finalmente obtener la evaluación del riesgo.

A continuación se detalla un ejemplo de cómo se determinan las amenazas, vulnerabilidades y el impacto de su explotación, para evaluar el riesgo.

Nodo: Calderón; **Equipo** UIOCLDE01

Vulnerabilidad: no se cuenta con un sistema anti-incendios, únicamente con un extinguidor.

Amenaza: incendio. En la actualidad no se han registrado este tipo de incidentes por lo que se podría considerar que la probabilidad de que ocurra este evento en dicho nodo es muy baja (Valor Pbdd=1); de acuerdo a la tabla 3.3.

Impacto: de producirse un hecho de tal magnitud la infraestructura y el funcionamiento del equipo se verían gravemente afectados, se dejaría de ofrecer el servicio a los clientes que dependan de este equipo (Imp1) y el tiempo de recuperación del servicio o del equipo sería muy amplio (Imp2).

De este equipo dependen un total de 852 clientes entre masivos y corporativos, por lo que el impacto en este sentido se valora como: Imp1 = 4; de acuerdo a la tabla 3.4.

Un incendio implicaría el reemplazo del equipo y la reparación de las instalaciones y de la infraestructura del nodo en general, lo cual tomaría un tiempo considerable y el cliente exigiría que se reponga el servicio a la brevedad posible, por lo que el impacto en este sentido se podría valorar como: Imp2 = 5; de acuerdo a la tabla 3.5.

Riesgo: de acuerdo a la fórmula descrita en la sección 3.1.2.4, se calcula el nivel del riesgo: NR = 1*4*5 = 20 y se concluye según la tabla 3.6 que se trata de un riesgo alto.

NODO CALDERÓN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCLDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con un sistema anti-incendios*, únicamente con un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se podría ver gravemente afectada.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a éste o a otros nodos de la red.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se lo realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 1 de 86)

* Sistema anti-incendios: sistema compuesto por elementos detectores y extintores de incendios.

NODO CALDERÓN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCLDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	*No existe suficiente control de acceso físico a las instalaciones del nodo. * Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* El acceso a la administración del dispositivo no se realiza mediante el ACS . * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 2 de 86)

NODO CALDERÓN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCLDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Abuso de derechos	* El equipo no se encuentra anexado al Sistema de Control de Acceso Cisco ACS . * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24
NODO CARAPUNGO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCRPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	2	5	10
	Filtraciones de agua	* El sistema de climatización no se encuentra instalado correctamente.	El funcionamiento de los equipos se vería afectado.	1	2	3	6
	Polvo y sobrecalentamiento	* Sistema de climatización defectuoso. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	2	2	8
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	2	5	10
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 3 de 86)

NODO CARAPUNGO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCRPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	2	5	10
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	* La confidencialidad de a información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con un respaldo de su archivo de configuración.	Los servicios ofrecidos se verían afectados.	1	2	3	6
	Mal funcionamiento de los equipos			1	2	4	8
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	1	2	2
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se dispone respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	2	4	16
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	2	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 4 de 86)

NODO CARAPUNGO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCRPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	2	3	6
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	2	3	12
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	2	3	12
	Falsificación de derechos			1	2	3	6
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	2	2	12
NODO CARCELÉN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCCLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 5 de 86)

NODO CARCELÉN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCCLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * No dispone de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16
Acciones no autorizadas	Desconexión de puertos de los equipos	* No se realiza suficiente control de acceso físico a las instalaciones del nodo. * Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware* . * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 6 de 86)

NODO CARCELÉN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCCLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Uso no autorizado de los equipos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* El acceso a la administración del dispositivo no se realiza mediante el ACS . * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 7 de 86)

NODO CARONDELET							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCRDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se lo realiza periódicamente.	La entrega de servicios se vería afectada.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 8 de 86)

NODO CARONDELET							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCRDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 9 de 86)

NODO CAYAMBE							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCAYE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* El sistema de climatización no está implementado correctamente.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Se afectaría la entrega de servicios.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 10 de 86)

NODO CAYAMBE							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCAYE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	3	4	4	48
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 11 de 86)

NODO COLLALOMA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCLME01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con ningún tipo de dispositivo anti-incendio.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* No se dispone de un UPS (Sistema Ininterrumpido de Energía).	El funcionamiento del equipo se vería afectado.	1	3	3	9
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con respaldo de su archivo de configuración.	La entrega de servicios se vería afectada.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 12 de 86)

NODO COLLALOMA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCLME01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del su archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 13 de 86)

NODO CONDADO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCNDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* El mantenimiento del Sistema de climatización no se realiza de forma periódica.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con respaldo del archivo de configuración.	La entrega de servicios se vería afectada.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 14 de 86)

NODO CONDADO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCNDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 15 de 86)

NODO COTOCOLLAO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCTCE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * No dispone de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 16 de 86)

NODO COTOCOLLAO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCTCE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * No se realiza un control de acceso físico estricto a las instalaciones del nodo.	La entrega de servicios se vería interrumpida.	1	4	2	8
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 17 de 86)

NODO CUMBAYÁ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCBYE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* Falencias en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 18 de 86)

NODO CUMBAYÁ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCBYE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 19 de 86)

NODO CUMBAYÁ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOCBYE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24
NODO EL PINTADO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOPTDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El funcionamiento del equipo se vería afectado.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipo	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 20 de 86)

NODO EL PINTADO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOPTDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	3	15
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	3	15
	Mal funcionamiento de los equipos			1	5	4	20
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	5	2	10
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* EL equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	3	5	4	60
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			3	5	4	60
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	3	15
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	3	30

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 21 de 86)

NODO EL PINTADO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOPTDE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Abuso de derechos	* EL equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	3	5	3	45
	Falsificación de derechos			2	5	3	30
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	2	30
NODO EL QUINCHE							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti incendios.	Los equipos podrían dejar de funcionar en su totalidad.	1	3	5	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El funcionamiento del equipo se vería afectado.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 22 de 86)

NODO EL QUINCHE							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 23 de 86)

NODO EL QUINCHE							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO ESCUELA ESPEJO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEEPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* UPS (Sistema Ininterrumpido de Energía) defectuoso.	El funcionamiento del equipo se vería afectado.	1	3	3	9
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 24 de 86)

NODO ESCUELA ESPEJO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEEPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con respaldo del archivo de configuración.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* El equipo no se encuentra anexado al ACS. * No se cuenta con respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	3	4	4	48
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 25 de 86)

NODO ESCUELA ESPEJO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEEPE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* El equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	3	3	3	27
	Falsificación de derechos			3	3	3	27
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO ESTACIÓN TERRENA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEETE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* UPS (Sistema Ininterrumpido de Energía) defectuoso.	El funcionamiento del equipo se vería afectado.	1	3	3	9

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 26 de 86)

NODO ESTACIÓN TERRENA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEETE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 27 de 86)

NODO ESTACIÓN TERRENA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOEETE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO GUAJALÓ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGJLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 28 de 86)

NODO GUAJALÓ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGJLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * No dispone de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 29 de 86)

NODO GUAJALÓ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGJLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* El equipo no se encuentra anexado en el ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	3	5	4	60
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			3	4	4	48
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* El equipo no se encuentra anexado en el ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	3	4	3	36
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24
NODO GUAMANÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGMNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 30 de 86)

NODO GUAMANÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGMNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* UPS (Sistema Ininterrumpido de Energía) defectuoso.	El funcionamiento del equipo se vería afectado.	1	4	3	12
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 31 de 86)

NODO GUAMANÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGMNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 32 de 86)

NODO GUAMANÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOGMNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24
NODO IÑAQUITO (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* Las tuberías no han sido revisadas hace mucho tiempo, se desconoce su estado.	El funcionamiento de los equipos se vería afectado.	1	5	3	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	5	5	50
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	5	5	25
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 33 de 86)

NODO IÑAQUITO (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	4	4	16
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	5	25
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	5	25
	Mal funcionamiento de los equipos			1	5	5	25
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * No se realiza un control estricto de acceso físico a las instalaciones del nodo.	La entrega de servicios se vería interrumpida.	1	5	5	25
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	5	75
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	5	50
	Copia malintencionada del archivo de configuración			1	5	5	25
	Corrupción de los datos			2	5	5	50
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	4	4	48

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 34 de 86)

NODO IÑAQUITO (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	4	20
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	5	50
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	4	40
	Falsificación de derechos			1	5	4	20
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	4	60
NODO IÑAQUITO (Equipo PE _1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* Las tuberías no han sido revisadas hace mucho tiempo, se desconoce su estado.	El funcionamiento de los equipos se vería afectado.	1	5	3	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	3	3	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 35 de 86)

NODO IÑAQUITO (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	5	4	20
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	3	15
	Mal funcionamiento de los equipos			1	5	4	20
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	4	3	12
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	5	75
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	5	4	40

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 36 de 86)

NODO IÑAQUITO (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	3	15
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	3	30
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	3	30
	Falsificación de derechos			1	5	3	15
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	2	30
NODO IÑAQUITO (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* Las tuberías no han sido revisadas hace mucho tiempo, se desconoce su estado.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 37 de 86)

NODO IÑAQUITO (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 38 de 86)

NODO IÑAQUITO (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOINQE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 39 de 86)

NODO LA BOTA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLBTE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 40 de 86)

NODO LA BOTA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLBTE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 41 de 86)

NODO LA CAROLINA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLCLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* El sistema de climatización no se encuentra correctamente implementado.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 42 de 86)

NODO LA CAROLINA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLCLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* El equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	3	5	4	60
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* El equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	3	4	3	36
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 43 de 86)

NODO LA FLORIDA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLFLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* Solo se dispone de un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El funcionamiento del equipo se vería afectado.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipo	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 44 de 86)

NODO LA FLORIDA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLFLE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO LA LUZ (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* El sistema de climatización no se encuentra implementado correctamente.	El funcionamiento de los equipos se vería afectado.	1	4	3	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 45 de 86)

NODO LA LUZ (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
	Fenómenos sísmicos	* Infraestructura no antisísmica.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipo	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 46 de 86)

NODO LA LUZ (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24
NODO LA LUZ (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* El sistema anti-incendio no es revisado periódicamente.	Toda la infraestructura del nodo se vería gravemente afectada.	1	2	5	10
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	2	3	6

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 47 de 86)

NODO LA LUZ (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	1	2	2	4
Eventos naturales	Fenómenos sísmicos	* Infraestructura no antisísmica.	Toda la infraestructura del nodo se vería gravemente afectada.	1	2	5	10
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipo	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	2	5	10
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	2	3	6
	Mal funcionamiento de los equipos			1	2	4	8
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	1	2	2
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 48 de 86)

NODO LA LUZ (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLLZE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	3	4	24
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	2	4	16
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	2	3	6
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	2	3	12
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	2	3	12
	Falsificación de derechos			1	2	3	6
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	2	2	12
NODO LA PAZ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLPZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 49 de 86)

NODO LA PAZ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLPZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 50 de 86)

NODO LA PAZ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLPZE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 51 de 86)

NODO LAS CASAS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLCSE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 52 de 86)

NODO LAS CASAS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLCSE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con el respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 53 de 86)

NODO LOS NEVADOS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLNVE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* UPS (Sistema Ininterrumpido de Energía) defectuoso.	El funcionamiento del equipo se vería afectado.	1	3	3	9
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 54 de 86)

NODO LOS NEVADOS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLNVE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con respaldo del archivo de configuración.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	4	4	16
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 55 de 86)

NODO LOS NEVADOS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOLNVE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO MACHACHI							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 56 de 86)

NODO MACHACHI							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 57 de 86)

NODO MACHACHI							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMCHE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO MARISCAL (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	5	4	20
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	3	30
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	5	5	25

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 58 de 86)

NODO MARISCAL (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	5	5	50
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	5	5	25
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna. * EL equipo no cuenta con *rack* cerrado.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	4	4	16
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	5	25
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	5	25
	Mal funcionamiento de los equipos			1	5	5	25
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	5	5	25
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	5	75
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	5	50
	Copia malintencionada del archivo de configuración			1	5	5	25
	Corrupción de los datos			2	5	5	50

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 59 de 86)

NODO MARISCAL (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	4	4	48
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	4	20
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	5	50
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	4	40
	Falsificación de derechos			1	5	4	20
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	4	60
NODO MARISCAL (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	5	3	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	5	5	25

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 60 de 86)

NODO MARISCAL (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	3	15
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	3	15
	Mal funcionamiento de los equipos			1	5	4	20
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	5	2	10
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 61 de 86)

NODO MARISCAL (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	5	4	40
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	3	15
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	3	30
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	3	30
	Falsificación de derechos			1	5	3	15
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	2	30
NODO MARISCAL (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 62 de 86)

NODO MARISCAL (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 63 de 86)

NODO MARISCAL (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18
NODO MARISCAL (Equipo PE_3)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE03			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 64 de 86)

NODO MARISCAL (Equipo PE_3)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE03			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	1	3	2	6
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 65 de 86)

NODO MARISCAL (Equipo PE_3)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE03			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 66 de 86)

NODO MARISCAL (Equipo PE_4)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE04			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 67 de 86)

NODO MARISCAL (Equipo PE_4)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSCE04			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 68 de 86)

NODO MONJAS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMNJE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	4	5	20
Pérdida de los servicios esenciales	Pérdida del suministro eléctrico	* UPS (Sistema Ininterrumpido de Energía) defectuoso.	El funcionamiento del equipo se vería afectado.	1	4	3	12
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 69 de 86)

NODO MONJAS							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMNJE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* El equipo no se encuentra configurado en el ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* El equipo no se encuentra configurando en el ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 70 de 86)

NODO MONTESERRÍN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSRE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 71 de 86)

NODO MONTESERRÍN							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOMSRE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 72 de 86)

NODO QUITO CENTRO (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	5	4	20
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	3	30
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	5	5	50
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	5	5	25
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	4	4	16
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	5	25
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	5	25
	Mal funcionamiento de los equipos			1	5	5	25

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 73 de 86)

NODO QUITO CENTRO (Equipo P)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNP01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	5	4	20
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	5	75
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometido, podría afectarse el normal funcionamiento de la red.	2	5	5	50
	Copia malintencionada del archivo de configuración			1	5	5	25
	Corrupción de los datos			2	5	5	50
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	4	4	48
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	4	20
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	5	50
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	4	40
	Falsificación de derechos			1	5	4	20
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	4	60

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 74 de 86)

NODO QUITO CENTRO (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	5	3	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	3	15
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	3	15
	Mal funcionamiento de los equipos			1	5	4	20

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 75 de 86)

NODO QUITO CENTRO (Equipo PE_1)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	4	2	8
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	5	4	40
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	3	15
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	3	30
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	5	3	30
	Falsificación de derechos			1	5	3	15
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	2	30

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 76 de 86)

NODO QUITO CENTRO (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 77 de 86)

NODO QUITO CENTRO (Equipo PE_2)							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOQCNE02			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 78 de 86)

NODO SAN ISIDRO DEL INCA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOSNIE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 79 de 86)

NODO SAN ISIDRO DEL INCA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOSNIE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 80 de 86)

NODO SANGOLQUÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOSGQE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	5	5	25
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	5	3	15
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	5	2	20
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	5	5	25
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	5	5	25
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	Los servicios ofrecidos se verían afectados.	1	5	3	15
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.		1	5	3	15
	Mal funcionamiento de los equipos			1	5	4	20

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 81 de 86)

NODO SANGOLQUÍ							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOSGQE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	4	2	8
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* El equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	5	4	40
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	5	3	15
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	5	3	30
	Abuso de derechos	*El equipo no se encuentra anexado al ACS. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	3	5	3	45
	Falsificación de derechos			1	5	3	15
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	5	2	30

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 82 de 86)

NODO TUMBACO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOTMBE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	3	5	15
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	3	3	9
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	3	2	12
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	3	5	15
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	3	5	15
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	Los servicios ofrecidos se verían afectados.	1	3	3	9
	Mal funcionamiento de los equipos			1	3	4	12

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 83 de 86)

NODO TUMBACO							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOTMBE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	La entrega de servicios se vería interrumpida.	1	2	2	4
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	4	4	32
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	3	4	24
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	3	3	9
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	3	3	18
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	3	3	18
	Falsificación de derechos			1	3	3	9
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	3	2	18

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 84 de 86)

NODO VILLAFLORA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOVLFE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Daño físico	Incendio	* No se cuenta con dispositivos anti-incendios. Únicamente un extinguidor.	Toda la infraestructura del nodo se vería gravemente afectada.	1	4	5	20
	Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	El funcionamiento de los equipos se vería afectado.	1	4	3	12
	Polvo y sobrecalentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	El equipo podría dejar de funcionar o funcionar erróneamente.	2	4	2	16
Eventos naturales	Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	Toda la infraestructura del nodo se vería gravemente afectada dependiendo del grado del sismo.	1	4	5	20
Compromiso de la información	Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	La confidencialidad de la información se vería comprometida.	2	1	1	2
	Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	La confidencialidad de la información se vería comprometida.	1	1	1	1
	Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	Los servicios se verían interrumpidos y la información obtenida podría usarse para futuros ataques, a este o a otros nodos.	1	4	5	20
	Recuperación de medios con información importante	* No se dispone de políticas de reciclaje o desecho de medios con información importante.	La confidencialidad de la información se vería comprometida.	1	1	1	1
Fallas técnicas	Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	Los servicios ofrecidos se verían afectados.	1	4	3	12
	Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente. * No se cuenta con respaldo del archivo de configuración.		1	4	3	12
	Mal funcionamiento de los equipos			1	4	4	16

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 85 de 86)

NODO VILLAFLORA							
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	IMPACTO	UIOVLFE01			
				Pbdd	Imp 1	Imp 2	Riesgo
Acciones no autorizadas	Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	La entrega de servicios se vería interrumpida.	1	3	2	6
	Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware.* * Contraseñas no robustas.	El funcionamiento de los equipos y de los servicios podría verse afectado gravemente.	3	5	4	60
	Uso no autorizado de los equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	La confidencialidad, integridad y disponibilidad del archivo de configuración se vería seriamente comprometida, podría afectarse el normal funcionamiento de la red.	2	5	4	40
	Copia malintencionada del archivo de configuración			1	1	1	1
	Corrupción de los datos			2	4	4	32
Compromiso de las funciones	Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	La confidencialidad de la información se vería comprometida.	3	1	1	3
	Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	La resolución de problemas, mantenimiento y configuración de la red tarda más tiempo.	1	4	3	12
	Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	Se podría afectar el funcionamiento correcto del equipo y de los servicios ofrecidos.	2	4	3	24
	Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tiene usuarios locales configurados en los equipos para varios usuarios. * Falta de políticas para el control de acceso a la administración de los equipos.	Se afectaría seriamente la integridad y confidencialidad de la información, se podrían ejecutar acciones inapropiadas comprometiendo la entrega de los servicios.	2	4	3	24
	Falsificación de derechos			1	4	3	12
	Negación de acciones		Las acciones cometidas intencionales o no intencionales, graves o no tan graves, que afecten a la red, podrían repetirse con frecuencia.	3	4	2	24

Tabla 3.16: Evaluación del riesgo en los activos de la red IP/MPLS de la CNT E.P. (Página 86 de 86)

Tras la evaluación del riesgo en los activos de soporte físico de la red IP/MPLS de la CNT E.P. se determinan las siguientes observaciones.

- Los riesgos identificados en color rojo constituyen el valor de riesgo más alto y se deben tener muy en cuenta al momento de establecer controles.
- En algunos equipos a pesar de presentarse la misma amenaza y vulnerabilidad, se determina un nivel de riesgo diferente; esto debido a que el impacto que estas amenazas generan varía de acuerdo al equipo en el cual se presentan.
- Una de las amenazas evaluadas con mayor nivel de riesgo son los ataques informáticos, pues su impacto en la entrega de servicios es grave y hasta catastrófico, tanto en la cantidad de clientes afectados como en el tiempo de recuperación del servicio; la probabilidad de su ocurrencia producto del aumento de *hackers*, *crackers* y demás atacantes, es alta.
- Las amenazas presentes en los equipos tipo P de la red IP/MPLS de la CNT E.P. a pesar de ser en algunos casos poco probables, generan graves consecuencias, ya que al ser equipos de *core* su correcto funcionamiento es vital en la entrega de servicios en toda la red.
- Las amenazas de tipo natural como eventos sísmicos, a pesar de ser muy improbables deben tomarse en cuenta puesto que generarían un alto impacto en la entrega de servicios.
- Los nodos Mariscal, Iñaquito y Quitocentro, al alojar a los equipos más críticos y de mayor funcionalidad de la red, deberán poseer mejores medidas de seguridad para evitar daños y accesos físicos no deseados.
- El nivel de riesgo producto de errores personales, se determina como alto en la mayoría de los equipos analizados, por lo que se debe tener muy en cuenta concientizar de este hecho al personal relacionado con la administración de la red IP/MPLS.

- Las falencias identificadas en el ACS constituyen una vulnerabilidad que podría ser muy explotada, se debe tomar en cuenta su breve corrección.

3.3 TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Una vez identificados los riesgos, se procede a tratarlos, según la tabla 3.7, “Criterios de tratamiento del riesgo”; se identificarán aquellos riesgos que se retendrán y aquellos que se reducirán.

Para los riesgos a reducir, en la tabla 3.17 se muestran los controles que se recomienda implementar, para contrarrestar las vulnerabilidades explotadas por las amenazas que ocasionan dichos riesgos.

En base a la fórmula descrita en la sección 3.1.2.6, se determina la prioridad con la que se deberán implementar los controles en cada equipo, esta prioridad se evalúa en base a la tabla 3.8.

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Abuso de derechos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo.	UIOPTDE01	45	32	16
			UIOEEPE01	27	32	12
			UIOGJLE01	36	32	16
			UIOCCLE01	24	48	12
			UIOSGQE01	45	16	8
			UIOLCLE01	36	16	8
			UIOCLDE01	24	16	6
			UIOMNJE01	24	16	6

.

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar (Página 1 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con el respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOLCSE01	18	32	12
	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOINQP01	40	125	20
			UIOMSCP01	40	125	20
			UIOQCNE01	30	48	12
			UIOINQE01	30	80	15
			UIOMSCE01	30	32	12
			UIOCNDE01	18	32	12
			UIOCTCE01	24	32	12
			UIOCBYE01	24	32	12
			UIOEETE01	18	24	9
			UIOINQE02	18	24	9
			UIOLFLE01	18	32	12
			UIOLLZE01	24	32	12
			UIOLPZE01	18	32	12
			UIOMSCE04	18	32	12
			UIOMSRE01	18	32	12
			UIOQCNP01	40	125	20
			UIOVLFE01	24	32	12
			UIOCRDE01	18	16	6

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar (Página 2 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Abuso de derechos	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOCAYE01	18	16	6
			UIOCLME01	18	16	6
			UIOQCHE01	18	16	6
			UIOGMNE01	24	16	6
			UIOLBTE01	18	16	6
			UIOLNVE01	18	16	6
			UIOMCHE01	18	16	6
			UIOMSCE02	18	12	6
			UIOMSCE03	18	12	6
			UIOQCNE02	18	12	6
			UIOSNIE01	18	16	6
			UIOTMBE01	18	16	6
Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	* Es necesaria la implementación de un sistema IPS, de planes de contingencia y políticas ante ataques informáticos. * Se deben limitar los tiempos de conexión. * Exigir la configuración de contraseñas robustas y utilizar la mejor encriptación como sea posible. *Exigir periódicamente el cambio de contraseñas.	UIOINQP01	75	125	25
			UIOMSCP01	75	125	25
			UIOINQE01	75	80	25
			UIOQCNE01	60	48	20
			UIOCCLE01	60	48	20
			UIOMSCE01	60	32	20
			UIOCNDE01	60	32	20
			UIOCTCE01	60	32	20
			UIOCBYE01	60	32	20
			UIOPTDE01	60	32	20
			UIOEEPE01	60	32	20
			UIOEETE01	60	24	15
			UIOGJLE01	60	32	20
			UIOINQE02	60	24	15
			UIOLFLE01	60	32	20
			UIOLLZE01	60	32	20
			UIOLPZE01	60	32	20
			UIOLCSE01	60	32	20
			UIOMSCE04	60	32	20
			UIOMSRE01	60	32	20
			UIOVLFE01	60	32	20
			UIOQCNP01	75	125	25

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar (Página 3 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Ataques informáticos	* No se cuenta con sistemas IDS o IPS. * No se dispone de un plan de contingencia contra ataques de denegación de servicio. * No se dispone de protección contra *Malware*. * Contraseñas no robustas.	* Es necesaria la implementación de un sistema IPS, de planes de contingencia y políticas ante ataques informáticos. * Limitar los tiempos de conexión. * Exigir la configuración de contraseñas robustas y utilizar la mejor encriptación como sea posible. *Exigir periódicamente el cambio de contraseñas. *Mantener actulizado el IOS de los equipos de red, teniendo en cuenta que éste debe cumplir con los requerimientos de la red.	UIOCLDE01	60	16	10
			UIOCRPE01	60	12	10
			UIOCRDE01	60	16	10
			UIOCAYE01	60	16	10
			UIOCLME01	60	16	10
			UIOQCHE01	60	16	10
			UIOGMNE01	60	16	10
			UIOLBTE01	60	16	10
			UIOLCLE01	60	16	10
			UIOLLZE02	60	12	10
			UIOLNVE01	60	16	10
			UIOMCHE01	60	16	10
			UIOMSCE02	60	12	10
			UIOMSCE03	60	12	10
			UIOMNJE01	60	16	10
			UIOQCNE02	60	12	10
			UIOSNIE01	60	16	10
			UIOSGQE01	60	16	10
			UIOTMBE01	60	16	10
Copia malintencionada del archivo de configuración	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo, éste será conocido solo por el Responsable de la red. *Establecer responsabilidades por el uso de los activos y documentar los procedimientos realizados. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOINQP01	25	125	15
			UIOMSCP01	.	125	25
			UIOQCNP01	25	125	15

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar (Página 4 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Corrupción de los datos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * No se cuenta con respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración.	UIOEEPE01	g	32	20
	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo.	UIOPTDE01	60	32	20
			UIOGJLE01	48	32	16
			UIOCCLE01	32	48	16
			UIOMNJE01	32	16	8
			UIOLCLE01	32	16	8
			UIOSGQE01	40	16	8
			UIOCLDE01	40	16	8
	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOCNDE01	24	32	12
			UIOLCSE01	24	32	12
			UIOVLFE01	32	32	16

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 5 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Corrupción de los datos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOLNVE01	24	16	6
			UIOCLME01	24	16	6
	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOINQP01	50	125	20
			UIOCTCE01	32	32	16
			UIOCBYE01	32	32	16
			UIOCRDE01	24	16	6
			UIOCAYE01	24	16	6
			UIOEETE01	24	24	9
			UIOGMNE01	32	16	8
			UIOQCHE01	24	16	6
			UIOMSCP01	50	125	20
			UIOINQE01	40	80	20
			UIOLPZE01	24	32	12
			UIOMSRE01	24	32	12
			UIOQCNE01	40	48	16
			UIOMSCE01	40	32	16
			UIOINQE02	24	24	9
			UIOLFLE01	24	32	12
			UIOLLZE01	32	32	16
			UIOMCHE01	24	16	6
			UIOMSCE03	32	12	8
			UIOMSCE04	24	32	12
			UIOQCNP01	50	125	20
			UIOSNIE01	24	16	6
			UIOLBTE01	24	16	6
			UIOMSCE02	24	12	6
			UIOQCNE02	24	12	6
			UIOTMBE01	24	16	6

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 6 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Desconexión de puertos de los equipos	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * No se realiza un control estricto de acceso físico a las instalaciones del nodo.	*Advertir al personal de limpieza y demás personas que soliciten acceso al nodo, acerca de tener cuidado al movilizarse dentro de él. * Implementar cámaras de seguridad dentro del nodo.	UIOINQP01	25	125	15
	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. * El equipo no se encuentra en *rack* cerrado.	*Advertir al personal de limpieza y demás personas que soliciten acceso al nodo, acerca de tener cuidado al movilizarse dentro de él. * Los equipos deberán estar dentro de un *rack* cerrado.	UIOMSCP01	25	125	15
	* Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	*Advertir al personal de limpieza y demás personas que soliciten acceso al nodo, acerca de tener cuidado al movilizarse dentro de él. * Implementar cámaras de seguridad dentro del nodo.	UIOQCNP01	20	125	15
Divulgación de la información	* No existe acuerdo de confidencialidad establecido con el personal cuando pasa a formar parte de la empresa.	* Establecer acuerdos de confidencialidad con el personal que forma parte de la empresa; así como, con el personal externo que maneje información sensible de la empresa. * Definidas las políticas de seguridad, éstas deben ser difundidas a todoel personal involucrado en las mismas.	UIOINQP01	48	125	20
			UIOMSCP01	48	125	20
			UIOQCNP01	48	125	20
Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	* Mantener una copia segura del archivo de configuración. * Las configuraciones importantes las deberá realizar solo personal suficientemente experimentado. *Establecer responsabilidades por el uso de los activos y documentar los procedimientos realizados.	UIOINQP01	50	125	20
			UIOMSCP01	50	125	20
			UIOQCNE01	30	48	12
			UIOINQE01	30	80	15
			UIOMSCE01	30	32	12
			UIOPTDE01	30	32	12
			UIOCCLE01	24	48	12
			UIOQCNP01	50	125	20
			UIOCNDE01	18	32	12
			UIOCTCE01	24	32	12
			UIOCBYE01	24	32	12
			UIOEEPE01	18	32	12
			UIOEETE01	18	24	9
			UIOGJLE01	24	32	12
			UIOINQE02	18	24	9
			UIOLFLE01	18	32	12
			UIOLLZE01	24	32	12
			UIOLPZE01	18	32	12
			UIOLCSE01	18	32	12

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 7 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Error en el uso	* Errores de configuración por personal nuevo de la empresa o errores involuntarios del personal.	* Mantener una copia segura del archivo de configuración. * Las configuraciones importantes las deberá realizar solo personal suficientemente experimentado. *Establecer responsabilidades por el uso de los activos y documentar los procedimientos realizados.	UIOMSCE04	18	32	12
			UIOMSRE01	18	32	12
			UIOSGQE01	30	16	6
			UIOVLFE01	24	32	12
			UIOCLDE01	24	16	6
			UIOCRDE01	18	16	6
			UIOCAYE01	18	16	6
			UIOCLME01	18	16	6
			UIOQCHE01	18	16	6
			UIOGMNE01	24	16	6
			UIOLBTE01	18	16	6
			UIOLCLE01	24	16	6
			UIOLNVE01	18	16	6
			UIOMCHE01	18	16	6
			UIOMSCE02	18	12	6
			UIOMSCE03	18	12	6
			UIOMNJE01	24	16	6
			UIOQCNE02	18	12	6
			UIOSNIE01	18	16	6
			UIOTMBE01	18	16	6
Espionaje remoto y escucha encubierta	* No se cuenta con sistemas IDS o IPS. * Se utiliza Telnet para conexiones remotas, los datos se transmiten en texto plano.	* Es necesaria la implementación de un sistema IPS, planes de contingencia y políticas ante ataques informáticos. *Deshabilitar puertos e interfaces no utilizados, así como servicios innecesarios. * Siempre que sea posible utilizar SSH , HTTPS para conexiones remotas con fines administrativos .	UIOINQP01	50	125	20
			UIOMSCP01	50	125	20
			UIOINQE01	18	80	15
			UIOQCNP01	50	125	20
Falla de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	*Establecer un cronograma de mantenimiento preventivo y correctivo de equipos (definir fechas y responsables).	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNP01	25	125	15
Falsificación de derechos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. *Limitar el número de intentos de acceso fallidos a la administración de los dispositivos.	UIOINQP01	20	125	15
			UIOMSCP01	20	125	15

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 8 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Falsificación de derechos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. *Limitar el número de intentos de acceso fallidos a la administración de los dispositivos.	UIOPTDE01	30	32	12
			UIOEEPE01	27	32	12
			UIOQCNP01	20	125	15
Fenómenos sísmicos	* La infraestructura del nodo no está diseñada para soportar este tipo de eventos.	* Transferir el riesgo.	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNE01	25	48	12
			UIOCCLE01	20	48	12
			UIOINQE01	25	80	15
			UIOMSCE01	25	32	12
			UIOCTCE01	20	32	12
			UIOCBYE01	20	32	12
			UIOPTDE01	25	32	12
			UIOGJLE01	20	32	12
			UIOLLZE01	20	32	12
			UIOVLFE01	20	32	12
			UIOCLDE01	20	16	6
			UIOGMNE01	20	16	6
			UIOLCLE01	20	16	6
			UIOMNJE01	20	16	6
			UIOQCNP01	25	125	15
			UIOSGQE01	25	16	6
Filtraciones de agua	* No se cuenta con una correcta evacuación del agua utilizada en el sistema de climatización.	* Dar mantenimiento, reparar o sustituir el sistema de climatización para evitar este problema.	UIOMSCP01	20	125	15
			UIOQCNP01	20	125	15
Hurto de equipos	* Seguridad física insuficiente. * Equipo no cuenta con *rack* cerrado. * Falta de vigilancia interna.	* Se debe mejorar la seguridad física en el nodo. * Los equipos deberán estar en un *rack* cerrado.	UIOMSCE01	25	32	12
			UIOPTDE01	25	32	12
			UIOCBYE01	20	32	12
			UIOGJLE01	20	32	12
			UIOCLDE01	20	16	6
			UIOGMNE01	20	16	6
			UIOMNJE01	20	16	6

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 9 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Hurto de equipos	* Seguridad física insuficiente. * Falta de vigilancia interna.	* Mejorar la seguridad física en el nodo (cámaras, registros de entrada y salida).	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNE01	25	48	12
			UIOCCLE01	20	48	12
			UIOINQE01	25	80	15
			UIOLLZE01	20	32	12
			UIOCTCE01	20	32	12
			UIOVLFE01	20	32	12
			UIOLCLE01	20	16	6
			UIOQCNP01	25	125	15
			UIOSGQE01	25	16	6
Hurto de medios o documentos	* Descuido en el manejo de documentos y medios de información.	* Establecer responsabilidades y normas sobre el manejo de información importante.	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNP01	25	125	15
Incendio	* El sistema anti-incendios no es revisado periódicamente.	* El mantenimiento a los nodos deberá incluir la revisión y mantenimiento del sistema anti-incendios.	UIOINQP01	25	125	15
			UIOCCLE01	20	48	12
			UIOINQE01	25	80	15
			UIOCTCE01	20	32	12
			UIOCBYE01	20	32	12
			UIOGJLE01	20	32	12
			UIOLLZE01	20	32	12
			UIOGMNE01	20	16	6
			UIOLCLE01	20	16	6
	* No se cuenta con dispositivos anti-incendios. Únicamente un extintor.	* Se deberá instalar en el nodo un sistema anti-incendios.	UIOMSCP01	25	125	15
			UIOQCNE01	25	48	12
			UIOMSCE01	25	32	12
			UIOPTDE01	25	32	12
			UIOVLFE01	20	32	12
			UIOMNJE01	20	16	6
			UIOQCNP01	25	125	15
			UIOSGQE01	25	16	6
			UIOCLDE01	20	16	6
Incumplimiento en la disponibilidad del personal	* El personal es insuficiente.	* Contratar más personal con el objetivo de cumplir todos los requerimientos de la red y de los clientes.	UIOINQP01	20	125	15
			UIOMSCP01	20	125	15
			UIOQCNP01	20	125	15
Mal funcionamiento de los equipos	* Falta de mantenimiento, no se realiza periódicamente.	*Establecer un cronograma de mantenimiento preventivo y correctivo de equipos (definir fechas y responsables).	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNE01	20	48	12
			UIOINQE01	20	80	15
			UIOMSCE01	20	32	12
			UIOPTDE01	20	32	12
			UIOQCNP01	25	125	15
			UIOSGQE01	20	16	6

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 10 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Negación de acciones	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo.	UIOPTDE01	30	32	12
			UIOCCLE01	24	48	12
			UIOEEPE01	18	32	12
			UIOGJLE01	24	32	12
			UIOSGQE01	30	16	6
			UIOLCLE01	24	16	6
			UIOCLDE01	24	16	6
			UIOMNJE01	24	16	6
	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con el respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración.	UIOLCSE01	18	32	12

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 11 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Negación de acciones	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOINQP01	60	125	25
			UIOMSCP01	60	125	25
			UIOQCNE01	30	48	12
			UIOINQE01	30	80	15
			UIOMSCE01	30	32	12
			UIOQCNP01	60	125	25
			UIOCNDE01	18	32	12
			UIOCTCE01	24	32	12
			UIOCBYE01	24	32	12
			UIOEETE01	18	24	9
			UIOINQE02	18	24	9
			UIOLFLE01	18	32	12
			UIOLLZE01	24	32	12
			UIOLPZE01	18	32	12
			UIOMSCE04	18	32	12
			UIOMSRE01	18	32	12
			UIOVLFE01	24	32	12
			UIOCRDE01	18	16	6
			UIOCAYE01	18	16	6
			UIOCLME01	18	16	6
			UIOQCHE01	18	16	6
			UIOGMNE01	24	16	6
			UIOLBTE01	18	16	6
			UIOLNVE01	18	16	6
			UIOMCHE01	18	16	6
			UIOMSCE02	18	12	6
			UIOMSCE03	18	12	6
			UIOQCNE02	18	12	6
			UIOSNIE01	18	16	6
			UIOTMBE01	18	16	6
Polvo y sobre-calentamiento	* No existe mantenimiento periódico del sistema de climatización. * Susceptibilidad al polvo y el calor.	* Establecer un cronograma de mantenimiento de los equipos de climatización.	UIOMSCP01	30	125	15
			UIOINQP01	20	125	15
			UIOQCNE01	20	48	12
			UIOINQE01	20	80	15
			UIOMSCE01	20	32	12
			UIOPTDE01	20	32	12
			UIOQCNP01	30	125	15
			UIOSGQE01	20	16	6
Saturación de la red	* Una gran cantidad de servicios dependen de este activo.	* Monitorizar constantemente el tráfico, buscar balancearlo.	UIOINQP01	25	125	15
			UIOMSCP01	25	125	15
			UIOQCNP01	25	125	15

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 12 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Saturación de la red	* Una gran cantidad de servicios dependen de este activo. * Falta de enlaces redundantes.	* Monitorizar constantemente el tráfico, buscar balancearlo. * Establecer redundancia a nivel de enlaces.	UIOINQE01	20	80	15
Uso no autorizado de equipos	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * No se cuenta con respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración.	UIOEEPE01	48	32	16
	* El acceso a la administración del dispositivo no se realiza mediante el ACS. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo, éste será conocido solo por el Responsable de la red.	UIOCCLE01	40	48	16
			UIOPTDE01	60	32	20
			UIOGJLE01	60	32	20
			UIOLCLE01	60	16	10
			UIOCLDE01	40	16	8
			UIOSGQE01	40	16	8
			UIOMNJE01	40	16	8

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 13 de 14)

AMENAZA	VULNERABILIDAD	CONTROLES	EQUIPO	RIESG	NI	PRIORIDAD
Uso no autorizado de equipos	* Falencias en el Sistema de Control de Acceso y en su configuración. * No se cuenta con respaldo del archivo de configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como método de autenticación de respaldo. * Mantener una copia segura del archivo de configuración.	UIOCNDE01	32	32	16
			UIOLCSE01	32	32	16
			UIOVLFE01	40	32	16
			UIOLNVE01	32	16	8
			UIOCLME01	32	16	8
	* Falencias en el Sistema de Control de Acceso y en su configuración. * Se tienen varios usuarios locales configurados en el equipo. * Falta de políticas para el control de acceso a la administración de los equipos.	* Implementar un modelo de políticas para el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. * El ingreso a la administración de los dispositivos de toda la red IP/MPLS de la CNT E.P. se deberá realizar únicamente a través del ACS. * Configurar únicamente un nombre de usuario local como respaldo. * Mantener una copia segura del archivo de configuración.. * Actualizar el Sistema de Control de Acceso para corregir falencias.	UIOINQP01	50	125	20
			UIOMSCP01	50	125	20
			UIOQCNE01	40	48	16
			UIOINQE01	40	40	16
			UIOMSCE01	40	32	16
			UIOCTCE01	40	32	16
			UIOCBYE01	40	32	16
			UIOEETE01	32	24	12
			UIOINQE02	32	24	12
			UIOLFLE01	32	32	16
			UIOLLZE01	40	32	16
			UIOLPZE01	32	32	16
			UIOMSCE04	32	32	16
			UIOMSRE01	32	32	16
			UIOCAYE01	48	16	8
			UIOQCNP01	50	125	20
			UIOCRDE01	32	16	8
			UIOQCHE01	32	16	8
			UIOGMNE01	40	16	8
			UIOLBTE01	32	16	8
			UIOMCHE01	18	16	6
			UIOMSCE02	32	12	8
			UIOMSCE03	32	12	8
			UIOQCNE02	32	12	8
			UIOSNIE01	32	16	8
			UIOTMBE01	32	16	8
			UIOLLZE02	24	12	6

Tabla 3.17: Tratamiento del Riesgo. Controles a implementar. (Página 14 de 14)

Como se pudo apreciar, el control sugerido para contrarrestar la amenaza referente a fenómenos sísmicos es transferir el riesgo que ésta supone, ya que reducirlo implicaría reconstruir o construir nuevas instalaciones para que soporten o minimicen estos fenómenos.

Una vez identificados los controles y su prioridad de implementación, se debe tomar mayor interés en los resultados de color rojo, pues son los más prioritarios se sugiere iniciar inmediatamente la aplicación de los controles y las medidas a aplicar en estos equipos, según las posibilidades y necesidades del área O&M Plataforma IP/MPLS.

Los ataques informáticos constituyen amenazas que generan alto riesgo y dependiendo del valor del activo, se constituyen en las amenazas que se recomienda atender con un mayor nivel de prioridad.

CAPÍTULO 4

PROPUESTA DE MEJORAMIENTO DEL CONTROL DE ACCESO A LA ADMINISTRACIÓN DE LOS DISPOSITIVOS DE LA RED IP/MPLS DE LA CNT E.P.

Con la finalidad de mejorar el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P., así como evitar el acceso no autorizado y minimizar los riesgos que esto implica, se resumen a continuación algunos procedimientos que se desarrollan a lo largo del presente capítulo.

Se establecen normas y procedimientos que regulen el acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P. los cuales podrían pasar a constituir una política formal.

Se redefinen los atributos en los cuales basa su funcionamiento el Sistema de Control de Acceso, adaptándolos a los requerimientos y necesidades del área O&M Plataforma IP/MPLS y las otras áreas relacionadas con la administración de los dispositivos de la red IP/MPLS de la CNT E.P.

Se propone la actualización del Sistema de Control de Acceso a la versión más reciente que permita aplicar los atributos redefinidos antes mencionados y corregir las falencias y errores de funcionamiento del sistema actual, descritos en el Capítulo 2, sección 2.5.3.3 del presente Proyecto de Titulación. Como parte de dicha propuesta se realiza una guía de configuración del Sistema de Control de Acceso Cisco v5.2, que incluye las principales recomendaciones para mejorar el control de acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P.

La implementación de esta propuesta se deja a criterio del área O&M Plataforma IP/MPLS.

4.1 NORMAS Y PROCEDIMIENTOS PARA EL ACCESO A LA ADMINISTRACIÓN DE LOS DISPOSITIVOS DE LA RED IP/MPLS DE LA CNT E.P.

4.1.1 NORMAS GENERALES

- El acceso local y remoto a la administración de los dispositivos de la red IP/MPLS se realizará por medio de un nombre de usuario y contraseña, manejados a través del sistema de control de acceso. Se deberá contar con un sistema secundario, con la finalidad de ofrecer alta disponibilidad.

- El acceso remoto a la administración de los dispositivos de la red IP/MPLS se realizará únicamente mediante el protocolo SSH. Se prohíbe utilizar Telnet a menos que las capacidades del equipo lo requieran.

- Como medida de precaución, en caso de que se perdiera la conexión tanto con el Sistema de Control de Acceso primario como con el secundario, se configurará un único usuario local y contraseña en cada equipo de la red IP/MPLS con la finalidad de tener un medio de acceso adicional a su administración. Este usuario local será de conocimiento exclusivo del Responsable de la red.

- Se deberán limitar los tiempos de conexión al horario normal de oficina, excepto para aquellos usuarios con requerimientos operativos de horas extra de trabajo.

- Se deberá desplegar un aviso general advirtiendo que el acceso está permitido solo para personal autorizado y que se registrará, monitoreará y perseguirá cualquier tipo de acceso no autorizado.

- Se deberá evitar desplegar mensajes que pudieren asistir a un tipo de usuario no autorizado durante el proceso de conexión.

- La información que ingrese la persona que esté deseando establecer una conexión deberá ser validada una vez que éste haya ingresado los datos en su totalidad, de tal forma que el sistema no indique algún indicio de qué parte de los datos es correcta o incorrecta.

- Para acceder a la administración del Sistema de Control de Acceso será necesario contar con una cuenta provista por el Administrador del mismo.

- Se deberá limitar el tiempo máximo permitido para el procedimiento de conexión; si éste es excedido el Sistema de Control de Acceso deberá bloquear la conexión inmediatamente.

- Se deberá registrar el número de intentos de conexión no exitosos en el Sistema de Control de Acceso.

- El acceso a la administración de los dispositivos de la red IP/MPLS y del Sistema de Control de Acceso desde una red pública estará permitido únicamente a través de una VPN específica para el efecto. A esta VPN únicamente podrán ingresar el Administrador y personal del Área.

4.1.2 DEL SISTEMA DE CONTROL DE ACCESO

Objetivo: Llevar a cabo una correcta administración del Sistema de Control de Acceso, con la finalidad de evitar y detectar el acceso de usuarios no autorizados.

4.1.2.1 De los Administradores

- Se denomina Administrador al encargado de configurar, monitorear y garantizar que los parámetros configurados en el Sistema de Control de Acceso cumplan con las normas y procedimientos para el acceso a la administración de los dispositivos de la red IP/MPLS.

- El Administrador será el encargado de asignar los nombres de usuario y contraseñas al personal que requiera acceder a la administración de los

dispositivos de la red IP/MPLS.

- Eventualmente, el Administrador podrá delegar sus funciones o parte de ellas a personal del Área, con la finalidad de distribuir el trabajo. Para delegar funciones se crearán cuentas de administración las cuales deberán seguir los lineamientos de nombre de usuario y contraseña.

- Si una cuenta de administración ha estado inactiva por 30 días se solicitará el cambio de contraseña y si la cuenta ha estado inactiva por 60 días se la deshabilitará.

4.1.2.2 De la Administración de Usuarios

- Se denominan usuarios al personal de la CNT E.P. que requiere acceso a la administración de los dispositivos de la red IP/MPLS y que para ello necesita de una cuenta en el Sistema de Control de Acceso.

- Se deberán asignar identificadores únicos de usuario, de manera que cada usuario sea responsable de las acciones que con dicho identificador se realicen y garantizar así el no repudio. Se podrá permitir identificadores grupales cuando sea conveniente debido a razones operativas, siempre y cuando exista responsabilidad de una persona que represente a dicho grupo.

- El identificador único de usuario se basará en el nombre del usuario, así pues, el identificador estará compuesto por la inicial del nombre seguido de su primer apellido, todo en minúsculas.

Ejemplo: Nombre de Usuario: Pedro Larrea Bustamante

Identificador de Usuario: plarrea

- De existir dos o más usuarios con las mismas características de nombre y apellido, se utilizará al final un número basado en el orden de registro,

empezando en “1” con el primer usuario.

Ejemplo:	Nombre de Usuario:	Pablo Larrea Heredia
	Identificador de Usuario:	plarrea1
	Nombre de Usuario:	Patricia Larrea Ortiz.
	Identificador de Usuario:	plarrea2

- En caso de requerir un identificador grupal se deberá asignar un nombre que identifique al grupo o a las actividades operativas que se vayan a desarrollar. Por ejemplo pruebas_huawei, pruebas_alcatel.

- El Administrador al ingresar un nuevo usuario le asignará una contraseña provisional, la cual deberá ser obligatoriamente cambiada por el usuario en el primer acceso.

- Los usuarios se manejarán en grupos para facilitar las acciones referentes a asignación y gestión de privilegios de acceso.

- Quienes requieran de un identificador de usuario para acceder a la administración del Sistema de Control de Acceso o de los dispositivos de la red IP/MPLS, deberán emitir una solicitud dirigida al Jefe del Área con copia al Administrador, indicando el área a la que pertenecen, las actividades a realizar, y el tiempo de concesión necesario. Tras analizar la solicitud en conjunto y de ser aprobada, el Administrador designará el nombre de usuario y contraseña provisional; le asignará un grupo de usuario y los permisos de acceso correspondientes. En caso de que la solicitud no sea aprobada se deberá notificar al solicitante el por qué de la negativa.

- Se deberán bloquear las cuentas de aquellos usuarios que intenten por tercera vez consecutiva ingresar a la administración de los dispositivos de la red IP/MPLS sin conseguirlo.

- En caso de requerirse una asignación de una nueva contraseña de usuario por olvido, caducidad de la cuenta o por superar el máximo número de intentos fallidos de acceso, el usuario deberá solicitarla al Administrador, quien una vez que verifique los datos del usuario procederá a realizar dicha asignación.

- Se deberá contar con un registro de todas las cuentas de usuario a las cuales se les haya otorgado acceso a la administración del Sistema de Control de Acceso o de los dispositivos de la red IP/MPLS. Se registrará información relevante de cada usuario, nombres completos, identificador de usuario, área a la que pertenece, funciones, fecha de activación y caducidad de la cuenta de usuario.

- Se deberán inhabilitar inmediatamente las cuentas de usuario de aquellos empleados que cambien sus funciones dentro de la empresa, dejen de pertenecer a la misma o por algún otro motivo en particular.

- Si una persona que asciende en sus funciones dentro de la empresa, desea modificar sus permisos de acceso a la administración de los dispositivos de la red IP/MPLS, deberá realizar una solicitud dirigida al Jefe del Área O&M Plataforma IP/MPLS con copia al Administrador, quienes se encargarán de verificar tal ascenso y aprobar dicha solicitud. El Administrador modificará y registrará los permisos de acceso de acuerdo a las nuevas funciones de trabajo del solicitante.

- El Administrador deberá efectuar un control periódico de las cuentas de usuario que hayan sido configuradas, con el fin de eliminar aquellas que hayan sido inhabilitadas y ya no vayan a utilizarse, o habilitar aquellas que así lo requieran. Una cuenta se deshabilitará cuando ha cumplido su fecha de caducidad o cuando se registren varios intentos fallidos de acceso.

4.1.2.3 De la Administración de Dispositivos

- Los dispositivos constituyen todos los equipos de la red IP/MPLS para los

cuales el acceso a su administración se proveerá a través del Sistema de Control de Acceso.

- Para llevar a cabo una gestión óptima se agruparán a los dispositivos según criterios de localización, marca y funcionalidad.

- Los equipos de la red IP/MPLS deberán ser configurados para enviar las peticiones al Sistema de Control de Acceso secundario en caso de no poder conectarse con el primario. En caso de perderse la conexión también al secundario se deberá tener configurado un usuario local en cada equipo de la red.

4.1.2.4 De la Administración de Privilegios

- Los privilegios constituyen el nivel de acceso y conjunto de comandos permitidos dependiendo del grupo de usuario y condiciones de horario, de localización, marca o funcionalidad del dispositivo al que un usuario requiere administrar.

- Se limitará y controlará la asignación y uso de privilegios, puesto que el abuso o desconocimiento de los permisos de acceso otorgados, constituyen frecuentemente uno de los factores más importantes para que se cometan alteraciones o irregularidades en las funciones de trabajo.

- El Jefe del Área O&M Plataforma IP/MPLS deberá registrar y acordar con los jefes de cada una de las otras áreas de la CNT E.P., que soliciten acceso a la administración de los dispositivos de la red IP/MPLS, los requerimientos para poder cumplir a cabalidad sus funciones de trabajo. En estos requerimientos se deberán definir los equipos y el horario de trabajo en los cuales se solicite acceso, y los comandos que se requieran ejecutar al ingresar a la administración de los dispositivos de la red IP/MPLS.

- Los privilegios acordados con cada una de las áreas de la CNT E.P. estarán sujetos a cambios, ya sea por reestructuración de la empresa o modificación de las obligaciones y responsabilidades de las áreas.

- Se deberá contar con un registro de los privilegios de acceso otorgados tanto al personal del Área O&M Plataforma IP/MPLS y de las otras áreas de la CNT E.P., vinculadas a la administración de los dispositivos de la red IP/MPLS.

4.1.2.5 De la Administración de Contraseñas

- El Sistema de Control de Acceso deberá verificar que se cumplan los parámetros de calidad de las contraseñas que se indican en la sección 4.1.3.

- El Sistema de Control de Acceso deberá notificar al usuario la cercanía de caducidad de su contraseña y solicitar al usuario el cambio de la misma. En caso de no cambiarse la contraseña, el Sistema deberá deshabilitar la cuenta del usuario.

4.1.2.6 Del Monitoreo y Reporte de Actividades

- Se deberá monitorear las actividades realizadas en la administración de los dispositivos de la red IP/MPLS registrando:

  - ✓ Los usuarios que acceden o intentan acceder a la administración de los dispositivos de la red IP/MPLS.

  - ✓ El grupo de usuarios del que forma parte el usuario que se autentica satisfactoriamente.

  - ✓ El nivel de privilegio con el que accede un usuario.

  - ✓ El nombre del dispositivo al que se accede o se intenta acceder.

  - ✓ Los comandos que se ejecuten o se intenten ejecutar.

  - ✓ Fecha y hora de inicio y terminación de cada una de las sesiones establecidas y no establecidas.

- ✓ Dirección IP desde donde se inicia la conexión y la dirección IP del equipo con el que se establece la conexión.
- ✓ El protocolo utilizado en la autenticación.

- Se recomienda contar con un respaldo de los registros, estos registros deberán estar debidamente protegidos y tendrán acceso a ellos únicamente el Administrador y el Jefe del Área.
- Se establecerá la revisión periódica de estos registros con la finalidad de detectar anomalías en el acceso a la administración de los dispositivos de la red IP/MPLS.
- Se deberán emitir alarmas ante incidentes como: número máximo de intentos de conexión fallidos, ingreso de comandos no autorizados, anomalías en el funcionamiento del Sistema de Control de Acceso; estas alarmas deberán ser notificadas al Administrador, ya sea vía correo electrónico o almacenadas en un servidor de *logs* externo.

4.1.2.7 De la Ubicación

- Tanto el Sistema de Control de Acceso principal como el secundario, deberán estar ubicados en *racks* cerrados en los nodos más seguros de la Corporación bajo condiciones de climatización adecuadas y con provisión de energía ininterrumpida.
- Tanto el Sistema de Control de Acceso principal como el secundario, deberán conectarse directamente a la red IP/MPLS, para así no depender de otras redes de la Corporación; por seguridad se deberán ubicar detrás de un *Firewall*.

4.1.3 DE LAS CONTRASEÑAS

Objetivo: Fortalecer el acceso a la administración de los dispositivos de la red

IP/MPLS de la CNT E.P., mediante la regulación del uso de contraseñas y medidas para robustecer las mismas.

A continuación se indican los lineamientos para regular el uso de contraseñas en la red IP/MPLS.

- Se prohíbe que las claves provisorias asignadas por el Administrador del Sistema de Control de Acceso a los usuarios para su primer uso sean las mismas para todos, es decir, deberán proveerse contraseñas temporales únicas para cada usuario.
- Se prohíbe almacenar contraseñas en sistemas de computación o en algún otro dispositivo sin ningún tipo de protección.
- Deberán ser cambiadas todas las contraseñas que vienen por defecto configuradas en el software de los equipos de la red IP/MPLS y del Sistema de Control de Acceso.
- No se deberá mostrar las contraseñas en pantalla en texto plano cuando se estén digitando.
- Las contraseñas ingresadas no deberán estar almacenadas en texto plano, se deberán utilizar métodos de encriptación de claves.

Con la finalidad de que se manejen contraseñas robustas se deberán cumplir los siguientes requerimientos:

- Las contraseñas deberán tener como mínimo 10 caracteres, tanto alfanuméricos como no alfanuméricos, es decir, mayúsculas, minúsculas, números y símbolos.
- No se deberá usar el nombre de usuario como parte de la contraseña.
- No se deberán utilizar caracteres repetidos consecutivamente.

- Se deberá exigir el cambio de contraseñas provisionales en el primer uso.
- Cuando se requiera cambiar la contraseña, la nueva no podrá ser la misma que las dos últimas contraseñas utilizadas.
- Se deberá exigir el cambio de contraseñas cada 45 días.
- Las contraseñas de configuración de servicios de los equipos de conectividad como, SNMP, IS-IS, AAA, VTP, etc. deberán ser de al menos 12 caracteres alfanuméricos y no alfanuméricos y se deberá utilizar el nivel de encripción más alto posible disponible en los dispositivos de red.

4.1.4 DE LAS RESPONSABILIDADES DEL USUARIO

Objetivo: Concientizar y formar al personal vinculado con la administración del Sistema de Control de Acceso y de los dispositivos de la red IP/MPLS, sobre la importancia de la aplicación de las normas y procedimientos descritos.

- Se deberá proporcionar a cada uno de los usuarios que se le otorgue acceso, un documento escrito en el cual se indique cuáles son sus responsabilidades al acceder a la administración del Sistema de Control de Acceso o de los dispositivos de la red IP/MPLS. Por lo cual, será necesario mantener una copia firmada por el usuario aceptando las condiciones establecidas en tal documento, esto con la finalidad de que quede constancia de lo descrito.
- Es fundamental que en los contratos del personal de trabajo se estipulen las sanciones pertinentes a intentos de acceso o accesos no autorizados a la administración del Sistema de Control de Acceso o a los dispositivos de la red IP/MPLS de la CNT E.P.

4.1.4.1 Uso de contraseñas

Las contraseñas constituyen el medio de validación y autenticación de la identidad

de un usuario. La principal estrategia para que los usuarios utilicen sus contraseñas de forma segura, es que reciban información sobre su correcto uso, para ello se establecen los siguientes lineamientos:

- Formar a los usuarios en la selección y empleo de sus contraseñas, para garantizar que las mismas tengan robustez frente a intentos de usurpación; se deberá cumplir con los requerimientos establecidos en la sección 4.1.2.5.

- Concientizar a los usuarios acerca de la importancia de mantener su contraseña confidencial, y de que la revelación de la misma supondría una suplantación de su identidad digital, que puede tener repercusiones disciplinarias y legales.

- Las contraseñas deberán ser de conocimiento exclusivo de cada persona dueña de una cuenta de usuario o del grupo de trabajo, en caso de tratarse de una contraseña grupal; es decir, se debe mantener en absoluta confidencialidad.

- El usuario deberá cambiar inmediatamente la contraseña, ante un posible indicio de compromiso del uso de su cuenta de usuario.

- Se deberá evitar el uso de contraseñas utilizadas para otro tipo de actividades, como correo electrónico, redes sociales, etc.

- Seleccionar contraseñas que al usuario le resulten fáciles de recordar y no verse en la necesidad de mantenerlas escritas en sus estaciones de trabajo o en algún otro lado para su uso.

- No incluir en sus contraseñas datos demasiado obvios, que a terceros les resultare fácil adivinar, como fechas de cumpleaños, números telefónicos, nombres de familiares cercanos, etc.

- Las contraseñas deberán ser cambiadas cada vez que se solicite, además se deberá evitar reutilizar contraseñas que hayan sido empleadas en

ocasiones anteriores.

- Se deberá acatar la orden de cambiar las contraseñas en el primer uso.

4.1.4.2 Escritorio limpio y seguridad de equipo desatendido

- El escritorio del equipo informático y el entorno de trabajo de los usuarios que requieren acceso a la administración de los dispositivos de la red IP/MPLS y del Sistema de Control de Acceso, son dos elementos cuyo uso inapropiado puede generar amenazas como acceso a información confidencial por personas no autorizadas, robos de información o suplantación de identidad.

- Los requisitos y procedimientos de seguridad en cuanto a escritorio limpio y seguridad de equipo desatendido, están enfocados al personal del Área O&M Plataforma IP/MPLS; sin embargo, pueden ser tomados como referencia y ser informados para su aplicabilidad a las otras áreas de la CNT E.P. vinculadas a la administración de la red.

- Se debe adoptar una política de escritorio limpio de papeles y medios de almacenamiento extraíbles, una política de pantalla limpia para las aplicaciones informáticas, así como normas de seguridad para proteger la información cuando el usuario abandona el entorno de trabajo. Para lo cual se deben acatar los siguientes puntos:

  - ✓ Si una estación de trabajo se encuentra en inactividad por más de 5 minutos o el usuario debe abandonar su puesto de trabajo, se deberá habilitar inmediatamente el protector de pantalla, el cual requiera de una contraseña personal para volver a continuar con la sesión.

  - ✓ Se deberá exigir al personal del área que terminada su jornada laboral apague las estaciones de trabajo, salvo el caso de que por algún motivo en particular se requiera dejar la máquina encendida; de ser así, se deberá dejar con el protector de pantalla activado y

que requiera de una contraseña personal para inicio de sesión.

- ✓ Toda información que se considere importante y sensible sobre la red, el Área, o toda la empresa, esté impresa o almacenada en algún dispositivo de almacenamiento electrónico, deberá permanecer bajo llave, a la que solo tendrá acceso el Jefe de Área.

4.1.4.3 Manejo de medios

- Se debe tener especial cuidado con el uso de medios que puedan comprometer seriamente información confidencial en cuanto al acceso a la administración de los dispositivos de la red IP/MPLS. Se pueden considerar como medios: *Notebooks*, *Laptops*, teléfonos celulares, tarjetas de memorias, dispositivos de almacenamiento removibles tales como CDs, DVDs, o cualquier otro dispositivo de almacenamiento de conexión USB, entre otros.

- Los medios son frecuentemente susceptibles a incidentes de pérdida, robo o hurto, es por ello que el personal que haga uso de este tipo de dispositivos deberá tener especial cuidado y no poner en riesgo la información contenida en ellos, para lo cual es preciso que se acaten las siguientes recomendaciones:

- Se deberá permanecer cerca del dispositivo móvil y evitar dejarlos desatendidos.

- No llamar la atención acerca de portar equipos valiosos al encontrarse en lugares públicos.

- Evitar poner en los equipos identificaciones relacionadas con la empresa.

- Se deberá reportar inmediatamente al Jefe del Área cualquier incidente suscitado con alguno de los dispositivos móviles propiedad de la

empresa, con la finalidad tomar acciones preventivas al respecto.

4.1.5 DE LOS MEDIOS Y DISPOSITIVOS

Objetivo: Garantizar la seguridad física de los equipos y medios, así como de la información contenida en éstos.

4.1.5.1 Identificación de los equipos en las redes

- Los dispositivos de la red IP/MPLS deberán permitir identificar su función dentro de la red, ser inventariados y permanecer en un lugar con acceso restringido a personal no autorizado.

- El identificador se relacionará con la provincia y nodo donde esté ubicado el equipo y con su función dentro de la red. Es necesario considerar que al ver el identificador del equipo se deberá tener una percepción de su importancia dentro de la red.

  Por ejemplo:

  PROVINCIA: PICHINCHA (Quito)

  NODO: MARISCAL

  FUNCIÓN: EQUIPO P

  } **IDENTIFICADOR**: UIOMSCP01

4.1.5.2 Medidas de reemplazo, reutilización y eliminación de medios y dispositivos

- Cuando un medio o equipo vaya a ser reemplazado, desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él.

- Deben ser objeto de un proceso de eliminación o borrado de los datos que almacenan, para evitar posteriores accesos no autorizados a la información que contienen, que puedan comprometer la seguridad en el acceso a la administración de los dispositivos de la red IP/MPLS o del Sistema de Control de Acceso; previamente se procederá a su baja en el inventario.

4.1.5.3 Protección contra fallos en el suministro eléctrico

- Todos los nodos de la red IP/MPLS deberán disponer de un suministro ininterrumpido de energía, con la finalidad de garantizar la continuidad del servicio.

- Se debe contar con un diseño adecuado del sistema de suministro eléctrico provisto por el área encargada de esta labor, incluyendo sistemas reguladores de tensión y sistemas de respaldo (UPS's) para suministrar energía estabilizada en caso de fallo en el suministro.

4.1.5.4 Aseguramiento físico

Se deben tener en cuenta las siguientes normas de seguridad física de los dispositivos de la red IP/MPLS.

- Los dispositivos de la red IP/MPLS deberán estar ubicados en *racks* cerrados.

- El acceso a los nodos de la red IP/MPLS deberá ser estrictamente controlado y se mantendrán registros del personal que accede a las instalaciones.

- En los nodos principales o en aquellos en donde la afluencia de personal es considerable se recomienda la instalación de cámaras de seguridad.

4.2 REDEFINICIÓN DE ATRIBUTOS DEL SISTEMA DE CONTROL DE ACCESO

Se ha visto necesario redefinir los atributos en los cuales basa su funcionamiento el Sistema de Control de Acceso, con la finalidad de cubrir los requerimientos del Área y mejorar el control de acceso a la administración de los dispositivos de la red IP/MPLS.

4.2.1 GRUPOS DE DISPOSITIVOS

Para llevar un registro ordenado de los equipos que conforman la red IP/MPLS y cumpliendo con lo establecido en la sección 4.1.2.3, se propone clasificarlos por su función dentro de la red IP/MPLS, por la marca del dispositivo y puesto que la estructura actual de la CNT E.P. está dada por Regiones también por su localización. Los equipos utilizados para el acceso a la red IP/MPLS se los considerará en adelante como parte de ésta.

4.2.1.1 Grupos de dispositivos de la red IP/MPLS según su función

En la tabla 4.1 se plantean los subgrupos de dispositivos que se deberán crear de acuerdo a la función que cumplen dentro de la red IP/MPLS.

SUBGRUPO	DESCRIPCIÓN
Equipos P	Equipos tipo P de la red IP/MPLS.
Equipos PE	Equipos tipo PE de la red IP/MPLS.
Equipos L2	Equipos de capa 2 para el acceso a la red IP/MPLS.
Equipos RR	Equipos *Route Reflectors* de la red IP/MPLS.

Tabla 4.1: Equipos de la red IP/MPLS agrupados por su función

4.2.1.2 Grupos de dispositivos de la red IP/MPLS según su marca

El área O&M Plataforma IP/MPLS tiene planificado la ampliación de la red IP/MPLS incluyendo equipos de las marcas Huawei y Alcatel, por lo que se propone que los dispositivos de la red deben estar clasificados en tres subgrupos según su marca como lo indica la tabla 4.2.

SUBGRUPO	DESCRIPCIÓN
Alcatel	Equipos de la marca Alcatel.
Cisco	Equipos de la marca Cisco.
Huawei	Equipos de la marca Huawei.

Tabla 4.2: Equipos de la red IP/MPLS agrupados por su marca

4.2.1.3 Grupos de dispositivos de la red IP/MPLS según su localización

La nueva estructura política del Estado, unifica las 24 provincias a través de 7 regionales, y puesto que la CNT E.P. adopta esta estructura al ser una empresa pública, se propone que los dispositivos de la red deberán estar agrupados también por regionales. La tabla 4.3 contiene los subgrupos en los cuales se propone clasificar a los dispositivos según la regional en la que se localizan.

SUBGRUPO	PROVINCIAS	DESCRIPCIÓN
Regional R1	IMBABURA, ESMERALDAS,CARCHI, SUCUMBÍOS.	Equipos localizados en la Regional 1.
Regional R2	PICHINCHA, NAPO, ORELLANA.	Equipos localizados en la Regional 2.
Regional R3	TUNGURAHUA, PASTAZA, COTOPAXI, CHIMBORAZO.	Equipos localizados en la Regional 3.
Regional R4	SANTO DOMINGO, GALÁPAGOS, MANABÍ.	Equipos localizados en la Regional 4.
Regional R5	GUAYAS, SANTA ELENA, LOS RÍOS, BOLÍVAR.	Equipos localizados en la Regional 5.
Regional R6	AZUAY, CAÑAR, MORONA SANTIAGO.	Equipos localizados en la Regional 6.
Regional R7	EL ORO, LOJA, ZAMORA CHINCHIPE.	Equipos localizados en la Regional 7.

Tabla 4.3: Equipos agrupados de acuerdo a su localización

En la figura 4.1 se puede apreciar de forma resumida la clasificación de los dispositivos de la red IP/MPLS.

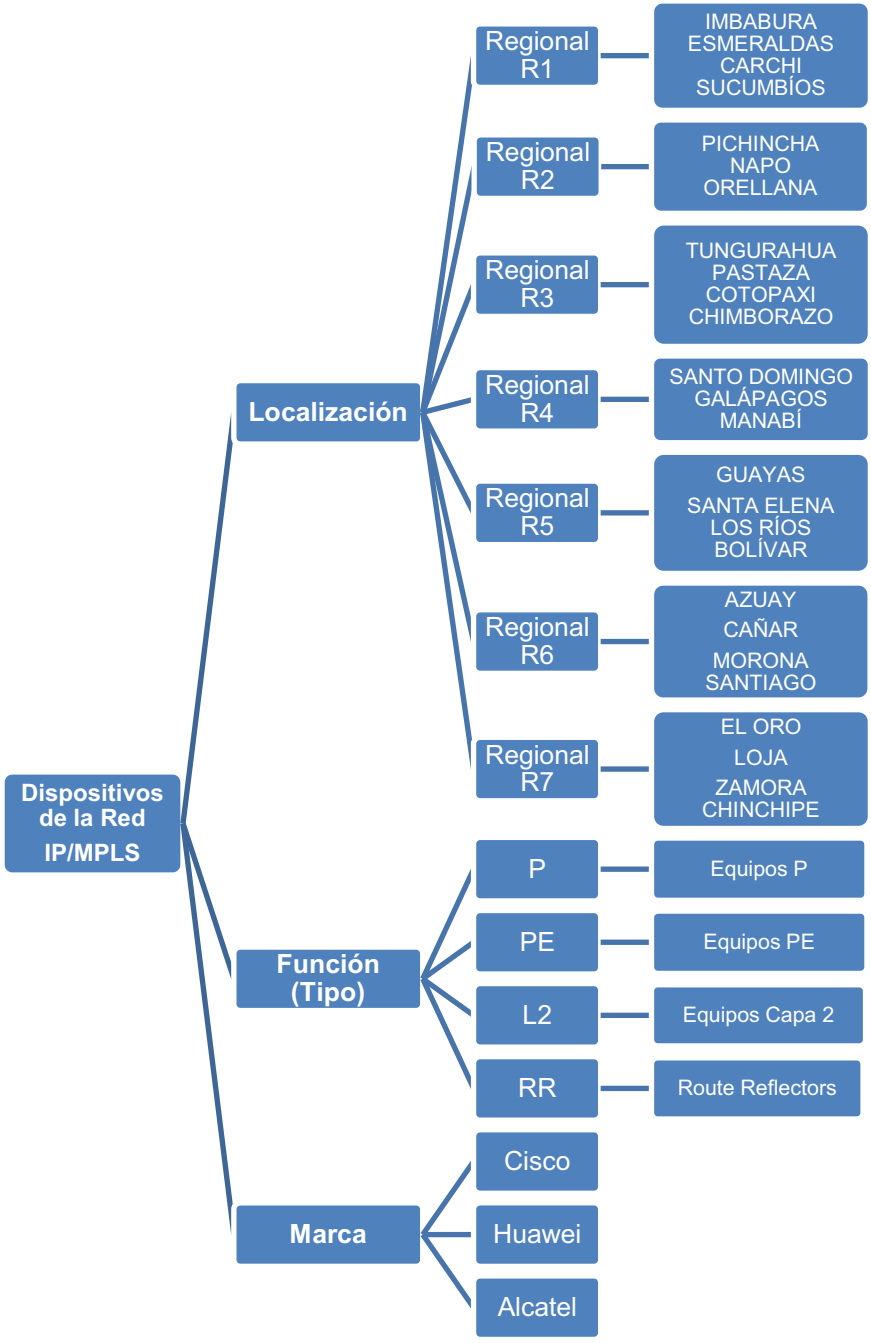


Figura 4.1: Agrupación de los dispositivos de la red IP/MPLS, considerando su localización, función y marca

4.2.2 GRUPOS DE USUARIOS

La creación de grupos de usuarios propuesta está de acuerdo a los grupos de trabajo de la CNT E.P. que necesitan tener acceso a los dispositivos de la red IP/MPLS, los cuales en coordinación con el Responsable de la red IP/MPLS fueron redefinidos.

Se ha creído conveniente además subdividir al Área O&M Plataforma IP/MPLS en dos subgrupos: Nivel1 y Nivel2, de tal forma que se puedan proveer diferentes tipos de privilegios.

Los grupos de usuarios que se proponen son:

- ***CALL CENTER***.- Usuarios del área de trabajo *Call Center*.
- **NOC**.- Usuarios del área de trabajo NOC.
- **INGENIERÍA**: Usuarios del área de trabajo Ingeniería.
- **GESTIÓN RED:** Usuarios del área de trabajo Gestión de Red.
- **O&M DATOS, INTERNET, TV y TELEF**: Usuarios del área de trabajo O&M soluciones datos, Internet, televisión y telefonía, antes conocidos como Gestión XDSL.
- **REG 1**: Personal de la Regional 1 encargados de monitorizar los equipos de su respectiva región.
- **REG 2:** Personal de la Regional 2 encargados de monitorizar los equipos de su respectiva región; cabe indicar que este grupo de usuarios era conocido como Multiservicios, pero como la reestructuración de la CNT E.P. pasaron a formar parte de la Regional 2.
- **REG 3:** Personal de la Regional 3 encargados de monitorizar los equipos de su respectiva región.

- **REG 4**: Personal de la Regional 4 encargados de monitorizar los equipos de su respectiva región.

- **REG 5:** Personal de la Regional 5 encargados de monitorizar los equipos de su respectiva región.

- **REG 6**: Personal de la Regional 6 encargados de monitorizar los equipos de su respectiva región.

- **REG 7**: Personal de la Regional 7 encargados de monitorizar los equipos de su respectiva región.

- **DESCA:** Personal de la empresa DESCA encargados de dar soporte a los equipos (Cisco) de la red IP/MPLS provistos por dicha empresa.

- **MPLS_Nivel1**.- Estará formado por personal nuevo que se integra al Área y por el personal de trabajo que administra la red del Pacífico de la ex Pacifictel y que con la absorción de esta red por parte de la red IP/MPLS de la CNT E.P. necesitan acceder a la administración de sus dispositivos mediante el Sistema de Control de Acceso.

- **MPLS_Nivel2**.- Personal del área O&M Plataforma IP/MPLS que administra la red y que tiene la suficiente experiencia, conocimientos y responsabilidad para tener acceso total a los equipos.

4.2.3 PERFILES DE ACCESO

En base a los requerimientos del área O&M Plataforma IP/MPLS, en cuanto a la redefinición de los perfiles de acceso otorgados para la administración de los dispositivos de la red, a continuación se determinan los elementos necesarios para manejar el acceso a la administración de los dispositivos de la red.

4.2.3.1 Perfil de acceso

Es el perfil otorgado al usuario, dependiendo de ciertas condiciones en base al

cual accederá a la administración de los dispositivos de la red IP/MPLS. El perfil de acceso definirá el nivel de acceso y el conjunto de comandos asignados.

4.2.3.2 Condiciones de acceso

En base a las cuales se otorga un perfil de acceso a un usuario o grupo de usuarios. Las siguientes condiciones se tendrán en cuenta al momento de otorgar un perfil de acceso: usuario o grupo de usuarios, horarios de trabajo, tipo, localización y marca del dispositivo al cual se solicita acceso administrativo. Hasta el momento se encuentran definidos los grupos de usuarios y grupos de dispositivos, por lo que, a continuación se definen los horarios de trabajo.

Los horarios en los que se otorgará el perfil de acceso, están basados en los requerimientos de la CNT E.P., se definen los siguientes horarios:

- ***All Day*** (Todo el tiempo). Se asignará a grupos de usuarios que por sus funciones requieran acceso permanente a la administración de los equipos de la red.
- **7 - 19 L-D** (7am - 7pm todos los días). Se asignará a grupos de usuarios que requieran acceso a la administración de los dispositivos de la red en su horario normal de trabajo y fines de semana.
- **8 - 21 L-V** (8am - 9pm; Lunes - Viernes). Se asignará a grupos de usuarios, cuyo horario de trabajo fluctúe en este intervalo de tiempo.

4.2.3.3 Nivel de acceso

Es el nivel de privilegio con el cual un usuario accede a la administración de los dispositivos de la red IP/MPLS. Puesto que se maneja un conjunto de comandos, se asignará el máximo nivel de acceso a todos los usuarios.

4.2.3.4 Conjuntos de comandos

Son los comandos permitidos o no a ejecutarse en un dispositivo una vez que se tenga acceso a la administración del mismo. Se manejarán los siguientes conjuntos de comandos:

4.2.3.4.1 Visualización

En este conjunto se deberán considerar los comandos que permitan establecer y cerrar conexiones remotas, obtener información acerca del equipo, estado de las interfaces y protocolos, así como verificar conectividad IP, con la finalidad de detectar la causa de problemas relativamente sencillos de atender.

4.2.3.4.2 Visualización Plus

En este conjunto se deberán considerar los comandos definidos en el anterior además de aquellos que permitan obtener información acerca de VLANs, tablas de enrutamiento y ARP. Se permite ya la configuración (y guardarla) de ciertos parámetros: *hostname,* interfaces y VLANs, pero no permite su inhabilitación.

4.2.3.4.3 Configuración

En este conjunto se deberán considerar los comandos definidos en el anterior (e implícitamente en el primero), y aquellos que permitan obtener información acerca de todos los parámetros posibles excepto de la configuración inicial y del sistema de control de acceso que administra el dispositivo. Como su nombre lo indica permitirá la configuración de varios parámetros, restringiendo aquellos que podrían afectar seriamente el funcionamiento de la red.

4.2.3.4.4 Administración

Permitirá la ejecución de todos los comandos sin restricción alguna.

4.2.3.5 Asignación de perfiles de acceso

En la tabla 4.4 se muestra la asignación de perfiles de acceso, basándose en los elementos: grupo de usuarios, grupo de dispositivos y horarios de trabajo. La letra V hace referencia al conjunto de comandos “Visualización”, las letras VP a “Visualización Plus”, la letra C a “Configuración” y la letra A corresponde a “Administración”.

La combinación de las condiciones mostradas en la tabla 4.4 determina un perfil de acceso en particular.

Al grupo *CALL CENTER* se le asigna el conjunto de comandos “Visualización” para los equipos P, PE y L2 del grupo “Función” de cualquier regional y marca; en el horario *ALL DAY.*

Los grupos REG 1, REG 3, REG 4, REG 5, REG 6, REG 7 poseen las mismas características que el grupo *CALL CENTER* con la diferencia que el acceso a la administración se permite solo a los equipos localizados en la Regional correspondiente y únicamente en el horario “8 – 21 L-V”.

El grupo O&M DATOS INTERNET TV Y TELEFONÍA posee las mismas características que el grupo *CALL CENTER* a diferencia que se le facilita el conjunto de comandos “Visualización” para los equipos RR”.

Al grupo NOC se le asigna el conjunto de comandos “Visualización Plus” para los equipos L2 y PE y “Visualización” para los equipos P, en todas la marcas y regionales, en el horario *ALL DAY.*

El grupo INGENIERÍA posee las mismas características que el grupo NOC a diferencia que se le facilita el conjunto de comandos “Visualización” para los equipos RR.

GRUPO DE USUARIOS	GRUPOS DE DISPOSITIVOS														Horario de Trabajo
	NIVEL DE ACCESO										SET DE COMANDOS				
	MARCA			UBICACIÓN							FUNCIÓN				
	Cisco	Huawei	Alcatel	R1	R2	R3	R4	R5	R6	R7	P	PE	L2	RR*	
CALL CENTER	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	V	V	V	-	All Day
NOC	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	V	VP	VP	-	7 - 19 L-D
INGENIERÍA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	V	VP	VP	V	7 - 19 L-D
GESTIÓN RED	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	VP	C	C	VP	All Day
O&M DATOS INTERNET TV Y TELEFONÍA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	V	V	V	V	All Day
REG 1	SI	SI	SI	SI	NO	NO	NO	NO	NO	NO	V	V	V	-	8 - 21 L-V
REG 2	SI	SI	SI	NO	SI	NO	NO	NO	NO	NO	V	VP	VP	-	All Day
REG 3	SI	SI	SI	NO	NO	SI	NO	NO	NO	NO	V	V	V	-	8 - 21 L-V
REG 4	SI	SI	SI	NO	NO	NO	SI	NO	NO	NO	V	V	V	-	8 - 21 L-V
REG 5	SI	SI	SI	NO	NO	NO	NO	SI	NO	NO	V	V	V	-	8 - 21 L-V
REG 6	SI	SI	SI	NO	NO	NO	NO	NO	SI	NO	V	V	V	-	8 - 21 L-V
REG 7	SI	SI	SI	NO	NO	NO	NO	NO	NO	SI	V	V	V	-	8 - 21 L-V
DESCA	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	A	A	A	A	8 - 21 L-V
MPLS_Nivel 1	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	VP	C	A	VP	All Day
MPLS_Nivel 2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	A	A	A	A	All Day

Tabla 4.4: Asignación de perfiles de acceso

* Para los Equipo RR, se indica con un guión (-) los grupos de trabajo que no tendrán acceso a su administración.

Al grupo GESTIÓN RED se le asigna el conjunto de comandos “Visualización Plus” para los equipos P y RR, y “Configuración” para los equipos PE y L2, en todas la marcas y regionales, en el horario *ALL DAY.*

Al grupo MPLS_Nivel1 se le asigna el conjunto de comandos “Visualización Plus” para los equipos P y RR, “Configuración” para los equipos PE y “Administración” para L2, en todas la marcas y regionales, en el horario *ALL DAY.*

Al grupo DESCA se le asigna el conjunto de comandos “Administración”, pero únicamente se le permite el acceso a los equipos marca Cisco. Horario *ALL DAY.*

Al grupo MPLS_Nivel2 se le asigna el conjunto de comandos “Administración” para todos los equipos de la red IP/MPLS y en el horario *ALL DAY.*

4.3 PROPUESTA DE ACTUALIZACIÓN DEL SISTEMA DE CONTROL DE ACCESO

4.3.1 SISTEMA DE CONTROL DE ACCESO CISCO v5.2 [1]

4.3.1.1 Características

- El Sistema de Control de Acceso Cisco v5.2 en adelante ACS v5.2, es un servidor AAA basado en el sistema operativo Linux.
- Representa la solución adecuada para las empresas que requieren tener el mayor nivel de información de las actividades realizadas en la administración de la red y control sobre las mismas.
- Soporta redundancia, los cambios de configuración son realizados en el servidor primario y son replicados al servidor o servidores secundarios.
- En escenarios de gran tamaño se puede tener balanceo de carga, es decir

distribuir las peticiones AAA entres varios servidores, simplificar la administración de clientes AAA y ofrecer alta disponibilidad.

- El servidor del ACS v5.2 primario o secundario puede constituir el colector de registros para un posterior monitoreo y análisis de los mismos. Sólo los servidores que se encuentren sincronizados con el servidor colector de registros le podrán enviar sus registros.
- Soporta hasta 300.000 cuentas de usuario y 50.000 clientes AAA en su base de datos interna.
- Requiere de una licencia para su funcionamiento.
- Se requiere una licencia por dirección IP si la cantidad de dispositivos configurados supera los 500.

4.3.1.2 Ventajas frente a la versión 3.2

- El ACS v5.2 dispone de una interfaz de línea de comandos, a través de la cual se pueden realizar varias tareas de administración del sistema.
- El ACS v5.2 soporta el envío y almacenamiento de registros en servidores *Syslog* externos.
- Se corrigen los *bugs* de programación reportados en las versiones anteriores.
- Ofrece al administrador del sistema mayores facilidades para una gestión óptima del control de acceso; da la posibilidad de establecer reglas más específicas para el acceso basándose además de la identidad en otros atributos como la hora de conexión, tipo de dispositivos al que se solicita el acceso o la ubicación del mismo.
- Presenta mayores funcionalidades en su Interfaz Web. Las cuales se listan a continuación:

- ✓ Maneja el protocolo HTTPS para el acceso a la Interfaz Web.
- ✓ Ofrece el más alto nivel de visualización de reportes, alertas y dispone de herramientas para probar conectividad en la red.
- ✓ Proporciona la máxima visibilidad en la configuración de políticas y actividades de autenticación y autorización del acceso a los dispositivos de la red.
- ✓ Una visión integral de monitoreo de la red, detección y posible solución de problemas de acceso a los dispositivos de la red.
- ✓ Simplifica la generación y acceso a reportes predefinidos y personalizados.
- ✓ La capacidad de alertas con umbrales y factores desencadenantes sobre las actividades de autenticación sobre la detección a tiempo de operaciones anormales o el intento de éstas.

4.3.2 GUÍA DE CONFIGURACIÓN DEL ACS v5.2 [1]

La presente guía se desarrolla con la finalidad de dar al Área O&M Plataforma IP/MPLS de la CNT E.P. los lineamientos necesarios para la configuración de los principales ejes, en caso de tomar en cuenta la propuesta de actualizar el Sistema de Control de Acceso.

Los lineamientos a configurar se basan en las normas, procedimientos y redefinición de atributos propuestos en el presente capítulo, para cubrir los requerimientos del Área O&M Plataforma IP/MPLS de la CNT E.P, en cuanto al control de acceso a la administración de los dispositivos de red.

Para el efecto se adquirió la versión y licencia de prueba, mediante solicitud a DESCA, *partner* Cisco y empresa encargada de dar soporte a la red IP/MPLS de la CNT E.P., puesto que esta versión solo se facilita a este tipo de empresas.

4.3.2.1 Instalación de la versión de prueba del ACS v5.2

Las versiones de prueba del ACS v5.2, se entregan como imágenes ISO y se deben instalar en plataformas de virtualización robustas; las versiones admitidas son VMWare Server ESX 3.5 y 4.0. Para el presente trabajo se ha instalado y utilizado la VMWare Server ESX 3.5.

Se omitirán los pasos de instalación de la plataforma VMware Server ESX 3.5, y de la imagen ISO en la misma, puesto que el énfasis de esta guía es la configuración del ACS v5.2.

Una vez instalada la imagen ISO ACS v5.2 nos encontraremos en el shell de comandos; para verificar la correcta instalación se puede ejecutar el comando ***show application status acs*** que despliega los procesos que corren en el ACS v5.2. La figura 4.2 muestra la salida de dicho comando, los procesos "corriendo" satisfactoriamente indican que la instalación está completa.

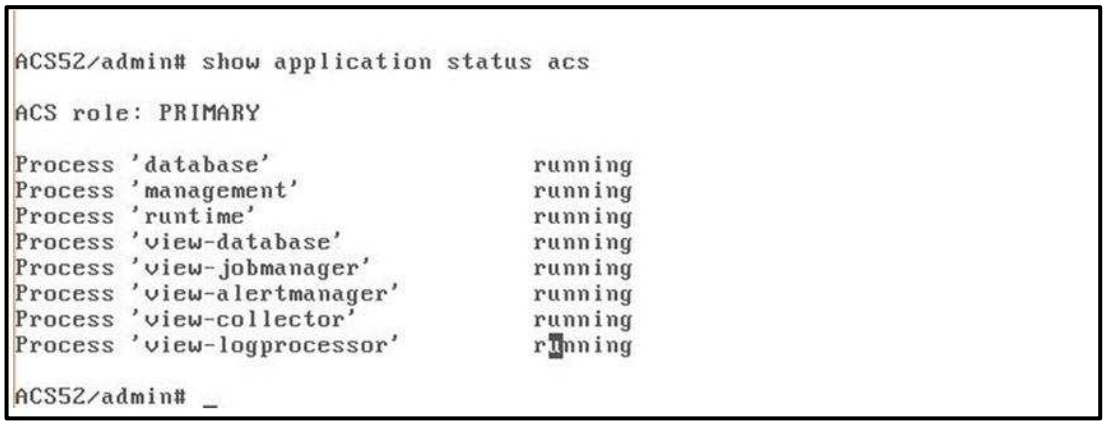


Figura 4.2: Procesos en el ACS v5.2

4.3.2.2 Topología para pruebas del ACS v5.2

Se empleará la topología que se muestra en la figura 4.3 con la finalidad de implementar y comprobar las principales características del ACS v5.2 utilizando para ello equipos de conectividad de las marcas Cisco, Alcatel y Huawei.

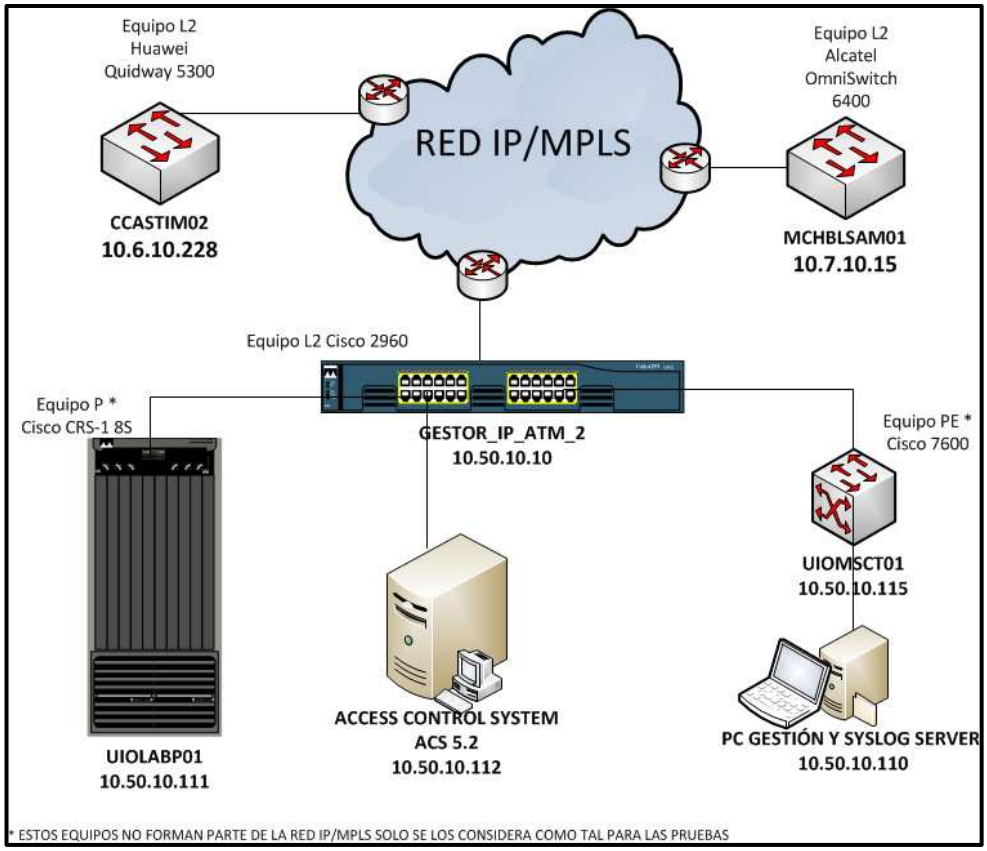


Figura 4.3: Topología para pruebas del ACS v5.2

Esta topología está integrada por:

- Dos equipos de capa 2 CCASTIM02, MCHBLSAM01, de las marcas Huawei y Alcatel respectivamente, conectados directamente a la red IP/MPLS.

- Un equipo PE (UIOMSCT01), y un equipo P (UIOLABP01) que se conectan a través del equipo L2 (GESTOR_IP_ATM_2) a la red IP/MPLS; todos estos equipos son de marca Cisco.

- Un servidor sobre el cual se instaló el ACS v5.2 para pruebas y una PC de gestión a través de la cual se accede a la interfaz web del ACS v5.2 para realizar las configuraciones respectivas y que además servirá como

servidor de *Syslog*[59].

Ninguno de estos equipos se encuentran en producción, se utilizaron con la finalidad de elaborar la presente guía y las pruebas respectivas. Los equipos Cisco pertenecen al laboratorio de pruebas del Área O&M Plataforma IP/MPLS y los equipos Alcatel y Huawei fueron facilitados por dichas empresas al Área, puesto que se encuentran en pruebas para su futura adquisición y se debía probar sus características AAA.

4.3.2.3 Accediendo a la interfaz web del ACS v5.2

Para acceder a la interfaz web se utiliza un navegador; se recomienda el Internet Explorer versión 6 o 7 o Firefox versión 3 en adelante. Se digita la URL: *https://10.50.10.112/acsadmin*; en el primer ingreso se despliega la pantalla que se muestra en la figura 4.4, en donde se solicita la licencia respectiva para su funcionamiento. Se instala la licencia provista por DESCA.

Figura 4.4: Pantalla inicial del ACS v5.2, solicitando licencia

Una vez especificada la licencia se accede a la página de inicio del ACS v5.2.; se

[59] *Syslog*: es un estándar para el envío de mensajes de registro en una red informática IP.

ingresa con el username “ACSAdmin” (el campo no es sensible a mayúsculas y minúsculas) y con la contraseña “default”. Se solicitará el cambio de la contraseña por defecto para poder ingresar al área de trabajo.

4.3.2.4 Área de trabajo del ACS v5.2

Una vez que se haya realizado la autenticación correctamente se ingresa al área de trabajo, la cual se divide en 3 secciones como se muestra en la figura 4.5: 1.Encabezado, 2.Panel de navegación y 3.Área de contenido.

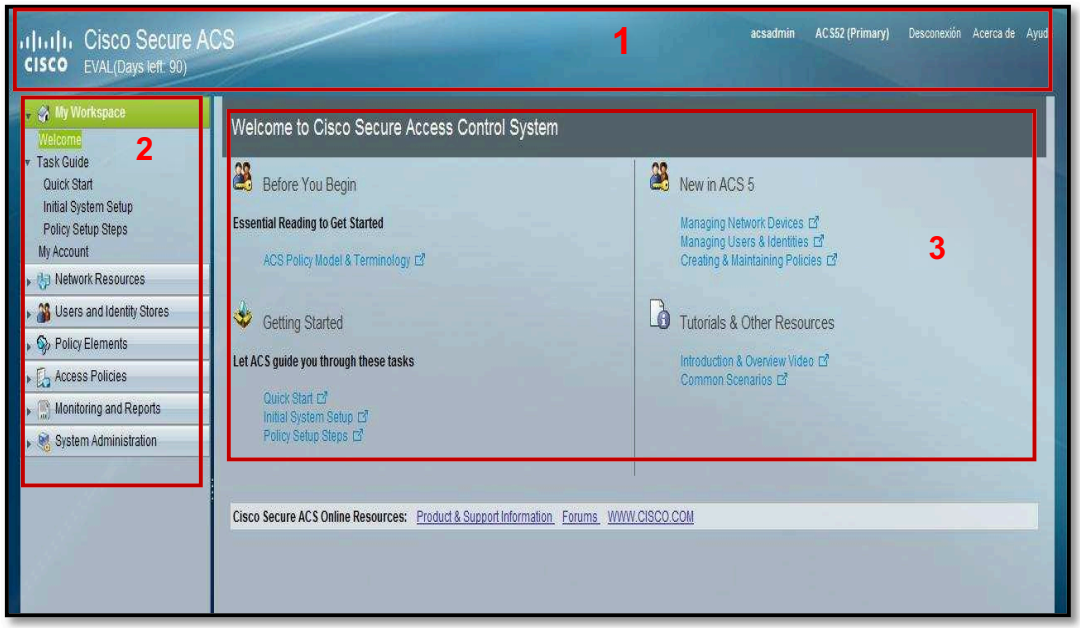


Figura 4.5: Área de trabajo del ACS v5.2

4.3.2.5 Configuración de los atributos en el ACS v5.2

Previamente a configurar los atributos en los que basa su funcionamiento el ACS v5.2, se configurarán ciertas restricciones sobre contraseñas y cuentas de administración, con el fin de asegurar el acceso a la configuración del sistema.

4.3.2.5.1 Configuración para la administración del ACS v5.2

a) Roles para la administración

El ACS v5.2 utiliza una administración basada en roles, los cuales se explican a breves rasgos en la figura 4.6. Para ello se debe dirigir a la opción:

System Administration > Administrators > Roles

	Name	Description
○	ChangeAdminPassword	Allows password change operation for administrators
○	ChangeUserPassword	Dedicated role for changing users passwords only
○	NetworkDeviceAdmin	Network Devices Administrator
○	PolicyAdmin	Policy Administrator
○	ReadOnlyAdmin	Read only access to all resources
○	ReportAdmin	Read Only Access on Logs
○	SecurityAdmin	Permissions Administrator for ACS
○	SuperAdmin	Super Administrator for ACS
○	SystemAdmin	System Administrator
○	UserAdmin	Users Administrator

Figura 4.6: Administración del ACS v5.2 basada en roles

b) Configuración de contraseñas

Cumpliendo con lo estipulado en la sección 4.1.2.5, se establecerán los parámetros para asegurar que el ACS v5.2 exija contraseñas robustas. Para configurar las contraseñas de administración del Sistema de Control de Acceso se debe dirigir a:

System Administration > Administrators > Settings > Authentication

- ***Password Complexity***

En esta pestaña se definen los parámetros necesarios para obligar a tener claves más robustas; se marcan las opciones como se indica en la figura 4.7.

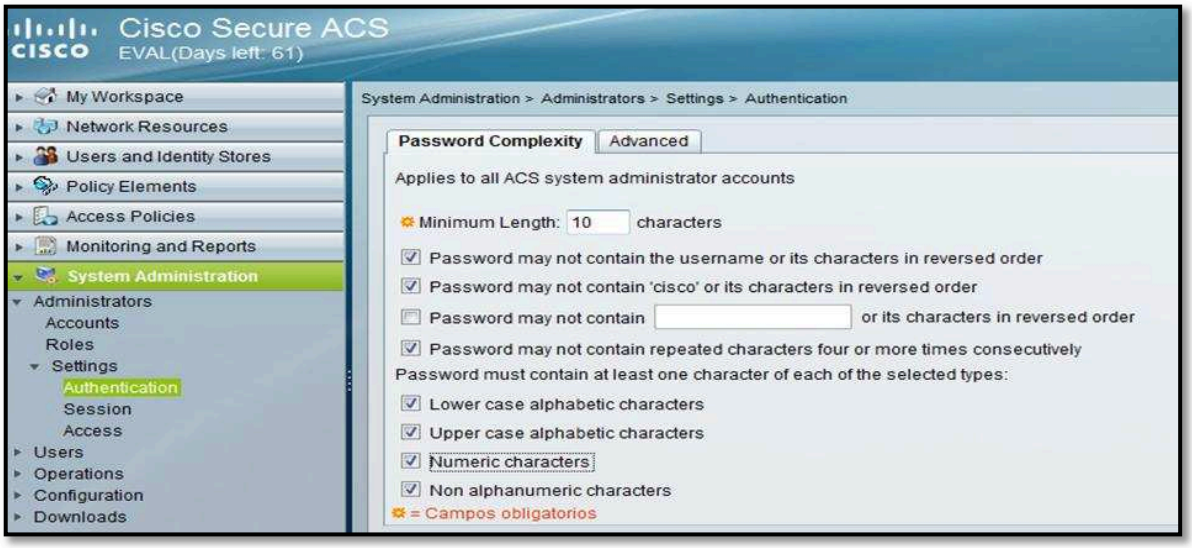


Figura 4.7: Administración de contraseñas de Administradores, *Password Complexity*

- ***Advanced***

En esta pestaña se toman medidas en cuanto a cambios periódicos de claves, no utilización de claves anteriores, intentos sucesivos fallidos de clave e inactividad de sesión. Se procede a configurar dichos parámetros tal como se indica en la figura 4.8.

c) Tiempo de inactividad

Cumpliendo con lo establecido en la sección 4.1.4.2 de la seguridad de equipos desatendidos, como se ve en la figura 4.9, se ha establecido el tiempo de inactividad después del cual la sesión se cerrará. Para ello se debe dirigir a la opción: ***System Administration > Administrators > Settings > Session***

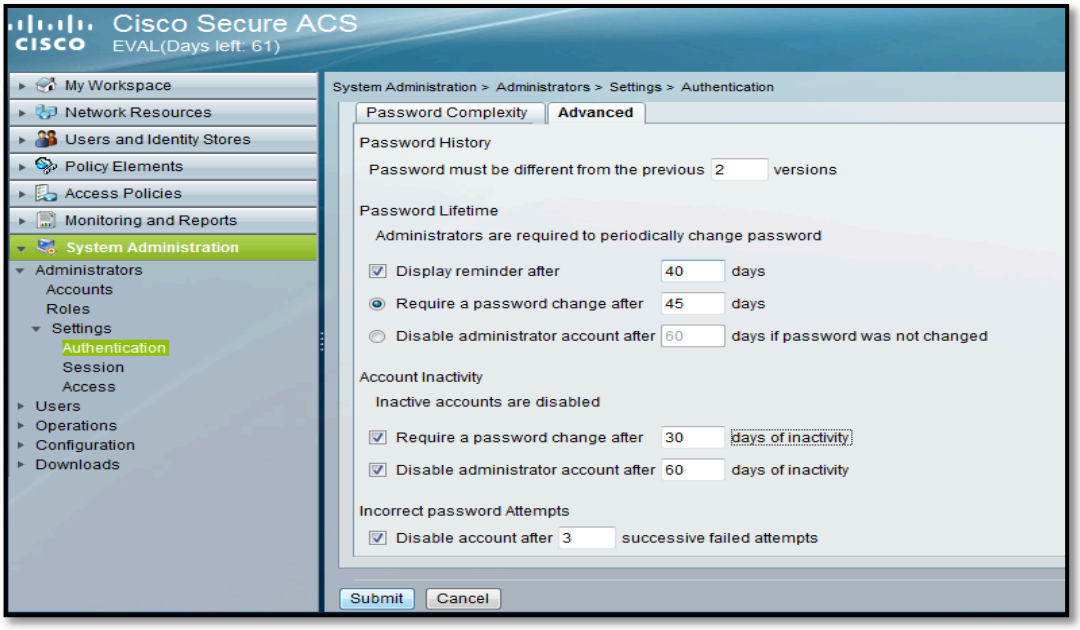


Figura 4.8: Administración de contraseñas de Administradores, *Advanced*

Figura 4.9: Inactividad de sesión

d) Restricción de direcciones IP

Se limitará el acceso al ACS v5.2 mediante filtros de direcciones IP; se restringe el acceso al ACS v5.2 solo para las IP que pertenezcan al área O&M Plataforma IP/MPLS. Para ello se debe dirigir a la opción:

System Administration > Administrators > Settings > Access

No se publica la configuración por confidencialidad de las direcciones IP del Área.

e) Configuración de los administradores

Como ejemplo para la presente guía se plantea la creación de dos cuentas de usuario con el rol de *SuperAdmin* y dos cuentas de usuario con los roles de *ChangeUserPassword y NetworkDeviceAdmin*. Se crean dos cuentas adicionales con el rol *SuperAdmin* para los autores del presente proyecto de titulación, para efectos de la elaboración de la presente guía.

La interfaz amigable que presenta el ACS v5.2 hace la creación de usuarios relativamente fácil; se deben llenar los campos como lo indica la figura 4.10 según las reglas establecidas en las secciones 4.1.2.2 y 4.1.2.5. Se asigna el nombre de usuario registrando su nombre completo y función en el campo “descripción”. Al tratarse de un administrador se marca la opción de que esta cuenta bajo ningún concepto pueda deshabilitarse; se asigna la contraseña provisional y se exige el cambio de contraseña en el primer inicio de sesión.

Para ello se debe dirigir a la opción: ***System Administration > Administrators > Accounts > Create***

Explicada la creación de una cuenta de Administrador, se crean de igual forma las demás y se seleccionan los roles correspondientes; se guardan los cambios efectuados y se cierra la sesión. Se puede iniciar la sesión nuevamente utilizando una de las cuentas de Administrador creadas, cabe indicar que la cuenta por defecto ACSAdmin no podrá ser removida. La figura 4.11 muestra los administradores configurados. Para ello se debe dirigir a la opción: ***System Administration > Administrators > Accounts***

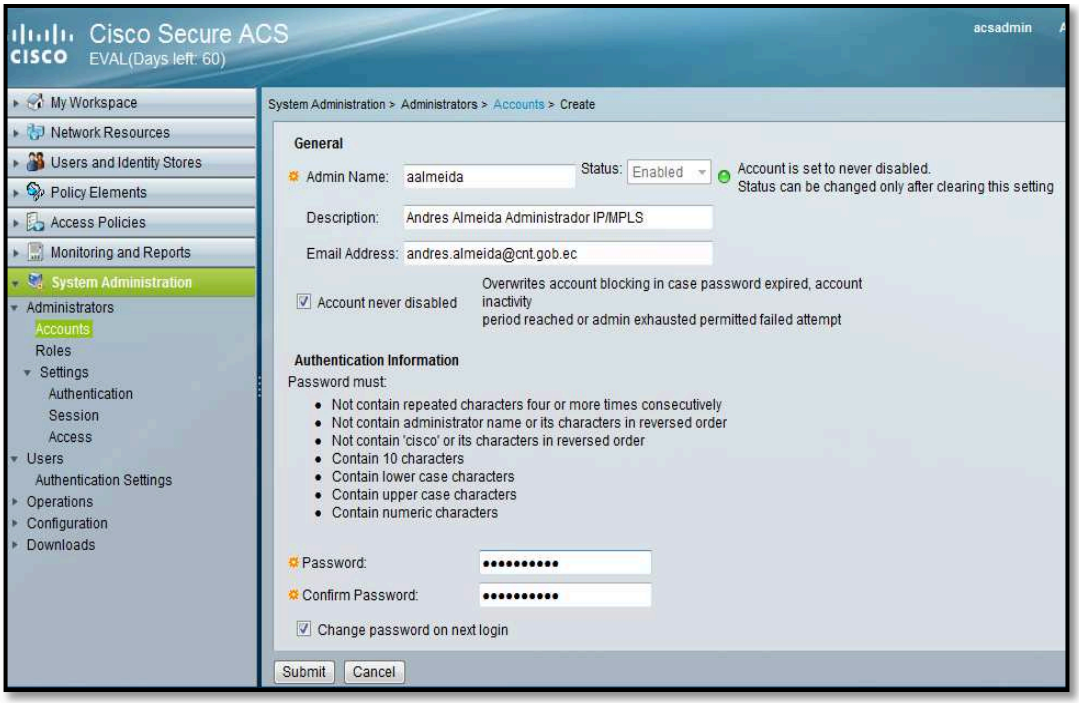


Figura 4.10: Configuración de Administradores del Cisco ACS v5.2

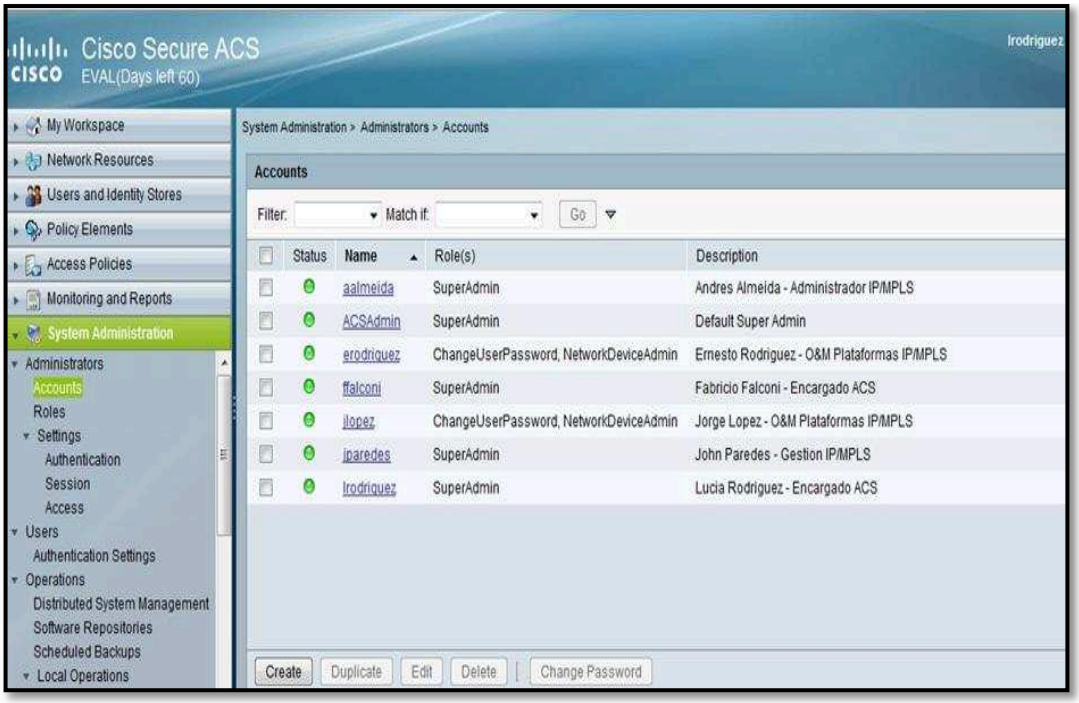


Figura 4.11: Cuentas de Administradores configuradas en el ACS v5.2

4.3.2.5.2 Configuración de dispositivos y grupos de dispositivos

a) Creación de grupos

Para la creación de los grupos y subgrupos de dispositivos se seguirá la recomendación propuesta en la sección 4.2.1.

Por defecto el sistema trae creados dos grupos, *Location* y *DeviceType*, los cuales son adecuados para nuestro propósito; se utilizará *Location* para definir los subgrupos según su distribución geográfica (localización) y *DeviceType* para los subgrupos de acuerdo a su función dentro de la red IP/MPLS (tipo). Se debe adicionar entonces el grupo Marca para los subgrupos de dispositivos según su marca como lo muestra la figura 4.12. Para ello se debe dirigir a la opción:

Network Resources > Network Device Groups > Create

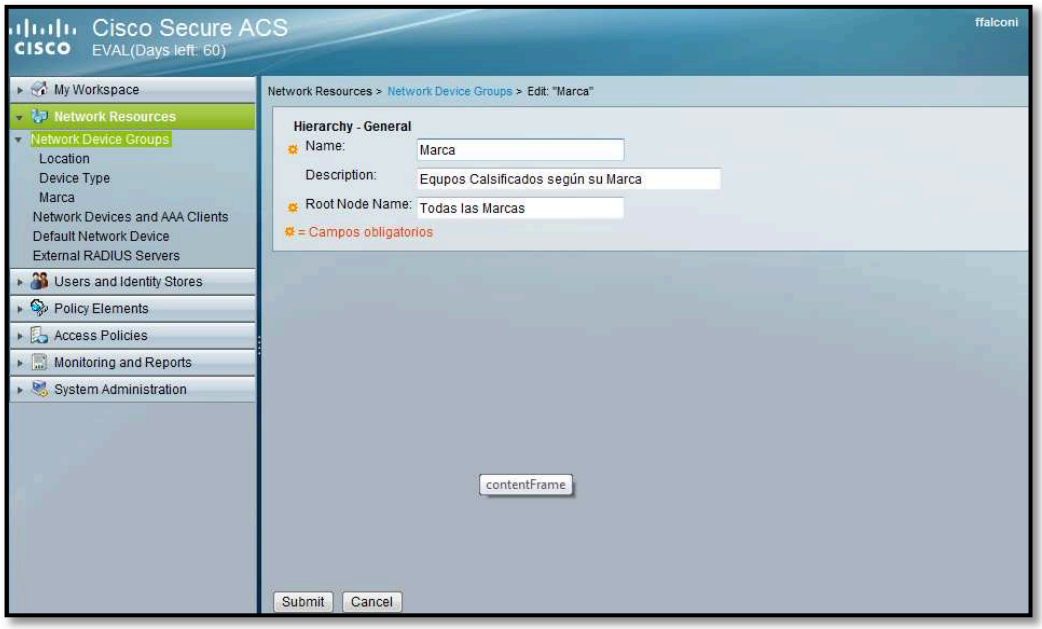


Figura 4.12: Configuración del grupo de dispositivos Marca

Se procede a crear los subgrupos correspondientes al grupo *Location*. En la figura 4.13 se puede apreciar la creación del subgrupo “Regional R1”.

Para ello se debe dirigir a la opción: ***Network Resources > Network Device Groups > Location > Create***

Figura 4.13: Configuración del subgrupo "Regional R1"

Para los grupos "*DeviceType"* y "Marca" se realiza el mismo proceso. En las figuras 4.14, 4.15 y 4.16 se muestran todos los grupos y subgrupos de dispositivos creados considerando su localización, tipo y marca respectivamente.

Para ello se debe dirigir a las opciones:

Network Resources > Network Device Groups > Location

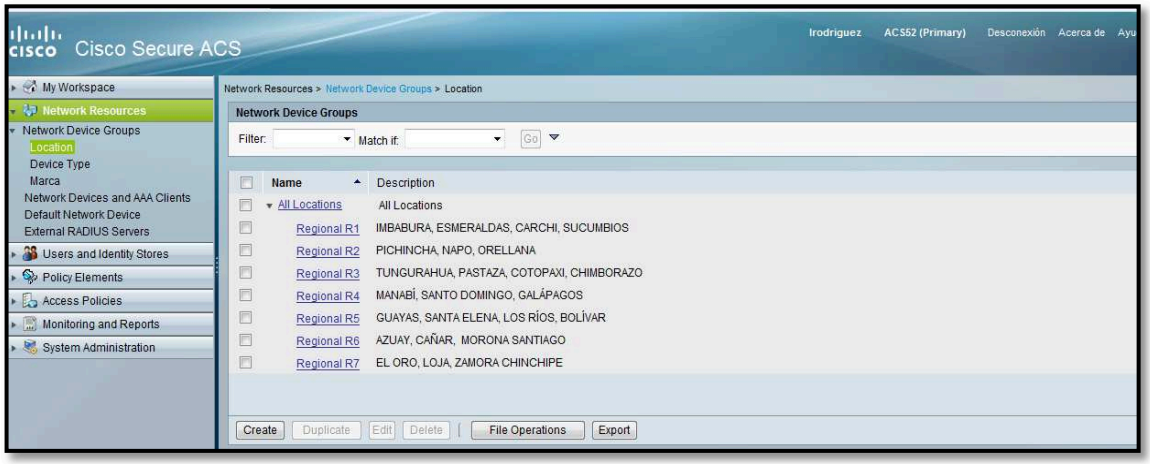


Figura 4.14: Subgrupos de dispositivos del grupo Localización

Network Resources > Network Device Groups > Device Type

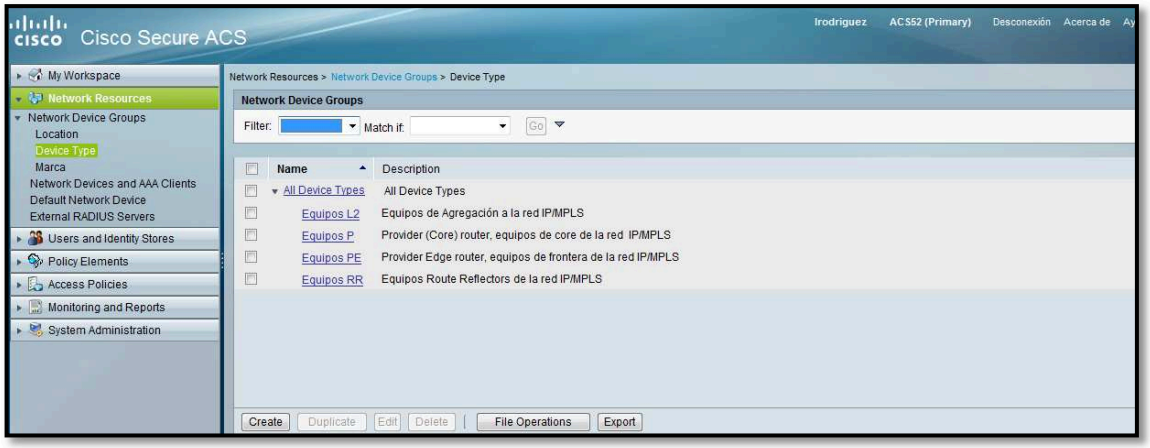


Figura 4.15: Subgrupos de dispositivos del grupo Tipo

Network Resources > Network Device Groups > Marca

Figura 4.16: Subgrupos de dispositivos del grupo Marca

b) Configuración de clientes AAA

Como ejemplo se muestra la configuración del equipo que para las pruebas actúa como Equipo tipo P y se encuentra en el nodo Mariscal, por lo tanto está localizado en la Regional 2; se selecciona el protocolo AAA TACACS+ y se asigna

la dirección IP. Esta configuración se muestra en la figura 4.17.

Para ello se debe dirigir a la opción:

Network Resources > Network Devices and AAA Clients > Create

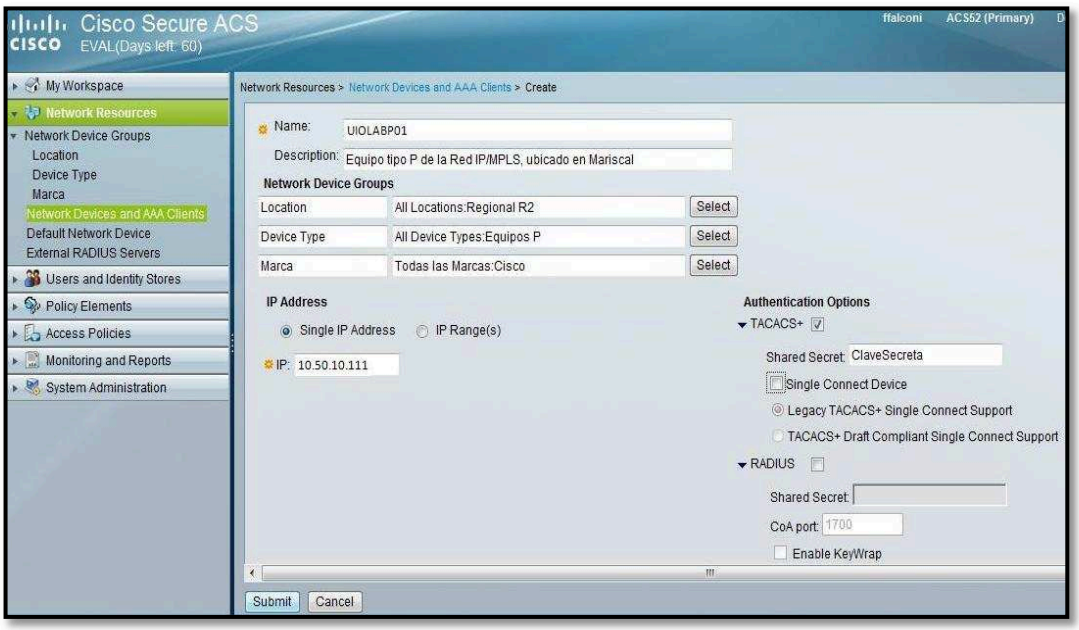


Figura 4.17: Configuración de un cliente AAA

4.3.2.5.3 Configuración de grupos de usuarios

Se configurarán los grupos de usuarios establecidos en la sección 4.2.2; como ejemplo se tiene la creación del grupo CALL CENTER. En la figura 4.18 se muestra la configuración del grupo, en la que se asigna el nombre y una descripción.

Para ello se debe dirigir a la opción:

Users and Identity Stores > Identity Groups > Create

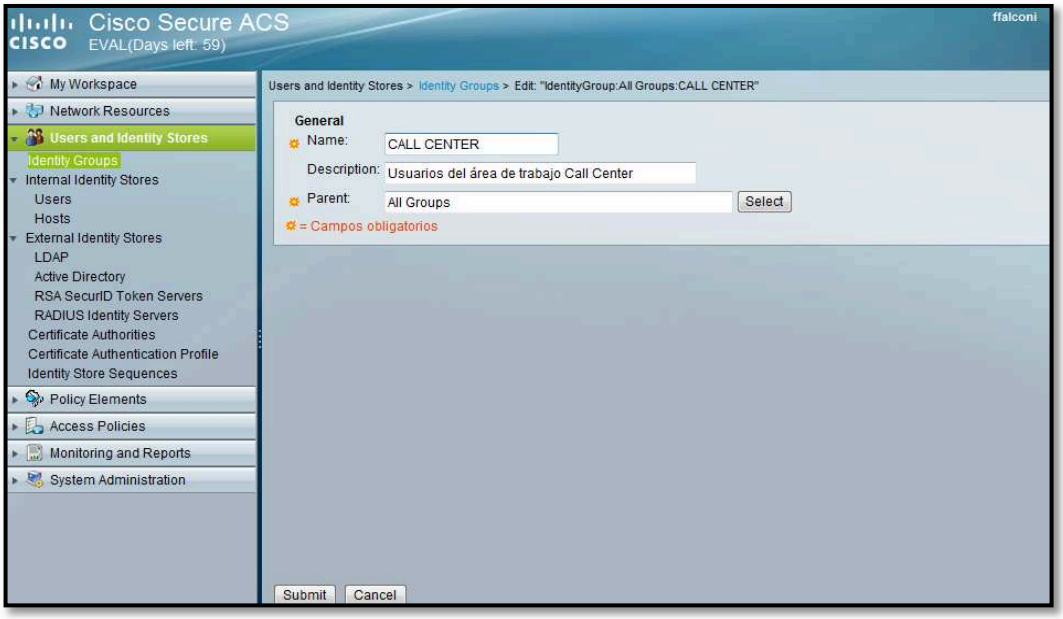


Figura 4.18: Configuración del grupo de usuario *CALL CENTER*

Después de realizar el mismo proceso para la creación de los demás grupos, se muestran todos los grupos de usarios configurados en la figura 4.19. Para ello se debe dirigir a la opción:

Users and Identity Stores > Identity Groups

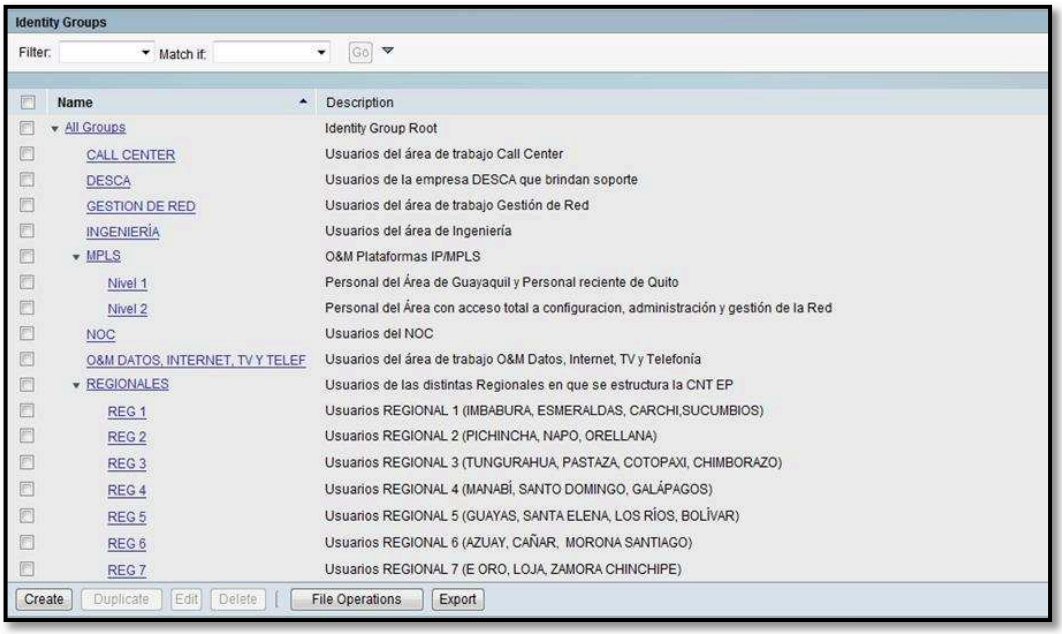


Figura 4.19: Grupos configurados de usuarios

4.3.2.5.4 Configuración de usuarios

a) Configuración de contraseñas

Al igual que para los administradores, para los usuarios también se deberán definir lineamientos de contraseñas cumpliendo lo estipulado en la sección 4.1.2.5 como se muestra en las figuras 4.20 y 4.21. Para ello se debe dirigir a la opción:

System Administration > Users > Authentication Settings

- ***Password complexity***

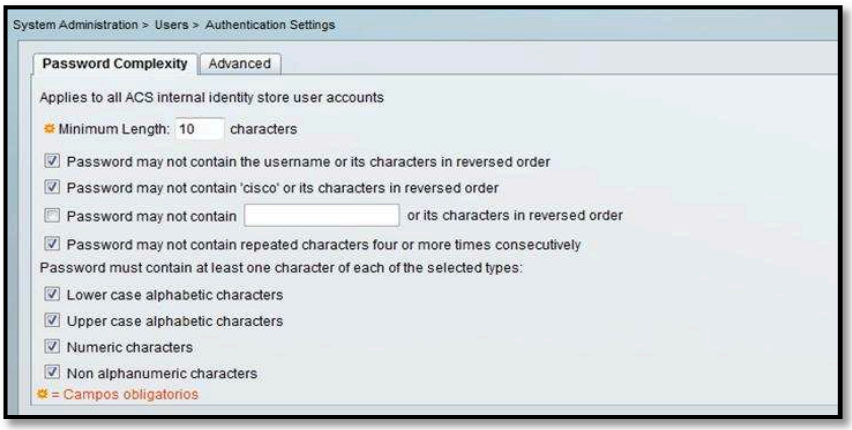


Figura 4.20: Administración de contraseñas de usuarios, *Complexity*

- ***Advanced***

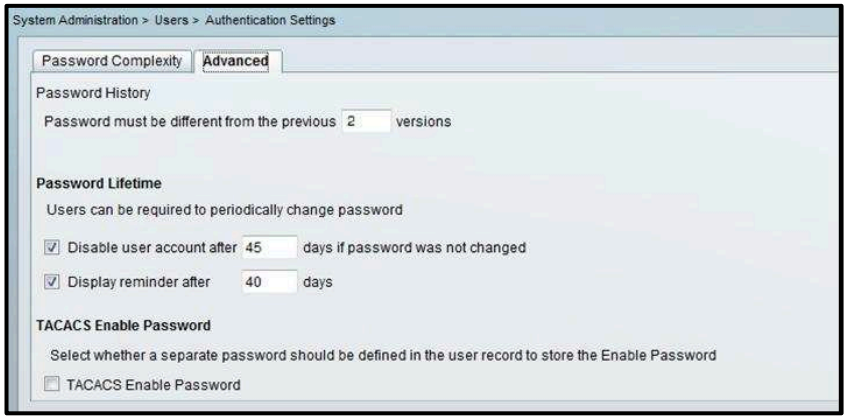


Figura 4.21: Administración de contraseñas de usuarios, *Advanced*

b) Creación de usuarios

Para la presente guía se creará un usuario para cada grupo de usuarios definido anteriormente. Como ejemplo, la figura 4.22 muestra la creación de una cuenta de usuario, se asigna el nombre de usuario, se registra el nombre y apellido, se selecciona el grupo de usuarios y se le asigna la contraseña provisional que deberá ser cambiada en el primer inicio de sesión. Para ello se debe dirigir a la opción:

Users and Identity Stores > Internal Identity Stores > Users > Create

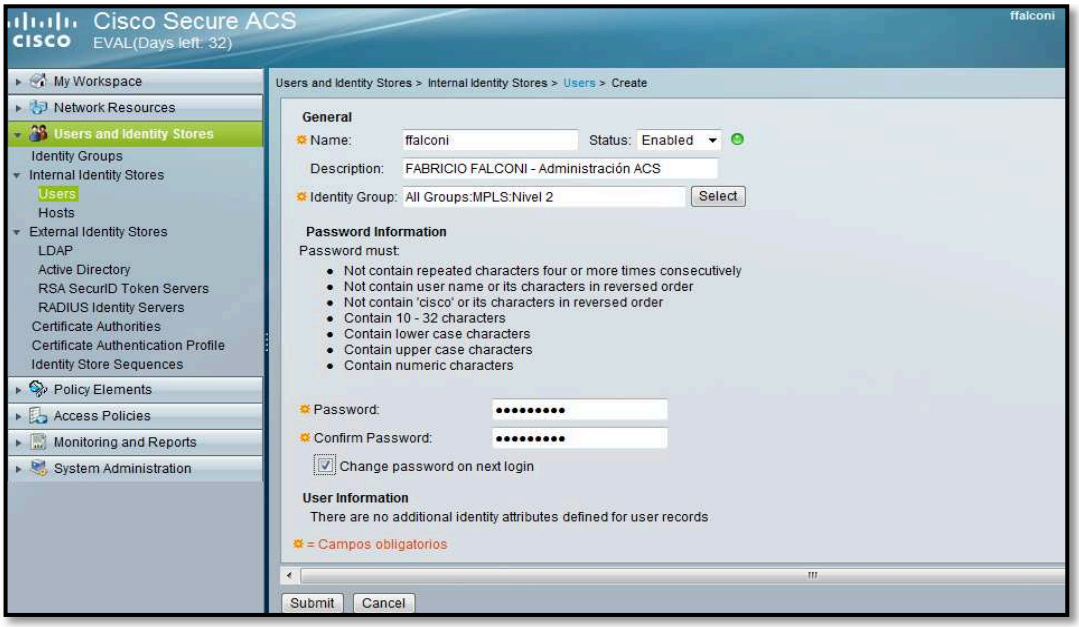


Figura 4.22: Configuración de una cuenta de usuario

Se repite el proceso para la creación de los demás usuarios, La figura 4.23 muestra algunos los diferentes usuarios que han sido creados para cada grupo de usuario. Para ello se debe dirigir a la opción:

Users and Identity Stores > Internal Identity Stores > Users

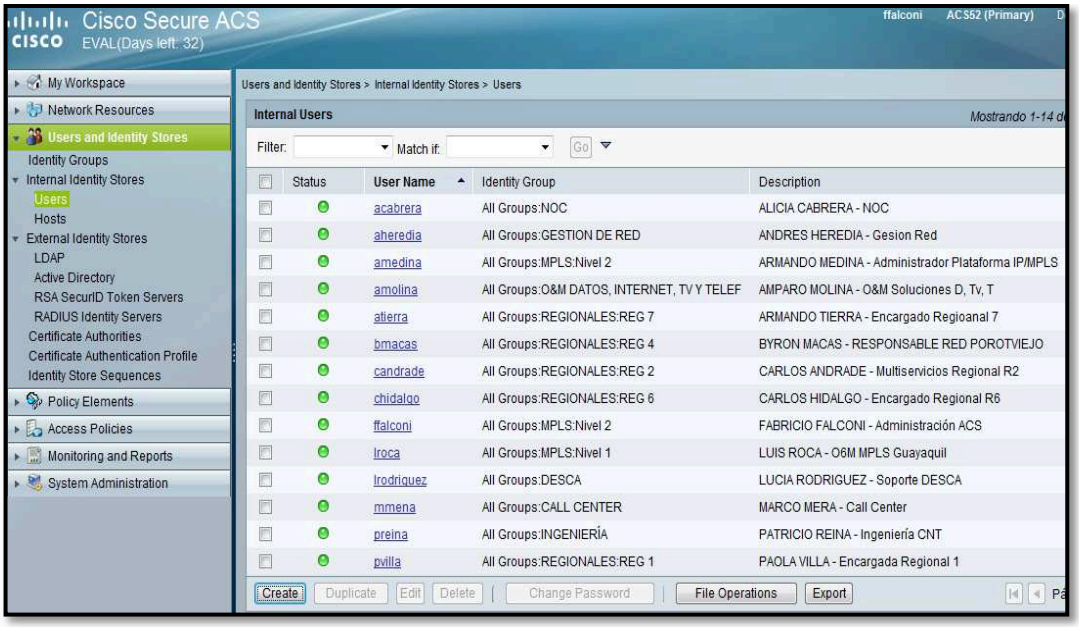


Figura 4.23: Cuentas de usuarios configuradas

4.3.2.5.5 Configuración de perfiles de acceso

a) Elementos de políticas

Los perfiles de acceso en el ACS v5.2 se manejan mediante elementos de políticas los cuales se verifican para asignar el respectivo perfil. Estos elementos hacen referencia a las condiciones definidas en la sección 4.2.3.2; los elementos a tomar en cuenta son: usuario o grupo de usuarios, horarios de trabajo, tipo, localización y marca del dispositivo al cual se solicita acceso administrativo. El elemento que restaría configurar es horario de trabajo; como ejemplo para la presente guía, la figura 4.24 muestra la configuración del horario de trabajo "8 – 21 L-V". Para ello se debe dirigir a la opción:

Policy Elements > Session Conditions > Date and Time > Create

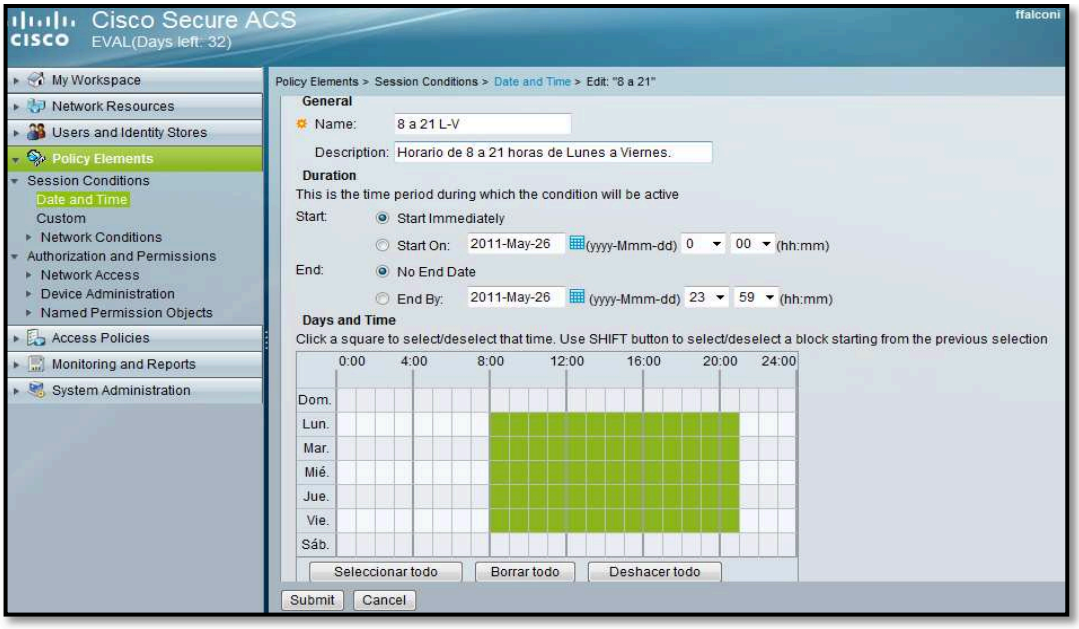


Figura 4.24: Configuración de horario de trabajo

Se repite el proceso para la creación de los demás horarios considerados. Se muestra en la figura 4.25 todos los horarios configurados. Para lo cual se debe dirigir a la opción:

Policy Elements > Session Conditions > Date and Time

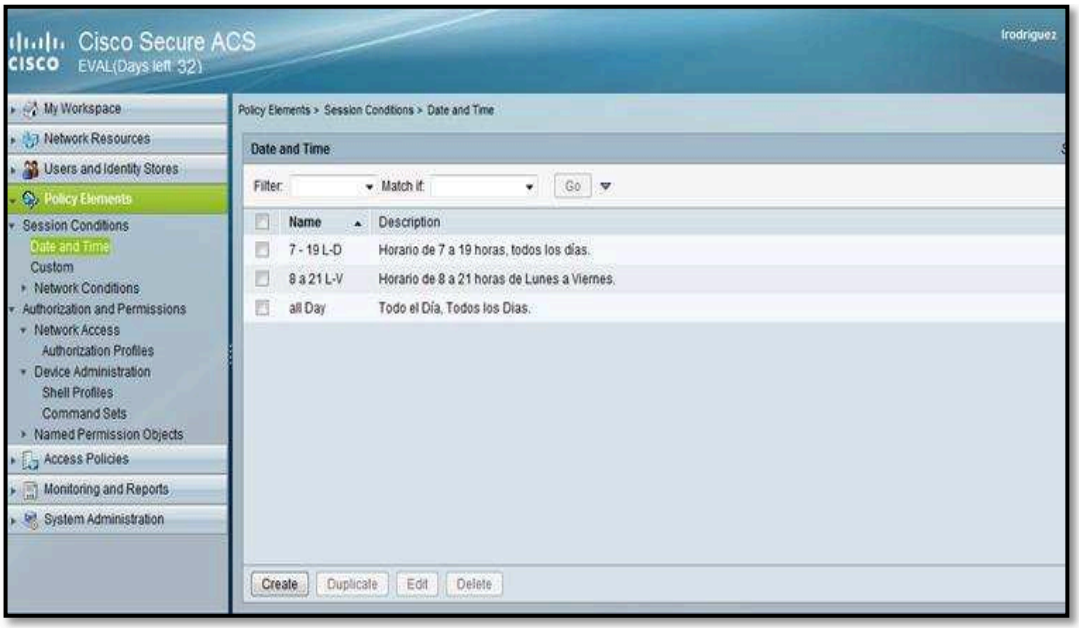


Figura 4.25: Horarios configurados de trabajo

b) Autorización y permisos

El *shell profile* y el *command set* ubicados dentro de la pestaña *Device Administration*, se combinan con el propósito de controlar el acceso a la administración de los dispositivos de la red. El *shell profile* y el *command set* proveen las funciones que podrá ejecutar el usuario que solicita acceso al dispositivo durante toda la sesión de usuario.

b.1) Shell Profile

El *shell profile*, indica el nivel de acceso con el que los usuarios autenticados accederán a la administración de los equipos de la red. Como se indicó en la sección 4.2.3.3, se configurará un único perfil de acceso "Perfil de Acceso Común" que se indica en la figura 4.26. Para ello se debe dirigir a la opción:

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create

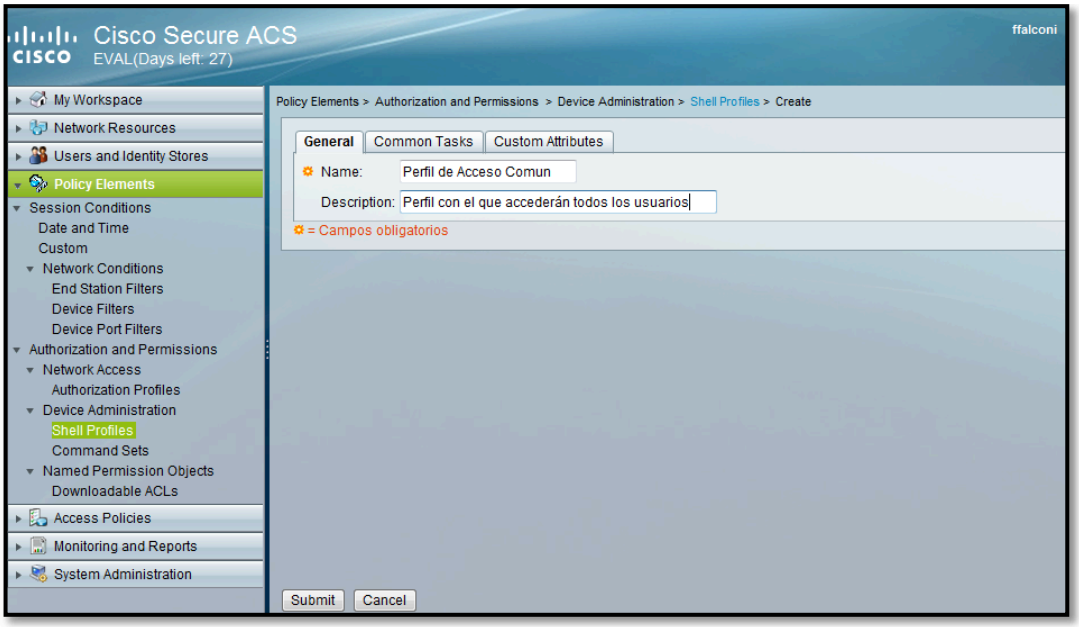


Figura 4.26: Configuración de un perfil de acceso común

En la pestaña *"Common Tasks"* se especifican los parámetros principales. Para cubrir los requerimientos se usarán los siguientes atributos:

- ***Default privilege**:* especifica el nivel de privilegio inicial para el perfil de acceso.
- ***Idle Time**:* especifica el valor del tiempo en minutos en que una sesión se cerrará si está inactiva.

En la figura 4.27 se muestra la configuración de los parámetros *default privilege*, *timeout* e *idle time* asignados al perfil de acceso común. Se ha establecido el nivel de privilegio en 15, se especifica el intervalo de tiempo que esperará el servidor para establecer una conexión (2 minutos) y que se cierre una sesión si ésta ha permanecido inactiva por más de 5 minutos.

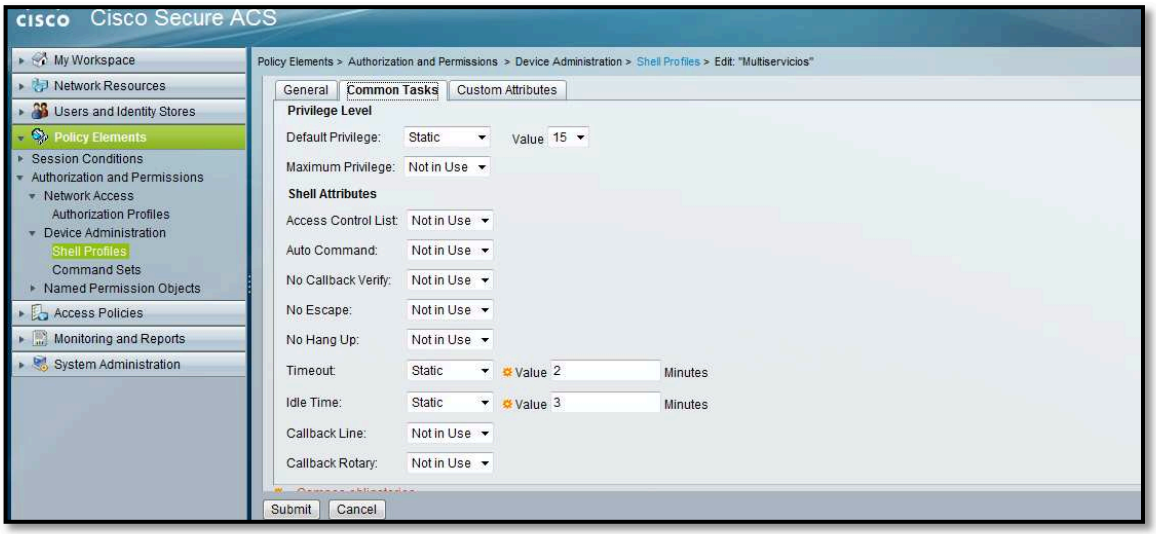


Figura 4.27: Parámetros de *Shell Profiles*

b.2) Command Sets

Se definen los comandos que se permitirán o denegarán. Se establecen los conjuntos de comandos establecidos en la sección 4.2.3.4. Al tener tres marcas de dispositivos, se configura un conjunto de comandos para cada marca.

- Visualización (Cisco, Alcatel y Huawei)
- Visualización Plus (Cisco, Alcatel y Huawei)
- Configuración (Cisco, Alcatel y Huawei)
- Administración (*PermitAll*) (Cisco, Alcatel y Huawei)

Como ejemplo se muestra la configuración del *command set* "Visualización Cisco" en la figura 4.28. Para ello se debe dirigir a la opción:

Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Create

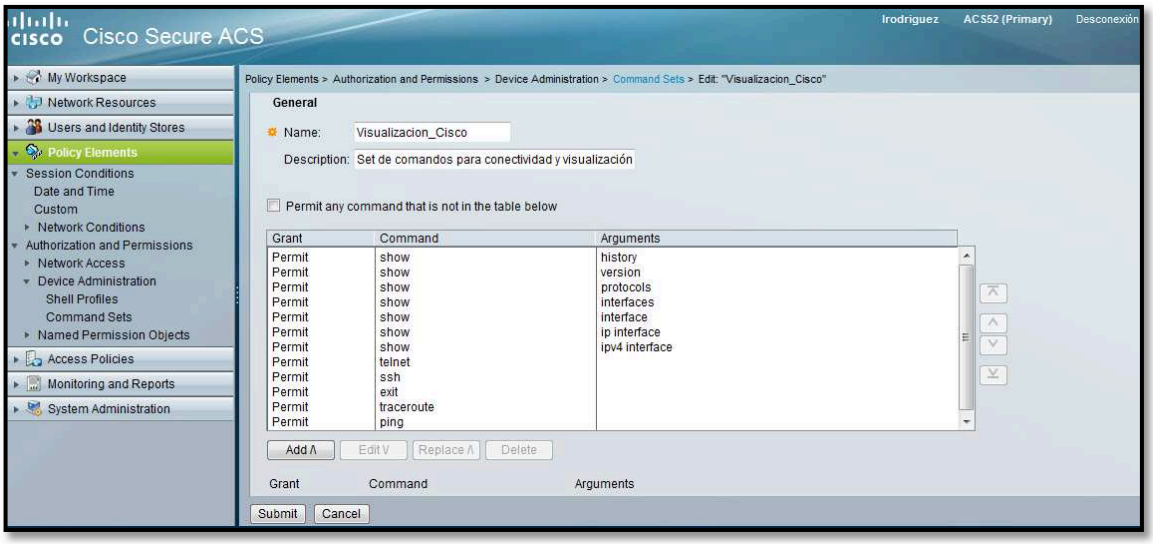


Figura 4.28: Conjunto de comandos "Visualización Cisco" [60]

Se aplica el principio de establecer los mínimos privilegios necesarios, es decir, se especifican los comandos que se permitirán y los comandos no indicados se denegarán; para ello se deja libre el *check "Permit any command that is not in the table below"* que indica que todos los comandos no mencionados no se permiten.

[60] **NOTA:** Al momento de configurar en el ACS v5.2 se debe evitar el uso de tildes puesto que se comprobó que se crean conflictos.

Se escribe el comando y los argumentos en las casillas respectivas y se los añade, "*add",* se pueden además editar y eliminar. Una vez listos se da *click* en "*submit".*

De acuerdo a la definición que se hizo en la sección 4.2.3.4 cada conjunto de comandos abarca los que fueron establecidos anteriormente de menor jerarquía; es así que para la creación de los comandos "VisualizaciónPlus_Cisco" ver la figura 4.29, se hará uso de la facilidad que presta la interfaz del ACS v5.2 que permite seleccionar los definidos en otro conjunto de comandos, en este caso los comandos "Visualización Cisco". Para ello se debe dirigir a la opción:

Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Create

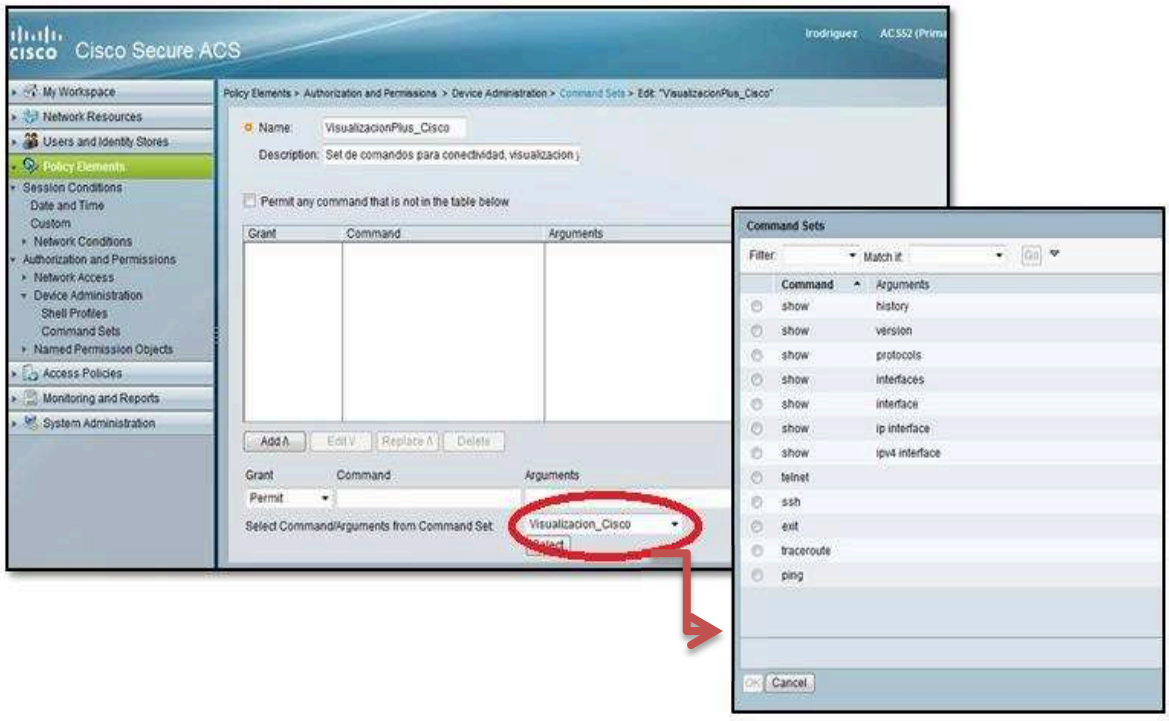


Figura 4.29: Configuración del conjunto de comandos "Visualización Plus"

Al seleccionar el conjunto de comandos "Visualización Cisco" se muestra la pantalla con los comandos definidos en este conjunto, de los cuales se puede

escoger algunos o todos los comandos. Así pues, para el conjunto de comandos "Visualización Plus Cisco" se han asignado todos los comandos del conjunto de comandos "Visualización Cisco", luego se adicionan los demás comandos como se indicó anteriormente.

La figura 4.30 muestra los conjuntos de comandos creados para las diferentes funciones que se utilizarán. Para ello se debe dirigir a la opción:

Policy Elements > Authorization and Permissions > Device Administration > Command Sets

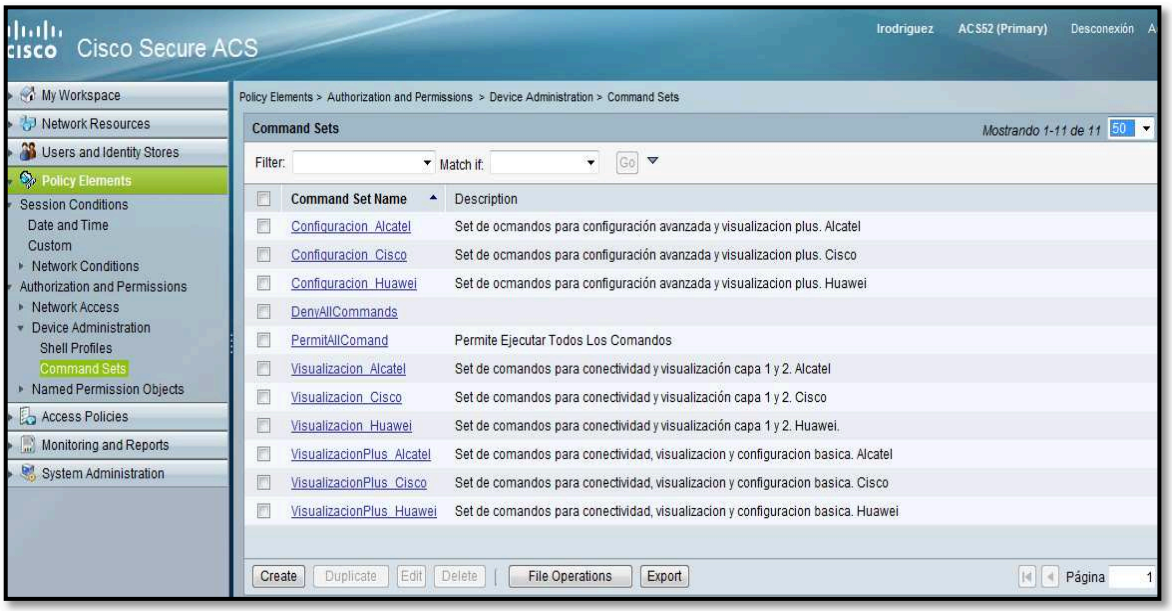


Figura 4.30: Conjunto de comandos configurados

c) Reglas de acceso

Una vez definidos los elementos, en base a éstos se construirán las reglas de acceso y uso. En primer lugar se cambia el nombre por "Acceso Administración Equipos" y se da la descripción respectiva, en los *checks* se marcan *"Identity"* y *"Authorization*" ya que los usuarios fueron agregados manualmente a cada grupo de usuario respectivo, como se indica en la figura 4.31.

Para ello se debe dirigir a la opción:

Access Policies > Access Services > Default Device Admin

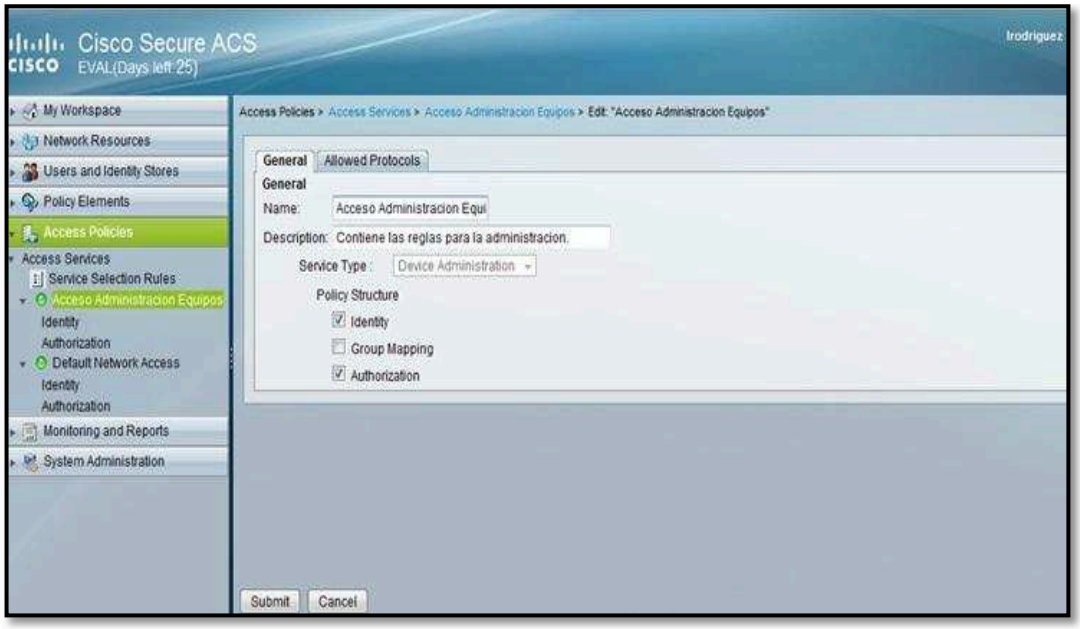


Figura 4.31: Creación de reglas, primer paso

Como siguiente paso se configuran los parámetros de identidad, ver la figura 4.32. Se seleccionan de dónde se buscará el nombre de usuario y lo que hará si la autenticación no se realiza satisfactoriamente; en el presente caso los usuarios están almacenados en la base de datos interna del ACS v5.2.

Para ello se debe dirigir a la opción:

Access Policies > Access Services > Acceso Administracion Equipos > Identity

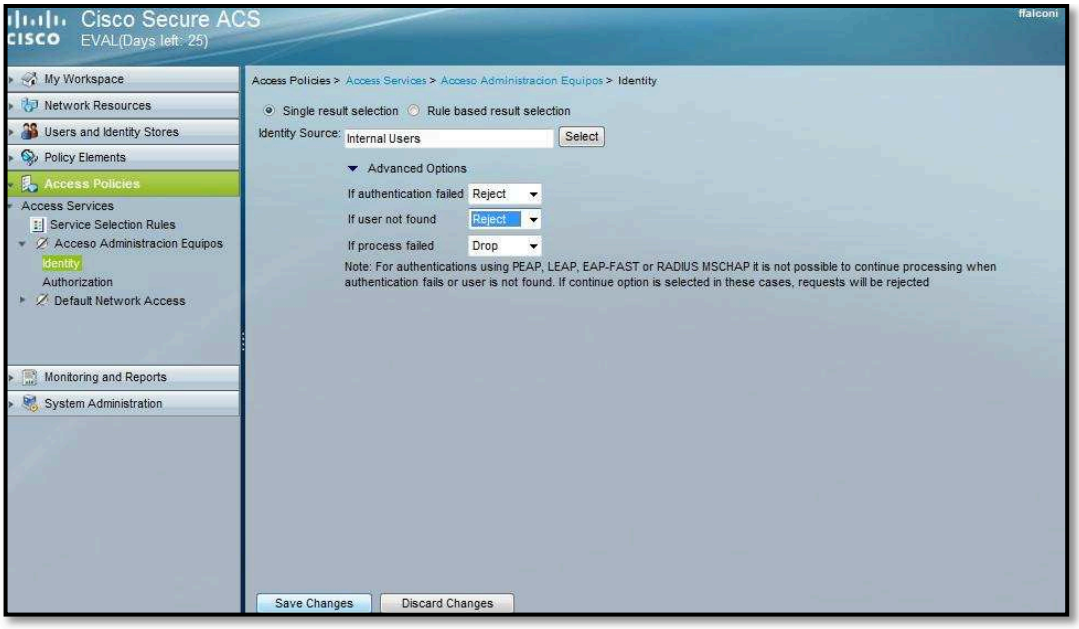


Figura 4.32: Creación de reglas, segundo paso

Como tercer paso se procede a personalizar los elementos que tendrán las reglas de autorización y los resultados que deberán proveer (figura 4.33). Para ello se debe dirigir a *Customize* en la opción:

Access Policies > Access Services > Acceso Administracion Equipos > Authorization

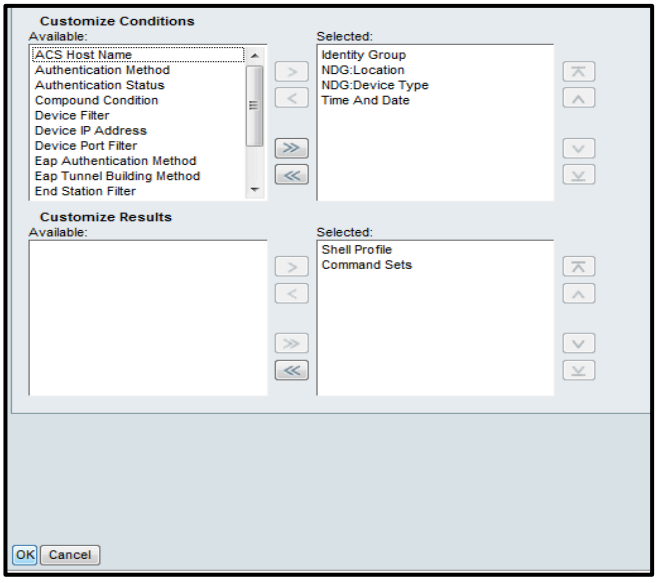


Figura 4.33: Selección de elementos y resultados para las reglas de autorización

Finalmente se procede a crear las reglas en sí; para ello se escogen *create*: aquí se crea la regla que se verificará en cada autenticación de usuario. Se muestra la creación de la regla para *CALL CENTER* en la figura 4.34.

Condiciones:

Grupo de Usuario: *CALL CENTER*

Ubicación del equipo: Cualquiera

Tipo de Equipo: Equipos L2

Resultados:

Perfil de Acceso: Común

Conjunto de Comandos: Visualización (Cisco, Huawei, Alcatel)

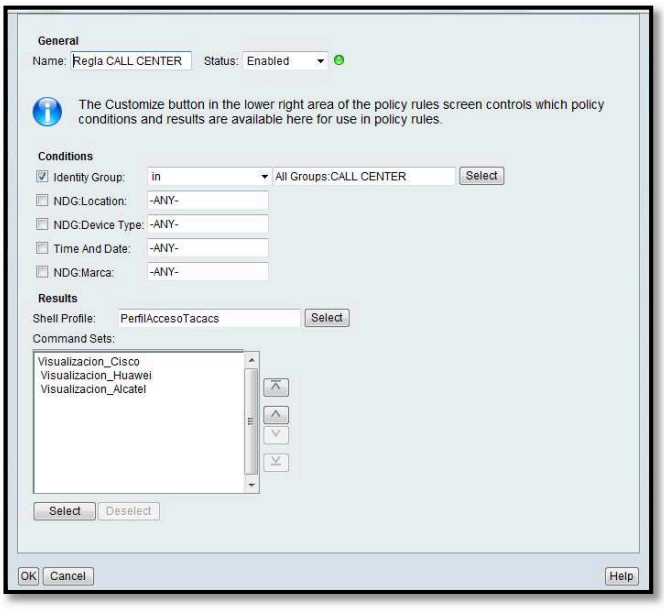


Figura 4.34: Configuración de la regla *CALL CENTER*

Una vez que se hayan configurado las reglas para todos los grupos de usuarios,

se debe tener en cuenta la regla por defecto que se aplicará si no se cumple ninguna de las establecidas, para ello se especifica no permitir la ejecución de ningún comando como lo indica la figura 4.35.

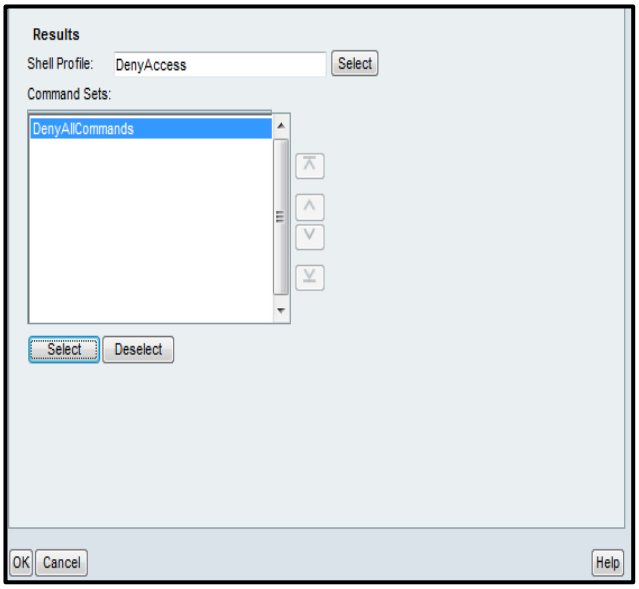


Figura 4.35: Configuración de la regla por defecto

4.3.2.6 Configuración de parámetros AAA en equipos Cisco, Alcatel y Huawei

Para pasar a la comprobación de las reglas establecidas, se necesita previamente configurar los equipos que integran la topología para que sean administrados a través del ACS v5.2.

4.3.2.6.1 Cisco IOS

1. Se configura un usuario local en el equipo, con el fin de tener un método de autenticación de respaldo si se llegara a perder la conexión con el ACS v5.2. Este usuario tendrá el máximo nivel de privilegio.

   UIOMSCT01(config)# username *usuarioSecreto* privilege 15 secret 5 *passwordCifrado*

2. Se habilita el servicio AAA en el equipo, este comando es un prerrequisito para poder ejecutar los otros comandos AAA.

UIOMSCT01(config)# aaa new-model

3. Habilitado el servicio AAA, se establecen los parámetros necesarios para llevar a cabo el proceso de autenticación.

3.1. Se establece que el ACS v5.2 proporcionará el servicio de autenticación utilizando el protocolo TACACS+. Como método de respaldo, se define que el usuario se autentique con la base de datos local en el equipo, en este caso con el usuario local previamente configurado; para ello, se utiliza la palabra clave *local* o *local-case*, la diferencia es que *local* no es sensible a letras mayúsculas o minúsculas al momento que el usuario ingrese sus credenciales y *local-case* si lo es; es recomendable utilizar *local-case*.

UIOMSCT01(config)# aaa authentication login default group tacacs+ local-case

La palabra *default* indica el nombre por defecto del método de autenticación que se utilizará.

3.2. Con el siguiente comando, se establece un nivel de seguridad adicional en el proceso de autenticación; se define el número máximo de intentos de conexión permitidos, en este caso se permiten tres intentos.

UIOMSCT01(config)# aaa authentication attempts login 3

3.3. Se configura un mensaje de prevención que se desplegará ante cada autenticación fallida.

UIOMSCT01(config)# aaa authentication fail-message # LE RECORDAMOS

QUE EL USO NO AUTORIZADO SERA, INVESTIGADO Y PENADO #

4. A continuación se definen los comandos necesarios para realizar el proceso de autorización.

4.1. Se define que, si un usuario es autenticado correctamente ingresará automáticamente al modo de configuración "*privileged exec*"; es decir, el *prompt* será "UIOMSCT01#".

UIOMSCT01(config)# aaa authorization exec default group tacacs+ local if-authenticated

4.2. Se define que la autorización para la ejecución de comandos, del nivel especificado, la provea el ACS v5.2 y de perderse la conexión que se realice de forma local.

UIOMSCT01(config)# aaa authorization commands 15 default group tacacs+ local

4.3. Se define que el mismo identificador de sesión asignado al momento que un usuario accede al cliente AAA sea utilizado para el proceso de autenticación, autorización y auditoría.

UIOMSCT01(config)# aaa session-id common

5. Una vez que se han definido los comandos necesarios para contar con los servicios de autenticación y autorización, a continuación se definen los parámetros necesarios para disponer del servicio de auditoría, con el fin de registrar todas las actividades que realice el usuario que ha ingresado al equipo, así como también los acciones fallidas o no autorizadas.

5.1. Se define que se lleve a cabo una auditoría de todas las sesiones que

empiezan y terminan en el modo de configuración "*privileged exec*".

UIOMSCT01(config)# aaa accounting exec default start-stop group tacacs+

5.2. El siguiente comando permitirá registrar los comandos, del nivel especificado, que sean utilizados.

UIOMSCT01(config)# aaa accounting commands 15 default start-stop group tacacs+

5.3. El siguiente comando define que se lleve a cabo una contabilidad de los eventos suscitados a nivel del sistema.

UIOMSCT01(config)# aaa accounting system default start-stop group tacacs+

6. Establecidos los parámetros necesarios para contar con el servicio AAA, a continuación se configuran los comandos necesarios para identificar al ACS v5.2 que se utilizará.

6.1. Se define la dirección IP del ACS v5.2.

UIOMSCT01(config)# tacacs-server host 10.50.10.112

6.2. Se establece que al servidor AAA le será enviado únicamente el *username* del usuario sin ningún tipo de dominio en particular.

UIOMSCT01(config)#tacacs-server directed-request

6.3. Se configura la clave secreta compartida, para que el cliente AAA se autentique con el ACS v5.2 y cifrar la transferencia de datos entre ellos.

UIOMSCT01(config)# tacacs-server key 7 *claveCompartidaCifrada*

7. Se indica que la autenticación por las líneas vty se realice utilizando los parámetros configurados anteriormente, es decir, el método *default*. Se define que se utilice el protocolo SSH para establecer conexiones remotas de forma segura.

UIOMSCT01(config)# line vty 0 15
UIOMSCT01(config-line)# login authentication default
UIOMSCT01(config-line)# transport input ssh

8. Finalmente se procede a guardar la configuración.

UIOMSCT01# write memory

4.3.2.6.2 Cisco IOS XR

1. Se configura un usuario local en el equipo, con el fin de tener un método de autenticación de respaldo si se llegara a perder la conexión con el ACS v5.2. Este usuario tendrá el máximo nivel de privilegio.

RP/0/RP0/CPU0:UIOLABP01(admin-config)# username *usuarioSecreto* secret 5 *passwordCifrado*

Se proporciona el máximo nivel de privilegio.

RP/0/RP0/CPU0:UIOLABP01(admin-config)# username *usuarioSecreto* group root- system

2. Se establecen los parámetros necesarios para llevar a cabo el proceso de autenticación.

2.1. Se define que el ACS v5.2 proporcionará el servicio de autenticación utilizando el protocolo TACACS+. Como método de respaldo se define que el usuario se autentique con la base de datos local en el equipo; en

este caso con el usuario local previamente configurado.

RP/0/RP0/CPU0:UIOLABP01(config)# aaa authentication login default group tacacs+ local-case

2.2. Se configura un mensaje de prevención, que se desplegará ante cada autenticación fallida.

RP/0/RP0/CPU0:UIOLABP01(config)# aaa authentication fail-message # LE RECORDAMOS QUE EL USO NO AUTORIZADO SERA, INVESTIGADO Y PENADO#

3. A continuación se definen los comandos necesarios para realizar el proceso de autorización.

3.1. Se define que si un usuario es autenticado correctamente ingresará automáticamente al modo de configuración "*privileged exec*".

RP/0/RP0/CPU0:UIOLABP01(config)# aaa authorization exec default group tacacs+ none

3.2. Se define que la autorización para la ejecución de comandos la provea el ACS v5.

RP/0/RP0/CPU0:UIOLABP01(config)#aaa authorization commands default group tacacs+ none

4. Una vez que se han definido los comandos necesarios para contar con los servicios de autenticación y autorización, a continuación se definen los parámetros necesarios para disponer del servicio de auditoría.

4.1. Se define que se lleve a cabo una contabilidad de todas las sesiones que empiezan y terminan en el modo de configuración "*privileged exec*".

RP/0/RP0/CPU0:UIOLABP01(config)# aaa accounting exec default start-stop group tacacs+

4.2. El siguiente comando permitirá registrar los comandos que sean utilizados.

RP/0/RP0/CPU0:UIOLABP01(config)# aaa accounting commands default start-stop group tacacs+

4.3. El siguiente comando define que se lleve a cabo una contabilidad de los eventos suscitados a nivel del sistema.

RP/0/RP0/CPU0:UIOLABP01(config)# aaa accounting system default start-stop group tacacs+

5. Establecidos los parámetros para contar con el servicio AAA, a continuación se configuran los comandos necesarios para identificar al ACS v5.2 que se utilizará.

5.1. Se define la dirección IP del ACS v5.2, además se establece un período de tiempo (segundos) en el cual el cliente AAA esperará recibir una respuesta del ACS v5.2, antes de que se genere un mensaje de error.

RP/0/RP0/CPU0:UIOLABP01(config)# tacacs-server host 10.50.10.112 timeout 5

5.2. Se configura la clave secreta compartida, para que el cliente AAA se autentique con el ACS v5.2 y cifrar la transferencia de datos entre ellos.

RP/0/RP0/CPU0:UIOLABP01(config)# tacacs-server host 10.50.10.112 key *claveCompartida*

5.3. Se indica que la autenticación por las líneas vty se realice utilizando los

parámetros configurados anteriormente, es decir, el método *default*. Se define que se utilice el protocolo SSH para establecer conexiones remotas de forma segura.

RP/0/RP0/CPU0:UIOLABP01(config)# line vty 0 4
RP/0/RP0/CPU0:UIOLABP01(config-line)# login authentication default
RP/0/RP0/CPU0:UIOLABP01(config)# ssh server enable

6. Finalmente se procede a guardar la configuración.

RP/0/RP0/CPU0:UIOLABP01# commit

4.3.2.6.3 Alcatel

1. Se configura un usuario local en el equipo, con el fin de tener un método de autenticación de respaldo si se llegara a perder la conexión con el ACS v5.2. A dicho usuario se le otorga permisos de lectura y escritura, es decir todos los privilegios.

MCHBLSAM01# user *usuarioSecreto* read-write all password *claveDeAdmin*

2. Se define el nombre asociado a la dirección IP que identifique al servidor TACACS+ (ACSv5.2), el período de tiempo que el cliente AAA esperará una respuesta del servidor AAA y la clave secreta compartida.

MCHBLSAM01# aaa tacacs+-server ACS52 host 10.50.10.112 timeout 5 key *claveCompartida*

3. Establecimiento de los parámetros necesarios para tener el servicio de Autenticación, Autorización y Auditoria a través del ACS v5.2.

3.1. Se configura la interfaz de acceso al equipo y se especifica el servidor que será utilizado para el efecto. En este caso, se configura el servicio

de autenticación utilizando el protocolo SSH. Como método de respaldo se define que el usuario se autentique con la base de datos local en el equipo, en este caso con el usuario local previamente configurado.

MCHBLSAM01# aaa authentication ssh ACS52 local

3.2. Se define que el proceso de autorización se realice a través del ACS v5.2, cuando se utilice SSH.

MCHBLSAM01# aaa authorization ssh ACS52 local

3.3. Con el fin de mantener un seguimiento de las actividades realizadas por el usuario que accede a la red, se define que el proceso de auditoria se realice a través del ACS v5.2.

MCHBLSAM01# aaa accounting session ACS52

4. Finalmente, se guardan los cambios realizados en la configuración.

MCHBLSAM01# write memory
MCHBLSAM01# copy working certified

4.3.2.6.4 Huawei

1. Se configura un usuario local en el equipo, con el fin de tener un método de autenticación de respaldo si se llegara a perder la conexión con el ACS v5.2. Este usuario tendrá el máximo nivel de privilegio. Se especifica que se aceptarán únicamente conexiones SSH.

[CCASTIM02] aaa
[CCASTIM02-aaa] local-user *usuarioSecreto* password cipher *passwordCifrado*
[CCASTIM02-aaa] local-user *usuarioSecreto* privilege level 15
[CCASTIM02-aaa] local-user *usuarioSecreto* service-type ssh

2. Establecimiento de una plantilla, necesaria para definir los parámetros del ACS v5.2.

2.1. Se define el nombre de la plantilla que será utilizada durante el proceso AAA. En este caso se denominará “pACS52”.

[CCASTIM02] hwtacacs-server template pACS52

2.2. Se define que en esta plantilla, los servicios de Autenticación, Autorización y Auditoria se los realizará por medio del ACS v5.2.

[CCASTIM02-hwtacacs-pACS52]hwtacacs-server authentication 10.50.10.112
[CCASTIM02-hwtacacs-pACS52]hwtacacs-server authorization 10.50.10.112
[CCASTIM02-hwtacacs-pACS52]hwtacacs-server accounting 10.50.10.112

2.3. Se define la clave compartida que esta plantilla utilizará en la negociación entre el equipo y el ACS v5.2.

[CCASTIM02-hwtacacs-pACS52] hwtacacs-server shared-key cipher *claveCompartidaCifrada*

2.4. En los equipos Huawei es necesario usar un dominio al momento de autenticarse; el siguiente comando le indica al equipo que el nombre de usuario se envíe sin el dominio al ACS v5.2 para el proceso de autenticación.

[CCASTIM02-hwtacacs-pACS52] undo hwtacacs-server user-name domain-included

3. Se definen los esquemas de Autenticación, Autorización y Auditoria que serán empleados.

3.1. Se configura el esquema de autenticación “eACS52”, indicando que este proceso se realizará a través del protocolo TACACS+ y como método de

respaldo se define que el usuario se autentique con la base de datos local en el equipo; en este caso con el usuario local previamente configurado.

[CCASTIM02] aaa
[CCASTIM02-aaa] authentication-scheme eACS52
[CCASTIM02-aaa-authen-eACS52] authentication-mode hwtacacs local
[CCASTIM02-aaa-authen-eACS52] quit

3.2. Se configura el esquema de autorización “eACS52”, indicando que este proceso se realizará a través del protocolo TACACS+ y que la autorización para la ejecución de comandos, del nivel especificado, la provea el ACS v5.2 y de perderse la conexión que se realice de forma local.

3.3. **[CCASTIM02-aaa]** authorization-scheme eACS52

[CCASTIM02-aaa-authorization-eACS52] authorization-mode hwtacacs
[CCASTIM02-aaa-authorization-eACS52] authorization-cmd 15 hwtacacs local
[CCASTIM02-aaa-authorization-eACS52] quit

3.4. Se configura el esquema de auditoría “eACS52”, indicando que este proceso se realizará a través del protocolo TACACS+.

[CCASTIM02-aaa] accounting-scheme eACS52
[CCASTIM02-aaa-accounting-eACS52] accounting-mode local hwtacacs
[CCASTIM02-aaa-accounting-eACS52] quit

4. Se configura el dominio que deberá utilizar el usuario al momento de autenticarse.

4.1. Se define el nombre del dominio “redmpls”.

[CCASTIM02-aaa] domain redmpls

4.2. Se indica qué plantilla se empleará, para definir el servidor AAA que utilizará este dominio

[CCASTIM02-aaa-domain-redmpls]hwtacacs-server pACS52

4.3. Se indican qué esquemas se emplearán para autenticación, autorización y auditoría para este dominio.

[CCASTIM02-aaa-domain-redmpls] authentication-scheme eACS52
[CCASTIM02-aaa-domain-redmpls] authorization-scheme eACS52
[CCASTIM02-aaa-domain-redmpls] accounting-scheme eACS52
[CCASTIM02-aaa-domain-redmpls] quit

5. Se definen las interfaces en las cuales se aplicará el servicio AAA a través del ACS v5.2. En este caso se aplica a la líneas vty, además se especifica que se aceptarán únicamente las conexiones remotas que utilicen el protocolo SSH.

[CCASTIM02] user-interface vty 0 14
[CCASTIM02-ui-vty0-14] authentication-mode aaa
[CCASTIM02-ui-vty0-14] protocol inbound ssh

6. Finalmente se guardan los cambios realizados en la configuración.

[CCASTIM02] quit
<CCASTIM02> save

Cabe indicar que al momento de autenticarse es necesario ingresar el nombre de usuario con el nombre del dominio; en el presente caso será:

nombreUsuario@redmpls

4.3.2.7 Configuración de reportes y alarmas

Como se describió en la sección 4.3.1.1 una las ventajas del ACS v5.2 es la mejora en cuanto a la presentación de reportes; además ofrece la configuración de alarmas que optimizan el control de acceso a la administración de los dispositivos de la red IP/MPLS. Los reportes y alarmas, (figura 4.36), se localizan en:

Monitoring and Reports > Launch Monitoring & Report Viewer

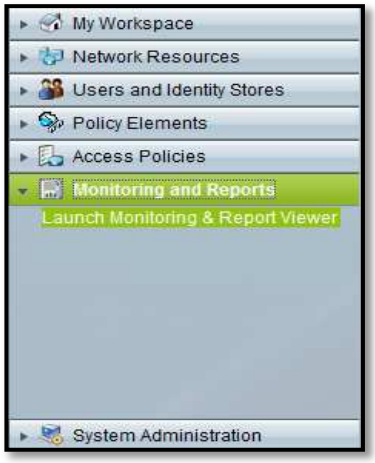


Figura 4.36: Alarmas y reportes

4.3.2.7.1 Reportes

Los reportes que se configuran en la presente guía, ver figura 4.37, tienen como fin registrar las actividades en cuanto a la administración de los equipos de la red IP/MPLS. Se determinan aquellos que hagan referencia al protocolo TACACS+ que es el que se ha utilizado.

Para ello se debe dirigir a la opción:

Monitoring & Reports > Reports > Catalog > AAA Protocol

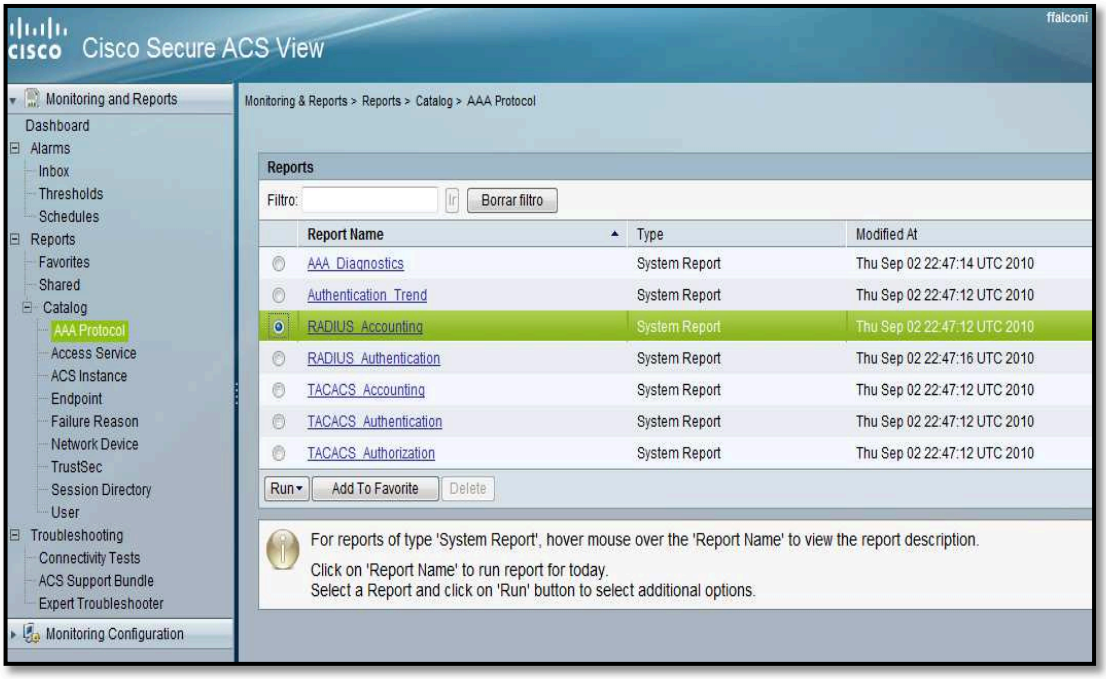
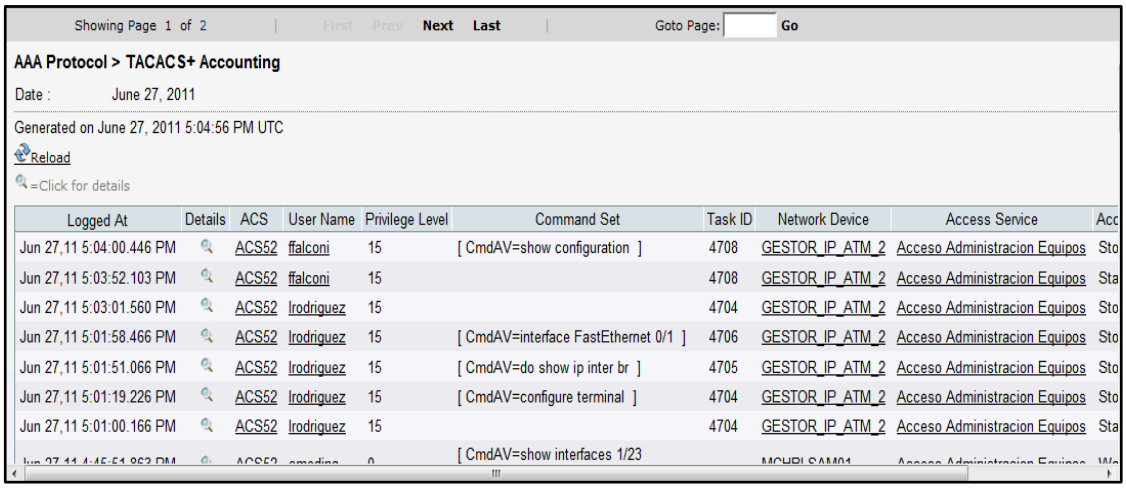


Figura 4.37: Reportes predefinidos

a) TACACS *Accounting*

Se registran la hora de conexión y desconexión de los usuarios autenticados, el nombre del usuario, el equipo al que se conecta y los comandos que se ejecutan. Se muestra en la figura 4.38 un ejemplo de este reporte.



Logged At	Details	ACS	User Name	Privilege Level	Command Set	Task ID	Network Device	Access Service	Acc
Jun 27,11 5:04:00.446 PM		ACS52	ffalconi	15	[CmdAV=show configuration]	4708	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sto
Jun 27,11 5:03:52.103 PM		ACS52	ffalconi	15		4708	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sta
Jun 27,11 5:03:01.560 PM		ACS52	lrodriguez	15		4704	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sto
Jun 27,11 5:01:58.466 PM		ACS52	lrodriguez	15	[CmdAV=interface FastEthernet 0/1]	4706	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sto
Jun 27,11 5:01:51.066 PM		ACS52	lrodriguez	15	[CmdAV=do show ip inter br]	4705	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sto
Jun 27,11 5:01:19.226 PM		ACS52	lrodriguez	15	[CmdAV=configure terminal]	4704	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sto
Jun 27,11 5:01:00.166 PM		ACS52	lrodriguez	15		4704	GESTOR_IP_ATM_2	Acceso Administracion Equipos	Sta
					[CmdAV=show interfaces 1/23				

Figura 4.38: Reporte TACACS *Accounting*

b) TACACS *Authentication*

Muestra los intentos de conexión a los diferentes equipos y si fueron validados o no; además se pueden ver los detalles de cada uno y encontrar mucha más información como la regla de acceso utilizada, la dirección IP desde la que se recibe la petición, el nombre del usuario, el grupo del usuario, etc. Estos atributos se pueden apreciar de forma más detallada en el campo *Details* haciendo *click* en la lupa. La figura 4.39 muestra un ejemplo de este reporte.

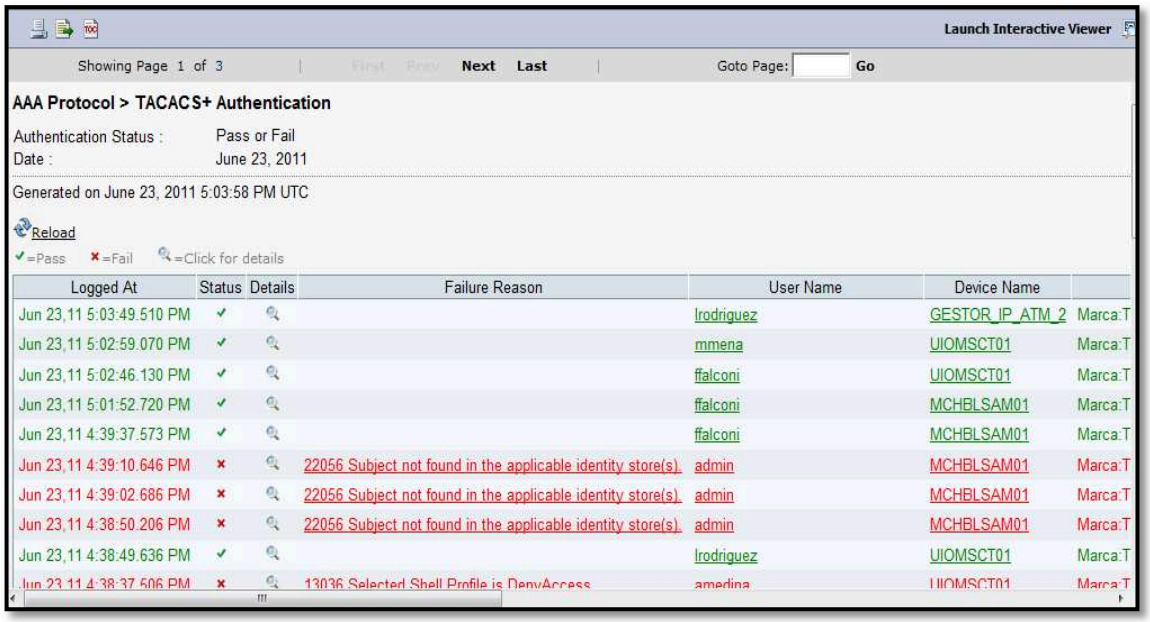


Figura 4.39: Reporte TACACS *Authentication*

c) TACACS *Authorization*

Muestra el nombre del usuario, los comandos ingresados y si éstos fueron o no autorizados a ejecutarse, el conjunto de comandos, nombre del dispositivo, etc. En la figura 4.40 se muestra un ejemplo de este reporte.

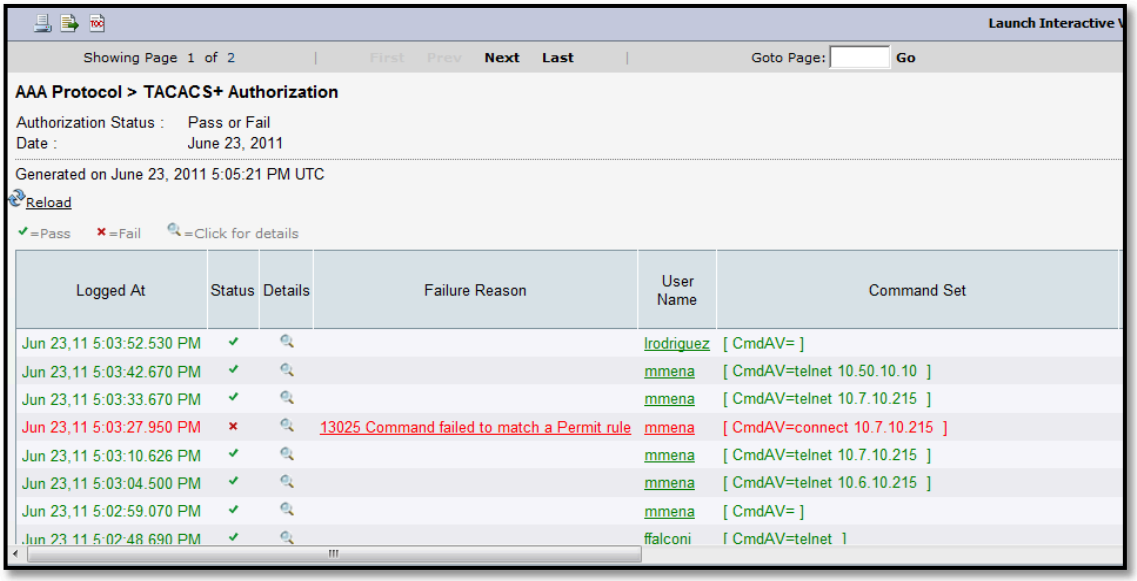


Figura 4.40: Reporte TACACS *Authorization*

4.3.2.7.2 Alarmas

Se pueden gestionar alarmas de manera que al ocurrir un evento éste se registre y se notifique. EL ACS v5.2 ofrece la posibilidad de notificar mediante *email* o mensajes *Syslog*. Para esta guía se utilizará la función de notificaciones mediante mensajes *Syslog*. Para ello se debe dirigir a la opción:

Monitoring and Reports > Alarms > Thresholds

Se pueden encontrar las alarmas creadas por defecto; se puede habilitarlas o deshabilitarlas, haciendo *click* en ellas y marcando o no la opción *enable*. La figura 4.41 muestra la configuración de la alarma "ACS – *System Errors*" creada por defecto.

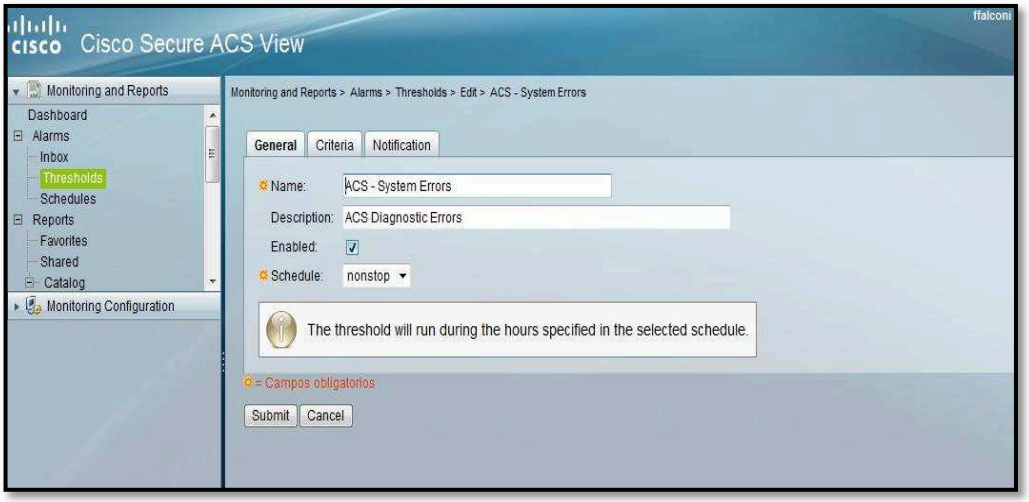


Figura 4.41: Alarma ACS –*System Errors*

a) Creación de una Alarma

Al seleccionar *Create* se muestra la pantalla para poder crear una alarma. Como ejemplo (figuras 4.42, 4.43 y 4.44), se creará una alarma que se "dispare" cada que con un mismo nombre de usuario se presenten varios intentos fallidos de conexión. Para ello se va a la opción:

Monitoring and Reports > Alarms > Thresholds > Add

En la pestaña *General* se especifica el nombre de la alarma, así como su descripción y horario.

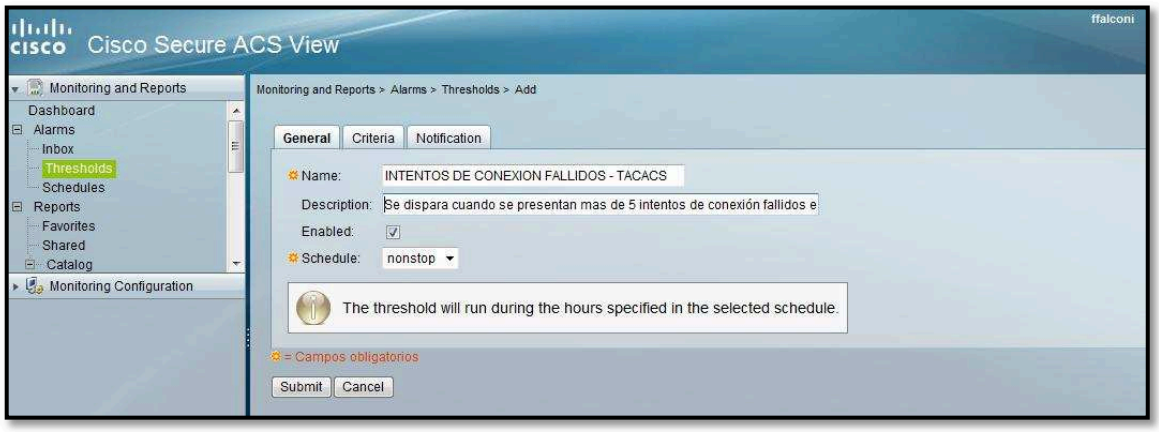


Figura 4.42: Creación de Alarmas: Pestaña *General*

En la pestaña *Criteria,* los parámetros más importantes a configurar son el tipo de alarma, el número de autenticaciones fallidas para que se “dispare” y el protocolo utilizado. Se pueden también filtrar las alarmas para seguir específicamente a un usuario, equipo, dirección MAC u otros.

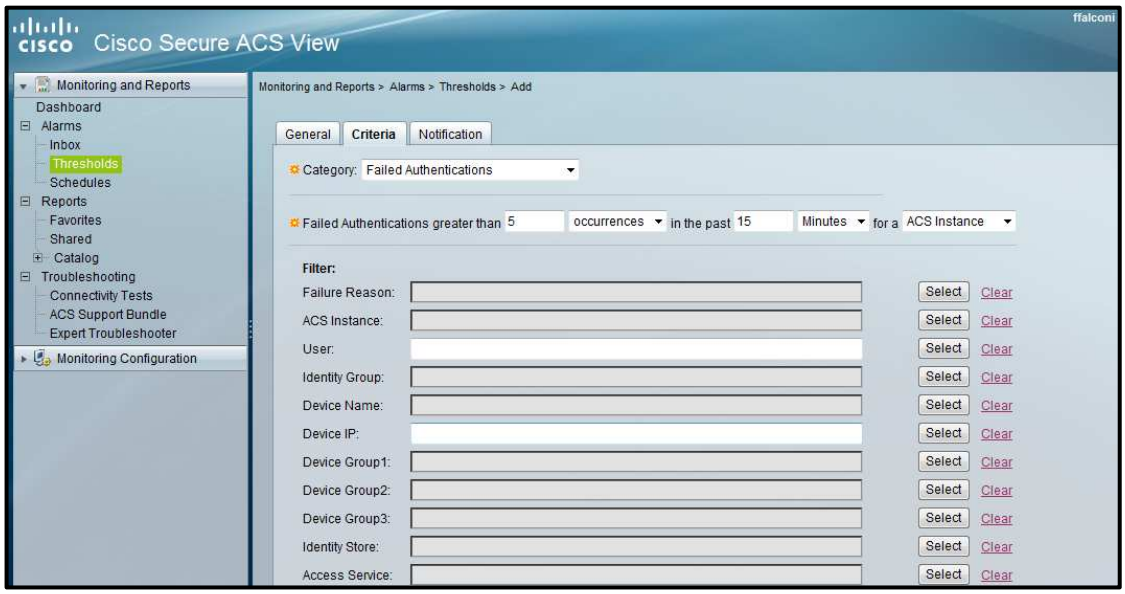


Figura 4.43: Creación de Alarmas: Pestaña *Criteria*

En la pestaña *Notification* se especifica la criticidad de la alarma y el cómo se deberá notificar.

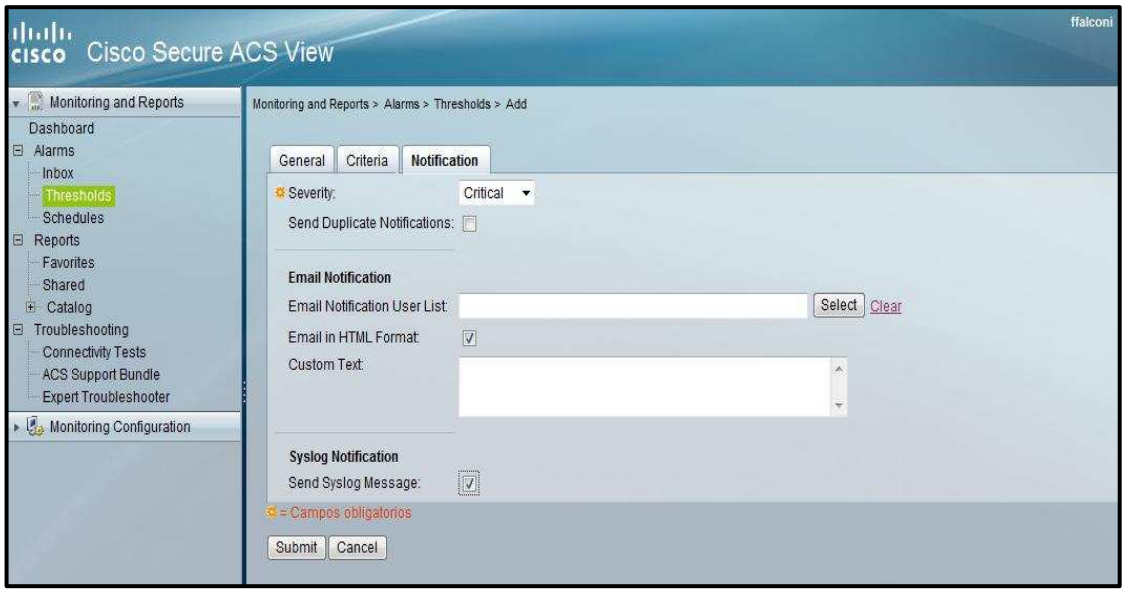


Figura 4.44: Creación de Alarmas: Pestaña *Notification*

Así se pueden crear alarmas para múltiples propósitos:

- Informar los usuarios conectados.
- Informar los comandos ingresados.
- Alarmar cuando se escribe un comando no autorizado.
- Seguir las acciones de un usuario y alarmar cuando éste realice alguna acción previamente establecida.
- Alertar cuando se cambien los parámetros del ACS v5.2 entre otros.

b) Configurar el envío de mensajes *Syslog*

Se deben definir en el ACS v5.2 los parámetros del servidor de *Syslog* al cual se enviarán las notificaciones generadas por las alarmas.

Para ello se debe ingresar a la opción:

System Administration > Configuration > Log Configuration > Remote Log Targets > Edit: "LogCollector"

En la figura 4.45 se aprecia la configuración de los parámetros del servidor de *Syslog* en el ACSv5.2; se especifica la dirección IP, el puerto definido y el tamaño máximo del mensaje. Únicamente se ingresa la IP y se deja los otros valores por defecto.

c) Ejemplo de alarma

Se utilizará la alarma creada anteriormente, “INTENTOS DE CONEXIÓN FALLIDOS”, para visualizar la generación de la alarma tanto en el ACSv5.2 como en el servidor de *Syslog*.

Figura 4.45: Configuración del Servidor de *Syslog*

Mediante un terminal en “PC GESTION” (10.50.10.112), se ingresa remotamente al equipo Alcatel MCHBLSAM01 (10.50.10.215) y se generan varios intentos fallidos de conexión utilizando el nombre de usuario “admin” que no se encuentra registrado en el ACS v5.2., ver figura 4.46.

Figura 4.46: Ingresos fallidos en MCHBLSAM01

Se debe ingresar a la opción: ***Monitoring and Reports > Alarms > Thresholds > Add***

En la pestaña *Inbox* se encontrarán las alarmas que se hayan generado para los

diversos escenarios establecidos. Se puede notar en la figura 4.47 que se ha generado una alarma para el caso en cuestión.

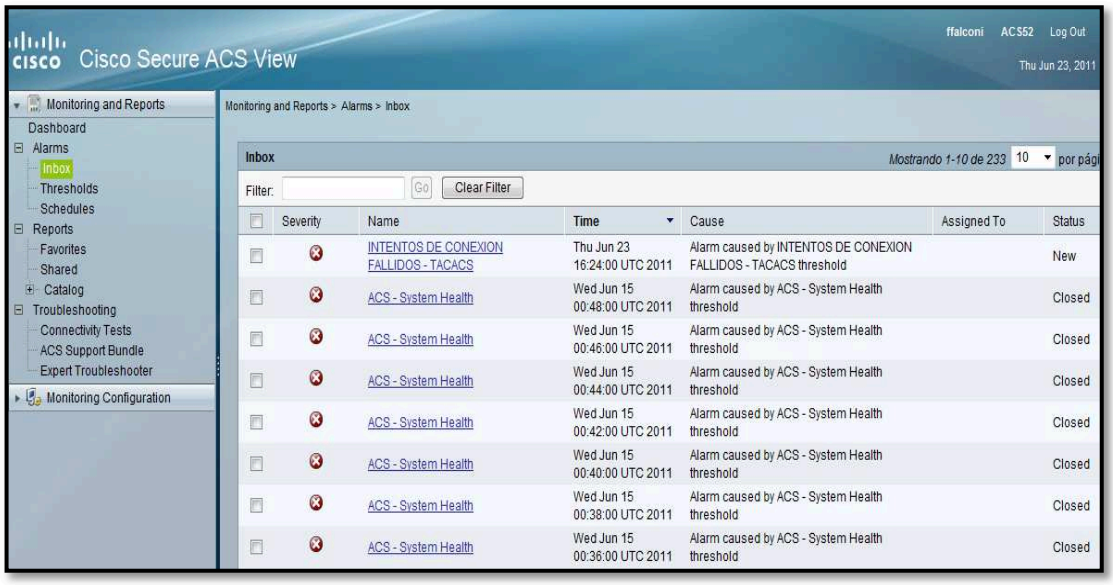


Figura 4.47: Alarma generada en el ACS v5.2

Se abre el evento “INTENTOS DE CONEXIÓN FALLIDOS - TACACS”, ver figura 4.48. Se aprecia el informe de la alarma generada, en el que se indican: fecha, causa de la alarma, el nombre de usuario y el número de intentos fallidos.

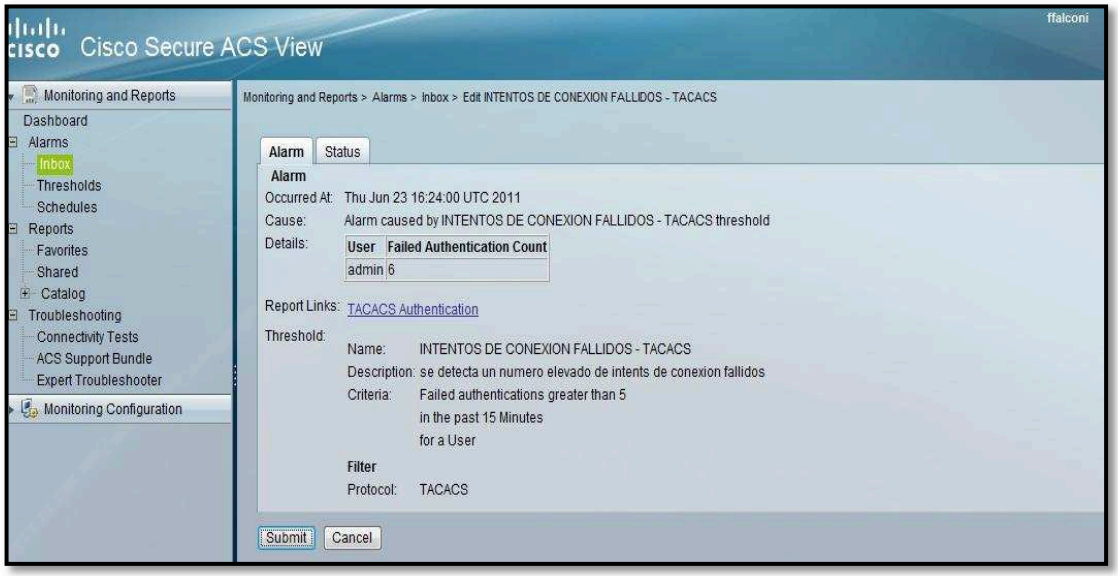


Figura 4.48: Informe de la alarma generada

Como se configuró, la alarma también se envía y se muestra en el servidor de *Syslog;* en la figura 4.49 se presenta el informe de la alarma generada y enviada al servidor de *Syslog*.

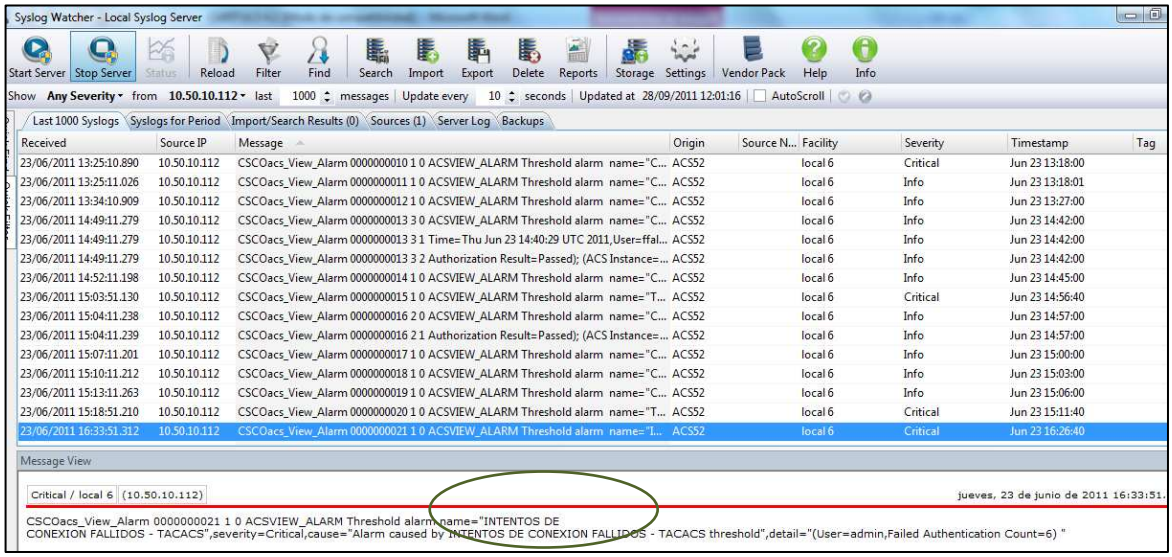


Figura 4.49: Informe de la alarma en el Servidor *Syslog*

4.3.3 PROTOCOLO DE PRUEBAS DE ACEPTACIÓN

Con la finalidad de probar las ventajas de la actualización del Sistema de Control de Acceso propuesta, se realiza el Protocolo de Pruebas de Aceptación que se encuentra en el anexo A.

4.3.4 REUBICACIÓN DEL SISTEMA DE CONTROL DE ACCESO CISCO v5.2

El Sistema de Control de Acceso al estar actualmente conectado a la red de Sistemas de la CNT E.P., depende de ésta y por ende el control de acceso a la administración de los dispositivos de red IP/MPLS. Considerando que en reiteradas ocasiones, por inconvenientes suscitados en la red de Sistemas, se ha perdido el control de acceso a la administración de los dispositivos de la red, quedando ésta sin gestión, se propone la reubicación del mismo.

Como se estableció en las normas y procedimientos para mejorar el control de acceso a la administración de los dispositivos de la red IP/MPLS, se debe contar con un Sistema de Control de Acceso primario y secundario. Se propone que éstos deben estar ubicados geográficamente distantes en las ciudades de Quito y Guayaquil. Por lo cual, se sugiere que el Sistema de Control de Acceso primario esté conectado a uno de los equipos principales de la red IP/MPLS en la ciudad de Quito, UIOMSCE01 y el secundario a otro de los nodos principales de la red en la ciudad de Guayaquil, GYECNTE01; éstos nodos cuentan actualmente con medidas de acceso restringido a sus instalaciones.

El estar físicamente ubicados en dos nodos geográficamente distantes, garantiza además de una redundancia lógica también una redundancia física.

Es necesario que tanto el Sistema de Control de Acceso primario como secundario, se ubiquen tras un *Firewall*, con la finalidad de bloquear cualquier tipo de ataque hacia éstos y solo permita el paso de tráfico autorizado. En la figura 4.50 se detalla el diagrama topológico propuesto de la reubicación del ACS v5.2.

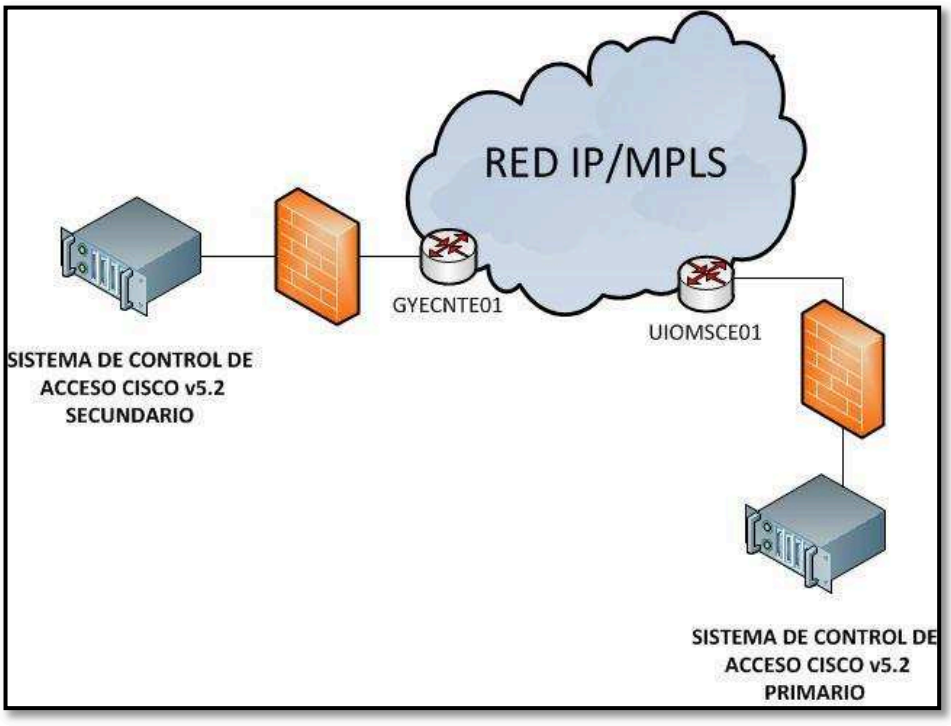


Figura 4.50: Diagrama topológico de la propuesta de reubicación del ACS v5.2

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se considera que se han cumplido todos los objetivos para los cuales fue desarrollado el presente Proyecto de Titulación.

- El objetivo principal del análisis de riesgos es identificar y valorar los riesgos a los que están expuestos todos los activos que representan un costo para la empresa, que no necesariamente tiene que ser medido en términos monetarios, y establecer los controles que se deberían implementar para minimizar o corregir los riesgos identificados.

- En la medida en que el alcance y los límites en un análisis de riesgos sean claramente establecidos, se optimizará el proceso y los resultados obtenidos serán más reales.

- Para determinar el nivel de riesgo, es necesario considerar la probabilidad de ocurrencia que tenga una amenaza y el impacto que podría ocasionar ésta, al explotar una determinada vulnerabilidad tanto en el número de clientes que se verían afectados como en el tiempo de recuperación ante el evento de riesgo.

- Los equipos tipo P en una red IP/MPLS constituyen un activo de gran importancia y por ende, será prioritario con respecto a los equipos tipo PE, aplicar los controles y medidas necesarias para mitigar los riesgos a los que éstos se encuentren expuestos.

- El éxito de los resultados obtenidos al término del proceso del análisis de riesgos, depende en gran medida de la colaboración que preste todo el recurso humano relacionado con la administración de los activos que forman parte del proceso.

- Producto del análisis de riesgos se ha determinado que en la red se presentan muchas vulnerabilidades por la falta de políticas de seguridad, por lo que se determina la importancia de contar y cumplir con las mismas.

- El desarrollo del presente proyecto de titulación ha servido como iniciativa al Área O&M Plataforma IP/MPLS para formular proyectos de seguridad referentes a aplicar los controles propuestos.

- El desarrollo del análisis de riesgos y las normas y procedimientos planteados, pueden tomarse como documento de apoyo para la implementación de un Sistema de Gestión de Seguridad de la Información, puesto que son requisitos obligatorios.

- Ciertas empresas suelen invertir grandes cantidades de dinero en herramientas tecnológicas para evitar ser víctimas de ataques externos, descuidando controlar el recurso humano mismo de la empresa, uno de los activos más importantes y difíciles de controlar, puesto que su estabilidad laboral no está garantizada. Por lo cual, concientizar al personal se vuelve una tarea necesaria para mitigar los riesgos que de ellos se puedan derivar.

- En el entorno actual, en el que el desarrollo de las telecomunicaciones ha dado pasos agigantados, los ataques informáticos se han convertido en una de las amenazas latentes para los sistemas de información; cientos de empresas han sido víctimas de este tipo de ataques. Es menester entonces, contar con herramientas tecnológicas como *firewalls*, IDSs, IPSs entre otros, implementados en las redes que reaccionen de forma

inmediata frente a este tipo de ataques y evitarlos.

- Disponer de un documento formal estableciendo los lineamientos y procedimientos para el acceso a la administración de los dispositivos de la red, garantizan indudablemente su correcta administración, además de establecer responsabilidades y poder aplicar las sanciones pertinentes ante el desacato de los mismos.

- En los inicios de las redes informáticas, las amenazas a las que se encontraban expuestas no constituían mayor preocupación, en la actualidad, se requieren niveles de seguridad más elevados, por el surgimiento exponencial de amenazas y vulnerabilidades.

- Establecer medidas de acceso a la información que viaja a través de las redes informáticas, se ha convertido en una parte importante de las decisiones de los directivos, con el único fin de garantizar su disponibilidad, confidencialidad e integridad.

- Un sistema de control de acceso proporciona los servicios de autenticación, autorización y auditoría, dando cumplimiento a una de las políticas de seguridad primordial dentro de las empresas, como es el permitir el acceso solo de personal autorizado con determinados privilegios a los activos de la red y registrar las actividades realizadas por los mismos.

- La elaboración del Protocolo de Pruebas de Aceptación, permitió verificar que el Sistema de Control de Acceso cumple los requisitos y necesidades del área O&M Plataforma IP/MPLS, en cuanto al control de acceso a la administración de los dispositivos de la red.

- Una correcta administración del Sistema de Control de Acceso garantiza el cumplimiento de las políticas de seguridad en cuanto al control de acceso

a los recursos y dispositivos de la red.

- Para que los usuarios puedan colaborar con la seguridad de la información, es preciso instruir al personal de forma apropiada sobre seguridad y sobre el uso correcto de los recursos de la empresa, a fin de que cumplan con las medidas establecidas por la organización en el desempeño habitual de sus funciones.

- La utilización de contraseñas robustas en los sistemas que las requieran es primordial al momento de evitar accesos no deseados a la información.

5.2 RECOMENDACIONES

- Se recomienda la implementación, supervisión y monitoreo de los controles propuestos para mitigar los riesgos en la red IP/MPLS de la CNT E.P. teniendo en cuenta la prioridad de los mismos.

- Realizar análisis de riesgo periódicos, con la finalidad de verificar la efectividad de los controles implementados, detectar y valorar nuevos riesgos, producto del incremento de vulnerabilidades y/o amenazas.

- Elaborar, difundir y hacer cumplir un documento formal de políticas de seguridad para el Área O&M Plataforma IP/MPLS.

- Actualizar el Sistema de Control de Acceso utilizado, con la finalidad de optimizar y supervisar de mejor manera el acceso a la administración de los dispositivos de la red IP/MPLS de la CNT E.P.

- A la hora de tomar la decisión de implementar controles que mejoren la seguridad informática en cualquiera de sus ámbitos, se debe tener en cuenta la relación costo-beneficio, es decir, si la inversión económica para

la implementación del control tiene una relación equitativa o menor con lo que se quiere proteger.

- Los controles establecidos para reducir el riesgo ante amenazas que han sido identificadas, deberán ser revisados periódicamente y modificados de ser el caso, puesto que diariamente se desarrollan nuevas formas de vulnerar la seguridad en las redes y sistemas; nuevas amenazas aparecen y se es más vulnerable.

- Los lineamientos y procedimientos establecidos para mejorar el acceso a la administración de los dispositivos de la red IP/MPLS deben ser de conocimiento de todo el personal involucrado con la red y se debe acatar a cabalidad lo establecido, solo así se podrá cumplir con su objetivo.

- Los controles establecidos para minimizar los riesgos identificados con nivel de prioridad alto, deberán ser implementados en la brevedad posible, puesto que, siempre es mejor tomar acciones correctivas y no esperar a que un evento suceda para tomar acciones al respecto.

- Los registros de auditoría almacenados en el Sistema de Control de Acceso deberán ser revisados y analizados periódicamente, se recomienda un lapso no mayor a una semana, con la finalidad de verificar el cumplimiento de las normas de seguridad del acceso a la administración de los dispositivos de la red IP/MPLS. En el caso de encontrar anomalías en el cumplimiento de tales normas se deberán tomar las medidas correctivas correspondientes.

- Se deberá disponer de un Sistema de Control de Acceso redundante, que garantice siempre los servicios de autenticación, autorización y auditoría en la administración de los dispositivos de la red IP/MPLS, siempre y cuando la relación costo beneficio así lo permita.

REFERENCIAS BIBLIOGRÁFICAS Y ELECTRÓNICAS

CAPÍTULO 1

[1] MPLS "*Multiprotocol Label Switching":* Una Arquitectura de *Backbone* para la Internet del Siglo XXI. http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MPLS.PDF

[2] MPLS-*Multiprotocol Label Switching.* http://www.ccapitalia.net/descarga/docs/2002-mpls-v3.pdf

[3] *Multiprotocol Label Switching.* http://www.intitec.org/memorias_conferencias/Memorias_MPLSv5.pdf

[4] Cisco: MPLS en Castellano. http://www.slideshare.net/proydesa/cisco-mpls-en-castellano

[5] Diseño y desarrollo de un simulador JAVA de redes MPLS sobre IP. http://upcommons.upc.edu/pfc/bitstream/2099.1/5152/1/memoria_PFC_AlfredoGarciaTorres.pdf

[6] MPLS. http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

[7] Calidad de servicio en redes IP. http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

[8] MPLS-Conmutación de etiquetas multiprotocolo.. http://es.kioskea.net/contents/internet/mpls.php3

[9] TUTORIAL TÉCNICO DE VPLS.
http://www.paratorpes.es/manuales/vpls.pdf

[10] IP/MPLS-*Based* VPNs.
http://www.brocade.com/downloads/documents/white_papers/wp-ip-mpls-based-vpns.pdf

[11] Redes MPLS y GMPLS, Servicio y Aplicaciones.
http://www.ccapitalia.net/netica/teleco/mpls-gmpls-v4.pdf

[12] Gestión de Riesgo en la Seguridad Informática.
http://protejete.wordpress.com/gdr_principal

[13] Manual de Seguridad en Redes.
http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

[14] Introducción a los conceptos de Seguridad de información.
http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%20Y%20MATERIAL%20DE%20ESTUDIO/Introducci%F3n%20a%20los%20conceptos%20de%20Seguridad.pdf

[15] TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS.
http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

[16] VIRUSinformatico.net
http://virusinformatico.net/conceptos-de-seguridad/tecnologias-y-herramientas/

[17] AMPLIACIÓN DE REDES DE COMPUTADORES, Listas de control de Acceso.
http://www.dsi.uclm.es/asignaturas/42550/PDFs/PRACTICA4.pdf

[18] *Overview* of Cisco *Secure* ACS.

http://www.cisco.com/application/pdf/en/us/guest/products/ps407/c2001/ccmigration_09186a00801085d0.pdf

[19] Soporte21*, Firewall.* http://www.soporte21.com/que_es_un_firewall.php

[20] *User Guide for Cisco Secure Access Control System 5.0.* http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/user/guide/ACSuserguide.pdf

[21] Publicada la norma ISO 27005: Gestión del riesgo http://www.xperimentos.com/2008/10/20/publicada-la-norma-iso-27005-gestion-del-riesgo/

[22] NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27005

CAPÍTULO 2

[1] Información proporcionada por el Área O&M Plataforma IP/MPLS de la CNT E.P.

[2] *Datasheets* Cisco.

[3] DSLAM. http://es.wikipedia.org/wiki/DSLAM

[4] *Unicast Streaming.* http://technet.microsoft.com/en-us/library/cc772130(WS.10).aspx

[5] Windows Media Video http://es.wikipedia.org/wiki/Windows_Media_Video

[6] *Delay.*
http://es.wiktionary.org/wiki/delay

CAPÍTULO 3

[1] Información proporcionada por el Área O&M Plataforma IP/MPLS de la CNT E.P.

CAPÍTULO 4

[1] Cisco Systems, Inc., User Guide for Cisco Secure Access Control System 5.2. Primera Edición. Cisco Systems, Inc. Estados Unidos. 2010.

ANEXO A

PROTOCOLO DE PRUEBAS DE ACEPTACIÓN DE FUNCIONALIDADES

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E.P.

PROPUESTA DE ACTUALIZACIÓN DEL SISTEMA DE CONTROL DE ACCESO

CISCO ACS v5.2

Protocolo de Pruebas de Aceptación de Funcionalidades

1 ASPECTOS GENERALES

1.1 Objetivo General

Verificar mediante las pruebas y procedimientos descritos más adelante, que el Sistema de Control de Acceso Cisco v5.2, en adelante ACS v5.2, presentado por Marco Fabricio Falconí Noriega y Lucia Silveria Rodriguez Garcia como propuesta de actualización al sistema utilizado actualmente, cumple con los requerimientos del Área O&M Plataforma IP/MPLS para el control de acceso a la administración de los dispositivos de la red IP/MPLS y está en la capacidad de ofrecer servicios AAA a equipos de las marcas Cisco, Huawei y Alcatel existentes y por adquirir.

1.2 Derechos del Documento

El presente documento ha sido elaborado por quienes presentan la propuesta y supervisado y evaluado por el Responsable de la red IP/MPLS de la CNT E.P.

1.3 Distribución

El ATP comprende dos (2) ejemplares, uno (1) para el Área O&M Plataforma IP/MPLS y uno (1) para quienes presentan la propuesta.

2 PROCEDIMIENTO DE ACEPTACIÓN

2.1 Descripción General

El proceso del ATP utilizará el escenario indicado en la figura A.1.

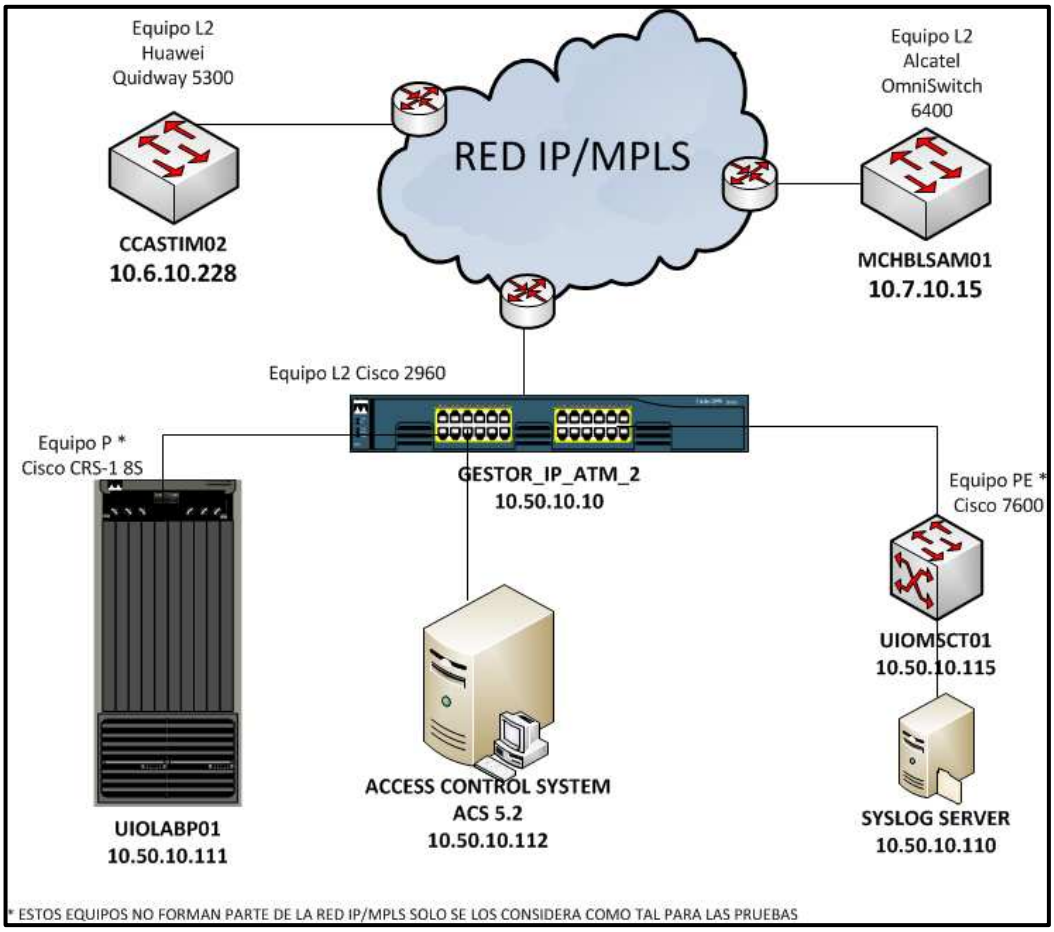


Figura A.1: Escenario utilizado para la ejecución del ATP

El proceso del ATP se puede personalizar de acuerdo al escenario particular de prueba, mediante el uso de las líneas construidas en el presente documento y que se describen a continuación.

2.2 Fases de la Prueba

- Servicios AAA

La fase de prueba Servicios AAA, se describe en la tabla A.1.

FASE DE LA PRUEBA	ELEMENTO DE PRUEBA	TÍTULO DE LA PRUEBA
Servicios AAA	ACS v5.2	Servicio de Autenticación
		Servicio de Autorización, equipo P
		Servicio de Autorización, equipo PE
		Servicio de Autorización, equipos L2
		Servicios de Auditoría

Tabla A.1: Fase Servicios AAA

- Servicios de Monitoreo

La fase de prueba Servicios de Monitoreo, se describe en la tabla A.2

FASE DE LA PRUEBA	ELEMENTOS DE PRUEBA	TÍTULO DE LA PRUEBA
Servicios de Monitoreo	ACS v5.2	Emisión y registro de alarmas

Tabla A.2: Estructura de la prueba, Servicios de Monitoreo

2.3 Escalas de Tiempo

- Fecha de inicio: 24/06/2011
- Fecha de fin: 24/06/2011

2.4 Asistentes

- Ing. Andrés Almeida, responsable de la red IP/MPLS a nivel nacional, en representación del Área O&M Plataforma IP/MPLS.
- Lucia Rodríguez y Fabricio Falconí, quienes presentan la propuesta.

2.5 Equipos de Prueba

En la tabla A.3 se detallan los equipos que intervienen para el desarrollo del ATP.

EQUIPO	MODELO	DESCRIPCIÓN
UIOMSCP01	CRS-1 8Slot	Equipo de pruebas utilizado por el Área O&M Plataforma IP/MPLS. Para el desarrollo del ATP hará las funciones de Equipo tipo P. IOS XR Cisco.
UIOMSCT01	Cisco 7600	Equipo del Área O&M Plataforma IP/MPLS. Para el desarrollo del ATP hará las funciones de Equipo tipo PE. IOS Cisco.
GESTOR_IP_ATM_2	Cisco 2960	Equipo de conmutación del laboratorio de pruebas del Área O&M Plataforma IP/MPLS. Para el desarrollo del ATP hará las funciones de Equipo tipo L2. IOS Cisco.
MCHBLSAM01	Alcatel OmniSwitch 6400	Equipo en proceso de pruebas conectado a la red IP/MPLS. Equipo tipo L2. IOS Alcatel.
CCASTIM01	Huawei Quidway 5300	Equipo en proceso de pruebas conectado a la red IP/MPLS. Equipo tipo L2. IOS Huawei.
PC GESTIÓN	Xtratech	PC del Área O&M Plataformas IP/MPLS desde la cual se realizarán las verificaciones necesarias. Windows XP.
SERVIDOR SYSLOG	HP Pavilion dv4	PC de la topología de prueba que funciona como servidor Syslog. Windows 7.

Tabla A.3: Equipos de prueba

2.6 Programación de la Prueba

Prueba No.	Descripción de la Prueba	Resultado

Pruebas de Servicios AAA

SA1	Servicio de Autenticación	Pasó	Falló
SA2	Servicio de Autorización, equipo P	Pasó	Falló
SA3	Servicio de Autorización, equipo PE	Pasó	Falló
SA4	Servicio de Autorización, equipos L2	Pasó	Falló
SA5	Servicio de Auditoría	Pasó	Falló

Para las pruebas de autorización, en la tabla A.4 se describen los conjuntos de comandos para los diferentes IOS Cisco, Alcatel y Huawei, que en conjunto con el Responsable de la red IP/MPLS, Ing. Andrés Almeida, se han definido como ejemplo considerando la redefinición propuesta. Se recuerda que el conjunto de comandos de mayor jerarquía abarca los comandos definidos en el menos jerárquico.

Pruebas de Servicios de Monitoreo

SM1	Emisión y registro de alarmas	Pasó	Falló

2.7 Criterios de Éxito

Todas las pruebas de servicio AAA deben tener como criterio PASÓ después de la finalización del ATP.

SET DE COMANDOS	CISCO		IOS ALCATEL	IOS HUAWEI
	IOS XR CISCO	IOS CISCO		
VISUALIZACIÓN	ping	ping	ping	ping
	ssh	ssh	ssh	ssh
	telnet	telnet	telnet	telnet
	traceroute	traceroute	traceroute	tracert
	exit	exit	exit	quit
	show history	show history	show history	display history
	show version	show version	show chassis	display version
	show protocols	show ip protocols	show ip protocols	display ip protocols
	show interface	show interface	show interface	display interface
	show interfaces	show interfaces	show interfaces	display interfaces
	show ipv4 interface	show ip interface	show ip interface	display ip interface
VISUALIZACIÓN PLUS	configure	configure terminal		system-view
	interface	interface		interface
	description	description	interface alias	description
	clock set	clock set	system time	clock
	hostname	hostname	system name	sysname
	show clock	show clock	show time	display clock
	show mac-address-table	show mac-address-table	show mac-address-table	display mac-address-table
	show vlan interface	show vlan	show vlan	display vlan
	show arp	show arp	show arp	display arp
	show ip route	show ip route	show ip route	display ip routing-table
	show route static	show ip route static	show ip router database	display ip routing-table static
	commit	write memory	write memory	save
	copy running-config startup-config	copy running-config startup-config	copy working certified	save
CONFIGURACIÓN	ipv4 address	ip address	ip interface	ip address
	router static	ip route	ip static-route	ip route-static
	dot1q vlan	vlan	vlan	vlan
		switchport mode trunk	vlan 802.1q	port link-type trunk
	snmp-server engineid local	snmp-server	snmp station	snmp-agent
	router ospf	router ospf	ip ospf interface	ospf
	router isis	router isis	ip isis interface	isis
	qos group	mls qos cos	qos	qos car
	policy-map	policy-map	policy rule	qos policy
	no shutdown	no shutdown	no shutdown	undo shutdown
	no router static	no ip route	no ip static-route	undo ip route-static
	no interface	no interface	no ip interface	undo interface
	no policy-map	no policy-map	no policy rule	undo qos policy
	show spanning-tree	show spanning-tree	show spantree	display stp
	show processes cpu	show processes cpu	show health all	display processes cpu
	show processes memory	show processes memory	show health all	display processes memory
	show snmp engineid	show snmp-server	show snmp-station	display snmp-agent
	show access-list ipv4	show access-list	show ip access-list	display acl
	show ip ospf	show ip route ospf	show ip ospf	display ospf
ADMINISTRACIÓN	Todos los comandos	Todos los comandos	Todos los comandos	Todos los comandos

Tabla A.4: Conjuntos de comandos Cisco, Alcatel y Huawei

3 EJECUCIÓN DEL PROCEDIMIENTO DE LA PRUEBA DE ACEPTACIÓN

3.1 Servicios AAA

3.1.1 Servicio de Autenticación

Prueba No.	SA1	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	
Categoría de la Prueba:		Servicios AAA	
Título de la Prueba:		Servicio de Autenticación	
Propósito de la Prueba:		Verificar que el ACS v5.2 está en la capacidad de autenticar a los usuarios que desean acceder a la administración de los dispositivos en las marcas Cisco, Alcatel y Huawei.	
Marca:		Cisco	
IOS:		IOS XR Cisco	
Modelo del Equipo:		CSR-1 8-Slot	
Tipo de Dispositivo:		Equipo tipo P	
Hostname:		UIOLABP01	
Configuración de la Prueba:		El equipo UIOLABP01 tiene conectividad con el ACS v5.2 al momento de ejecutarse el ATP.	

Procedimiento:	1. Autenticarse con el usuario **aalmeida** (“MPLS_Nivel2”) para acceder a la administración del dispositivo UIOLABP01. 2. Autenticarse con el usuario **zandrade** (no configurado en el ACS v5.2) para acceder a la administración del dispositivo UIOLABP01. 3. Autenticarse con el usuario **bmacas** (“REG 4”) para acceder a la administración del dispositivo UIOLABP01. 4. Autenticarse con el usuario **candrade** (“REG 2”) para acceder a la administración del dispositivo UIOLABP01.
Resultado esperado:	1. El usuario **aalmeida** deberá autenticarse correctamente. 2. El usuario **zandrade** no deberá autenticarse, ya que no se encuentra registrado en la base de datos interna de usuarios del ACS v5.2. 3. EL usuario **bmacas** no deberá autenticarse, restringido el acceso para los subgrupos regionales al equipo UIOLABP01, excepto para los usuarios del subgrupo “REG “2. 4. El usuario **candrade** deberá autenticarse correctamente.

Verificaciones:	
1. Autenticación con el usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autenticación con el usuario zandrade.	**Pasó:** ☐ **Falló:** ☐
3. Autenticación con el usuario bmacas.	**Pasó:** ☐ **Falló:** ☐
4. Autenticación con el usuario candrade.	**Pasó:** ☐ **Falló:** ☐

Marca:	Cisco
IOS	IOS Cisco
Modelo del Equipo:	Cisco 7600
Tipo de Dispositivo:	Equipo tipo PE
Hostname:	UIOMSCT01
Configuración de la Prueba:	El equipo UIOMSCT01 tiene conectividad con el ACS v5.2 al momento de ejecutarse el ATP.

Procedimiento:	1. Autenticarse con el usuario **aalmeida** (“MPLS_Nivel2”) para acceder a la administración del dispositivo UIOMSCT01. 2. Autenticarse con el usuario **cwendy** (no configurado en el ACS v5.2) para acceder a la administración del dispositivo UIOMSCT01. 3. Autenticarse con el usuario **amedina** (“REG 3”) para acceder a la administración del dispositivo UIOMSCT01. 4. Autenticarse con el usuario **candrade** (“REG 2”) para acceder a la administración del dispositivo UIOMSCT01.
Resultado esperado:	1. El usuario **aalmeida** deberá autenticarse correctamente. 2. El usuario **cwendy** no deberá autenticarse, ya que no se encuentra registrado en la base de datos interna de usuarios del ACS v5.2. 3. EL usuario **amedina** no deberá autenticarse, restringido el acceso para los subgrupos regionales al equipo UIOMSCT01, excepto para los usuarios del subgrupo “REG 2”. 4. El usuario **candrade** deberá autenticarse correctamente.

Verificaciones:	
1. Autenticación con el usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autenticación con el usuario cwendy.	**Pasó:** ☐ **Falló:** ☐
3. Autenticación con el usuario amedina.	**Pasó:** ☐ **Falló:** ☐
4. Autenticación con el usuario candrade.	**Pasó:** ☐ **Falló:** ☐

Marca:	Alcatel
Modelo del Equipo:	OmniSwitch 6400
Tipo de Dispositivo:	Equipo tipo L2

Hostname:	MCHBLSAM01
Configuración de la Prueba:	El equipo MCHBLSAM01 tiene conectividad con el ACS v5.2 al momento de ejecutarse el ATP.
Procedimiento:	1. Autenticarse con el usuario **aalmeida** (“MPLS_Nivel2”) para acceder a la administración del dispositivo MCHBLSAM01. 2. Autenticarse con el usuario **bguevara** (no configurado en el ACSv5.2) para acceder a la administración del dispositivo MCHBLSAM01. 3. Autenticarse con el usuario **chidalgo** (“REG 6”) para acceder a la administración del dispositivo MCHBLSAM01. 4. Autenticarse con el usuario **atierra** (“REG 7”) para acceder a la administración del dispositivo MCHBLSAM01.
Resultado esperado:	1. El usuario **aalmeida** deberá autenticarse correctamente. 2. El usuario **bguevara** no deberá autenticarse, ya que no se encuentra registrado en la base de datos interna de usuarios del ACS v5.2. 3. EL usuario **chidalgo** no deberá autenticarse, restringido el acceso para los subgrupos regionales al equipo MCHBLSAM01, excepto para los usuarios del subgrupo “REG 7”. 4. El usuario **atierra** deberá autenticarse correctamente.

Verificaciones:	
1. Autenticación con el usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autenticación con el usuario bguevara.	**Pasó:** ☐ **Falló:** ☐
3. Autenticación con el usuario chidalgo.	**Pasó:** ☐ **Falló:** ☐
4. Autenticación con el usuario atierra.	**Pasó:** ☐ **Falló:** ☐

Marca:	Huawei
Modelo del Equipo:	Quidway 6524
Tipo de Dispositivo:	Equipo tipo L2

Hostname:	CCASTIM02
Configuración de la Prueba:	El ACS v5.2 tiene conectividad con el equipo CCASTIM02 al momento de ejecutarse el ATP.
Procedimiento:	1. Autenticarse con el usuario **aalmeida** (“MPLS_Nivel2”) para acceder a la administración del dispositivo CCASTIM02. 2. Autenticarse con el usuario **asaavedra** (no configurado en el ACSv5.2) para acceder a la administración del dispositivo CCASTIM02. 3. Autenticarse con el usuario **pvilla** (“REG 1”) para acceder a la administración del dispositivo CCASTIM02. 4. Autenticarse con el usuario **chidalgo** (“REG 6”) para acceder a la administración del dispositivo CCASTIM02.
Resultado esperado:	1. El usuario **aalmeida** deberá autenticarse correctamente. 2. El usuario **asaavedra** no deberá autenticarse, ya que no se encuentra registrado en la base de datos interna de usuarios del ACS v5.2. 3. El usuario **pvilla** no deberá autenticarse, restringido el acceso para los subgrupos regionales al equipo CCASTIM02, excepto para los usuarios del subgrupo REG 6. 4. El usuario **chidalgo** deberá autenticarse correctamente.

Verificaciones:

1. Autenticación con el usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autenticación con el usuario asaavedra.	**Pasó:** ☐ **Falló:** ☐
3. Autenticación con el usuario pvilla.	**Pasó:** ☐ **Falló:** ☐
4. Autenticación con el usuario chidalgo.	**Pasó:** ☐ **Falló:** ☐

3.1.2 Servicio de Autorización, equipo P

Prueba No.	SA2	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	
Categoría de la Prueba:		Servicios AAA	
Título de la Prueba:		Servicio de Autorización, equipo P	
Propósito de la Prueba:		Verificar que el Sistema de Control de Acceso ACS v5.2 está en la capacidad de autorizar la ejecución de ciertos comandos al acceder a la administración de los dispositivos tipo P, tomando en cuenta el grupo de usuario y el set de comandos asignado.	
Marca:		Cisco	
IOS:		IOS XR Cisco	
Modelo del Equipo:		CSR-1 8-Slot	
Tipo de Dispositivo:		Equipo tipo P	
Hostname:		UIOLABP01	
Configuración de la Prueba:		El equipo UIOLABP01 tiene conectividad con el ACS v5.2 al momento de ejecutarse el ATP.	
Procedimiento:		1. Acceder al dispositivo UIOLABP01 con el usuario **aalmeida** (“MPLS_Nivel2”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 2. Acceder al dispositivo UIOLABP01 con el usuario **lrodriguez** (“DESCA”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 3. Acceder al dispositivo UIOLABP01 con el usuario **lroca** (“MPLS_Nivel1”, “Visualización Plus”) e ingresar comandos correspondientes a los sets “Visualización”	

	y “Visualización Plus” (tabla 2.4). 4. Acceder al dispositivo UIOLABP01 con el usuario **lroca** (“MPLS_Nivel1”, “Visualización Plus”) e ingresar comandos que no estén definidos en los sets “Visualización” y “Visualización Plus” (tabla 2.4). 5. Acceder al dispositivo UIOLABP01 con el usuario **aheredia** (“GESTIÓN DE RED”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 3 y 4. 6. Acceder al dispositivo UIOLABP01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos correspondientes al set “Visualización” (tabla 2.4). 7. Acceder al dispositivo UIOLABP01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos no definidos en el set de comandos “Visualización” (tabla 2.4). 8. Acceder al dispositivo UIOLABP01 con el usuario **acabrera** (“NOC”, “Visualización”) e ingresar los comandos indicados en los puntos 6 y 7. 9. Acceder al dispositivo UIOLABP01 con el usuario **preina** (“INGENIERÍA”, “Visualización”) e ingresar los comandos indicados en los puntos 6 y 7. 10. Acceder al dispositivo UIOLABP01 con el usuario **candrade** (“REG 2”, “Visualización”) e ingresar los comandos indicados en los puntos 6 y 7. 11. Acceder al dispositivo UIOLABP01 con el usuario **amolina** (“O&M DATOS INTERNET, TV Y TELEF”, “Visualización”) e ingresar los comandos indicados en los puntos 6 y 7.
Resultado esperado:	1. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 2. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 3. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 4. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 5. Se deberán tener los mismos resultados de los puntos 3 y 4. 6. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 7. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 8. Se deberán tener los mismos resultados de los puntos 6 y 7. 9. Se deberán tener los mismos resultados de los puntos

	6 y 7. 10. Se deberán tener los mismos resultados de los puntos 6 y 7. 11. Se deberán tener los mismos resultados de los puntos 6 y 7.
Verificaciones:	
1. Autorización al usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autorización al usuario lrodriguez.	**Pasó:** ☐ **Falló:** ☐
3. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
4. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
5. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
6. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
7. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
8. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
9. Autorización al usuario preina.	**Pasó:** ☐ **Falló:** ☐
10. Autorización al usuario candrade.	**Pasó:** ☐ **Falló:** ☐
11. Autorización al usuario amolina.	**Pasó:** ☐ **Falló:** ☐

3.1.3 Servicio de Autorización, equipo PE

Prueba No.	SA3	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	

Categoría de la Prueba:	Servicios AAA
Título de la Prueba:	Servicio de Autorización, equipo PE
Propósito de la Prueba:	Verificar que el Sistema de Control de Acceso ACS v5.2 está en la capacidad de autorizar ejecutar ciertos comandos al acceder a la administración de los dispositivos tipo PE, tomando en cuenta el grupo de usuario y el set de comandos asignado.
Marca:	Cisco
IOS:	IOS Cisco
Modelo del Equipo:	Cisco 7600
Tipo de Dispositivo:	Equipo tipo PE
Hostname:	UIOMSCT01
Configuración de la Prueba:	El equipo UIOMSCT01 tiene conectividad con el ACS v5.2 al momento de ejecutarse el ATP.
Procedimiento:	1. Acceder al dispositivo UIOMSCT01 con el usuario **aalmeida** (“MPLS_Nivel2”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 2. Acceder al dispositivo UIOMSCT01 con el usuario **lrodriguez** (“DESCA”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 3. Acceder al dispositivo UIOMSCT01 con el usuario **lroca** (“MPLS Nivel1”, “Configuración”) e ingresar comandos correspondientes a los sets “Visualización” “Visualización Plus” y “Configuración” (tabla 2.4). 4. Acceder al dispositivo UIOMSCT01 con el usuario **lroca** (“MPLS Nivel1”, “Configuración”) e ingresar comandos no definidos en los sets “Visualización” “Visualización Plus” y “Configuración” (tabla 2.4). 5. Acceder al dispositivo UIOMSCT01 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar los comandos indicados en los puntos 3 y 4. 6. Acceder al dispositivo UIOMSCT01 con el usuario **candrade** (“REG 2”, “Visualización Plus”) e ingresar los comandos correspondientes a los sets “Visualización” y “Visualización Plus” (tabla 2.4). 7. Acceder al dispositivo UIOMSCT01 con el usuario **candrade** (“REG 2”, “Visualización Plus”) e ingresar

	comandos no definidos en los sets “Visualización” y “Visualización Plus” (tabla 2.4). 8. Acceder al dispositivo UIOMSCT01 con el usuario **preina** (“INGENIERÍA”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 9. Acceder al dispositivo UIOMSCT01 con el usuario **acabrera** (“NOC”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 10. Acceder al dispositivo UIOMSCT01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar los comandos definidos en el set “Visualización” (tabla 2.4). 11. Acceder al dispositivo UIOMSCT01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos no definidos en el set “Visualización” (tabla 2.4). 12. Acceder al dispositivo UIOMSCT01 con el usuario **amolina** (“O&M DATOS, INTERNET, TV Y TELF”, “Visualización”) e ingresar los comandos indicados en los puntos 10 y 11.
Resultado esperado:	1. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 2. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 3. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 4. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 5. Se deberán obtener los mismos resultados de los puntos 3 y 4. 6. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 7. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 8. Se deberán obtener los mismos resultados de los puntos 6 y 7. 9. Se deberán obtener los mismos resultados de los puntos 6 y 7. 10. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 11. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 12. Se deberán obtener los mismos resultados de los puntos 10 y 11.
Verificaciones:	

1. Autorización al usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autorización al usuario lrodriguez.	**Pasó:** ☐ **Falló:** ☐
3. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
4. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
5. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
6. Autorización al usuario candrade.	**Pasó:** ☐ **Falló:** ☐
7. Autorización al usuario candrade.	**Pasó:** ☐ **Falló:** ☐
8. Autorización al usuario preina.	**Pasó:** ☐ **Falló:** ☐
9. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
10. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
11. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
12. Autorización al usuario amolina.	**Pasó:** ☐ **Falló:** ☐

3.1.4 Servicio de Autorización, equipos L2

Prueba No.	SA4	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	
Categoría de la Prueba:		Servicios AAA	
Título de la Prueba:		Servicio de Autorización, equipos L2	
Propósito de la Prueba:		Verificar que el Sistema de Control de Acceso ACS v5.2 está en la capacidad de autorizar ejecutar ciertos comandos al acceder a la administración de los dispositivos tipo L2 de las marcas Cisco, Alcatel y Huawei, tomando en cuenta el grupo de usuario y el set de comandos asignado.	
Marca:		Cisco	

IOS:	IOS Cisco
Modelo del Equipo:	Cisco 2960
Tipo de Dispositivo:	Equipo tipo L2
Hostname:	GESTOR_IP_ATM_2
Configuración de la Prueba:	El ACS v5.2 tiene conectividad con el equipo UIOMSCT01 al momento de ejecutarse el ATP.
Procedimiento:	1. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **aalmeida** (“MPLS_Nivel2”, “Administración”) e ingresar comandos correspondientes al set “Administración”. 2. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **lrodriguez** (“DESCA”, “Administración”) e ingresar comandos correspondientes al set “Administración. 3. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **lroca** (“MPLS_Nivel1”, “Administración”) e ingresar comandos correspondientes al set “Administración”. 4. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar comandos correspondientes a los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 5. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar comandos no definidos en los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 6. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **candrade** (“REG 2”, “Visualización Plus”) e ingresar comandos correspondientes a los sets “Visualización” y “Visualización Plus” (tabla 2.4). 7. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **candrade** (“REG 2”, “Visualización Plus”) e ingresar comandos no definidos en los sets “Visualización” y “Visualización Plus” (tabla 2.4). 8. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **acabrera** (“NOC”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 9. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **preina** (“INGENIERÍA”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 10. Acceder al dispositivo UIOMSCT01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos correspondientes al set “Visualización”

	(tabla 2.4). 11. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos no definidos en el set “Visualización” (tabla 2.4). 12. Acceder al dispositivo GESTOR_IP_ATM_2 con el usuario **amolina** (“O&M SOLUCIONES DATOS, INTERNET, TV Y TELEF”, “Visualización”) e ingresar los comandos indicados en los puntos 10 y 11.
Resultado esperado:	1. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 2. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 3. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 4. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 5. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 6. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 7. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 8. Se deberán obtener los mismos resultados de los puntos 6 y 7. 9. Se deberán obtener los mismos resultados de los puntos 6 y 7. 10. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 11. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 12. Se deberán obtener los mismos resultados de los puntos 10 y 11.
Verificaciones:	
1. Autorización al usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autorización al usuario lrodriguez.	**Pasó:** ☐ **Falló:** ☐
3. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
4. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐

5. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
6. Autorización al usuario candrade.	**Pasó:** ☐ **Falló:** ☐
7. Autorización al usuario candrade.	**Pasó:** ☐ **Falló:** ☐
8. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
9. Autorización al usuario preina.	**Pasó:** ☐ **Falló:** ☐
10. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
11. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
12. Autorización al usuario amolina.	**Pasó:** ☐ **Falló:** ☐

Marca:	Alcatel
Modelo del Equipo:	OmniSwitch 6400
Tipo de Dispositivo:	Equipo L2
Hostname:	MCHBLSAM01
Configuración de la Prueba:	El ACS v5.2 tiene conectividad con el equipo MCHBLSAM01 al momento de ejecutarse el ATP.
Procedimiento:	1. Acceder al dispositivo MCHBLSAM01 con el usuario **aalmeida** (“MPLS_Nivel2”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 2. Acceder al dispositivo MCHBLSAM01 con el usuario **lrodriguez** (“DESCA”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 3. Acceder al dispositivo MCHBLSAM01 con el usuario **lroca** (“MPLS_Nivel1”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 4. Acceder al dispositivo MCHBLSAM01 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar comandos correspondientes a los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 5. Acceder al dispositivo MCHBLSAM01 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e

	ingresar comandos no definidos en los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 6. Acceder al dispositivo MCHBLSAM01 con el usuario **acabrera** (“NOC”, “Visualización Plus”) e ingresar comandos correspondientes a los sets “Visualización” y “Visualización Plus” (tabla 2.4). 7. Acceder al dispositivo MCHBLSAM01 con el usuario **acabrera** (“NOC”, “Visualización Plus”) e ingresar comandos no definidos en los sets “Visualización” y “Visualización Plus” (tabla 2.4). 8. Acceder al dispositivo MCHBLSAM01 con el usuario **preina** (“INGENIERÍA”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 9. Acceder al dispositivo MCHBLSAM01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos correspondientes al set “Visualización” (tabla 2.4). 10. Acceder al dispositivo MCHBLSAM01 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos no definidos en el set “Visualización” (tabla 2.4). 11. Acceder al dispositivo MCHBLSAM01 con el usuario **amolina** (“O&M SOLUCIONES DATOS, INTERNET, TV Y TELEF”, “Visualización”) e ingresar los comandos indicados en los puntos 9 y 10. 12. Acceder al dispositivo MCHBLSAM01 con el usuario **atierra** (“REG 7”, “Visualización”) e ingresar los comandos indicados en los puntos 9 y 10.
Resultado esperado:	1. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 2. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 3. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 4. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 5. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 6. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 7. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 8. Se deberán obtener los mismos resultados de los puntos 6 y 7. 9. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 10. Al usuario autenticado no se le autorizará ejecutar

	ningún comando ingresado. 11. Se deberán obtener los mismos resultados de los puntos 9 y 10. 12. Se deberán obtener los mismos resultados de los puntos 9 y 10.

Verificaciones:	
1. Autorización al usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autorización al usuario lrodriguez.	**Pasó:** ☐ **Falló:** ☐
3. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
4. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
5. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
6. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
7. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
8. Autorización al usuario preina.	**Pasó:** ☐ **Falló:** ☐
9. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
10. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
11. Autorización al usuario amolina.	**Pasó:** ☐ **Falló:** ☐
12. Autorización al usuario atierra.	**Pasó:** ☐ **Falló:** ☐

Marca:	Huawei
Modelo del Equipo:	Quidway 5300
Tipo de Dispositivo:	Equipo tipo L2
Hostname:	CCASTIM02
Configuración de la Prueba:	El equipo UIOMSCT01 tiene conectividad con el ACS v5.2 al

	momento de ejecutarse el ATP.
Procedimiento:	1. Acceder al dispositivo CCASTIM02 con el usuario **aalmeida** (“MPLS_Nivel2”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 2. Acceder al dispositivo CCASTIM02 con el usuario **lrodriguez** (“DESCA”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 3. Acceder al dispositivo CCASTIM02 con el usuario **lroca** (“MPLS_Nivel1”, “Administración”) e ingresar comandos correspondientes al set “Administración” (tabla 2.4). 4. Acceder al dispositivo CCASTIM02 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar comandos correspondientes a los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 5. Acceder al dispositivo CCASTIM02 con el usuario **aheredia** (“GESTIÓN DE RED”, “Configuración”) e ingresar comandos no definidos en los sets “Visualización”, “Visualización Plus” y “Configuración” (tabla 2.4). 6. Acceder al dispositivo CCASTIM02 con el usuario **acabrera** (“NOC”, “Visualización Plus”) e ingresar comandos correspondientes a los sets “Visualización” y “Visualización Plus” (tabla 2.4). 7. Acceder al dispositivo CCASTIM02 con el usuario **acabrera** (“NOC”, “Visualización Plus”) y ejecutar los comandos no definidos en los sets de comandos “Visualización” y “Visualización Plus” (tabla 2.4). 8. Acceder al dispositivo CCASTIM02 con el usuario **preina** (“INGENIERÍA”, “Visualización Plus”) e ingresar los comandos indicados en los puntos 6 y 7. 9. Acceder al dispositivo CCASTIM02 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos correspondientes al set “Visualización” (tabla 2.4). 10. Acceder al dispositivo CCASTIM02 con el usuario **mmena** (“CALL CENTER”, “Visualización”) e ingresar comandos no definidos en el set “Visualización” (tabla 2.4). 11. Acceder al dispositivo CCASTIM02 con el usuario **amolina** (“O&M SOLUCIONES DATOS, INTERNET, TV Y TELEF”, “Visualización”) e ingresar los comandos indicados en los puntos 9 y 10. 12. Acceder al dispositivo CCASTIM02 con el usuario **chidalgo** (“REG 6”, “Visualización”) e ingresar los comandos indicados en los puntos 9 y 10.

Resultado esperado:	1. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 2. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 3. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 4. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 5. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 6. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 7. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 8. Se deberán obtener los mismos resultados de los puntos 6 y 7. 9. Al usuario autenticado se le autorizará ejecutar todos los comandos ingresados. 10. Al usuario autenticado no se le autorizará ejecutar ningún comando ingresado. 11. Se deberán obtener los mismos resultados de los puntos 9 y 10. 12. Se deberán obtener los mismos resultados de los puntos 9 y 10.

Verificaciones:

1. Autorización al usuario aalmeida.	**Pasó:** ☐ **Falló:** ☐
2. Autorización al usuario lrodriguez.	**Pasó:** ☐ **Falló:** ☐
3. Autorización al usuario lroca.	**Pasó:** ☐ **Falló:** ☐
4. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
5. Autorización al usuario aheredia.	**Pasó:** ☐ **Falló:** ☐
6. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
7. Autorización al usuario acabrera.	**Pasó:** ☐ **Falló:** ☐
8. Autorización al usuario preina.	**Pasó:** ☐ **Falló:** ☐

9. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
10. Autorización al usuario mmena.	**Pasó:** ☐ **Falló:** ☐
11. Autorización al usuario amolina.	**Pasó:** ☐ **Falló:** ☐
12. Autorización al usuario chidalgo.	**Pasó:** ☐ **Falló:** ☐

3.1.5 Servicio de Auditoría

Prueba No.	SA5	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	
Categoría de la Prueba:		Servicios AAA	
Título de la Prueba:		Servicio de Auditoría	
Propósito de la Prueba:		Verificar que el ACS v5.2 está en la capacidad de almacenar registros de auditoría, autenticación y autorización al acceder a la administración de los dispositivos de la red IP/MPLS de las marcas Cisco, Alcatel y Huawei.	
Equipo:		Sistema de Control de Acceso Cisco	
Versión:		v5.2	
Configuración de la Prueba:		El ACS tiene conectividad con los equipos UIOLABP01, GESTOR_IP_ATM_2, UIOMSCT01, CCASTIM02 y MCHBLSAM01 al momento de ejecutarse el ATP.	
Procedimiento:		1. Verificar que en el ACS v5.2 se almacenan registros de auditoría al acceder a la administración de los dispositivos de red, de las marcas Cisco, Alcatel y Huawei. 2. Verificar que en el ACS v5.2 se almacenan registros de autenticación al acceder a la administración de los dispositivos de red, de las marcas Cisco, Alcatel y Huawei. 3. Verificar que en el ACS v5.2 se almacenan registros de autorización al acceder a la administración de los dispositivos de red, de las marcas Cisco, Alcatel y	

	Huawei.
Resultado esperado:	1. Los registros de auditoría deberán mostrar los siguientes datos: • Hora y fecha de conexión. • *Username* del usuario autenticado. • *Hostname* del dispositivo de red al que se accedió. • Comandos ejecutados. 2. Los registros de autenticación deberán mostrar: • Fecha y hora de conexión. • Estado de la conexión (*pass* o *fail*). • Username del usuario autenticado o que intenta acceder. • Grupo de usuario correspondiente al usuario autenticado. • *Hostname* del dispositivo de red al que se intenta acceder o se accede. • Grupo de dispositivo correspondiente al dispositivo de red al que se intenta acceder o se accede. • Direccion IP origen de la petición de autenticación. 3. Los registros de autorización deberán mostrar: • Fecha y hora de conexión. • *Username* del usuario autenticado. • Grupo de usuario correspondiente al usuario autenticado. • *Hostname* del dispositivo de red al que se accedió. • Grupo de dispositivo correspondiente al dispositivo de red al que se accedió. • Comandos ingresados por el usuario autenticado.
Verificaciones:	
1. En el ACS v5.2 se encuentran almacenados registros de auditoría con la información indicada.	**Pasó:** ☐ **Falló:** ☐
2. En el ACS v5.2 se encuentran almacenados registros de autenticación con la información indicada.	**Pasó:** ☐ **Falló:** ☐

3. **En el ACS v5.2 se encuentran almacenados registros de autorización con la información indicada.**	**Pasó:** ☐ **Falló:** ☐

3.2 Servicios de Monitoreo

3.2.1 Emisión y registro de alarmas

Prueba No.	SM1	**Fecha:**	24/06/2011
Autores:		Lucia Rodríguez Fabricio Falconí	
Supervisado por:		Ing. Andrés Almeida	
Categoría de la Prueba:		Servicios de Monitoreo	
Título de la Prueba:		Emisión y registro de alarmas	
Propósito de la Prueba:		Verificar que el ACS v5.2 dispara alarmas previamente configuradas y son enviadas al Servidor Syslog.	

Equipo:	Sistema de Control de Acceso Cisco.
Versión:	v5.2
Configuración de la Prueba:	El equipo UIOLABP01 tiene conectividad con el ACS v5.2 y éste último con el Servidor Syslog al momento de ejecutarse el ATP. En el ACS v5.2 se han configurado el siguiente tipo de alarmas: • "INTENTOS DE CONEXIÓN FALLIDOS": Se emite una alarma si un usuario no registrado en la base de datos interna del ACS v5.2 intenta acceder a la administración de un dispositivo repetidamente. • "COMANDOS NO AUTORIZADOS": Se emite una alarma si un usuario intenta ejecutar un comando no autorizado. • "CAMBIOS EN EL ACS": Se emite una alarma cuando se realizan cambios en el ACS v5.2. El servidor Syslog se encuentra configurado para recibir mensajes provenientes del ACS v5.2.
Procedimiento:	1. Intentar acceder a la administración del equipo

	UIOLABP01, con el usuario **jguaman** (no registrado en la base de datos interna de usuarios del ACS) 6 veces. 2. Ingresar a la administración del dispositivo UIOLABP01 con el usuario **mmena** (CALL CENTER, "Visualización") y ejecutar el comando **show tacacs.** 3. Ingresar a la administración del ACS v5.2 con la cuenta de usuario **aalmeida** y realizar cambios en la cuenta de usuario **aheredia**.
Resultado esperado:	1. El ACS v5.2 emitirá y mostrará la alarma "INTENTOS DE CONEXIÓN FALLIDOS" que deberá ser enviada y visualizada en el Servidor Syslog. 2. El ACS v5.2 emitirá y mostrará la alarma "COMANDOS NO AUTORIZADOS" que deberá ser enviada y visualizada en el Servidor Syslog. 3. El ACS v5.2 emitirá y mostrará la alarma "CAMBIOS EN EL ACS v5.2" que deberá ser enviada y visualizada en el Servidor Syslog.
Verificaciones:	
1. La alarma "INTENTOS DE CONEXIÓN FALLIDOS" fue generada, mostrada en el ACS v5.2, y en el Servidor Syslog.	**Pasó:** ☐ **Falló:** ☐
2. La alarma "COMANDOS NO AUTORIZADOS" fue generada, mostrada en el ACS v5.2, y en el Servidor Syslog.	**Pasó:** ☐ **Falló:** ☐
3. La alarma "CAMBIOS EN EL ACS" fue generada, mostrada en el ACS v5.2, y en el Servidor Syslog.	**Pasó:** ☐ **Falló:** ☐

4 ACEPTACIÓN

En su testimonio los responsables de llevar a cabo la ejecución de este ATP, firman este documento como una aceptación de sus resultados.

Área O&M Plataforma IP/MPLS	CARGO	FECHA	FIRMA
Ing. Andrés Almeida	Responsable de la Red IP/MPLS CNT E.P.	24/06/2011	
Quienes proponen:			
NOMBRES		**FECHA**	**FIRMA**
Lucia S. Rodríguez García		24/06/2011	
Marco F. Falconí Noriega		24/06/2011	