ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DEL SISTEMA DE AUTENTICACIÓN DE USUARIOS DE UNA RED CORPORATIVA A TRAVÉS DE LA APLICACIÓN DE LA PLATAFORMA TECNOLÓGICA DE AUTENTICACIÓN CISCO ISE (IDENTITY SERVICES ENGINE) PARA LA EMPRESA NET IO SERVICIOS S.A.

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

MARCIA VANESSA ARIAS IZA

CARMEN GABRIELA CARRILLO RIVERA

DIRECTOR: ING. FABIO GONZÁLEZ, MSc.

Quito, Enero 2017

DECLARACIÓN

Nosotras, Marcia Vanessa Arias Iza, Carmen Gabriela Carrillo Rivera, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada 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.

_____ _____

Marcia Vanessa Arias Iza Carmen Gabriela Carrillo Rivera

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Marcia Vanessa Arias Iza y Carmen Gabriela Carrillo Rivera, bajo mi supervisión.

_____

Ing. Fabio González, MSc.

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a Dios, mi fuerza y esperanza, a mis padres Washington y Susana, mi hermana Evelyn, su apoyo incondicional y fuente de motivación para la culminación del presente proyecto, a mis tíos, tías, primos, primas y amigos en especial a mi mejor amiga Dianita, por sus consejos y apoyo, Llerman, Myri por su amistad sincera y constante. Un sincero agradecimiento al Ing. Fabio González por su incalculable ayuda desde el desarrollo del plan de proyecto de titulación hasta la culminación del mismo, Ing. Fabio Infinitamente gracias.

Marcia Vanessa Arias Iza

AGRADECIMIENTO

Primeramente quiero agradecer a Dios por haberme guiado y bendecido para poder culminar este proyecto.

A mi hermosa familia, quienes con su apoyo incondicional aportaron granito tras granito, en lo bueno y malo siempre.

A mi querido esposo David por ser mi fortaleza y apoyarme en todo lo que me proponga, realmente es una gran bendición en mi vida.

Al Ingeniero Pablito por brindarnos ayuda en todo lo que necesitábamos, gracias de todo corazón.

A Ingeniero Fabio González nuestro tutor por el valioso tiempo prestado y su gran ayuda en el presente proyecto.

A mis amigos, que de una u otra manera siempre estuvieron ahí, en todo este camino recorrido y Dios mediante seguirán.

Carmen Gabriela Carrillo Rivera

DEDICATORIA

El presente proyecto de titulación lo dedico primeramente a Dios, a mis padres y mi hermana, quienes han constituido mi guía y fuerza de cada día, para avanzar y alcanzar mis metas.

Marcia Vanessa Arias Iza

DEDICATORIA

A Dios por brindarme sabiduría y proporcionarme todas las herramientas para culminar esta etapa, y estar presente en mi vida.

A mis papas, Carmen y Hugo por guiar mi camino y brindarme su apoyo incondicional para alcanzar cada una de mis metas.

A mí querido esposo David por su valioso apoyo, que día tras día me alienta a lograr todo lo que me proponga, su comprensión me ayuda a superar las dificultades, me guía y me acompaña en todo momento.

Carmen Gabriela Carrillo Rivera

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación tiene por objetivo rediseñar el sistema de autenticación de usuarios de una red corporativa a través de la aplicación de la plataforma tecnológica de Autenticación Cisco *ISE* (*Identity Services Engine*) para la empresa NET IO SERVICIOS S.A, con el fin de proporcionar un control de acceso a recursos corporativos basado en la validación de usuarios y dispositivos finales (*endpoints*), monitoreo y gestión centralizada basada en políticas de autenticación, perfilamiento, postura y autorización. Se presentan las recomendaciones de la arquitectura Cisco *Borderless Network*, que son consideradas en el rediseño para implementar redundancia, escalabilidad, confiabilidad.

En el primer capítulo se presenta la descripción de las principales características de la plataforma de autenticación Cisco ISE junto con el análisis de los protocolos de autenticación (estándar IEEE 802.1x) que utiliza para el control de acceso.

En el segundo capítulo se presenta el estudio de la situación actual de la red, equipos, servicios, entre otros; para determinar los requerimientos actuales y futuros considerando principalmente la autenticación, seguridad, los estándares de operación y preferencia en la marca de equipos de la empresa.

En el tercer capítulo se presenta el rediseño de la red LAN de la empresa cableada e inalámbrica, contemplando principalmente los requisitos para la implementación de la plataforma de autenticación Cisco ISE. Se detalla las configuraciones necesarias para permitir autenticación con la plataforma Cisco ISE a través de los dispositivos de acceso de red (NAD), incluyendo la definición de nuevos perfiles de usuarios y políticas. Además, este capítulo incluye la implementación de un prototipo que simula dos bloques de la empresa para probar en un ambiente controlado perfiles de usuarios, políticas de seguridad definidas de autenticación, autorización y postura.

En el cuarto capítulo se presenta el respectivo presupuesto referencial del rediseño de la red, incluyendo el equipamiento de la plataforma tecnológica Cisco ISE.

En el quinto capítulo se presentan las conclusiones y recomendaciones obtenidas en el desarrollo y finalización del proyecto.

Finalmente en los anexos digitales, se encuentra en detalle las configuraciones de la plataforma de autenticación Cisco ISE, los equipos de acceso a la red, dimensionamiento de equipos, usuarios de los once bloques de operación de la empresa, incluyendo las encuestas realizadas a las áreas de la empresa para la determinación de la matriz de riesgos para la definición de la nuevas políticas de red y nuevos perfiles de usuario.

PRESENTACIÓN

El constante desarrollo tecnológico, el rápido crecimiento en el ámbito de las redes de información con sus formas de conectividad y comunicación, obliga a las compañías a incorporar sistemas, políticas, normas, estándares para mantenerse seguras y a la vanguardia de la tecnología.

Por esta razón la empresa petrolera necesita aumentar la visibilidad, controlar el acceso y contener las amenazas implementando una plataforma de gestión de políticas de seguridad que automatiza y aplica acceso seguro contextual a los recursos de la red compartiendo datos con soluciones integradas de *partners* con el fin de agilizar sus capacidades de identificación, mitigación y remediación de los efectos de las amenazas.

Cisco ISE (*Identity Services Engine*) es una plataforma de autenticación contextual, basada en identidad, que recolecta información en tiempo real de la red de datos de los usuarios y dispositivos. Luego utiliza esta información para tomar decisiones proactivas de gobernabilidad mediante la aplicación de las políticas en toda la infraestructura de red.

El presente proyecto de titulación tiene como objetivo rediseñar la red multiservicios para la empresa petrolera y las interconexiones entre sus bloques de operación ubicados en Quito, el distrito Amazónico y la zona del Litoral autenticados con la plataforma Cisco ISE, considerando la migración a una Cloud Computing de Modelo Híbrido que permita una Infraestructura como Servicio (IaaS) e implementar un prototipo de la red (telefonía IP, video y datos), autenticado con Cisco ISE, para realizar pruebas de operación y comprobar el funcionamiento.

CAPÍTULO I

MARCO TEÓRICO

En este capítulo se describen los conceptos básicos de los sistemas de autenticación de acceso de usuarios en redes corporativas, los protocolos de autenticación (802.1x), incluyendo las principales características y el funcionamiento de la plataforma de autenticación del fabricante Cisco (Cisco ISE[1]). El análisis e investigación de los protocolos de autenticación que implementa la plataforma tecnológica Cisco ISE, permitirá entender su funcionamiento.

1.1 INTRODUCCIÓN

Las redes empresariales ya no se encuentran dentro de cuatro paredes seguras de una empresa, hoy en día se extienden hasta donde llegan los requerimientos de información de los empleados, promoviendo el acceso a recursos empresariales en cualquier momento en cualquier lugar, a través de cualquier dispositivo (BYOD - *Bring your own device*).

Los empleados exigen ahora más que nunca el acceso a los recursos de trabajo desde sus dispositivos y a través de redes no empresariales. El *Internet* y la movilidad están cambiando la forma en que vivimos y trabajamos. Las empresas se encuentran ante el desafío de tener que brindar soporte de nuevos dispositivos habilitados para la red, mientras que una infinidad de amenazas de seguridad y violaciones de datos indican claramente la importancia de proteger el acceso a la red empresarial.

A medida que se expanden las rede, también crece la complejidad de poner en orden los recursos, administrar soluciones de seguridad y controlar los riesgos. La extendida conectividad, los restringidos recursos de las tecnologías de información y el impacto

---

[1] Cisco ISE: Cisco *Identity Services Engine*, es una plataforma de control y administración de políticas de Autenticación, Autorización y Contabilización junto con monitoreo de seguridad en la red, propietaria de la marca Cisco.

potencial de no lograr identificar y remediar las amenazas de seguridad, en conjunto, se vuelve ciertamente más grande.

Y surge la necesidad de contar con herramientas que disminuyan los riesgos de seguridad informática, en este caso el acceso a la red con la tecnología Cisco® *Identity Services Engine* (ISE), la cual es una plataforma de control y administración de políticas de seguridad, que automatiza y simplifica el control de acceso, y el cumplimiento de las normas de seguridad para redes cableadas, inalámbricas y conexiones mediante VPN[2](*Virtual Private Network)*.

1.2 SEGURIDAD EN LA RED [1] [2] [3]

Las redes cableadas o inalámbricas, con su constante evolución cada vez son más esenciales para las actividades cotidianas de las empresas y personas, ambas para su funcionamiento dependen de componentes, como estaciones de trabajo (dispositivos finales), dispositivos de interconexión y de los servicios (correo electrónico, administración de archivos, almacenamiento de datos, entre otros).

Los intrusos son personas no autorizadas que ocasionan interrupciones y pérdidas de trabajo a las empresas; los ataques a la red pueden ser devastadores y ocasionan pérdida de tiempo y de dinero. Las amenazas de seguridad causadas por intrusos pueden originarse tanto en forma interna como externa. A continuación se describirá cada una:

- Amenazas externas**:** Son personas que no tienen autorización para acceder a la red. Se introducen desde *Internet* por medios cableados, inalámbricos o servidores de acceso.
- Amenazas internas: Son personas que conocen información valiosa y saben cómo acceder a ella.

---

[2] VPN:Red Privada Virtual, Es una red privada aplicada sobre una red pública o sobre Internet.

La seguridad de acceso (validación de credenciales de usuario) se puede dividir en tres áreas importantes: confidencialidad, validación de identificación y control de integridad:

- Confidencialidad: Preservar y garantizar la información de las personas no autorizadas.
- Validación de la identificación: Comprobar con quién se ha establecido comunicación para posteriormente dejar ver la información de la red.
- Control de integridad: Confirmar y validar que un mensaje enviado sea exactamente igual al llegar a su destino.

La información de las empresas es confidencial y se deben tomar medidas preventivas para proteger esta, para esto existen dos soluciones: la seguridad física y la seguridad lógica.

1.2.1 SEGURIDAD FÍSICA

Consiste en la aplicación de procedimientos de control como medidas de prevención y detección de intrusos a los recursos de red. Su objetivo es prevenir que un intruso intente acceder físicamente al lugar donde están instalados los equipos de red, protegiendo el área donde se encuentran ubicados dichos equipos con la ayuda de sistemas de control de acceso y cámaras de seguridad.

1.2.2 SEGURIDAD LÓGICA

Consiste en detectar accesos no autorizados a la red, a través de la utilización de ciertos dispositivos con protocolos y políticas de seguridad, brindando acceso seguro solamente a los usuarios permitidos. Los objetivos que busca la seguridad lógica son:

- Restringir el acceso a los programas y archivos a usuarios. Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

- ❖ Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- ❖ Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro. Que la información recibida sea la misma que ha sido transmitida.
- ❖ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.3 PROTOCOLO AAA [4]

El protocolo AAA (Autenticación, Autorización y Contabilidad) es utilizado en el diseño de sistemas de control de acceso a redes de datos, proporcionando los servicios de autenticación, autorización y contabilidad de forma centralizada.

1.3.1 SERVIDOR AAA

El servidor AAA permite a un usuario, con sus credenciales (usuario y contraseña), acceder a la red corporativa, cuando se verifique que se encuentra registrado en su base de datos AD[3] (*Active Directory /* Directorio Activo). De esta manera previene el acceso de personas no autorizadas a la red. A continuación se describirá cada uno de los servicios que provee el servidor AAA.

1.3.1.1 Autenticación

Sirve de base a todo el sistema AAA por su directa relación con los procesos de autorización y contabilidad. La autenticación permite probar la identidad de un usuario a través de los siguientes elementos: algo que se conoce, contraseña; algo que se tiene, como una tarjeta inteligente; algo que identifique físicamente al usuario de forma

---

[3] AD: Implementación de servicio de directorio de red, ordenada de manera jerárquica.

única, como una huella dactilar, el reconocimiento de voz, entre otros. Utiliza más de un factor para identificar al usuario, añade credibilidad al proceso de autenticación.

1.3.1.2 Autorización

Proceso mediante el cual a un usuario se le asigna una determinada cantidad de recursos de red, en base a las actividades que realice y las políticas de acceso implantadas por el administrador. Está principalmente relacionado con el proceso de autenticación, si un usuario no se autentica los siguientes procesos se descartan. Para cumplir con el proceso de autorización, los sistemas AAA utilizan soluciones como bases de datos o directorios que permiten almacenar las políticas de acceso de los usuarios.

1.3.1.3 Contabilidad

Luego del proceso de autenticación y autorización se produce el proceso de contabilidad. Es el proceso estadístico y de recolección de datos sobre la conexión, la información recolectada durante el proceso de autenticación y autorización permite al administrador gestionar la futura demanda de sus sistemas para planificar su crecimiento a futuro. Se inicia cuando el equipo autenticador o NAS (Servidor de Acceso de Red) autoriza al suplicante acceder a los servicios de red.

1.3.1.4 Beneficios de AAA

- Incremento de flexibilidad y control de configuración de acceso
- Escalabilidad
- Métodos de autorización estandarizados

1.3.2 PROTOCOLOS AAA

Los protocolos AAA más utilizados para efectuar el control de acceso a la red de usuarios, son el protocolo RADIUS, TACACS+ y DIAMETER. Son protocolos de administración de acceso seguro, pero cada uno tiene diferentes capacidades y

funcionalidades. La elección de uno de estos protocolos depende de las necesidades específicas de una determinada empresa.

1.3.2.1 Protocolo RADIUS [5] [6]

El protocolo RADIUS (*Remote Authentication Dial In User Service* / Autenticación Remota para Usuarios de Servicio Telefónico), desarrollado por Livingston *Enterprise* en 1991 y publicado posteriormente en las RFC 2138 y 2139, actualmente está definido en la RFC 2865 (Autenticación y Autorización) y en la 2866 (Contabilidad).

Es un protocolo que se basa en un modelo cliente servidor, donde los servicios de autenticación, autorización y contabilidad son administrados por un equipo proveedor de recursos que es el servidor RADIUS y los clientes son aquellos que acceden a los servicios de la red. Consta de tres componentes**:** Un servidor de autenticación, un autenticador, y un suplicante o cliente. En la figura 1.1 se muestra la comunicación del protocolo RADIUS.

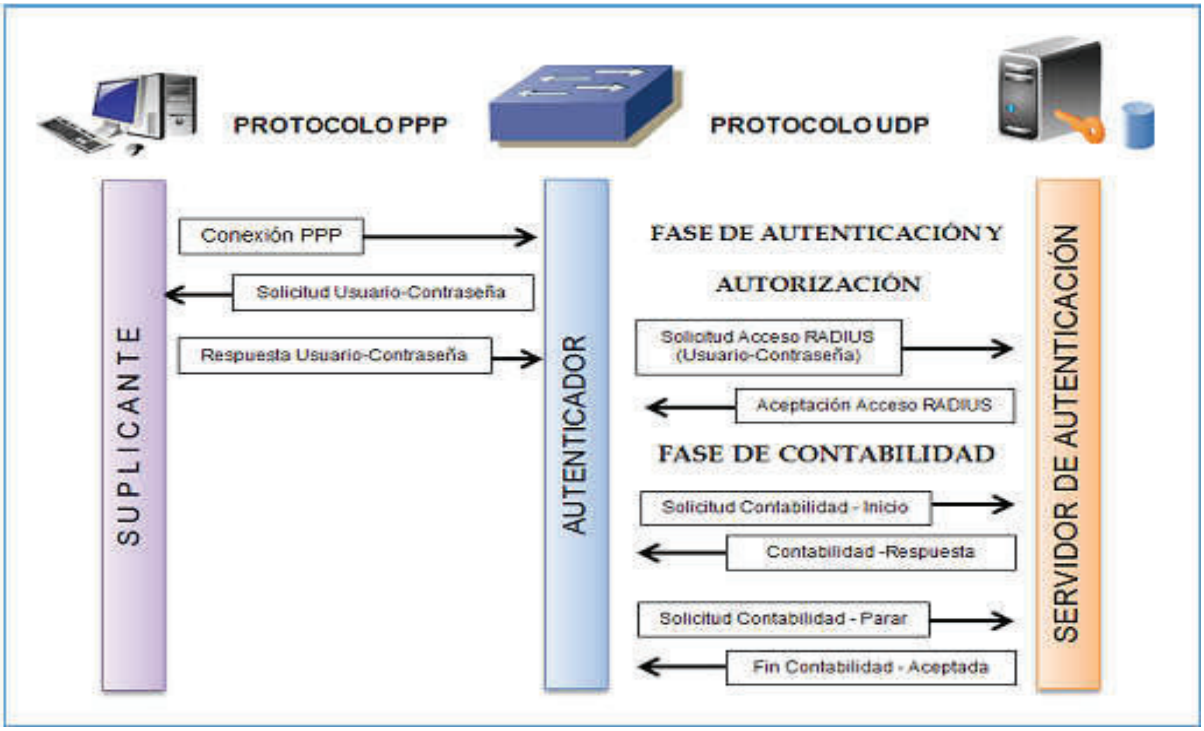

Figura 1.1 Comunicación protocolo RADIUS [4]

1.3.2.1.1 Funcionamiento

- Un usuario envía una solicitud a un NAS para obtener acceso a un recurso de red en particular, envía generalmente un nombre de usuario y una contraseña. Esta información se transfiere al dispositivo NAS a través de los protocolos de la capa de enlace
- (Por ejemplo PPP[4] *Point to Point Protocol* / Protocolo Punto a Punto) quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS solicitando el acceso a la red.
- El servidor RADIUS verifica que la información es correcta utilizando esquemas de autenticación. Y devuelve una de las tres respuestas siguientes:
  1. Acceso aceptado: Una vez que el usuario se ha autenticado, el servidor RADIUS le asigna los recursos de red y frecuentemente comprobará que el usuario está autorizado a utilizar el servicio de red solicitado.
  2. Reto de acceso: Solicita información adicional de usuario como PIN[5](*Personal Identification Number*), una contraseña secundaria o, simplemente se emplean diálogos de autenticación entre el usuario y el servidor RADIUS por medio del uso de túneles seguros, de manera que las credenciales de acceso están ocultas para el servidor de acceso a la red.
  3. Acceso rechazado**:** Se rechaza el acceso al usuario por algunas razones, por ejemplo porque la cuenta del usuario esté desactivada o sea desconocida, entre otras.

Una vez confirmado el acceso a la red, se podrá transmitir información y comienza un proceso de contabilización de uso de los servicios asignados a los usuarios.

En este proceso se registran datos del usuario como: identificación del usuario, dirección IP, punto de conexión y un identificador de sesión único. Estos datos son

---

[4] PPP: es un protocolo de la capa de enlace de datos, estandarizada por el RFC 1661.

[5] PIN: es un número que identifica un dispositivo de manera única.

actualizados periódicamente mientras está activa la sesión. De igual manera se procede cuando se termina la misma.

En la figura 1.2 se muestra la interacción entre el usuario, cliente y servidor RADIUS.

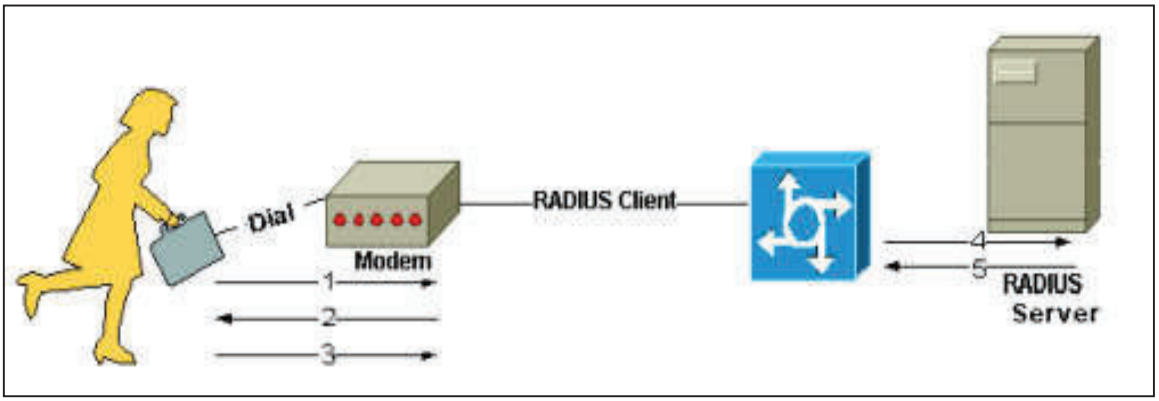

Figura 1.2 Interacción usuario, cliente y servidor RADIUS [5]

1.3.2.1.2 Principales características:

- Funciona bajo el modelo cliente-servidor: Demanda de un cliente RADIUS, que puede ser un NAS (*Network Access Server* / Servidor de Acceso a la Red), que interactúe con los servidores RADIUS.
- Ofrece nivel limitado de seguridad en la red: Aunque las comunicaciones entre el cliente y servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5[6]. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.
- Servidores RADIUS soportan varios esquemas de autenticación de usuario como**:** EAP (*Extensible Authentication Protocol* / Protocolo de Autenticación Extensible), PAP (*Password Authentication Protocol* / Protocolo de

[6] MD5: *Message-Digest Algorithm* 5, es un algoritmo de resumen criptográfico de 128 bits.

Autenticación de Contraseña) y CHAP (*Challenge Handshake Authentication Protocol* / Protocolo de Autenticación por Desafío Mutuo) y soportan varios orígenes de información como: una base de datos del sistema o una base de datos interna (del propio servidor RADIUS) y otros como AD (*Active Directory* / Directorio Activo), LDAP (*Lightweight Directory Access Protocol* / Protocolo Ligero/Simplificado de Acceso a Directorio) y Kerberos.

- Protocolo de la capa de aplicación que utiliza UDP como transporte: Los puertos oficialmente definidos por la IANA [7](*Internet Assigned Numbers Authority* / Autoridad para Asignación de Números de *Internet*) son el 1812 para la autenticación y el 1813 para la contabilización, pero están los puertos 1645 y 1646 no oficiales pero ampliamente usados en implementaciones de servidores y clientes RADIUS. Capacidad para el manejo de sesiones: Avisando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar.

1.3.2.1.3 Mensaje RADIUS

El mensaje RADIUS consta de una cabecera con sus atributos (ver Figura 1.3).

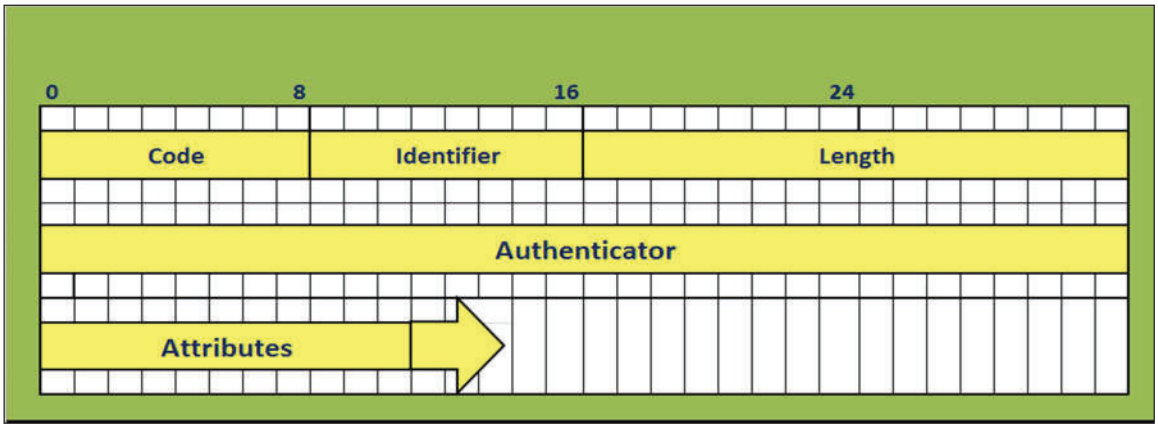

Figura 1.3 Mensaje RADIUS [6]

[7] IANA: función administrativa de *Internet* que lleva cuenta de las direcciones IP, los nombres de dominio y los identificadores para los parámetros de protocolo.

Los paquetes RADIUS tienen la siguiente estructura:

- *Code* (Código): 8 bits para definir el tipo de paquete. Existen 9 códigos para 9 tipos de paquetes.
- *Identifier* (Identificador): 1 octeto para relacionar una respuesta RADIUS con la solicitud correspondiente.
- *Length* (Longitud del paquete): 16 bits para la longitud total del paquete, incluyendo los campos desde el código hasta los atributos opcionales. Sirve para determinar cuál es el final de los atributos.
- *Authenticator* (Verificador): 32 bits para autenticar la respuesta del servidor RADIUS y para encriptar la clave.
- *Attributes* (Atributos): Campo que transporta datos en la solicitud y respuesta para la autenticación, autorización y contabilización.

1.3.2.2 Protocolo TACACS+ [6]

TACACS+ está basado en el protocolo TACACS (*Terminal Acces Controller Access Control System* / Sistema de Control de Acceso del Control de Acceso a Terminales) utilizado para el control de acceso mediante autenticación y autorización, definido desde 1997 por el IETF[8] (*Internet Engineering Task Force* / Grupo de Trabajo de Ingeniería de *Internet*).

TACACS+ evoluciona los protocolos anteriores, mientras que RADIUS combina la autenticación y autorización en un perfil de usuario, TACACS+ separa estos procesos.

Es un protocolo propietario de Cisco que funciona bajo el modelo cliente servidor y emplea el protocolo TCP (orientado a conexión) utilizando el puerto de red 49. Implementa encriptación no sólo en las credenciales sino también en los datos, utilizando el algoritmo de encriptación MD5.

---

[8] IETF: es la entidad que regula las propuestas y los estándares de *Internet*, conocidos como RFC.

La secuencia del proceso de autenticación, autorización y contabilización mediante el protocolo TACACS+, se detalla en la figura 1.4.

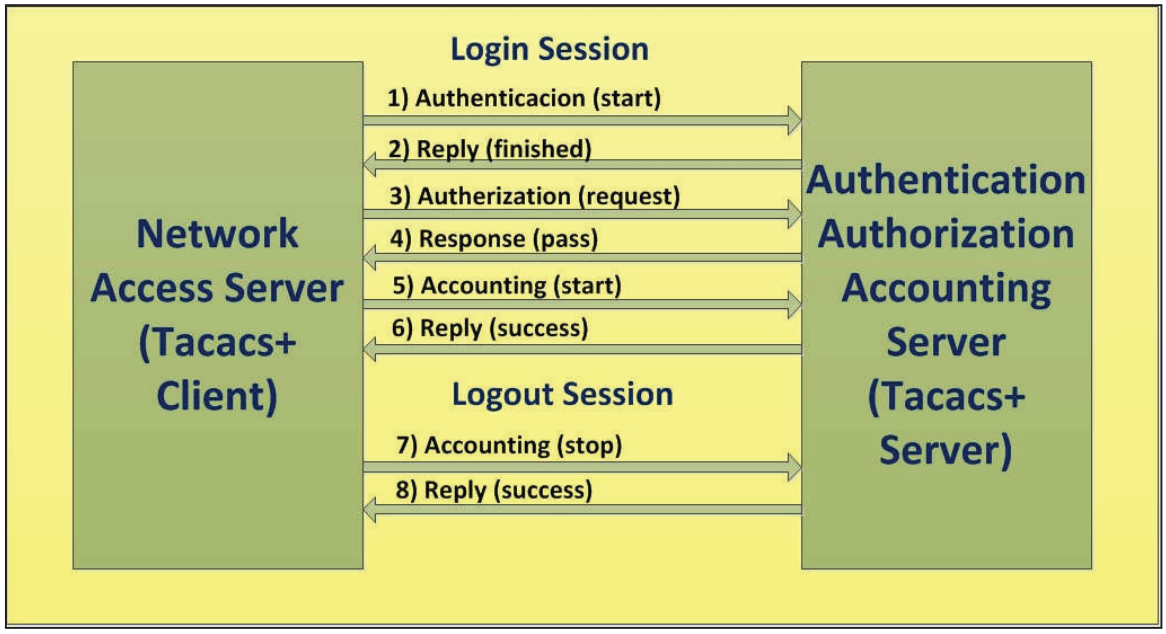

Figura 1.4 Secuencia de Proceso de Autenticación TACACS+ [6]

Los mensajes que se intercambian entre un cliente y un servidor TACACS+, tienen el formato siguiente:

- *Version* (Versión): 1 octeto para indicar el número de versión.
- *Type* (Tipo): 8 bits para indicar un tipo de mensaje dependiendo de la acción: autenticación autorización o contabilidad.
- Seq_no (Número de secuencia): 1 octeto para indicar el número de secuencia de paquetes de la sesión actual.
- *Flags* (Banderas): 1 octeto para indicar datos encriptados después del campo longitud.
- *Session_id* (identificador de sesión): 4 octetos para identificar la sesión en cada paquete de respuesta del servidor
- *Length* (Longitud): Longitud del paquete.

La Figura 1.5 muestra el formato de un paquete TACACS+.

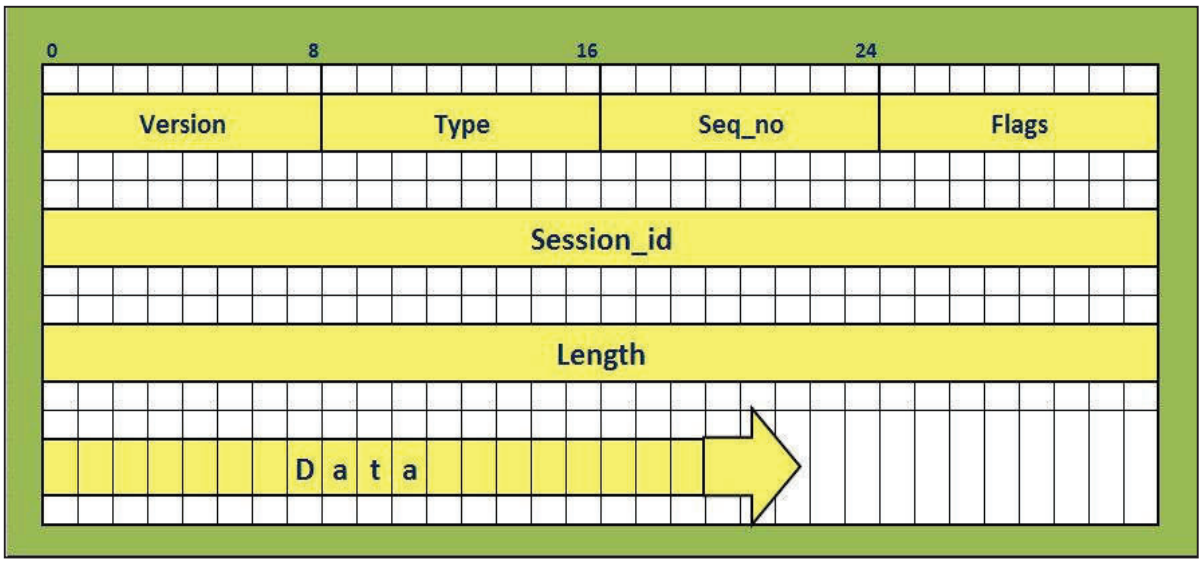

Figura 1.5 Formato Paquete TACACS+

1.3.2.3 Protocolo DIAMETER [6]

DIAMETER surge debido al crecimiento de *Internet* y la introducción de nuevas tecnologías de acceso, incluidas las inalámbricas y servidores de acceso de red cuya complejidad y densidad demandan nuevas exigencias en los protocolos AAA.

Desarrollado en 1998 y definido por la IETF desde el 2003 en la RFC 3588. DIAMETER usa los protocolos TCP o SCTP[9] (*Stream Control Transmission Protocol*) para el transporte por el puerto 3868 y emplea seguridad mediante el uso de TLS o IPSEC.

Este protocolo proporciona autenticación, autorización y contabilidad, para aplicaciones de acceso a la red o de movilidad IP.

Las AVP[10] (*Attributed Value Pairs*,) se usan para enviar información, algunas son empleadas para el funcionamiento propio de DIAMETER y otras para transmitir los datos de las aplicaciones que usan DIAMETER.

---

[9]SCTP: Es una protocolo alternativo a los protocolos de la capa de transporte TCP y UDP.

[10] AVP: es una forma de representación de datos llamados Atributos.

Dado que DIAMETER no es un protocolo completo en sí mismo, sino que requiere de extensiones específicas para cada aplicación referentes a la tecnología o arquitectura de acceso a la red.

Para su implementación es necesario garantizar la interoperabilidad, es decir que todos los nodos deben estar preparados para recibir mensajes DIAMETER y evitar el bloqueo, lo que significa que todos los nodos DIAMETER deberían usar SCTP (*Stream Control Transmission Protocol*/ Protocolo de Comunicación de Capa Transporte).

1.3.2.3.1 Mensaje DIAMETER

El mensaje esta formado por una cabecera DIAMETER y sus principales campos son:

- Versión del protocolo DIAMETER, normalmente seteado a 1, la longitud de mensaje que incluye la cabecera junto a los AVP respectivos y los comandos de banderas que pueden variar entre *request* (R) si se encuentra seteado a 1 es una solicitud mientras que el 0 indica una respuesta.
- *Proxiable*(P) si se encuentra activo el mensaje se redirige al proxy sino se procesa localmente.
- Error (E) que se cataloga como mensaje de error, normalmente no se utiliza este bit en los mensajes de solicitud.
- Retransmisión (T) si existe error se utiliza para indicar una retransmisión y evitar mensajes duplicados
- Código de comandos que indica específicamente la acción que una aplicación DIAMETER debe realizar al recibir el mensaje.
- Identificador de la aplicación DIAMETER activa, un identificador *Hop-by-Hop* que indica la coincidencia entre solicitud y respuesta.
- identificador *End-to-End* que identifica específicamente los extremos en una comunicación DIAMETER).
- Un número variable de AVP.

En la Figura 1.6 se muestra la estructura del mensaje DIAMETER.

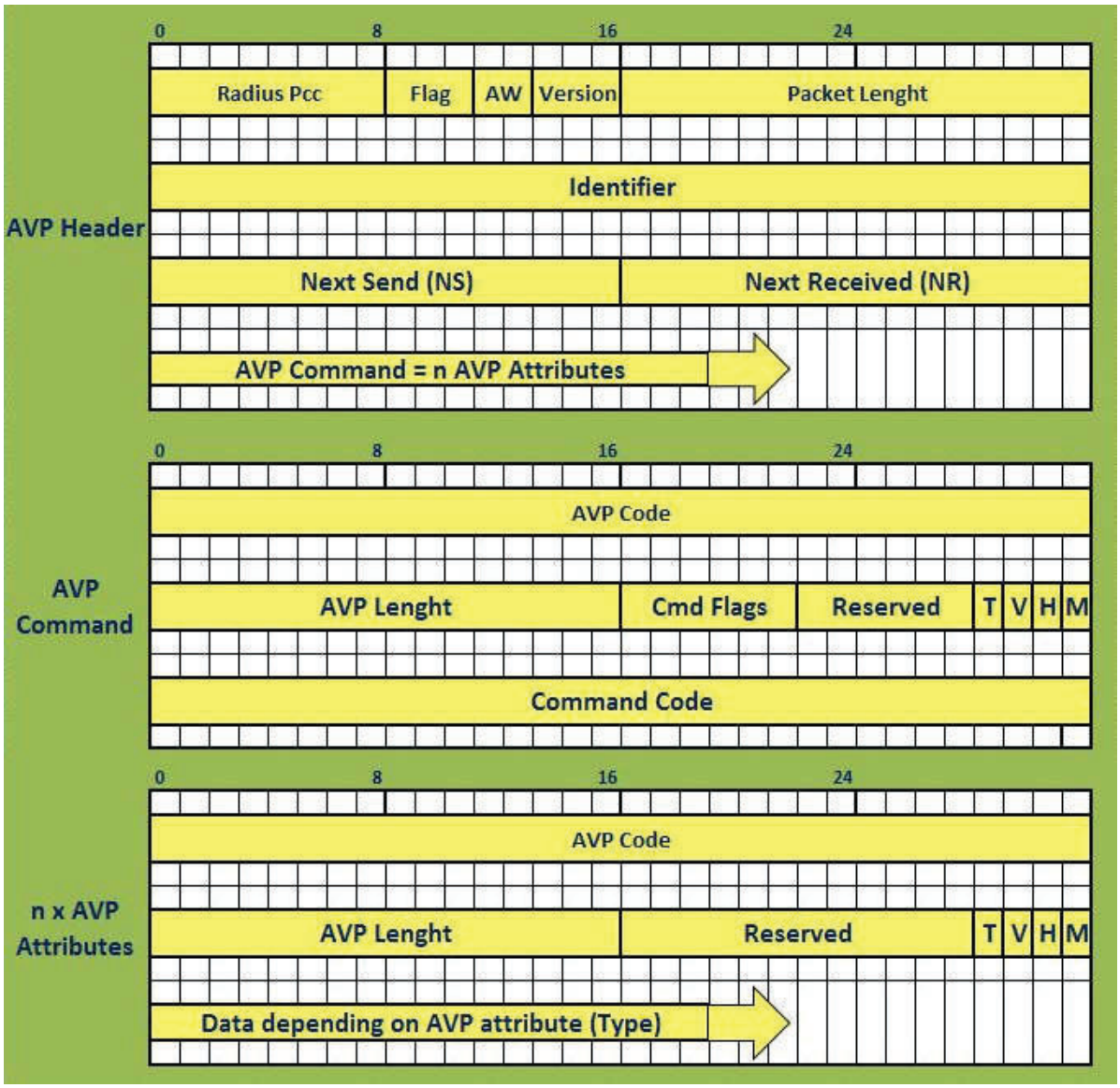

Figura 1.6 Mensaje DIAMETER [6]

1.3.2.3.2 Flujo de Mensajes DIAMETER

- El flujo de mensajes con DIAMETER se inicia con la estabilización de la conexión.
- Después el iniciador envía un mensaje de Solicitud e Intercambio de Capacidades (CER), la otra parte envía un mensaje de Respuesta de Intercambio de Capacidades (CEA), posteriormente puede negociarse si se

desea TLS[11] (*Transport Layer Security*), esto es opcional y la conexión está lista para el intercambio de mensajes de aplicación.

- Si no han ocurrido intercambios de mensajes por un tiempo, uno de los dos enviará una solicitud de dispositivo “perro guardián” (DWR) y el otro deberá responder con una respuesta al dispositivo “perro guardián” (DWA).
- La comunicación puede terminarse por cualquiera de las partes enviando una solicitud de desconexión (DPR) y la otra parte debe responder a la solicitud (DPA). Con esto ya queda desconectada la conexión.

La Figura 1.7 muestra el flujo de mensajes DIAMETER.

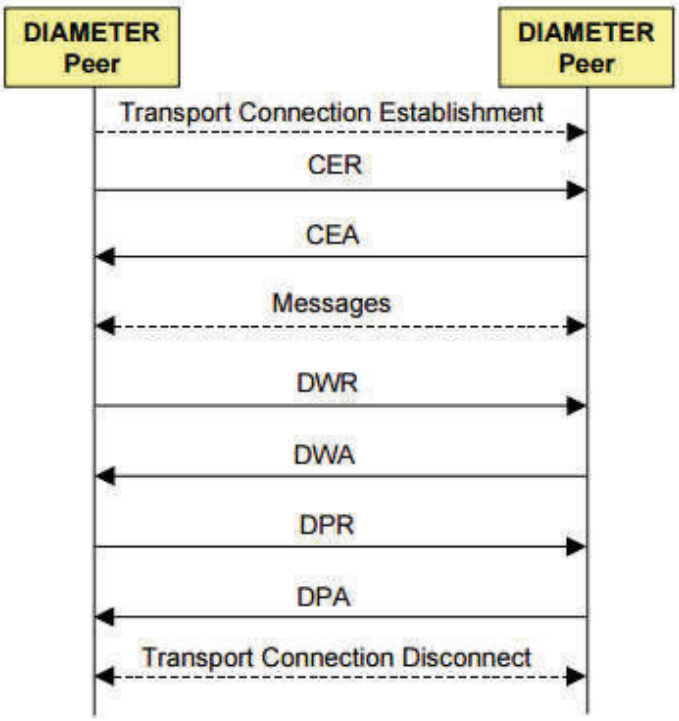

Figura 1.7 Flujo de mensaje DIAMETER [6]

En la Tabla 1.1, se muestra la comparación de los protocolos RADIUS, TACACS+ y DIAMETER.

[11] TLS: Es un protocolo criptográfica que permite comunicaciones seguras en una red

PARÁMETROS	RADIUS	TACACS+	DIAMETER
Protocolo de transporte	UDP	TCP	TCP o SCTP con TLS o IPSEC
Tipo de protocolo	Cliente /Servidor		Peer to Peer
Tipo de mensaje	Solicitud/Respuesta del cliente al servidor		Solicitud/Respuesta de una parte a otra
Encriptación de paquetes	Solo la contraseña en las respuestas al acceso. Otra información está vulnerable a ser capturada	Todo el cuerpo del paquete excepto la cabecera estándar	Todo el cuerpo del paquete
Algoritmo de encriptación	Secreto compartido con MD5		Secreto compartido con HMAC-MD5
Autenticación y Autorización	Combinado en un mismo perfil de usuario. Los paquetes de acceso aceptado generados por el servidor para el cliente contiene información de autorización	Independientes. Empleo de arquitectura AAA permitiendo separar en servidores diferentes las soluciones AAA.	Independientes
Soporte Multiprotocolo	Limitado, no soporta los protocolos (ARA) - Protocolo de Control de Tramas NetBIOS - (NASI) - Conexiones X.25 con PAD	Si	
Administración de *Routers*	No muy útil para la gestión ya que el usuario no tiene el control del comando	Proporciona dos métodos de control de autorización de los comandos: por usuarios o por grupos	Ofrece coporte para los comandos específicos del vendedor
Notificación de errores	No	Si	

Tabla 1.1 Cuadro comparativo de los protocolos RADIUS, TACACS+ y DIAMETER [7]

1.3.2.4 Métodos para implementar AAA [8]

Los tres métodos de implementar AAA son:

- Localmente**:** En un *router* o un NAS.
- En un ACS (*Access Control Server*) de Cisco por *software***:** Instalado en un Microsoft *Windows Server* permitiendo la comunicación con *routers* y NAS.

- En un ACS (*Access Control Server*) de Cisco por *hardware*: Servidor *hardware* dedicado que permite la comunicación con *routers* y NAS.

1.3.2.4.1 Métodos de Autenticación.

Existen dos métodos para autenticar usuarios: autenticación local o remota.

- Autenticación local: Consiste en autenticar directamente en el *router* o el NAS el nombre de usuario y contraseña. Está recomendado para pequeñas redes y no requiere base de datos externas. La autenticación funciona de la siguiente manera: el usuario solicita autenticarse, el *router* (o NAS) solicita el nombre de usuario y la contraseña, el usuario responde, el *router* comprueba los datos, acepta o deniega el acceso y comunica el veredicto al usuario.
- Autenticación remota: Uno o varios ACS (por *software* o *hardware*) pueden gestionar toda la autenticación de todos los dispositivos de red. La comunicación entre estos dispositivos y los ACS utilizan los siguientes protocolos: TACACS+ o RADIUS. La autenticación funciona de la siguiente manera: el usuario solicita autenticarse, el *router* (o NAS) solicita el nombre de usuario y la contraseña, el usuario responde, el *router* reenvía los datos al ACS, el ACS comprueba los datos y acepta o deniega el acceso, finalmente el ACS comunica el veredicto al *router* y este al usuario.

1.3.2.4.2 Niveles de seguridad de los métodos de autenticación:

- Sin usuario y contraseña: Un atacante encuentra el dispositivo y accede al mismo sin ninguna restricción. Si no hay validación de credenciales de ingreso a un dispositivo, para asegurarlo se cambia el puerto bien conocido de escucha del servicio a un puerto diferente.
- Con usuario, contraseña y sin caducidad: El administrador decide cuando cambiar la contraseña. Este método es vulnerable a ataques de repetición, fuerza bruta, robo e inspección de los paquetes.

- Con usuario, contraseña y con caducidad: Por cada tiempo el administrador es forzado a cambiar su contraseña. Este método tiene las mismas vulnerabilidades pero el tiempo para comprometer el equipo por fuerza bruta es menor.
- OTP (*One Time Password* /Contraseña de Uso Único): Es más seguro que los anteriores ya que la contraseña enviada solo tiene validez una vez, es decir, en el momento de ser interceptada por el atacante la contraseña caduca. S/*Key* es una implementación de OTP que genera un listado de contraseñas a partir de una palabra secreta.
- Tarjetas de testigo por *software* y por *hardware*: Está basado en la autenticación de doble factor; algo que el usuario tiene (*token card*) y algo que el usuario sabe (*token card PIN*).

1.4 ESTÁNDAR IEEE 802.1X [4] [7] [9]

El estándar de autenticación IEEE 802.1X permite controlar el acceso a los servicios de red a través de sus puertos, opera en la capa dos del modelo OSI, asegura el intercambio de las credenciales de usuario o dispositivo evitando cualquier acceso no autorizado a la red.

Una infraestructura de red 802.1x requiere de tres elementos para operar: suplicante, equipos autenticadores y servidor de autenticación:

- Suplicante: Es el cliente que por medio de un *software* solicita tener acceso a los recursos de la red.
- Autenticador: Puede ser un *switch* o un punto de acceso, es el componente a través del cual los usuarios acceden a los servicios de red, su función es forzar el proceso de autenticación y enrutar el tráfico.
- Servidor de autenticación: Se encarga de procesar la autenticación de las credenciales del usuario.
- Por lo general se emplean bases de datos para realizar este proceso tales como: SQL, Microsoft AD, LDAP, entre otros.

1.4.1 FUNCIONAMIENTO DEL ESTÁNDAR IEEE 802.1X

Para entender el funcionamiento del estándar IEEE 802.1X, se presenta el diagrama de flujo de la Figura 1.8, que indica las operaciones que se realizan en caso de que se cumplan o no las condiciones de compatibilidad, autenticación con IEEE 802.1x o con la dirección MAC o vía una interfaz *WEB* o se asigna al dispositivo a una red aislada (VLAN de cuarentena) si no cumple con algunas de la condiciones anteriores.

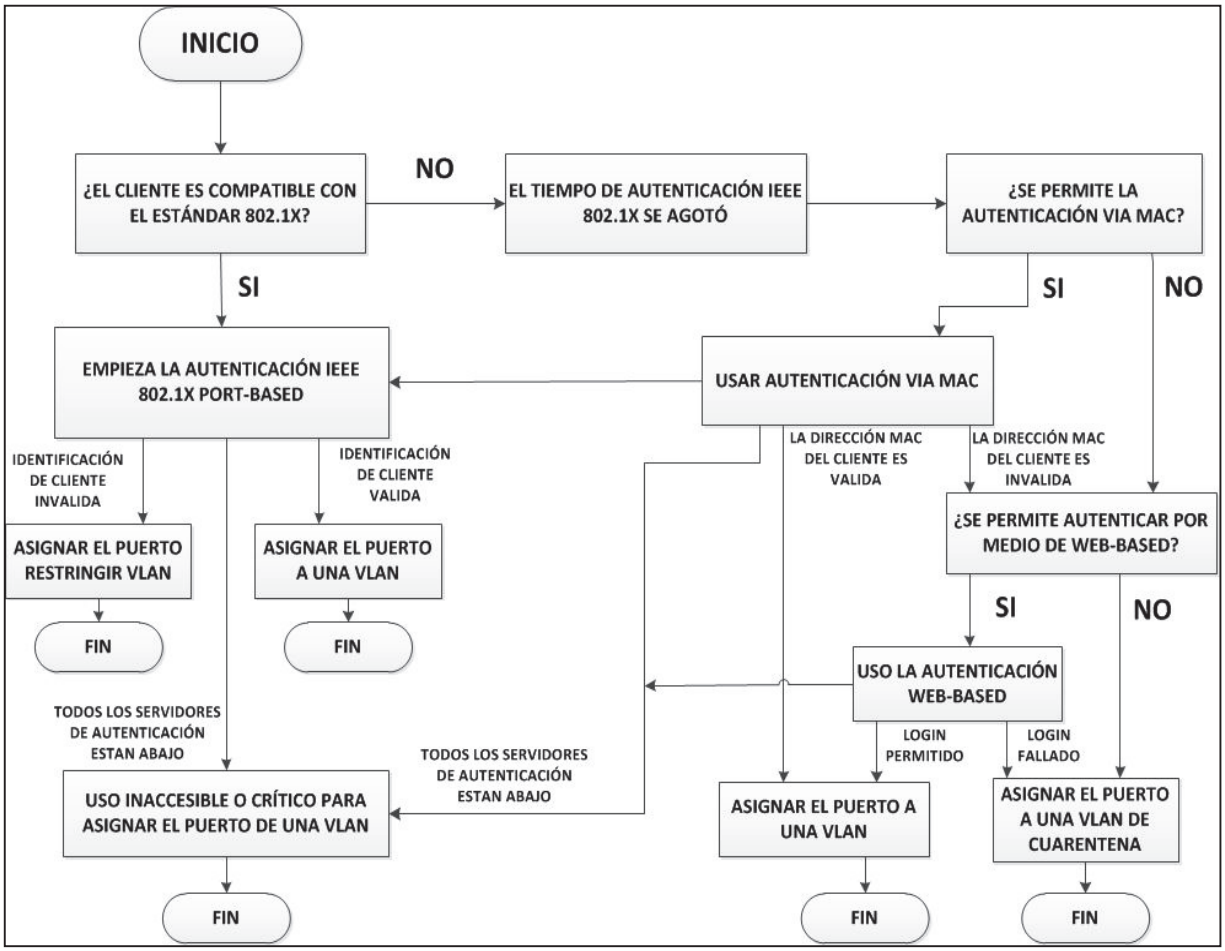

Figura 1.8 Diagrama de flujo del Estándar IEEE 802.1x [9]

- Un cliente envía un mensaje de "solicitud de acceso" a un punto de acceso.
- El punto de acceso solicita la identidad del cliente.
- El cliente responde con un paquete de identidad que se pasa al servidor de autenticación.

- El servidor de autenticación envía un paquete de "aceptación" al punto de acceso.
- El punto de acceso coloca el puerto del cliente en el estado autorizado y se permite el tráfico de datos y acceso a los servicios disponibles en el entorno de la red.

A continuación, en la Figura 1.9 se muestra el intercambio de mensajes entre los clientes, autenticador y servidor para el funcionamiento del estándar IEEE 802.1x, en este caso se utiliza el protocolo de autenticación EAP.

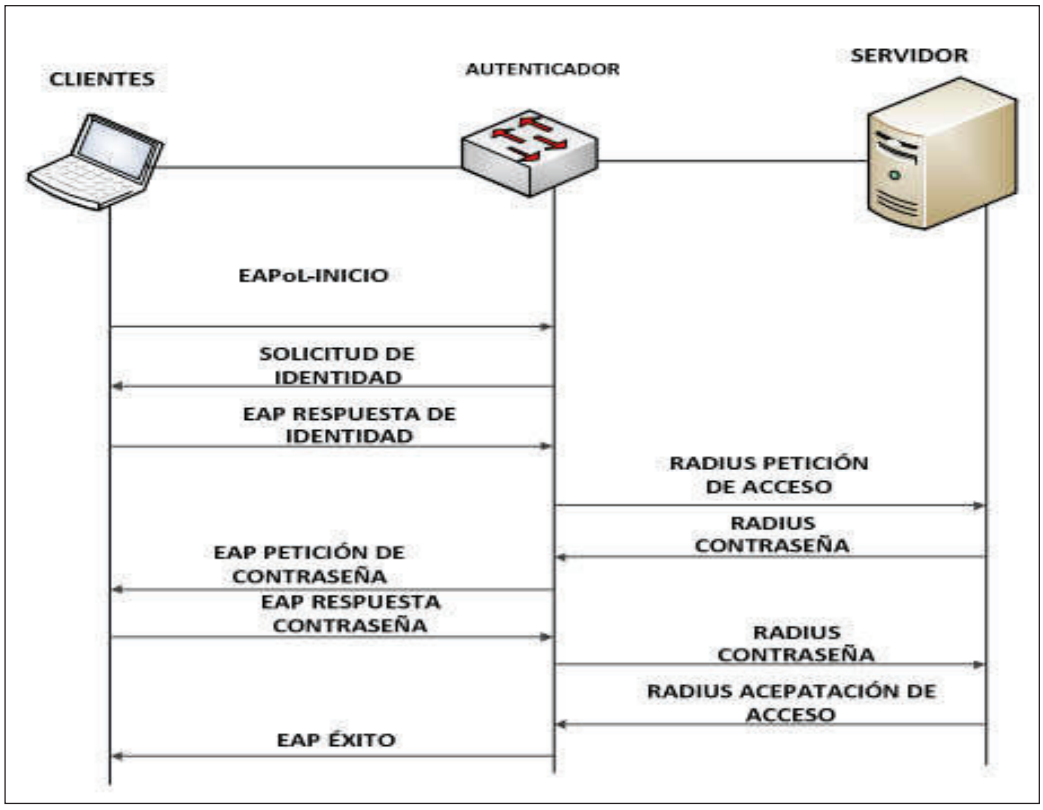

Figura 1.9 Funcionamiento del estándar IEEE 802.1x [9]

1. El suplicante inicia la comunicación enviando un mensaje en un paquete EAP-Inicio hacia el autenticador, pidiendo tener acceso a los recursos de red.
2. El autenticador le responde con un EAP-
3. Respuesta de Identidad a través de su puerto pidiendo las credenciales del usuario.

4. El suplicante le responde al autenticador con las credenciales.
5. El autenticador reenvía las credenciales al servidor de autenticación.

Este estándar trabaja con el protocolo de autenticación EAP[12] y admite varios métodos de autenticación como: certificados, tarjetas inteligentes, NTLM[13] , Kerberos y LDAP.

1.4.2 PROTOCOLO EAP

El protocolo EAP se basa en el uso de un controlador de acceso llamado autenticador, que le permite o deniega a un usuario el acceso a la red.

- El usuario: Denominado solicitante, quien desea ser validado mediante credenciales.
- El controlador de acceso: Es un *firewall* básico que actúa como intermediario entre el usuario y el servidor de autenticación, y que necesita muy pocos recursos para funcionar.
- El servidor de autenticación: NAS comprueba la identidad del usuario transmitida por el controlador de la red y otorgar el acceso según sus credenciales. Este servidor puede almacenar y hacer un seguimiento de la información relacionada con los usuarios.

Existen algunos tipos de protocolos EAP (*Extensible Authentication Protocol*):

1.4.2.1 EAP-TLS

Es un sistema de autenticación fuerte que se basa en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (*Public Key Infraestructure*) en ambos extremos. TLS (*Transport Layer Security*) es el nuevo estándar que sustituye a SSL (*Secure Socket Layer*).

---

[12] EAP: es un protocolo de autenticación en redes inalámbricas.

[13] NTLM: es un administrador de NT de Redes de Área Local.

1.4.2.2 EAP-TTLS

Es un sistema de autenticación que se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir que se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS solo requiere un certificado de servidor.

1.4.2.3 PEAP

El significado de PEAP corresponde con *Protected* EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

1.5 LDAP [4]

El protocolo LDAP es un conjunto de protocolos abiertos utilizados para acceder a la información almacenada a través de la red. Las especificaciones técnicas se definen en los RFC 4510 - 4519. LDAP es un protocolo que regula el acceso a los datos almacenados, para proporcionar una repuesta rápida a operaciones de búsqueda y lectura de la información.

LDAP es un protocolo modelo cliente/servidor, en el que el servidor puede usar una variedad de bases de datos para guardar un directorio. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede consultar un directorio o intentar modificarlo.

Si es una consulta, el servidor puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta y si la aplicación cliente está intentando modificar la información en un directorio LDAP, el servidor verifica que el usuario tenga permisos para efectuar el cambio y después añade o actualiza la información. LDAP puede consolidar información para toda una organización dentro de un repositorio central. LDAP soporta SSL y TLS.

1.6 SERVIDORES DE CONTROL DE ACCESO [10]

La importancia del control de acceso a redes radica en que las empresas cada vez tienen redes más distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas, todos con la necesidad de acceso a la red y sistemas de la compañía utilizando distintos medios de acceso desde tecnologías inalámbricas, *Internet*, VPN, entre otros.

Los requerimientos actuales son interconexión de entornos complejos, protección de los datos que poseen las empresas y acceso a los datos desde cualquier dispositivo y ubicación, sin comprometer la integridad, confidencialidad de la información, limitando la existencia de huecos de seguridad. En respuesta a esta demanda surgen iniciativas y tecnologías para resolverlas que se engloban dentro de lo que se conoce como NAC[14].(*Network Access Control* / Control de Acceso a la Red)

1.6.1 NAC

NAC Cisco es una arquitectura propietaria de Cisco, está en el lado del cliente se compone de un agente denominado *Cisco Trust Agent*, *software* gratuito descargable desde la página del fabricante. La función de CTA es la de recibir la información del estado de la seguridad del equipo a conectar a la red proporcionando toda la información recogida, para recopilar esta información pueden usarse aplicaciones de distintos fabricantes o una propietaria de Cisco, el Cisco *Secure Access.*

Para el *Trust Agent*, Cisco ha desarrollado un protocolo propietario: el EAP en dos versiones: una sobre UDP y otra sobre 802.1X. Sobre UDP se hace solo validación y en 802.1X se hace validación y autenticación.

En cuanto a servidores, Cisco lo implementa en base al ACS que ha desarrollado para tal fin, completando con interfaces de verificación, auditoría y autenticación de otros

---

[14] NAC: es un enfoque de la seguridad que define como asegurar los nodos de la red.

fabricantes. Cisco también ofrece una solución basada en *appliances* permitiendo una más rápida implementación.

- Cisco define a NAC como el control de la admisión de la red de Cisco, es una solución que utiliza la infraestructura en red para hacer cumplir políticas de seguridad en todos los dispositivos que intentan tener acceso a recursos de computación de la red.
- NAC ayuda a asegurar que todos los hosts cumplan con las últimas políticas de seguridad corporativa como: *antivirus*, *software* de seguridad, y *patch* (parche, consta de cambios específicos que se realizan sobre un programa para agregar funcionalidades adicionales, actualizarlo o corregir errores) del sistema operativo, antes de obtener el acceso de red normal, a esto se conoce como Postura (es el proceso de verificación de acuerdo a las políticas de seguridad. Se evalúa parches de sistemas operativos, *antivirus*, *antispyware*, certificados digitales, actualizados, entre otros).

La Figura 1.10 muestra la arquitectura de NAC:

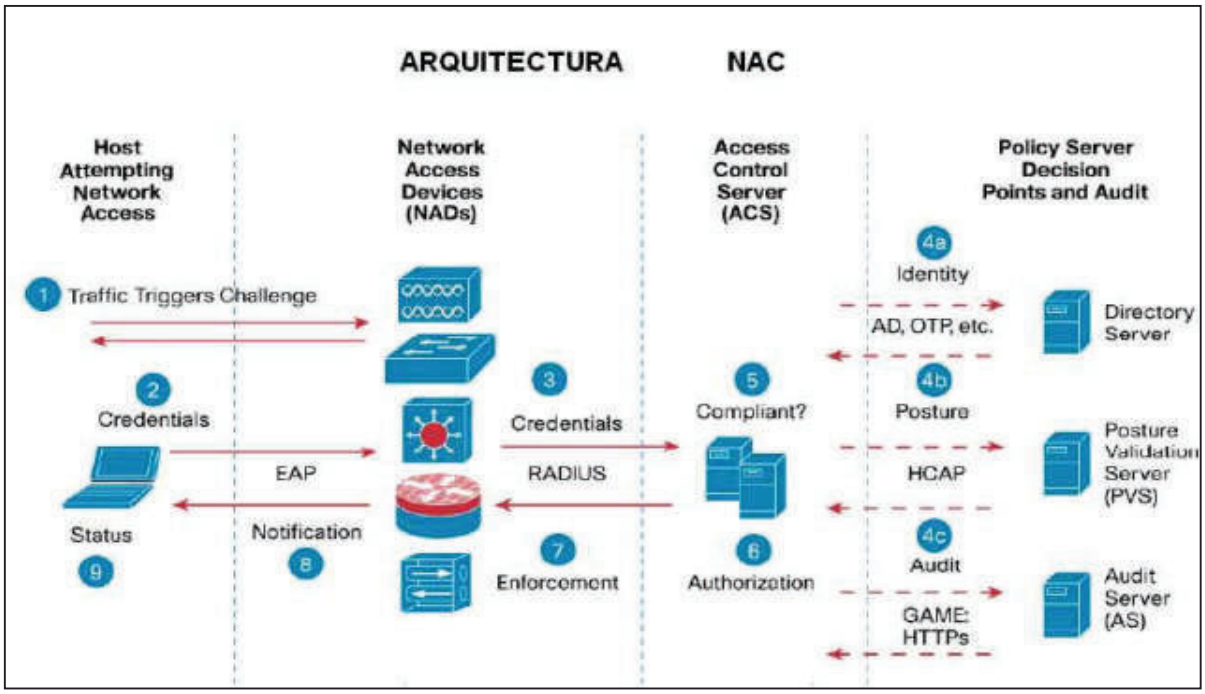

Figura 1.10 Arquitectura de NAC [10]

1. Validación de postura ocurre cuando un NAD[15](*Network Access Devices*) detecta que un *host* se quiere conectar o usar los recursos de la red.
2. Una vez detectado el nuevo dispositivo el NAD habilita una conexión entre el servidor AAA y ACS, una vez establecido el servidor AAA requiere las credenciales de postura al *host.*
3. El host responde a la petición con sus credenciales de postura desde el *software* compatible con NAC.
4. El servidor AAA valida la información de las posturas localmente, o puede delegar esta decisión a otros servidores de validación de posturas.
5. El servidor AAA agrega los resultados individuales de la postura, o símbolo *(token)* de postura, de todos los servidores para determinar la conformidad total del *host,* o del símbolo de postura del sistema.
6. La autenticación de identidad y el *token* de postura del sistema son luego chequeadas por una red de autorización, que puede consistir en: servidor RADIUS, asignación de VLAN o listas de acceso descargables.
7. Estas cualidades del RADIUS se envían al NAD para la aplicación en el *host.*
8. El CTA[16] en el host envía el estado de su postura para notificar a los *plugins* respectivos de su postura individual del uso así como la postura entera del sistema. Se puede enviar opcionalmente un mensaje al usuario final usando el diálogo de CTA notificando el estado actual del anfitrión en la red.

1.7 MÉTODO DE AUTENTICACIÓN POR MAB [11]

El método de autenticación MAB (*MAC Authentication By Pass*) permite el control de acceso a usuario basado en puertos, utilizando la dirección MAC[17] de los dispositivos. Un puerto habilitado por MAB se puede activar de forma dinámica basada en la

---

[15] NAD: (Dispositivo de acceso de red) equipo que permite conectar *endpoints* a la red.

[16] CTA: *Cognitive Threat Analytics*, realiza análisis en un equipo y posteriormente envía resultados.

[17] MAC: Control de Acceso al Medio Identificador único de 48 bits de una tarjeta o dispositivo de red.

dirección MAC del dispositivo que se conecta a este. La Figura 1.11 muestra el comportamiento del método MAB.

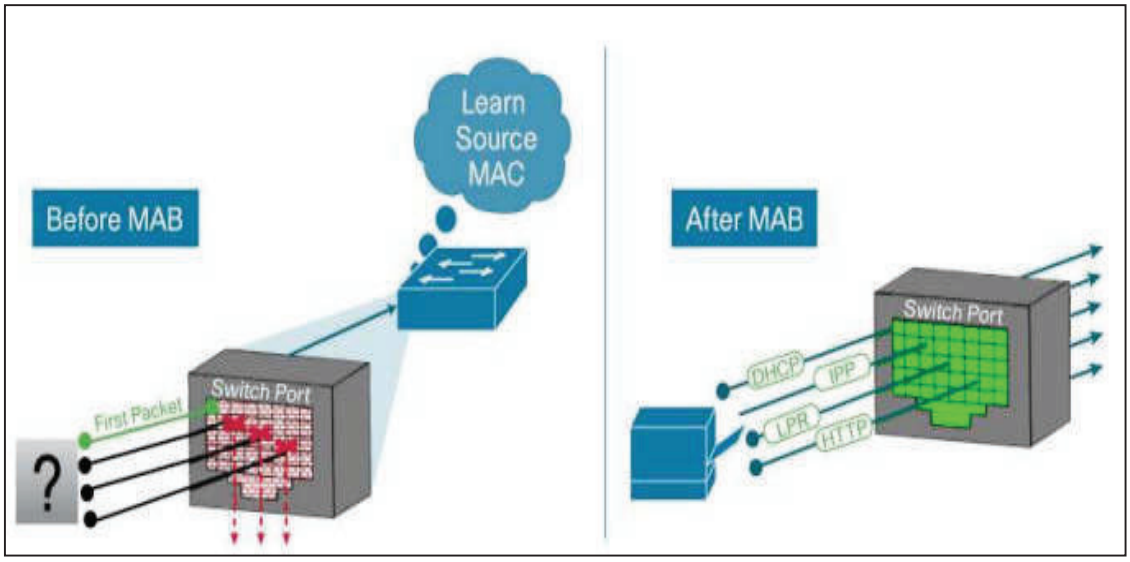

Figura 1.11 Comportamiento del método MAB [11]

Al desconocer la identidad del punto final, el tráfico para este está bloqueado, se examina un solo paquete para aprender y autenticar la MAC de origen, si el método de autenticación por MAB tuvo éxito, la identidad del dispositivo se conoce y se le permite todo el tráfico.

El *switch* realiza un filtrado de direcciones MAC para ayudar a garantizar que solo permita enviar tráfico al punto final MAB autenticado.

Este método valida las direcciones MAC que se almacenan en un sistema centralizado.

1.7.1 FUNCIONALIDAD DEL MÉTODO MAB

El método MAB permite o bloquea el acceso basado en la dirección MAC del dispositivo que se conecta el puerto y se configura como un mecanismo de reserva para el estándar IEEE 802.1x.

La Figura 1.12 muestra el funcionamiento del método MAB.

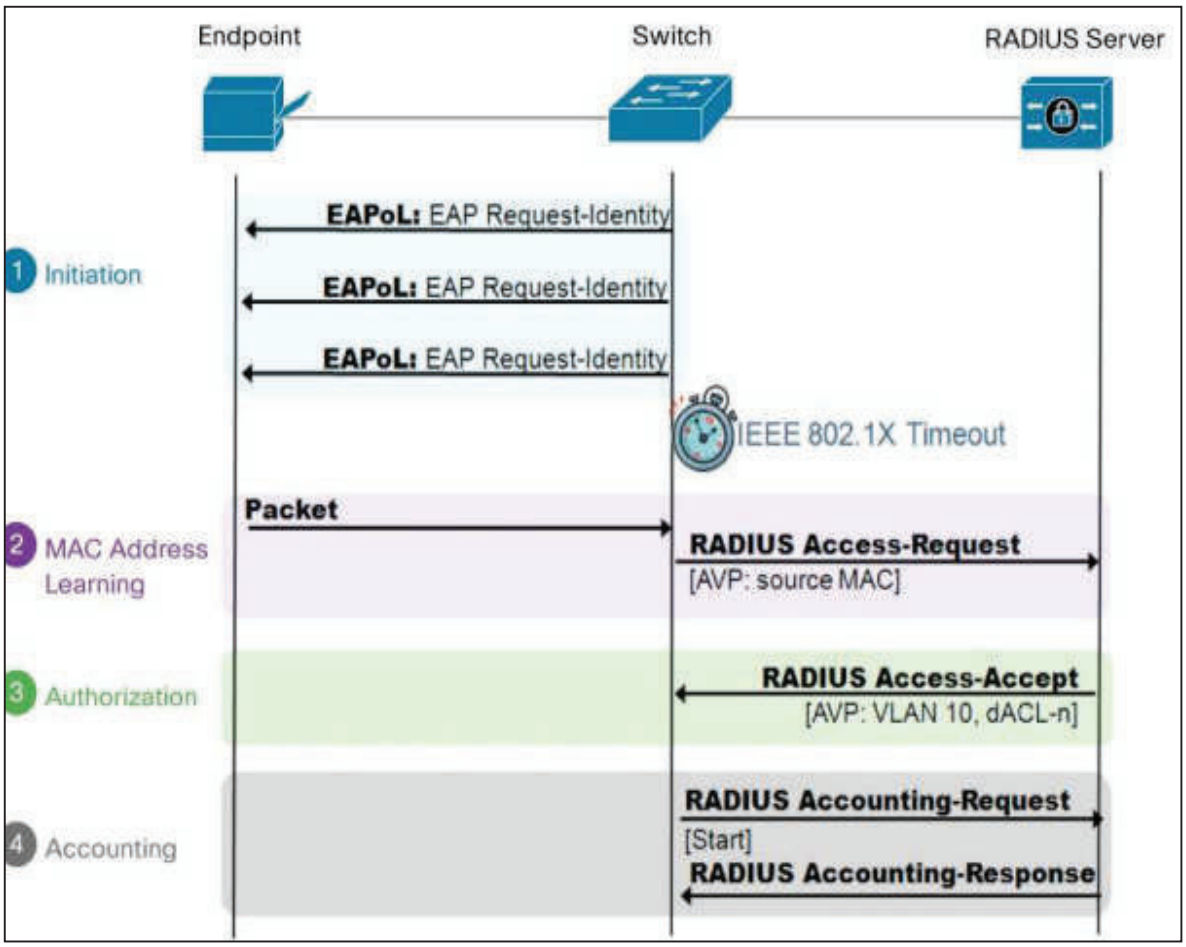

Figura 1.12 Funcionamiento del método MAB [11]

- Inicio de sesión
- Aprendizaje de direcciones MAC
- Autorización
- Contabilidad

1.7.2 BENEFICIOS

- Control de acceso en el borde: MAB actúa en la capa 2, que le permite controlar el acceso a la red en el borde de acceso.
- Visibilidad: Ofrece visibilidad de la red ya que el proceso de autenticación proporciona una forma de vincular la dirección IP de un dispositivo, direcciones MAC, *switch* y el puerto.

- Autenticación independiente**:** Una red trabaja con dispositivos que soportan o no el estándar IEEE 802.1X, en donde el MAB puede ser desplegado como un mecanismo de autenticación independiente.

1.7.3 LIMITACIONES MAB

- Base de datos MAC: Como requisito previo para el MAB, se debe tener una base de datos preexistente de direcciones MAC de los dispositivos que se permiten en la red.
- La creación y mantenimiento de una base de datos de direcciones MAC hasta la fecha es uno de los principales desafíos de la implementación del MAB.
- Retraso: MAB utiliza un tiempo de espera antes de la validación de la dirección MAC. Los retrasos en el acceso a la red pueden afectar negativamente a las funciones del dispositivo.
- Sin autenticación de usuario: MAB puede utilizarse para autenticar solo los dispositivos, y no los usuarios. Diferentes usuarios registrados en el mismo dispositivo tendrán el mismo acceso a la red.
- Fuerza de autenticación: A diferencia del estándar IEE 802.1X, el MAB no es un método de autenticación fuerte. MAB puede ser derrotado por la suplantación de la dirección MAC de un dispositivo válido.

1.8 ISO 27000 [12]

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional. La Figura 1.13 muestra la familia de las normas de Seguridad de la Información ISO 27000[18].

---

[18]ISO 27000: es un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información.

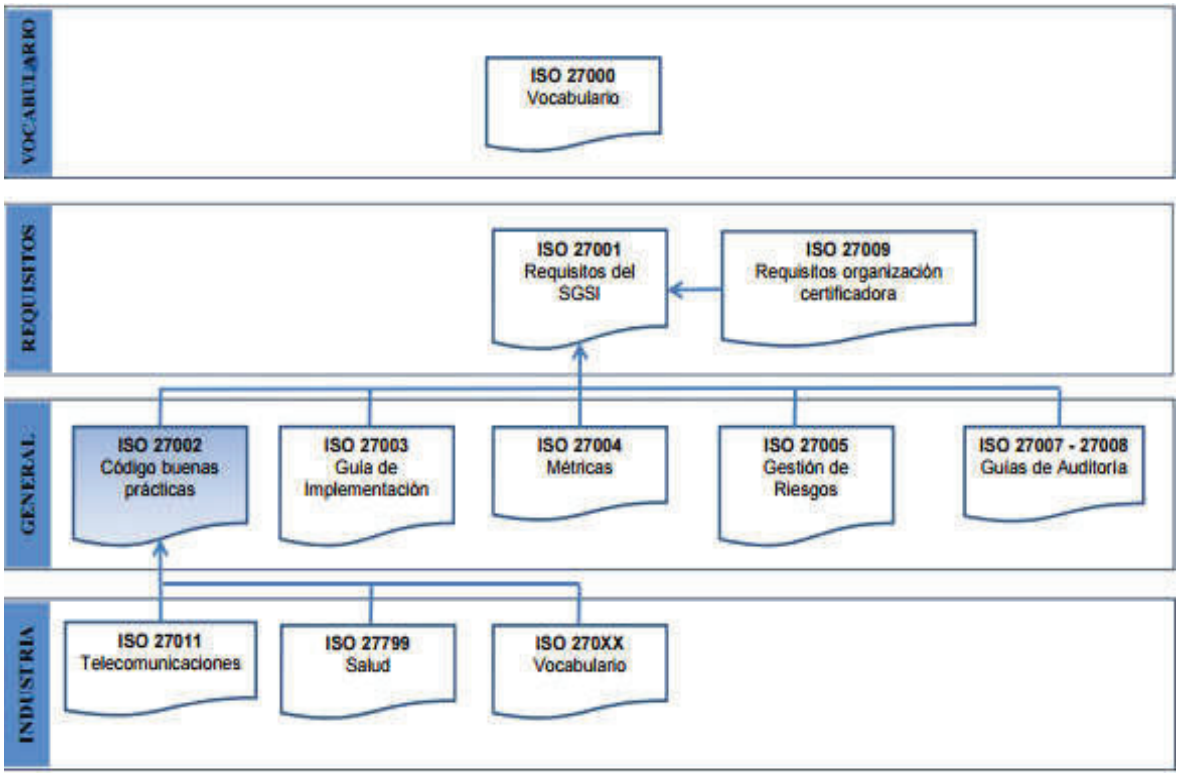

Figura 1.13 Familia de normas de seguridad ISO 27000 [12]

Este estándar internacional comprende todo un conjunto de normas relacionadas con la Seguridad de la Información, las más conocidas son: la ISO 27001 y la ISO 27002.

1.8.1 ISO 27001

La norma ISO 27001 resume los aspectos fundamentales que cubren el resto de los controles, para poder obtener como resultado una visión completa de lo que debe ser considerado en cualquier organización que desee preparar e implementar un verdadero Sistema de Gestión de la Seguridad de la Información (SGSI), y de esta forma se pueda preparar el camino para una certificación en el estándar ISO 27001.

Esta norma será uno de los pilares fundamentales para definir la “Calidad” con que se adoptan y gestionan acciones y medidas de seguridad sobre los recursos de una empresa. Los controles del estándar ISO 27001, permiten garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones:
- Control de accesos: No se debe confundir la actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente "sea, quien dice ser". El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas: Encauzar (o enjaular) al usuario debidamente y verificar el desvío de cualquier acceso, fuera de lo correcto.
- Adquisición de sistemas de información, desarrollo y mantenimiento.
- Administración de los incidentes de seguridad: Todo lo relativo a incidentes de seguridad queda resumido a dos formas de proceder: proteger y proceder y seguir y perseguir.
- Administración de la continuidad de negocio los presenta a través de un solo grupo.
- Marco legal y buenas prácticas.

1.8.2 ISO 27002

La norma ISO/IEC 27002, es una recopilación de las mejores prácticas para la Gestión de Seguridad de la Información. Una vez que se han determinado los requerimientos de seguridad, se deben seleccionar los controles apropiados que deben implementarse para asegurar que los riesgos se reduzcan a un nivel aceptable.

La Norma NTE INEN ISO/IEC 27002 contiene un total de 133 controles que se distribuyen en once secciones principales. Algunos autores también nombran a estas secciones como dominios o cláusulas y son los siguientes:

1. Política de Seguridad de la Información
2. Organización de la Seguridad de la Información
3. Gestión de Activos de Información
4. Seguridad de los Recursos Humanos
5. Seguridad Física y Ambiental
6. Gestión de las Comunicaciones y Operaciones
7. Control de Accesos
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
9. Gestión de Incidentes en la Seguridad de la Información
10. Gestión de Continuidad del Negocio
11. Cumplimiento

Cada sección tiene claramente definido sus objetivos de control. Para cumplir dichos objetivos, se especifican los distintos controles recomendados en base a las mejores prácticas relacionadas a la seguridad de la información.

1.8.2.1.1 Estructura de la Norma NTE INEN ISO/IEC 27002

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

Cláusulas: Cada cláusula contiene un número de categorías principales de seguridad.

Categorías principales de seguridad: cada categoría principal de seguridad contiene:

- Un objetivo de control declarando lo que se debe alcanzar.
- Uno o más controles que pueden ser aplicados para alcanzar el objetivo de control.

Las descripciones del control son estructuradas de la siguiente manera:

- Control: Describe la estructura necesaria para satisfacer el objetivo de control (donde se especifica lo que desea alcanzar).

- Guía de implementación: Provee información más detallada para apoyar la implementación del control y conocer el objetivo de control. Algunas guías pueden no ser convenientes para todos los casos, por lo tanto algunas otras formas de implementar el control pueden ser más apropiadas.
- Otra información: Provee información adicional que pueda ser necesaria, por ejemplo consideraciones legales y referencias de otros estándares.

Las recomendaciones que contiene la Norma están organizadas de la siguiente forma: en el primer nivel se mencionan las Cláusulas, en el segundo nivel se enlistan los Categorías Principales de Seguridad y en el tercer nivel del listado se mencionan los Controles Recomendados.

1.8.3 DIFERENCIAS ENTRE NORMAS ISO 27001 E ISO 27002

- La única norma a certificar de la serie es la ISO 27001. No así la ISO 27002, ya que tan solo establece una serie de recomendaciones y buenas prácticas.
- La ISO 27002 es mucho más detallada y mucho más precisa.
- Los controles de la norma ISO 27002 tienen la misma denominación que los indicados en el Anexo A de la ISO 27001.
- Pero la diferencia radica en el nivel de detalle; en general, la ISO 27002 explica un control en toda una página, mientras que la ISO 27001 solo le dedica una breve explicación a cada uno.
- La ISO 27002 no distingue entre los controles que son aplicables a una organización determinada y los que no lo son.
- Por otro lado, la ISO 27001 exige la realización de una evaluación de riesgos sobre cada control para identificar si es necesario disminuir los riesgos y, en caso que sea necesario, hasta qué punto deben aplicarse.
- Cada norma de la serie ISO 27001 está diseñada con un enfoque preciso: si desea crear la estructura de la seguridad de la información en su organización y definir su encuadre, debería usar la ISO 27001.
- Si se desea implementar controles, se usa la ISO 27002.

1.9 AUTENTICACIÓN ISE (*IDENTITY SERVICES ENGINE*) [13] [14]

La evolución tecnológica de la estructura de seguridad para acceso a la red ha venido incorporando las soluciones de autenticación ACS (*Access Control Server* / Servidor de Control de Acceso) para ser complementada por la solución NAC y ahora Cisco ha unido las dos tecnologías para ofrecer el sistema ISE.

La Figura 1.14 muestra la evolución de Cisco en ACS.

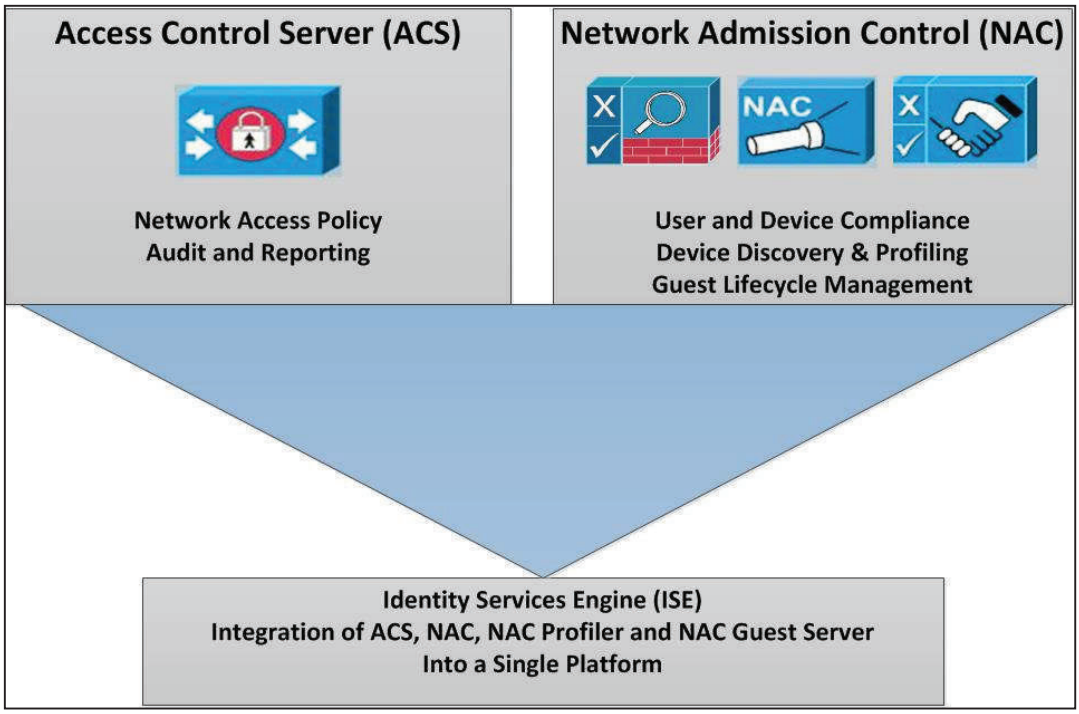

Figura 1.14 Evolución de Cisco en Control de Acceso a la Red [13]

Cisco *Identity Services Engine* (ISE) permite cumplir las políticas de seguridad de acceso en forma confiable, mejorar la seguridad de la infraestructura y agilizar las operaciones de servicio. Es una plataforma contextual, basada en identidad, que recolecta información en tiempo real de la red, los usuarios y los dispositivos. Luego utiliza esta información para tomar decisiones proactivas de gobernabilidad mediante la aplicación de las políticas en toda la infraestructura de la red.

La Figura 1.15 muestra la implementación de una red LAN con Cisco ISE.

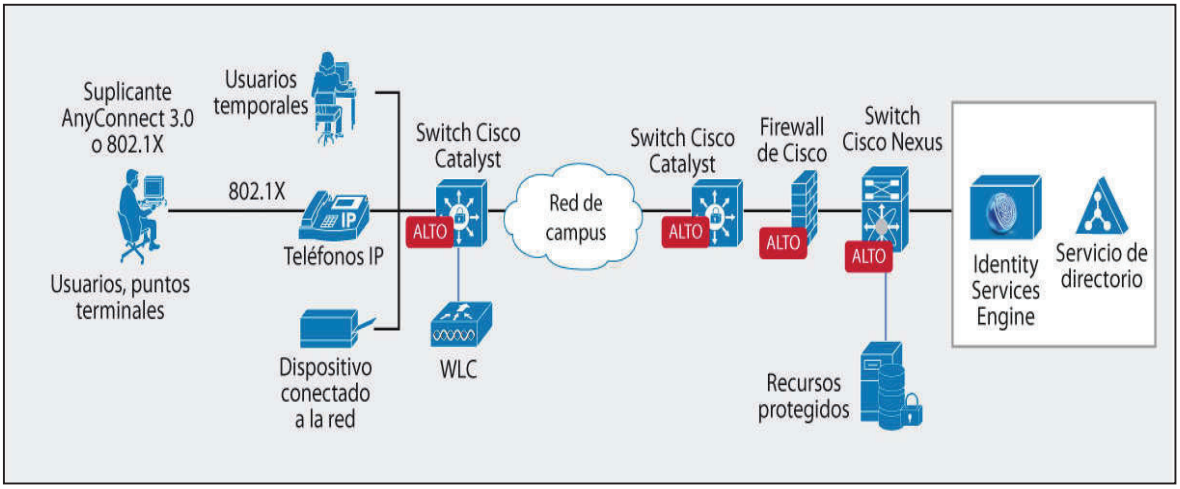

Figura 1.15 Implementación de una red LAN con Cisco ISE [14]

1.9.1 CARACTERÍSTICAS DE CISCO ISE

- Aplicación uniforme de políticas contextuales en las redes fijas e inalámbricas.
- Visibilidad de todo el sistema para saber qué y quiénes están en la red fija, inalámbrica o VPN.
- Autenticación, autorización y administración (AAA) integradas, perfiles (*Profiling*), estado (*Posture*) y servicios para usuarios temporales a fin de simplificar las implementaciones y reducir costos.
- Identificación automática y precisa de dispositivos mediante sondas basadas en ISE *(Profiling*), sensores integrados de dispositivos, exploración activa de puntos terminales.
- Cumplimiento de dispositivos móviles basado en políticas y aprovisionamiento de aplicaciones mediante soluciones integradas de administración de múltiples dispositivos.
- Integración BYOD simplificada mediante registro de autoservicio.
- Verificación de estado de Salud de dispositivos (*antivirus* y parches de sistema operativo).
- Automatiza la aplicación de políticas y la configuración de dispositivos de acceso.

- Maneja listas de acceso descargables conocidas como DACL[19] (*Downloadable Access Control List* / Lista de Control de Acceso Descargable).
- Sistema que puede trabajar de manera redundante con *Appliance* distribuidos y en modo jerárquico.

1.9.2 VENTAJAS DE CISCO ISE

- Seguridad: Mejora la visibilidad y el control de todas las actividades y dispositivos en la red física e infraestructura virtual.
- Cumplimiento: Establece políticas uniformes en toda la infraestructura para mejorar el cumplimiento de las normas empresariales.
- Eficiencia: Automatiza las tareas intensivas y simplifica la prestación de servicios para aumentar la productividad del personal de TI[20].

1.9.3 BENEFICIOS DE CISCO ISE

- Verificación rigurosa y reconocimiento automático del perfil de dispositivo: Es el primer perfilador de dispositivos de la industria capaz de identificar cada dispositivo en la red; coincidir con un usuario o función, además de otros atributos, incluyendo tiempo, ubicación y red.
- Permite realizar el reconocimiento automático de las características de los últimos equipos añadidos a la red. Reconocerá el último Smartphone antes que el personal de TI.
- ISE permitirá tener un control total de manera que ningún dispositivo se escape a la visibilidad de la red.
- Aplicación y cumplimiento de políticas de seguridad: Permite definir políticas de acceso de una forma dinámica y sencilla que cumpla con los requisitos de cambio que requiera la empresa. Por ejemplo, los administradores de TI pueden

---

[19] DACL: es una lista de control de acceso que se pueden descargar de una página de Cisco.

[20] TI: es un término que se utiliza para referirse a las tecnologías de la Información.

definir de forma sencilla políticas en el ISE que permitan diferenciar equipos de usuarios invitados de los equipos de los usuarios corporativos.

- Los usuarios invitados reciben un acceso limitado dentro de la red, mientras que los usuarios corporativos tienen acceso de acuerdo a las políticas asignadas.
- ISE cuenta con una interfaz gráfica que permite la creación, visibilidad y generación de reportes de todas las redes de la empresa, lo cual facilita la validación y cumplimiento de los requerimientos regulatorios y guías de la normativa 802.1x para auditorías.
- Integración automática de los dispositivos con acceso seguro y confiable desde cualquier lugar: Cuenta con un portal de auto registro que permite al usuario registrarse y proporcionar la información de los nuevos dispositivos según las políticas definidas por TI automáticamente.
- Esto permite a TI tener de forma automática la información del dispositivo, el perfilamiento y las características, para que este pueda cumplir con las políticas de seguridad, manteniendo el proceso de integración a la red simple para los usuarios sin requerir ayuda de TI.
- Las políticas de acceso en tiempo real de ISE permiten que tanto los usuarios móviles como remotos puedan tener acceso a los servicios de la red cableada e inalámbrica desde cualquier lugar que ingresen.
- Eficiencia Operativa: Automatización en la gestión y seguridad, control centralizado de políticas, visibilidad, resolución de problemas e integración con Cisco Prime, características que aseguran que el personal de TI pasará menos tiempo en la resolución de problemas de la red.

1.9.4 ARQUITECTURA CISCO ISE

La arquitectura de control de acceso a la red propuesta Cisco ISE, se basa en nodos que cumplen roles específicos.

La Figura 1.16 muestra los roles y funcionamiento de la plataforma Cisco ISE.

Figura 1.16 Funcionamiento de Cisco ISE [14]

1.9.4.1 Rol Administrador – ADM

Realiza todas las operaciones administrativas. Maneja todas las configuraciones relacionadas con el sistema y las configuraciones que se relacionan con la funcionalidad de autenticación, autorización y contabilidad.

En un entorno distribuido, puede tener solo uno o un máximo de dos nodos que ejecutan el rol de administración.

1.9.4.2 Rol Monitoreo - MON

Permite al Cisco ISE funcionar como el colector de mensajes de registro y de repositorio de toda la información de administración creada para usuarios, grupos y dispositivos, y repositorio de la información de políticas de servicio para los nodos ISE PSN[21] (*Police Server Network* / Servidor de Políticas de Red).

Este rol proporciona herramientas avanzadas de monitoreo y solución de problemas sobre los elementos de red y sus recursos.

Un nodo con este rol, permite agregar y correlacionar los datos que recopila para ofrecer información significativa mediante informes.

Cisco ISE permite tener un máximo de dos nodos con este rol que puede asumir funciones primarias o secundarias para alta disponibilidad.

1.9.4.3 Rol Políticas de Servicio - PSN.

Proporciona políticas de acceso a la red, postura, acceso de invitados, aprovisionamiento de clientes, y perfiles de servicio.

Este rol evalúa las políticas y toma todas las decisiones. Puede tener más de un nodo con este rol dentro de la red.

Todos los nodos de políticas de servicio de Cisco ISE residen detrás de un equilibrador de carga y comparten una dirección de multidifusión común, se pueden agrupar para formar un grupo de nodos. Si uno de los nodos en un grupo de nodos falla, los otros nodos detectan el fallo y restablecen las sesiones pendientes.

Las configuraciones son realizadas en *Admin* y son enviadas al PSN, cuando un dispositivo final accede a la red, el NAD se comunica con ISE usando RADIUS.

---

[21] PSN: rol del ISE que permite encargado de la ejecución de las políticas de red.

La Figura 1.17 muestra la arquitectura de Cisco ISE.

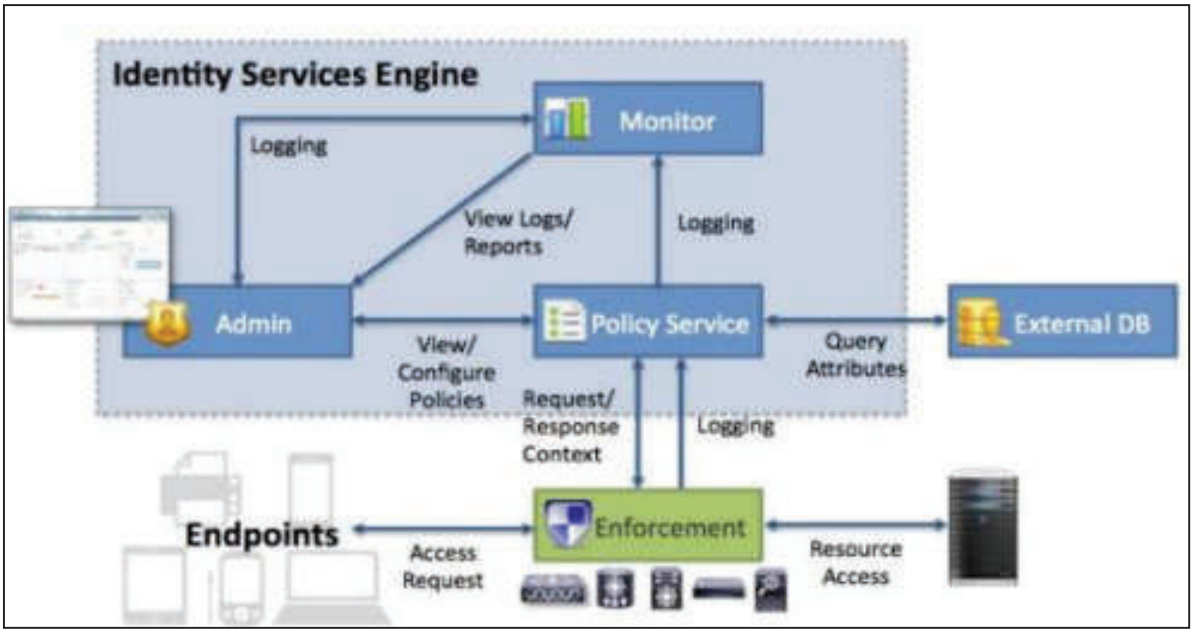

Figura 1.17 Arquitectura de Cisco ISE [13]

1.9.5 POLÍTICAS CONFIGURABLES EN LA PLATAFORMA CISCO ISE

- Autenticación: Proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un computador, una *tablet*, un teléfono y otros. Es un modo de asegurar que el usuario es quien dice ser.
- Autorización: Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
- Perfilamiento: Proceso de perfilamiento de dispositivos, identificación del tipo de equipo.
- Postura: Proceso para verificación de estado de salud de una computadora..

CAPÍTULO II

ANÁLISIS DE LA RED Y DEL DISEÑO DE AUTENTICACIÓN DE LA EMPRESA PETROLERA SOBRE LA CUAL NET IO SERVICIOS S.A. BRINDA CONSULTORÍA

2.1 INTRODUCCIÓN

Este capítulo tiene como objetivo analizar la infraestructura actual de la red para permitir la integración entre los equipos, servicios, usuarios de los diferentes bloques de la empresa petrolera a la plataforma de autenticación Cisco ISE.

Actualmente la empresa petrolera se divide en cuatro zonas independientes, todas vinculadas entre sí, se realizará el análisis para corregir los errores actuales de conexión e implementación de la solución Cisco ISE. Para poder realizar el análisis de la situación actual de la empresa y en base a ellos obtener los requerimientos necesarios para rediseñar la red se propone el siguiente procedimiento:

1. Definir qué comprende la empresa NET IO Servicios
2. Definir qué comprende la empresa petrolera a la cual NET IO Servicios brinda consultoría.
3. Descripción de la infraestructura actual de la empresa petrolera a la NET IO Servicios brinda consultoría.
4. Descripción de los usuarios y la cantidad de equipos de la empresa petrolera a la que NET IO Servicios brinda consultoría.
5. Análisis de tráfico actual y crecimiento futuro de la empresa petrolera.
6. Consideraciones para el rediseño de la empresa petrolera.
7. Compatibilidad de los equipos actuales de la empresa con la nueva solución de autenticación Cisco ISE.

2.2 EMPRESA NET IO SERVICIOS S.A.

La empresa NET IO Servicios S.A. fue creada en el año 2014 por el Ing. German Garófalo, su financiamiento fue única e íntegramente con inversión privada.

Es una empresa proveedora de servicios integrales de Tecnologías de la Información especializados en redes de datos empresariales, infraestructuras de redes de próxima generación, centros de datos, comunicaciones convergentes y colaboración; soluciones que engloban tanto a los sistemas fundamentales así como la infraestructura complementaria para su efectiva gestión y proactiva seguridad de la información procesada.

2.2.1 MISIÓN

NET IO Servicios S.A. tiene como misión ser una empresa de servicios de diseño, implementación, operación y optimización de soluciones basadas en tecnologías que potencian la productividad del negocio de los clientes.

2.2.2 VISIÓN

NET IO Servicios S.A. tiene como visión proyectarse permanentemente como una compañía conformada por profesionales expertos en tecnología que se ocupan del éxito de los negocios de los clientes así como de ser generadores de innovación, mejoramiento continuo e impacto social positivo.

2.2.3 SERVICIOS

Para satisfacer los requerimientos de información de sus clientes NET IO Servicios ofrece: consultoría, implementación, soporte y capacitación a sus clientes a nivel nacional**.** Cuenta con profesionales especializados y certificados, los servicios están desde la consultoría estratégica de negocios, apoyo en el diseño de integración de nuevas tecnologías, desarrollo e implementación de proyectos innovadores, posterior soporte y acompañamiento en la operación, y finalmente capacitación certificada.

2.2.4 DESCRIPCIÓN DE LAS INSTALACIONES

NET IO Servicios S.A. es una empresa dedicada a brindar servicios integrales de tecnologías de la información especializados en redes de datos empresariales a nivel nacional. Cuenta con una matriz en Quito, ubicada en la Baquedano E7-60 y Av. 6 de Diciembre, edificio Delgado Coronel, tercer piso, con aproximadamente 25 usuarios.

2.3 DESCRIPCIÓN DE LA EMPRESA PETROLERA

La empresa petrolera es una entidad pública ecuatoriana dedicada a la exploración y producción de hidrocarburos, opera en 11 bloques, ubicados en Quito, el oriente ecuatoriano y en la zona del litoral.

2.3.1 MISIÓN

La empresa petrolera tiene como misión desarrollar actividades estratégicas de exploración y explotación de hidrocarburos, de manera eficiente, sustentable y segura, con responsabilidad social y ambiental, con el aporte del mejor talento humano para contribuir al desarrollo energético del Ecuador.

2.3.2 VISIÓN

La empresa petrolera tiene como visión ser la empresa referente del Estado ecuatoriano y líder de la industria de exploración y explotación de hidrocarburos a nivel nacional y regional, por su eficiencia, integridad y confiabilidad, a la vanguardia de la responsabilidad social y ambiental.

2.3.3 SERVICIOS

La empresa petrolera pública está dedicada a la exploración y producción de hidrocarburos. Está a cargo de la operación de 11 Bloques, ubicados en Quito, en la cuenca del oriente del Ecuador y en la zona costera del Litoral. Varios puntos de su operación cuentan con certificaciones internacionales que avalan sus procedimientos

y prácticas. Las áreas de operación se encuentran ubicadas geográficamente en las provincias de Sucumbíos, Orellana, Napo, Pastaza, El Oro y Santa Elena.

2.3.4 DESCRIPCIÓN DE LAS INSTALACIONES

La empresa petrolera tiene su matriz en el edificio Banco del Pacífico en Quito, cuenta con sucursales en el oriente ecuatoriano y costa: Zona Centro, Zona Norte, Zona Oeste, Zona Este y la Zona del Litoral. A continuación se describirá cada una:

2.3.4.1 Matriz

La matriz de la empresa petrolera sobre la cual Net Io Servicios S.A. brinda consultoría está ubicada en la Av. Naciones Unidas E-7-95 y Av. De los Shyris. Edificio Banco del Pacífico.

2.3.4.2 Zona Centro

La zona centro está ubicada en el Río Napo y la provincia de Sucumbíos del Oriente Ecuatoriano. Esta se subdivide en los bloques 12 y 15 (ver Figura 2.1).

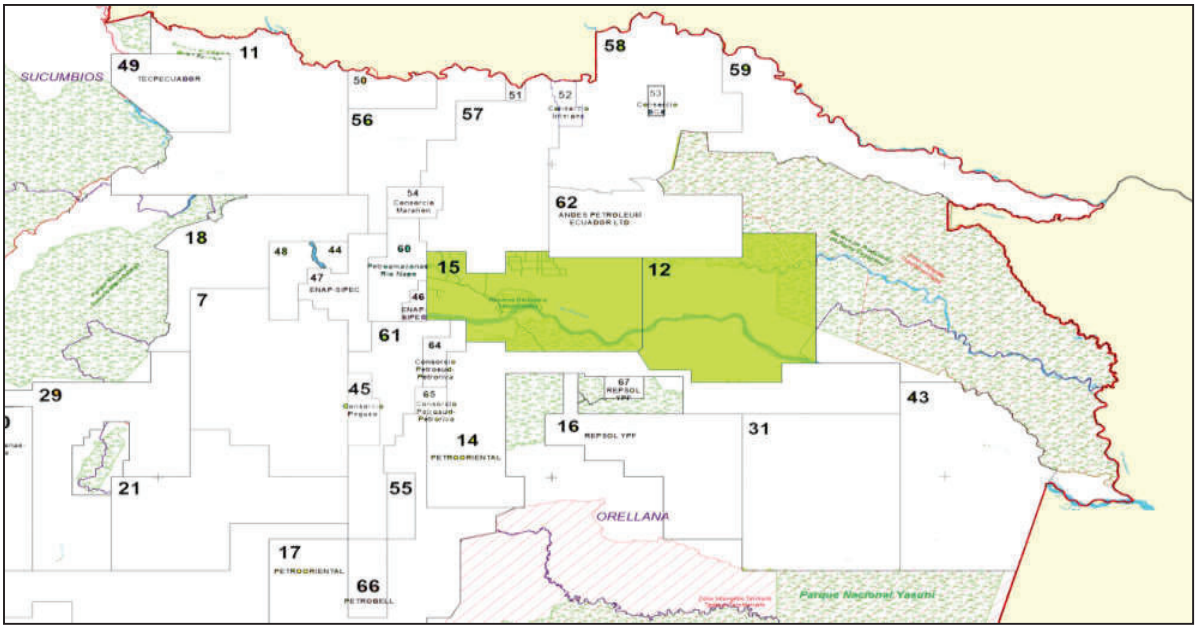

Figura 2.1 Zona centro de la empresa petrolera

- ❖ Bloque 12: Se compone de los campos Eden Yuturi (EPF) y Pañacocha.
- ❖ Bloque 15: Se compone del campo CPF.

2.3.4.3 Zona Norte

La zona norte está ubicada en la Provincia de Sucumbíos del Oriente Ecuatoriano. Esta se subdivide en los bloques 63 y 43 (Ver la Figura 2.2).

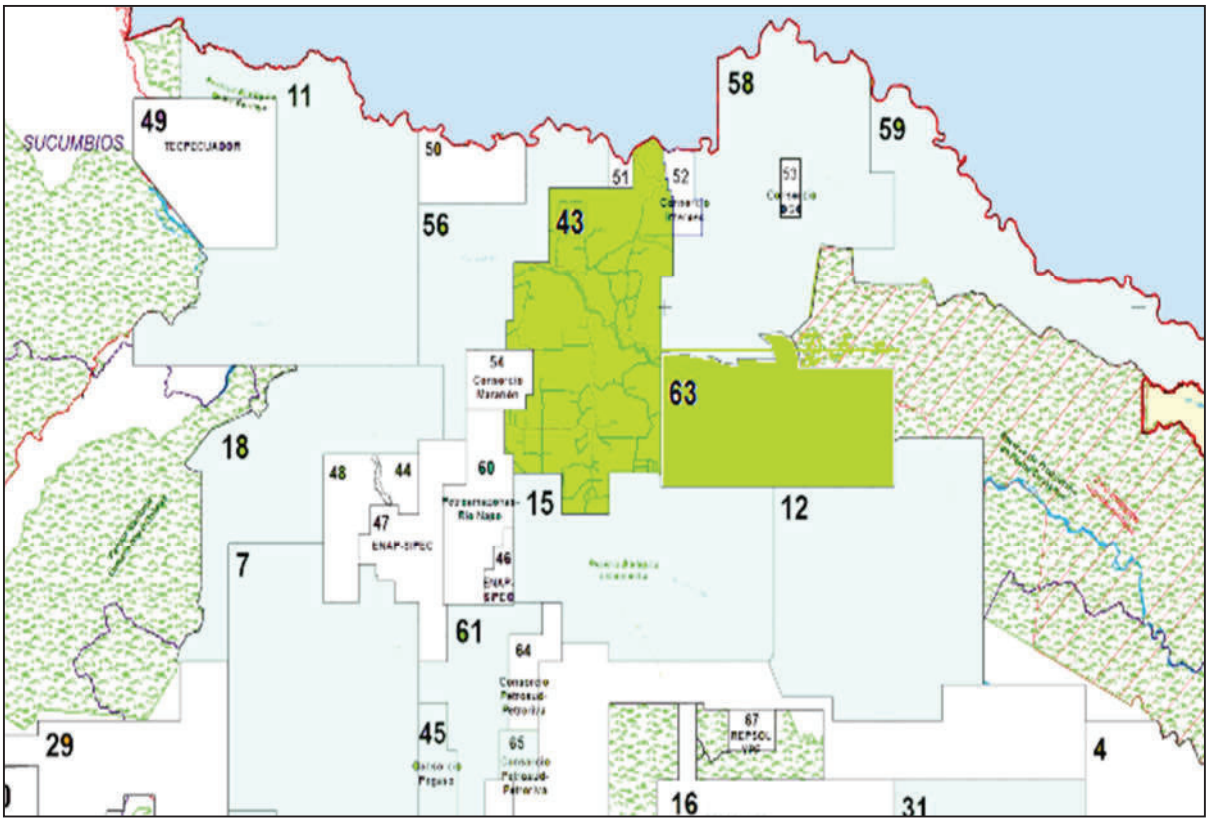

Figura 2.2 Zona Norte de la empresa petrolera

- ❖ Bloque 63: Se compone del campo Lago Agrio.
- ❖ Bloque 43: Se compone de los campos Libertador y Shushufindi.

2.3.4.4 Zona Oeste

La zona oeste está ubicada en la provincia de Orellana y Napo del Oriente Ecuatoriano. Esta se subdivide en los bloques 7, 18 y 21 (Ver la Figura 2.3).

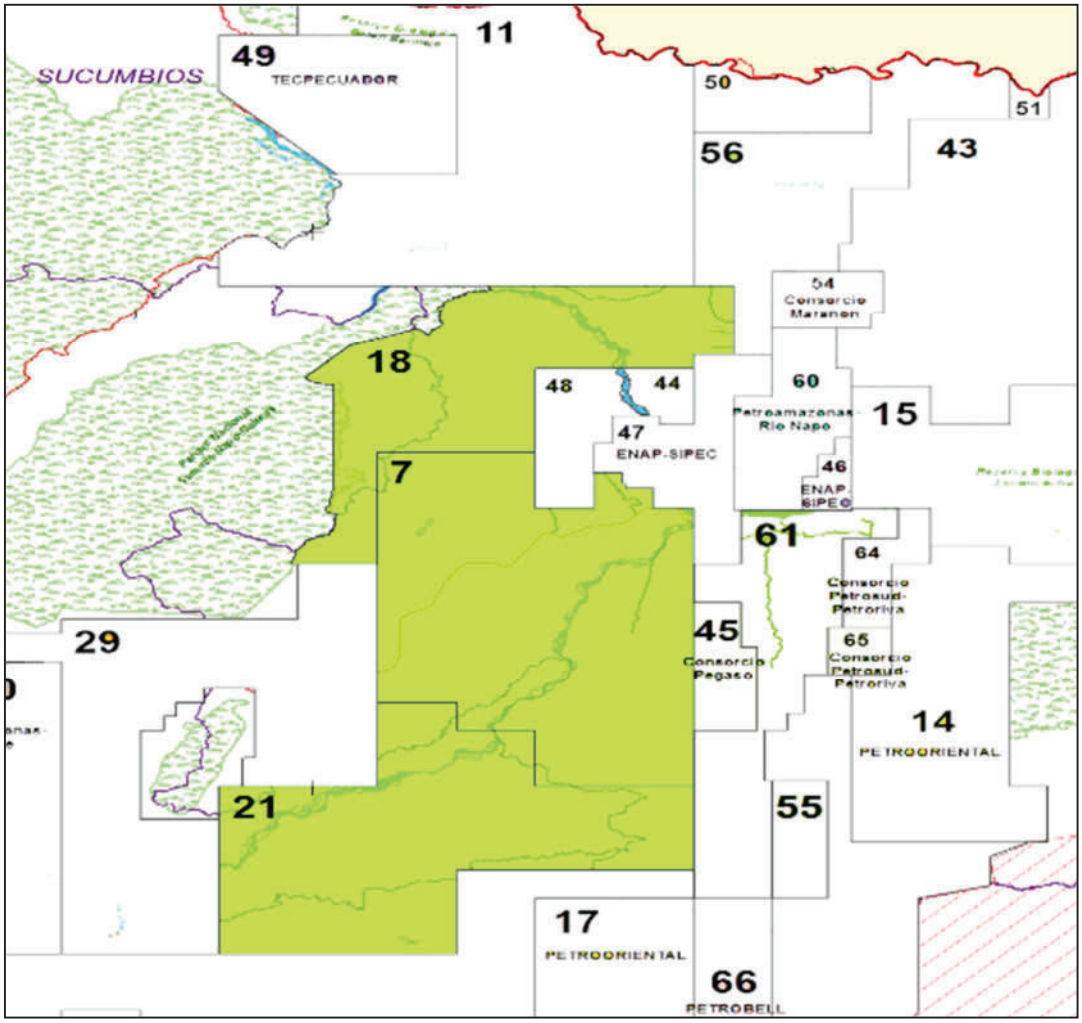

Figura 2.3 Ubicación de la Zona Oeste de la empresa petrolera

- Bloque 7: Se compone del campo Payamino
- Bloque 18: Se compone del campo Palo Azul
- Bloque 21: Se compone del campo Yuralpa

2.3.4.5 Zona Este

La zona está ubicada en la provincia de Orellana del Oriente Ecuatoriano.

Esta se subdivide en el bloque 31.

La Figura 2.4 muestra la ubicación de la zona este con sus bloques.

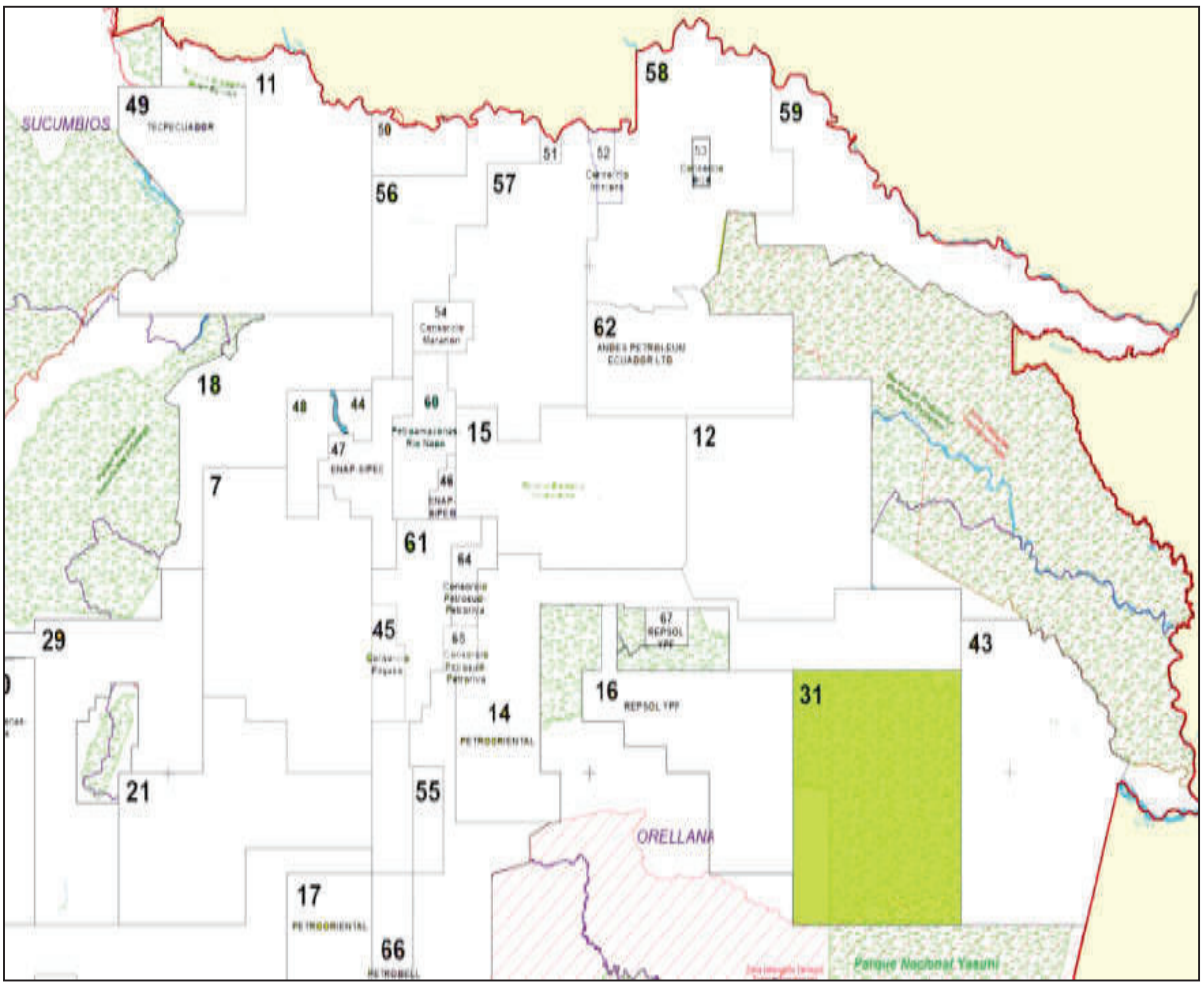

Figura 2.4 Ubicación de la Zona Este de la empresa petrolera

- Bloque 31: Se compone del campo Chiru-isla

2.3.4.6 Zona del Litoral

La zona del Litoral está ubicada en las provincias de Santa Elena y El Oro.

Esta se subdivide en:

- Bloques 1
- Bloques 6

La Figura 2.5 muestra la ubicación de la zona del litoral con sus bloques.

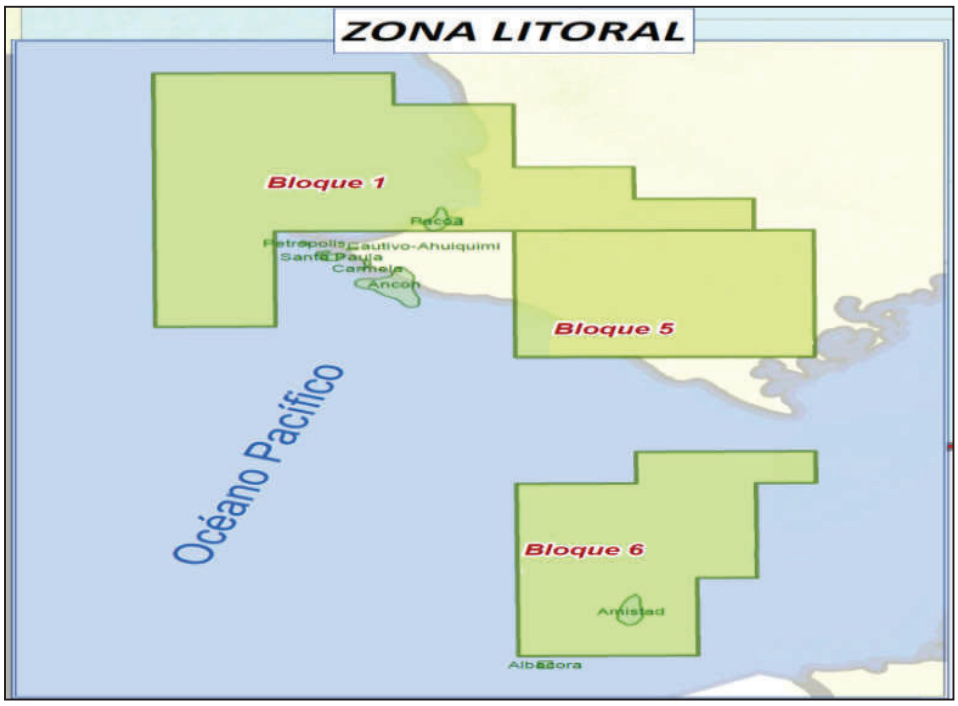

Figura 2.5 Ubicación de la Zona del Litoral

- Bloque 1: Se compone del campo Pacoa
- Bloque 6: Se compone del campo Amistad

2.4 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED

El personal de la empresa petrolera labora en la oficina de la matriz en Quito, en los bloques del Oriente Ecuatoriano y en los bloques de la zona del Litoral a nivel WAN (Wide Area Network) y cada uno cuenta con su propia red LAN (Local Area Network). A continuación se analiza la topología física y lógica de la red.

2.4.1 RED DE ÁREA EXTENDIDA DE LA EMPRESA PETROLERA

2.4.1.1 Topología Física y Lógica de la Red

La red WAN de la empresa petrolera tiene una interconexión física con sus nodos a nivel nacional. En la Figura 2.6 se muestra el diagrama a nivel WAN de la empresa petrolera.

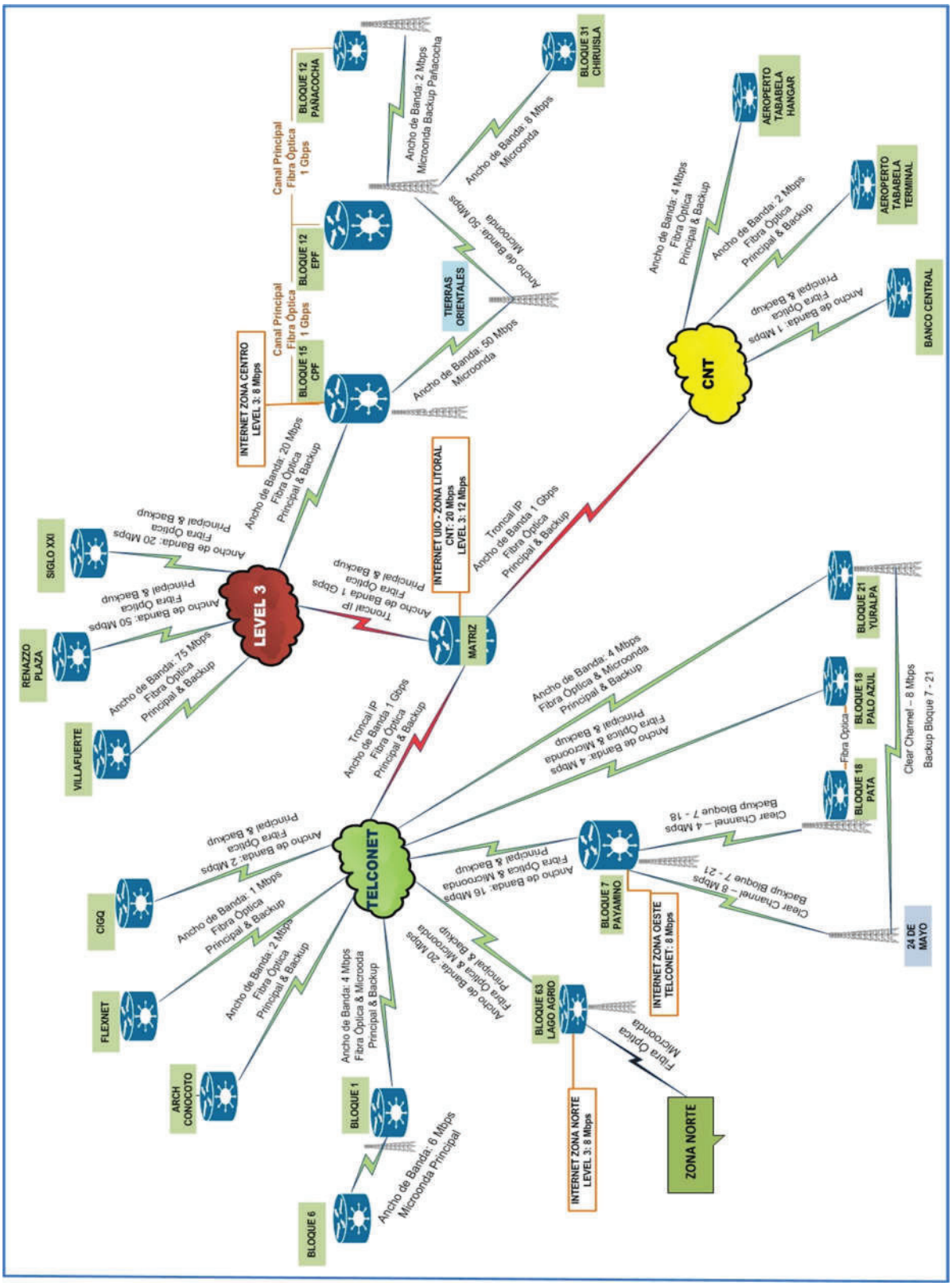

Figura 2.6 Diagrama de interconexión a nivel WAN de la empresa petrolera

2.4.1.2 Direccionamiento Lógico

La mayoría de los equipos de conectividad de la empresa petrolera son equipos de la marca Cisco, para la transmisión de datos a nivel WAN utiliza el protocolo MPLS (*Multiprotocol Label Switching*).

La red de la empresa petrolera para su direccionamiento en capa tres utiliza una dirección IP privada clase B (172.0.0.0), la misma que se divide en diferentes segmentos para que se distribuya entre sus redes a nivel WAN, LAN (direccionamiento IP se encuentra en el Anexo B1), y enlaces arrendados.

En la tabla 2.1 se sintetiza la información de cómo se distribuyen las direcciones IP para los diferentes enlaces WAN de la empresa.

NODO	DIRECCIÓN IP	MÁSCARA
BLOQUE 1	172.2.1.0	255.255.255.192
BLOQUE 6	172.2.2.0	255.255.255.192
BLOQUE 7	172.2.3.0	255.255.255.192
BLOQUE 12	172.2.4.0	255.255.255.192
BLOQUE 15	172.2.5.0	255.255.255.192
BLOQUE 18	172.2.6.0	255.255.255.192
BLOQUE 21	172.2.7.0	255.255.255.192
BLOQUE 31	172.2.8.0	255.255.255.192
BLOQUE 43	172.2.9.0	255.255.255.192
BLOQUE 63	172.2.10.0	255.255.255.192

Tabla 2.1 Direccionamiento WAN empresa Petrolera

2.4.1.3 Descripción de los Enlaces

La red WAN de la empresa petrolera, cuenta en su nivel físico con enlaces dedicados de datos arrendados a los siguientes proveedores: ISP Level 3, ISP Megadatos (Telconet) y el ISP CNT.

La Tabla 2.2 muestra las características de los enlaces a nivel WAN por proveedor.

ENLACES	SERVICIO	ANCHO DE BANDA	MEDIO DE TRANSMISION	PROVEEDOR
Matriz UIO	*Internet*	20 Mbps	Fibra Óptica	CNT
	Internet Backup	12 Mbps	Fibra Óptica	Telconet
Edificio Renazzo Plaza - Matriz UIO	Datos	50 Mbps	Fibra Óptica	Level 3
	Datos *Backup*	50 Mbps	Fibra Óptica	Level 3
Edificio Siglo XXI - Matriz UIO	Datos	20 Mbps	Fibra Óptica	Level 3
	Datos Backup	20 Mbps	Fibra Óptica	Level 3
Edificio Villafuerte - Matriz UIO	Datos	75 Mbps	Fibra Óptica	Level 3
	Datos Backup	75 Mbps	Fibra Óptica	Level 3
Zona Centro Bloque 15	*Internet*	8 Mbps	Fibra Óptica	Level 3
Zona Centro Bloque 15 - Matriz UIO	Datos	20 Mbps	Fibra Óptica	Level 3
	Datos Backup	20 Mbps	Fibra Óptica	Level 3
Edificio CIGQ San Rafael - Matriz UIO	Datos	2 Mbps	Fibra Óptica	Telconet
	Datos Backup	2 Mbps	Fibra Óptica	Telconet
Bodegas Flexnet Calderón - Matriz UIO	Datos	1 Mbps	Fibra Óptica	Telconet
	Datos Backup	1 Mbps	Fibra Óptica	Telconet
Edificio ARCH Conocoto - Matriz UIO	Datos	2 Mbps	Fibra Óptica	Telconet
	Datos Backup	2 Mbps	Fibra Óptica	Telconet
Zona Litoral Machala - Matriz UIO	Datos	4 Mbps	Fibra Óptica	Telconet
	Datos Backup	4 Mbps	Radio Enlace	Telconet
Zona Norte Bloque 63 Lago Agrio	*Internet*	8 Mbps	Fibra Óptica	Level 3
Zona Norte Bloque 43 - Matriz UIO	Datos	20 Mbps	Fibra Óptica	Telconet
Zona Norte Bloque 43 - Matriz UIO	Datos Backup	20 Mbps	Radio Enlace	Telconet
Zona Oeste Bloque 7 Payamino	*Internet*	8 Mbps	Fibra Óptica	Telconet
Zona Oeste Bloque 7 - Matriz UIO	Datos	16 Mbps	Fibra Óptica	Telconet
Zona Oeste Bloque 7 - Matriz UIO	Datos Backup	16 Mbps	Radio Enlace	Telconet
Bloque 18 - Matriz UIO	Datos	4 Mbps	Fibra Óptica	Telconet
	Datos Backup	4 Mbps	Radio Enlace	Telconet
Bloque 21 - Matriz UIO	Datos	4 Mbps	Fibra Óptica	Telconet
	Datos Backup	4 Mbps	Radio Enlace	Telconet
Aeropuerto Tababela Terminal - Matriz UIO	Datos	2 Mbps	Fibra Óptica	CNT
	Datos Backup	2 Mbps	Fibra Óptica	CNT
Aeropuerto Tababela Hangar - Matriz UIO	Datos	4 Mbps	Fibra Óptica	CNT
	Datos Backup	4 Mbps	Fibra Óptica	CNT

Tabla 2.2 Características de los enlaces a nivel WAN por proveedor de la empresa petrolera

2.4.2 RED DE ÁREA LOCAL DE LA EMPRESA PETROLERA

La empresa petrolera tiene algunas sucursales y cada una su propia red LAN que se describirá a continuación:

2.4.2.1 Matriz

La matriz de la empresa petrolera se encuentra ubicada en la Av. Naciones Unidas y Av. De los Shyris, edificio Banco del Pacífico, pisos 4 y 5.

Este edificio es de 8 pisos pero la empresa utiliza los pisos 4 y 5. En el piso 5 se encuentra ubicado el "cuarto de comunicaciones" en donde se encuentran los servidores, los *switches* de núcleo, *switches* de distribución y acceso, los *access point*, *routers*, central telefónica, entre otros.

Para comunicarse entre los pisos se lo realiza mediante un *backbone* vertical de fibra óptica. La figura 2.7 muestra el diagrama de interconexión de los pisos de la matriz.

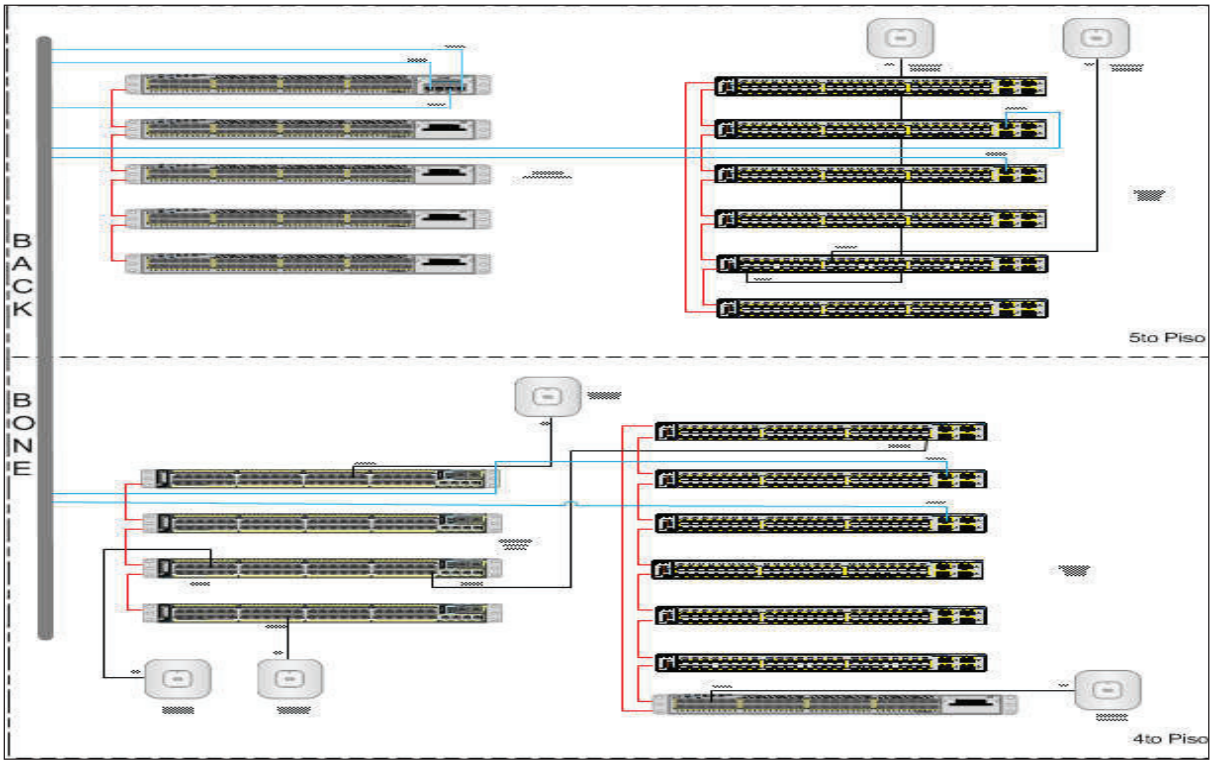

Figura 2.7 Diagrama de interconexión de la matriz de la empresa petrolera

La Tabla 2.3 indica los equipos de interconexión del piso cuarto y quinto de la matriz de la empresa petrolera.

MATRIZ	EQUIPO	CANTIDAD	MARCA	MODELO
PISO 4	*SWITCH*	7	CISCO	WS-C3750X-48P
	SWITCH	11	CISCO	WS-C3750X-48P-S
	ACCESS POINT	4	CISCO	AIR-LAP1131AG-A-K9
PISO 5	*SWITCH*	1	CISCO	WS-C2960-8TC-L
	SWITCH	13	CISCO	WS-C3750X-48P-S
	SWITCH	2	CISCO	WS-C3750X-48P-E
	WIRELESS CONTROLLER	1	CISCO	AIR-WLC4402-12-K9
	ACCESS POINT	4	CISCO	AIR-LAP1131AG-A-K9

Tabla 2.3 Equipos de interconexión de la matriz

2.4.2.1.1 Cuarto de Comunicaciones (Data Center)

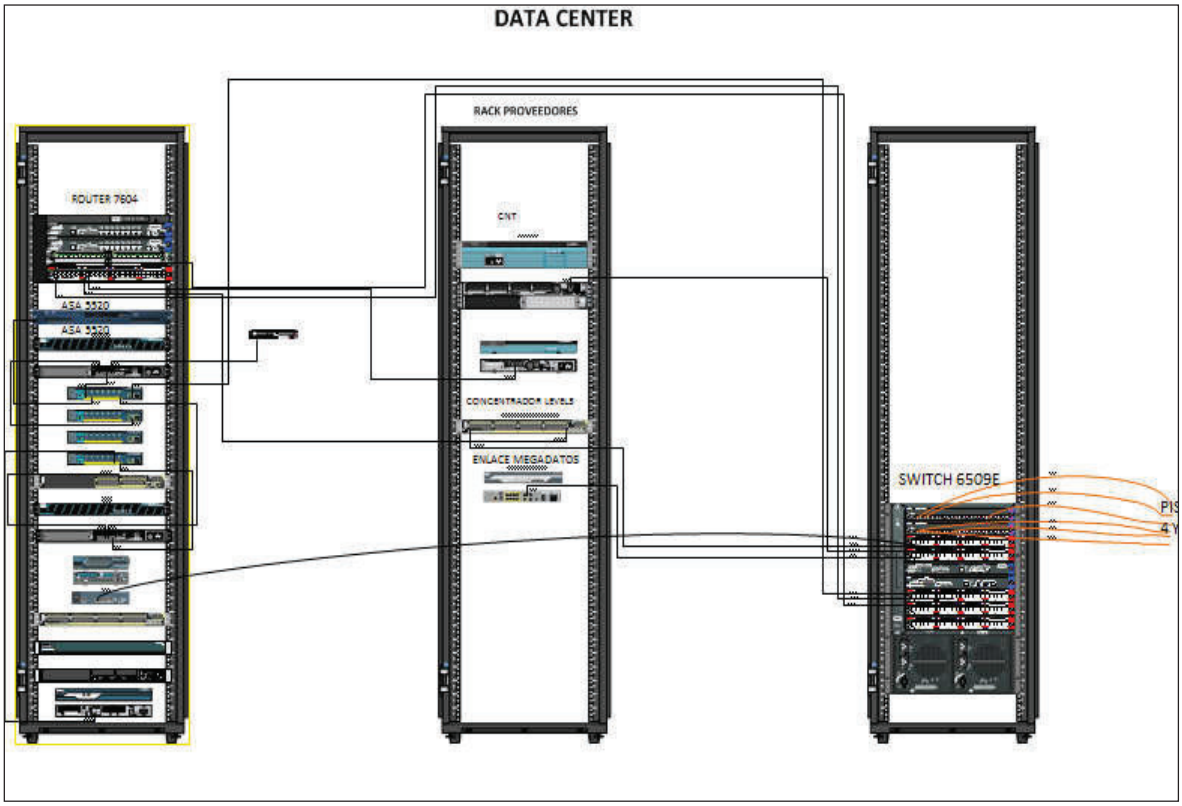

Figura 2.8 Diagrama físico del Data Center de la empresa petrolera

El cuarto de comunicaciones se encuentra en el piso quinto.

En este cuarto se encuentran los:

- Servidores
- *Access point*
- Equipos de los proveedores
- Central telefónica
- Todo lo que corresponde a equipos de comunicaciones

En la a Figura 2.8 se muestra el diagrama físico de interconexión del *Data Center* y en la tabla 2.4 se muestran los equipos de interconexión del cuarto de equipos.

MATRIZ	EQUIPO	CANTIDAD	MARCA	MODELO
DATA CENTER	*SWITCH*	5	CISCO	WS-C2960G-8TC-L
	SWITCH	2	CISCO	WS-C2960S-48LPS-L
	SWITCH	1	CISCO	WS-C2960S-24TS-S
	SWITCH CORE	1	CISCO	WS-C6509-E
	WIRELESS CONTROLLER	1	CISCO	AIR-CT2504-K9
	FIREWALL	1	CISCO	ASA5505
	FIREWALL	2	CISCO	ASA5520
	ROUTER	1	CISCO	7604

Tabla 2.4 Equipos de interconexión del cuarto de equipos

2.4.2.1.2 Servidores

Los servidores de la empresa petrolera se encuentran en el cuarto de comunicaciones del quinto piso de la matriz y algunos en cada campamento de la empresa.

Su detalle se presenta en el Anexo B1.1.

2.4.2.2 Zona Centro

Se compone de los bloques 12 y 15. Para comunicarse entre bloques se lo realiza mediante un *backbone* de fibra óptica y enlaces de radio.Bloque 12: Se compone de los campos Eden Yuturi (EPF) y Pañacocha. La Figura 2.9 muestra el diagrama de interconexión del bloque 12 del campamento EPF.

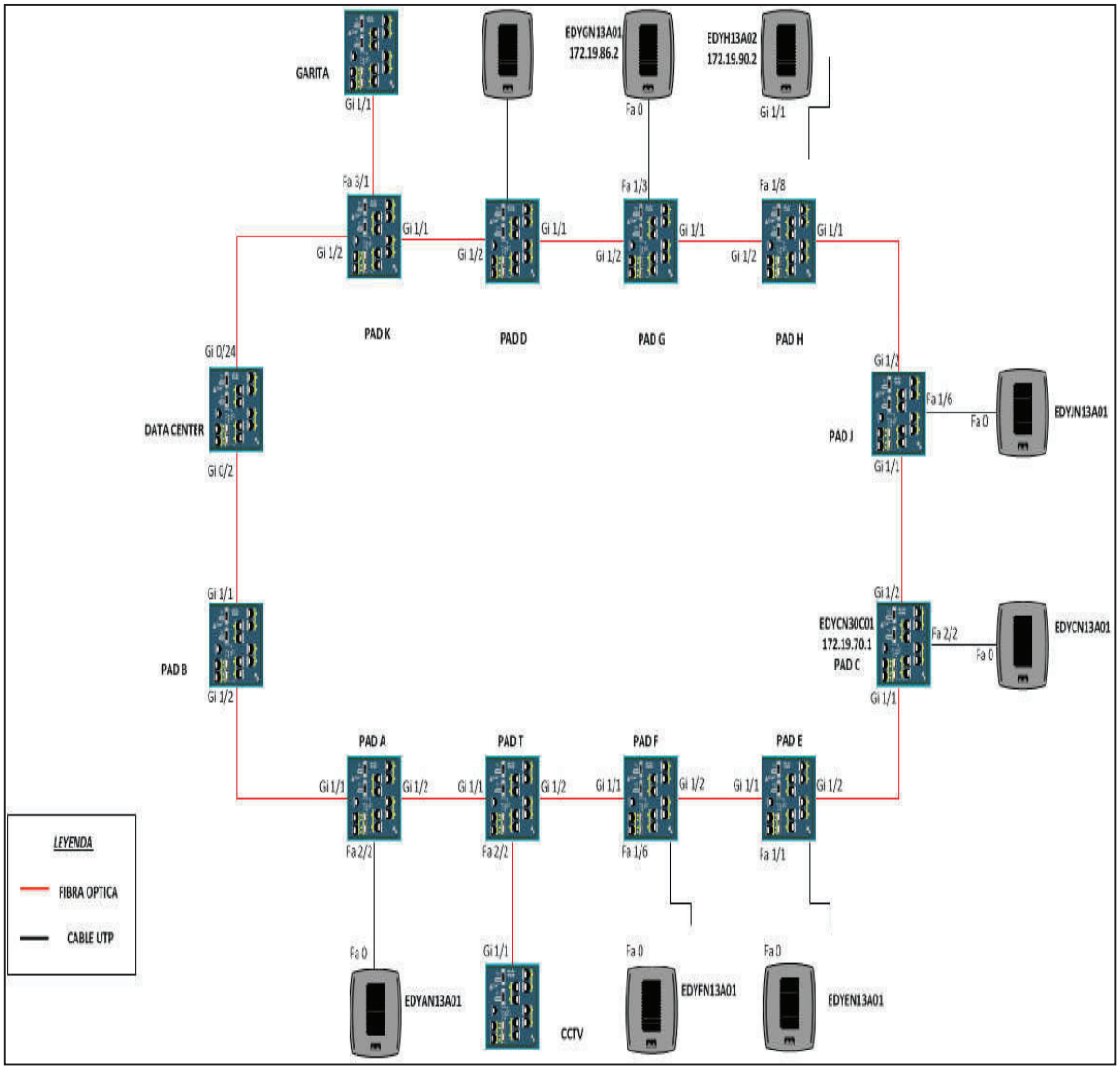

Figura 2.9 Diagrama de interconexión del campamento EPF bloque 12

La Tabla 2.5 muestra los equipos de interconexión del bloque 12 del campamento EPF.

EPF	EQUIPO	CANTIDAD	MARCA	MODELO
EPF	*SWITCH*	21	CISCO	WS-C2960G-8TC-L
	SWITCH	17	CISCO	WS-C3560G-24PS-S
	SWITCH	8	CISCO	WS-C3560G-48TS-S
	SWITCH	1	CISCO	WS-C2960S-48TS-L
	SWITCH	5	CISCO	WS-C2960S-24PS-L
	SWITCH	4	CISCO	WS-C3750G-48TS-S
	SWITCH	3	CISCO	WS-C3750G-24TS-E
	SWITCH CORE	1	CISCO	WS-C4510R+E
	ROUTER	2	CISCO	CISCO 2811
	ROUTER	1	CISCO	CISCO7604
	FIREWALL	2	CISCO	CISCO ASA 5510
	ACCESS POINT	20	CISCO	AIR-BR1310G-A-K9
	ACCESS POINT	6	CISCO	AIR-LAP1142N-A-K9
	WIRELESS CONTROLLER	1	CISCO	AIR-WLC4402-12-K9

Tabla 2.5 Equipos de interconexión del bloque 12 del campamento EPF

La Figura 2.10 muestra el diagrama de interconexión del bloque 12 (Pañacocha).

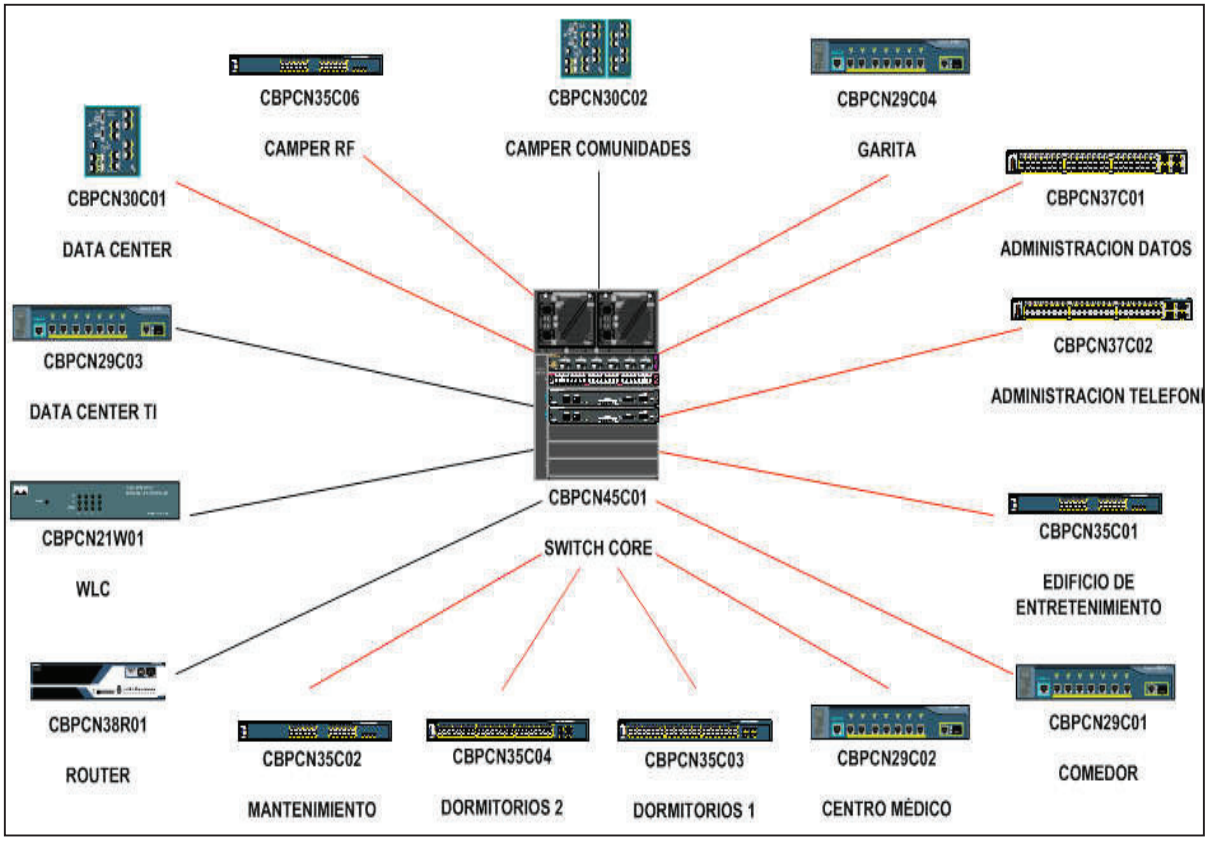

Figura 2.10 Diagrama de interconexión del campamento Pañacocha bloque 12

La Tabla 2.6 muestra los equipos de interconexión del bloque 12 (Pañacocha).

PAÑACOCHA	EQUIPO	CANTIDAD	MARCA	MODELO
PAÑACOCHA	*SWITCH*	5	CISCO	WS-C2960G-8TC-L
	SWITCH	1	CISCO	WS-C2950-24
	SWITCH	2	CISCO	WS-C3750G-48TS-S
	SWITCH	2	CISCO	WS-C3560G-48PS-S
	SWITCH	4	CISCO	WS-C3750G-24PS
	SWITCH CORE	1	CISCO	WS-C4507R-E
	ROUTER	1	CISCO	CISCO3825
	WIRELESS CONTROLLER	4	CISCO	AIR-WLC2106-K9
TI	*SWITCH*	2	CISCO	WS-C2960G-8TC-L
	SWITCH	1	CISCO	WS-2960S-48LPS-L
	WIRELESS CONTROLLER	1	CISCO	AIR-WLC4402-12-K9
	ROUTER	2	CISCO	CISCO2911/K9
	ACCESS POINT	3	CISCO	AIR-BR1310-A-K9

Tabla 2.6 Equipos de interconexión del bloque 12 del campamento Pañacocha

- Bloque 15: Se compone del campo CPF.

El detalle de los equipos de interconexión del bloque 15 del campamento CPF, se encuentra en el Anexo B1.2.

2.4.2.3 Zona Norte

Esta se subdivide en los:

- Bloque 43
- Bloque 63

Para comunicarse entre bloques se lo realiza mediante un *backbone* de fibra óptica y enlaces de radio. La figura 2.11 muestra el diagrama de interconexión del bloque 63 en el campamento Lago Agrio. Bloque 63: Se compone del campo Lago Agrio.

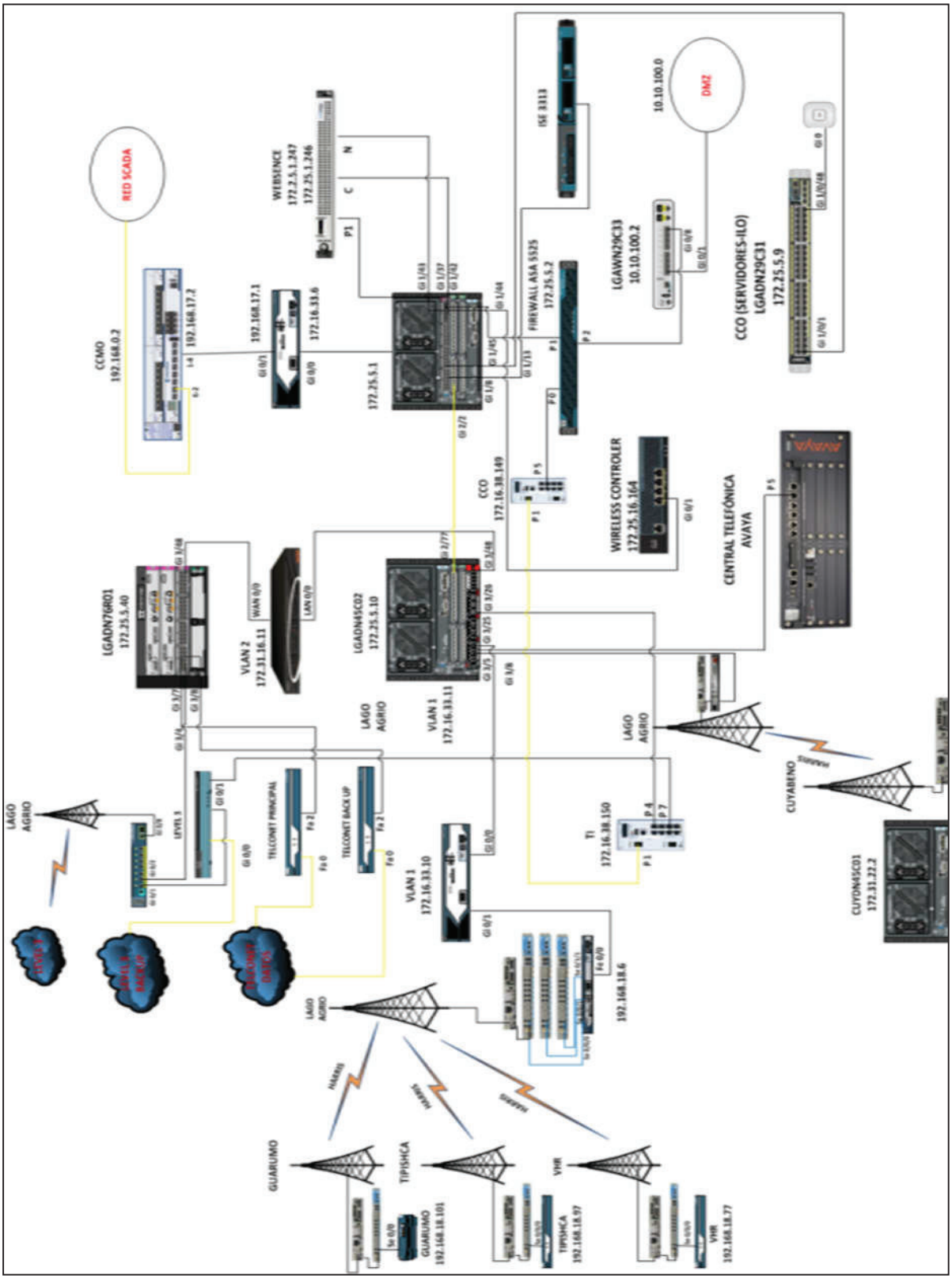

Figura 2.11 Diagrama de interconexión del campamento Lago Agrio bloque 63

La tabla 2.7 muestra los equipos de interconexión del Bloque 63 del campamento Lago Agrio.

BLOQUE 63	EQUIPO	CANTIDAD	MARCA	MODELO
CAMPAMENTO	*SWITCH*	2	CISCO	WS-C2960S-48LPS-L
	SWITCH	2	CISCO	WS-C2960S-24PS-L
	SWITCH	3	CISCO	WS-C2960G-8TC-L
	SWITCH CORE	1	CISCO	WS-C4510R+E
	WIRELESS CONTROLLER	1	CISCO	2504
	FIREWALL	1	CISCO	ASA 5525
	ACCESS POINT	1	CISCO	AIR-LAP1142N-A-K9
	ACCESS POINT	1	CISCO	AIR-CAP1552E-A-K9
	ACCESS POINT	1	CISCO	AIR-BR1310G-A-K9
GUANTA	*SWITCH*	1	CISCO	WS-C2960G-8TC-L
	SWITCH	1	CISCO	WS-C2960X-24TS-LL
	ACCESS POINT	1	CISCO	AIR-CAP1552E-A-K9
	ACCESS POINT	1	CISCO	AIR-BR1310G-A-K9

Tabla 2.7 Equipos de interconexión del bloque 63 del campamento Lago Agrio

El Bloque 43 se compone de los campos Libertador y Shushufindi. La Tabla 2.8 muestra los equipos de interconexión del bloque 43 del campamento Libertador. En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 43

LIBERTADOR	EQUIPO	CANTIDAD	MARCA	MODELO
GUARUMO	*SWITCH*	8	CISCO	WS-C2960CG-8TC-L
	SWITCH	7	CISCO	WS-C2960S-24PS-L
	SWITCH	3	CISCO	WS-C2950-12
	SWITCH	1	CISCO	WS-C2960S-48LPS-L
	SWITCH	3	CISCO	WS-C2950-24
	ROUTER	1	CISCO	CISCO 1751
	ROUTER	2	CISCO	CISCO 881
	ACCESS POINT	7	CISCO	AIR-BR1310G-A-K9-R
	ACCESS POINT	3	CISCO	AIR-LAP1142N-A-K9-R
	ACCESS POINT	2	CISCO	AIR-AP1231G-A-K9
	ACCESS POINT	4	CISCO	AIR-CAP1552E-A-K9
SECOYA	*SWITCH*	5	CISCO	WS-C2960CG-8TC-L
	SWITCH	1	CISCO	WS-C2950-12
	ACCESS POINT	6	CISCO	AIR-BR1310G-A-K9-R
	ACCESS POINT	1	CISCO	AIR-LAP1142N-A-K9

Tabla 2.8 Equipos de interconexión del bloque 43 del campamento Libertador

La Tabla 2.9 muestra los equipos de interconexión del bloque 43 del campamento Shushufindi.

BLOQUE 43 CAMPAMENTO SHUSHUFINDI				
SHUSHUFINDI	**EQUIPO**	**CANTIDAD**	**MARCA**	**MODELO**
BODEGA	*SWITCH*	1	CISCO	WS-C2960S-24PS-L
CAMPAMENTO	*SWITCH*	9	CISCO	WS-C2960S-24PS-L
	SWITCH	9	CISCO	WS-C2960G-8TC-L
	SWITCH	4	CISCO	WS-C2960S-48LPS-L
	SWITCH CORE	1	CISCO	WS-C4503-E
	SWITCH	3	CISCO	WS-C2950-12
	SWITCH	1	CISCO	WS-C3550-24PWR-SMI
	ROUTER	1	CISCO	1841
	ACCESS POINT	7	CISCO	AIR-CAP1552E-A-K9
	ACCESS POINT	3	CISCO	AIR-BR1310G-A-K9-R
SHUSHUFINDI NORTE	*SWITCH*	1	CISCO	WS-C2960G-8TC-L
	ACCESS POINT	2	CISCO	AIR-SAP1552E-A-K9

Tabla 2.9 Equipos de interconexión bloque 43 del campamento Shushufindi

2.4.2.4 Zona Oeste

Esta ubicada en la Provincia de Orellana y Napo del Oriente Ecuatoriano.

Esta se subdivide en los Bloques 7, 18 y 21,

Para comunicarse entre bloques se lo realiza mediante un *backbone* de fibra óptica y radio enlace.

- Bloque 7: Se compone del campo Payamino.

La Tabla 2.10 muestra los equipos de interconexión del bloque 7.

En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 7 de la empresa petrolera.

BLOQUE 7 CAMPAMENTO PAYAMINO				
PAYAMINO	**EQUIPO**	**CANTIDAD**	**MARCA**	**MODELO**
BODEGA COCA	*SWITCH*	2	CISCO	WS-C2960C-8TC-L
	SWITCH	2	CISCO	WS-C2960S-48LPS-L
	ROUTER	1	CISCO	CISCO2911/K9
	ROUTER	2	CISCO	CISCO1751
	ACCESS POINT	4	CISCO	AIR-BR1310G-A-K9
	ACCESS POINT	1	CISCO	AIR-LAP-1142N-A-K9
CAMPAMENTO	*SWITCH CORE*	1	CISCO	WS-C4510R
	SWITCH	7	CISCO	WS-C2960S-48LPS-L
	SWITCH	12	CISCO	WS-C2960-8TC-L
	SWITCH	2	CISCO	WS-C2960G-24TC-L
	SWITCH	1	CISCO	WS-C3750G-48TS-S
	SWITCH	1	CISCO	WS-C3560G-48PS-S
	SWITCH	1	CISCO	WS-C3560-8PC
	SWITCH	1	CISCO	WS-C3560G-24PS
	ROUTER	1	CISCO	CISCO7604
	ROUTER	4	CISCO	CISCO1841
	WIRELESS CONTROLLER	1	CISCO	AIR-WLC2106-K9
	FIREWALL	1	CISCO	ASA 5510
	ACCESS POINT	16	CISCO	AIR-BR1310G-A-K9
	ACCESS POINT	2	CISCO	AIR-LAP-1142N-A-K9
COCA	*SWITCH*	7	CISCO	WS-C2960G-8TC-L
	ROUTER	1	CISCO	CISCO2911/K9
	ACCESS POINT	9	CISCO	AIR-BR1310G-A-K9-R

Tabla 2.10 Equipos de interconexión del bloque 7 del campamento Payamino

- Bloque 18: Se compone del campo Palo Azul.

La Tabla 2.11 muestra los equipos de interconexión del bloque 18 del campamento Palo Azul.

En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 18 de la empresa petrolera.

BLOQUE 18 CAMPAMENTO PALO AZUL				
PALO AZUL	**EQUIPO**	**CANTIDAD**	**MARCA**	**MODELO**
AMAZONIA VIVA	*SWITCH*	3	CISCO	WS-C2960G-8TC-L
	SWITCH	2	CISCO	WS-C2960G-48TC-L
	SWITCH	1	CISCO	WS-C2950C-24
	ACCESS POINT	1	CISCO	AIR-LAP1142N-A-K9
	ACCESS POINT	1	CISCO	AIR-BR1310G-A-K9
PUCUNA	*SWITCH*	1	CISCO	WS-C2960G-8TC-L
	SWITCH	1	CISCO	WS-C3560-24P-S
	ROUTER	1	CISCO	CISCO2911/K9
RIO NAPO	*SWITCH*	1	CISCO	WS-C2960S-24PS-L
	ACCESS POINT	3	CISCO	AIR-BR1310G-A-K9
ZPF	*SWITCH*	8	CISCO	WS-2960G-8TC-L
	SWITCH	6	CISCO	WS-C3560-24PS-S
	SWITCH CORE	1	CISCO	WS-C4510R
	SWITCH	1	CISCO	WS-C2960S-48LPS-L
	SWITCH	2	CISCO	WS-C3560G-48PS-S
	SWITCH	2	CISCO	WS-C3750X-24P
	SWITCH	1	CISCO	WS-C3560-8PC-S
	SWITCH	1	CISCO	WS-C2950G-12-EI
	ROUTER	1	CISCO	3925
	WIRELESS CONTROLLER	1	CISCO	AIR-CT2504-K9
	ACCESS POINT	3	CISCO	AIR-BR1310G-A-K9-R
	ACCESS POINT	3	CISCO	AIR-LAP1142N-A-K9
	ACCESS POINT	1	CISCO	AIR-LAP1131AG-A-K9

Tabla 2.11 Equipos de interconexión del bloque 18 del campamento Palo Azul

- Bloque 21: Se compone del campo Yuralpa.

La Tabla 2.12 muestra los equipos de interconexión del Bloque 21 del campamento Yuralpa.

En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 21 de la empresa petrolera.

BLOQUE 21 CAMPAMENTO YURALPA				
YURALPA	**EQUIPO**	**CANTIDAD**	**MARCA**	**MODELO**
CAMPAMENTO	*SWITCH*	6	CISCO	WS-C2960G-8TC-L
	SWITCH	5	CISCO	WS-C2960G-24TC-L
	SWITCH	5	CISCO	WS-C2960S-48LPS-L
	SWITCH	4	CISCO	WS-C3560X-24P-S
	SWITCH	1	CISCO	WS-C3750G-48PS-S
	SWITCH	2	CISCO	WS-C3750X-24T-S
	SWITCH	1	CISCO	WS-C3560V2-24PS-S
	SWITCH	2	CISCO	WS-C3560-8PC-S
	SWITCH	1	CISCO	ME-3400G-12CS-A
	FIREWALL	2	CISCO	ASA 5510
	FIREWALL	1	CISCO	PIX 515E
	ROUTER	1	CISCO	CISCO 2811
	ROUTER	6	CISCO	2911/K9
	ROUTER	1	CISCO	CISCO 3825
	WIRELESS CONTROLLER	1	CISCO	AIR-WLC2106-K9
	ACCESS POINT	6	CISCO	AIR-LAP1142N-A-K9
	ACCESS POINT	10	CISCO	AIR-BR1310G-A-K9
	ACCESS POINT	2	CISCO	AIR-CAP1552E-A-K9
	ACCESS POINT	1	CISCO	AIR-SAP2602I-A-K9

Tabla 2.12 Equipos de interconexión del bloque 21 del campamento Yuralpa

2.4.2.5 Zona Este

- Bloque 31: Se compone del campo Chiru-isla.

La Tabla 2.13 muestra los equipos de interconexión del Bloque 31.

En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 31 de la empresa petrolera.

CHIRU-ISLA	EQUIPO	CANTIDAD	MARCA	MODELO
APAIKA	*SWITCH*	3	CISCO	WS-C2960G-8TC-L
	SWITCH	4	CISCO	WS-C2960S-24PS-L
	ROUTER	1	CISCO	CISCO3925
	ACCESS POINT	5	CISCO	AIR-BR1310G-A-K9
CHIRU-ISLA	*SWITCH*	6	CISCO	WS-C2960S-48LPS-L
	SWITCH CORE	1	CISCO	WS-C4507R+E
	SWITCH	8	CISCO	WS-C2960S-24PS-L
	SWITCH	6	CISCO	WS-C2960G-8TC-L
	SWITCH	2	CISCO	WS-C3560-24PS-S
	SWITCH	1	CISCO	WS-C2950G-12-EI
	SWITCH	1	CISCO	WS-C3750X-24S-E
	ROUTER	1	CISCO	CISCO2811
	ROUTER	1	CISCO	CISCO3925
	WIRELESS CONTROLLER	1	CISCO	AIR-CT2504-K9
	FIREWALL	2	CISCO	ASA5510
	ACCESS POINT	3	CISCO	AIR-BR1310G-A-K9-R
	ACCESS POINT	2	CISCO	AIR-LAP1142N-A-K9
ECB	*ROUTER*	1	CISCO	CISCO3925
	ACCESS POINT	1	CISCO	AIR-BR1310G-A-K9-R

Tabla 2.13 Equipos de interconexión del bloque 31

2.4.2.6 Zona del Litoral

Esta se subdivide en los bloques 1 (San Pablo) y 6. Para comunicarse entre bloques se lo realiza mediante un *backbone* de fibra óptica.La tabla 2.14 muestra los equipos de interconexión del bloque 1. En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 1 de la empresa petrolera.

LOCACIONES	EQUIPO	CANTIDAD	MARCA	MODELO
PACOA	*SWITCH*	1	CISCO	WS-C3750X-48P-S
	SWITCH	2	CISCO	WS-C2960CG-8TC-L
	ACCESS POINT	2	CISCO	AIR-SAP1552E-A-K9
	ACCESS POINT	1	CISCO	AIR-LAP1142N-A-K9

Tabla 2.14 Equipos de interconexión del bloque 1

- Bloque 6: Se compone del campo Amistad

La Tabla 2.15 muestra los equipos de interconexión del bloque 6. En el Anexo B1.3 se muestra el diagrama de interconexión del bloque 6.

LOCACIONES	EQUIPO	CANTIDAD	MARCA	MODELO
MACHALA	*SWITCH*	5	CISCO	WS-C2960S-48LPS-L
	SWITCH	8	CISCO	WS-C2960CG-8TC-L
	SWITCH	8	CISCO	WS-C2960S-24TS-L
	SWITCH	3	CISCO	WS-C3750X-24P-L
	SWITCH	2	CISCO	WS-C3750X-48P-S
	SWITCH	1	CISCO	WS-C3560X-24P-L
	ACCESS POINT	6	CISCO	AIR SAP1552E-A-K9
	ACCESS POINT	2	CISCO	AIR LAP1142N-A-K9
	ACCESS POINT	3	CISCO	AIR-CAP2602I-A-K9

Tabla 2.15 Equipos de interconexión del bloque 6

2.5 DESCRIPCIÓN DE LOS DEPARTAMENTOS DE LA EMPRESA PETROLERA

La empresa petrolera se encuentra en constante crecimiento y evolución. Los responsables de su correcto funcionamiento son sus empleados que pertenecen a departamentos o áreas, dependiendo de la función que desempeñan. La empresa se divide en las siguientes áreas:

- Gerencia
- *Staff* de Gerencia
- Proyectos Especiales
- Soporte Técnico y Operativo
- Soporte y Servicios Corporativos
- Exploración
- Desarrollo
- Operaciones
- *Offshore*

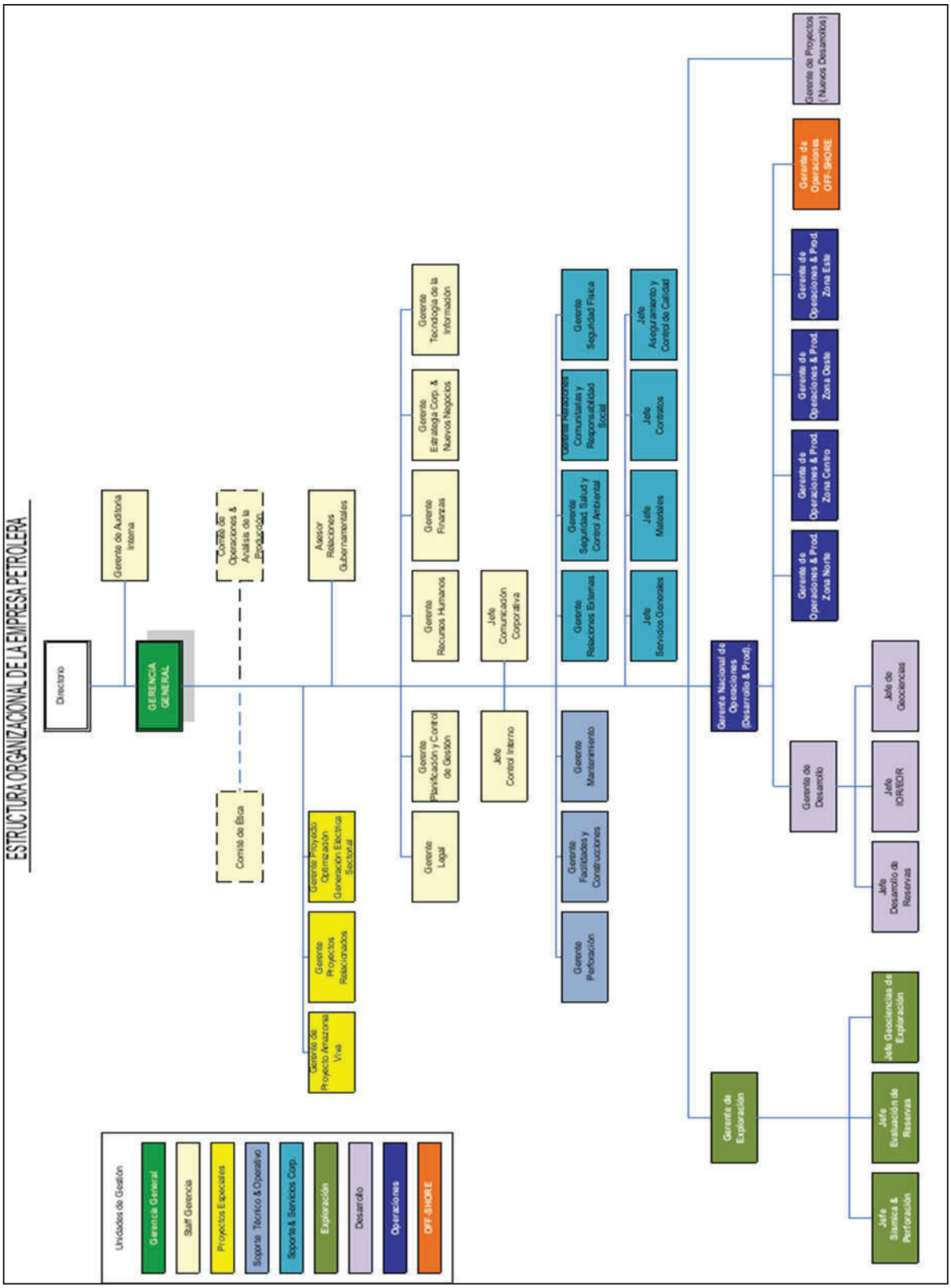

Figura 2.12 Estructura organizacional de la empresa petrolera

En la Figura 2.12 se muestra el diagrama de la estructura organizacional de la empresa petrolera elaborado en base a los departamentos con los que cuenta la empresa, es de tipo jerárquico, lo que permite ver las estructuras de la empresa y como están organizados.

2.5.1 DISTRIBUCIÓN DEPARTAMENTAL DE LA EMPRESA PETROLERA

La empresa petrolera tiene la siguiente distribución departamental en cada una de sus sucursales.

2.5.1.1 Matriz

La Tabla 2.16 muestra la distribución departamental de la matriz.

MATRIZ	
ÁREA DE TRABAJO	**CANTIDAD USUARIOS**
COMUNICACIÓN CORPORATIVA	8
CONTRATISTAS	45
CONTRATOS	20
DESARROLLO	2
EXPLORACIÓN	25
GERENCIA GENERAL	3
GERENCIA NACIONAL DE OPERACIONES	77
LEGAL	20
OPERACIONES	116
RELACIONES EXTERNAS	8
SEGURIDAD FÍSICA	53
TECNOLOGÍA DE LA INFORMACIÓN	40
TOTAL	**417**

Tabla 2.16 Cantidad de usuarios en la matriz

2.5.1.2 Zona Centro

Este se subdivide en los bloques 12 y 15. En el Anexo B2 (Digital) se indica la cantidad de usuarios de la zona centro.

2.5.1.3 Zona Norte

Este se subdivide en los bloques 43 y 63. En el Anexo B3 se indica la distribución departamental de los bloques de la zona norte.

2.5.1.4 Zona Oeste

Este se subdivide en los bloques 7, 18 y 21. En el Anexo B4 se indica la distribución departamental de los bloques de la zona oeste.

2.5.1.5 Zona Este

Este se compone del bloque 31. En el Anexo B5 se indica la distribución departamental del bloque de la zona este.

2.5.1.6 Zona del Litoral

Este se subdivide en los bloques 1 y 6.

En el Anexo B6 se indica la distribución departamental de los bloques de la zona litoral.

2.5.2 RECURSOS DE LA EMPRESA

Las empresas necesitan de equipos para conformar la red interna y para las conexiones entre sucursales.

Los equipos deben ser los adecuados para que el personal realice de una manera más eficiente las funciones que son asignadas a cada uno de ellos.

Para este caso es necesario realizar un análisis de requerimientos.

La empresa petrolera para el desarrollo de sus actividades y cumpliendo con las necesidades de la empresa, cuenta con los equipos de red que se detallan en las siguientes tablas:

2.5.2.1 Matriz

La tabla 2.17 muestra la cantidad de equipos de la matriz.

EQUIPOS MATRIZ	
EQUIPO	**CANTIDAD**
DESKTOP	10
LAPTOP	300
SPARE	50
SERVIDORES VIRTUALES	50
WORKSTATION	80
ESPECIALES AUTOMATIZACIÓN	0
CONTRATISTAS	40
TOTAL	**530**

Tabla 2.17 Cantidad de equipos en la matriz

2.5.2.2 Zona Centro

Este se subdivide en los bloques 12 y 15. En el Anexo B7 se indican los equipos de los bloques de la zona centro.

2.5.2.3 Zona Norte

Este se subdivide en los bloques 43 y 63. En el Anexo B8 se indican los equipos de los bloques de la zona norte.

2.5.2.4 Zona Oeste

Este se subdivide en los bloques 7, 18 y 21. En el Anexo B9 se indican los equipos de los bloques de la zona oeste.

2.5.2.5 Zona Este

Este se compone del bloque 31. En el Anexo B.10 se indican los equipos del bloque de la zona este.

2.5.2.6 Zona del Litoral

Este se subdivide en bloques 1 y 6. En el Anexo B.11 se indican los equipos de los bloques de la zona litoral.

2.6 ANÁLISIS DE TRÁFICO DE LA RED DE LA EMPRESA PETROLERA

En esta sección se realiza el análisis de tráfico entrante y saliente, para la verificación del porcentaje de uso de las capacidades en los enlaces de datos, acceso a *Internet* y las capacidades de las interfaces de los equipos de conectividad de la red de la empresa.

2.6.1 TRÁFICO DE LA RED

Para analizar el tráfico que circula por la red se realiza la instalación del programa PRTG *Network Monitor* (*Paessler Router Traffic Grapher*) con la versión 15.3.20.4114, que será el encargado de la captura de tráfico.

2.6.1.1 Matriz

El realiza el monitoreo del tráfico WAN y LAN (se analiza el tráfico que fluye desde la matriz a otros bloques y el generado dentro de la matriz de la empresa petrolera).

2.6.1.1.1 Tráfico WAN

La matriz de la empresa posee dos enlaces hacia el *Internet* en modo activo - activo.

- Un enlace principal y uno de respaldo

El enlace principal de la matriz tiene una capacidad de 20 Mbps contratado con CNT (Corporación Nacional de Telecomunicaciones).

La figura 2.13 muestra el tráfico total del enlace de *Internet* principal de la matriz, comprendido entre el 1 de enero y 30 de enero del 2016, cuyo valor máximo es 14959 Kbps.

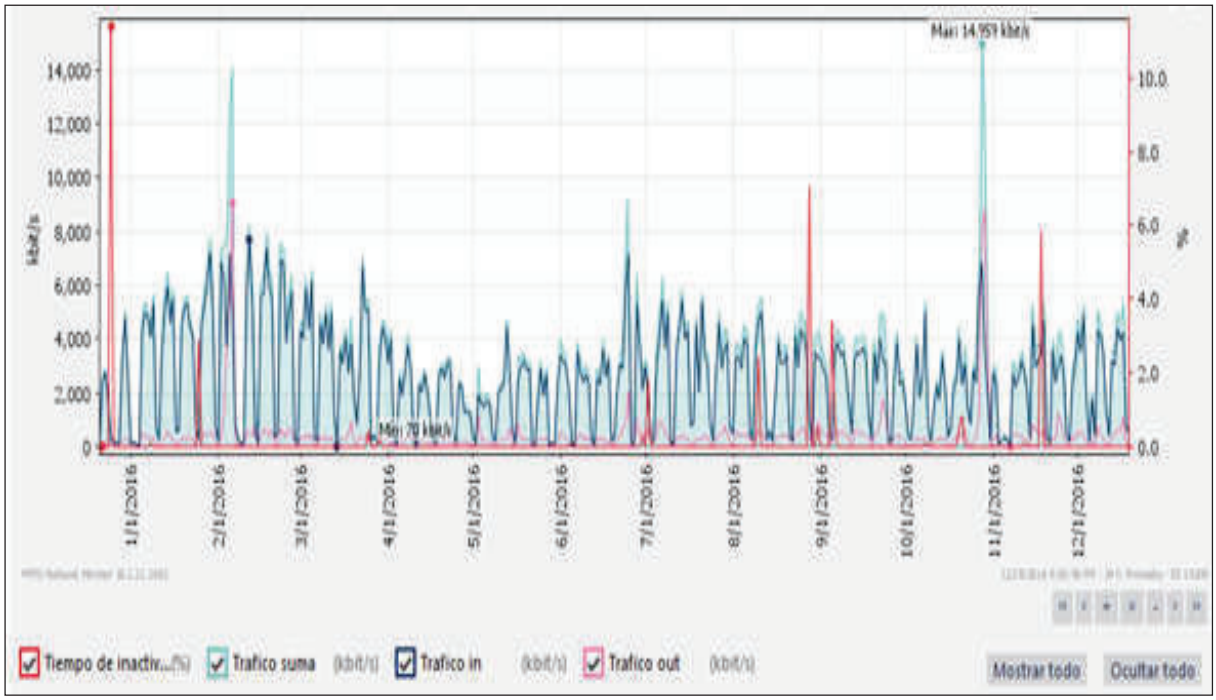

Figura 2.13 Monitoreo de la matriz del enlace de *Internet* principal de CNT

- El valor máximo aproximado es 14959 Kbps, por tanto el porcentaje de uso máximo es el 74,80%.

$$\frac{14959\ \text{Kbps}*100\%}{20000\ \text{Kbps}} = 74{,}80\%$$

- El valor mínimo de uso aproximado es 70 Kbps,

$$\frac{14959\ Kbps + 70\ \text{Kbps}}{2} = 7514{,}5\ \text{K}bps$$

- El valor promedio es 3785 Kbps, por tanto el porcentaje de uso es el 37,57 %.

$$\frac{7514{,}5\ \text{Kbps} * 100\%}{20000\ \text{Kbps}} = 37{,}57\ \%$$

Con los resultados anteriormente presentados podemos observar que no existe congestión en el enlace principal WAN contratado, el porcentaje de uso promedio es menor al 50%. Por tanto, no es necesario solicitar capacidad adicional al proveedor de *Internet*.

El enlace de respaldo de la matriz tiene una capacidad de 12 Mbps contratado con Telconet.

La Figura 2.14 representa el tráfico total de consumo del enlace de respaldo de *Internet* de la matriz, comprendido entre el 1 de enero y 30 de enero del 2016.

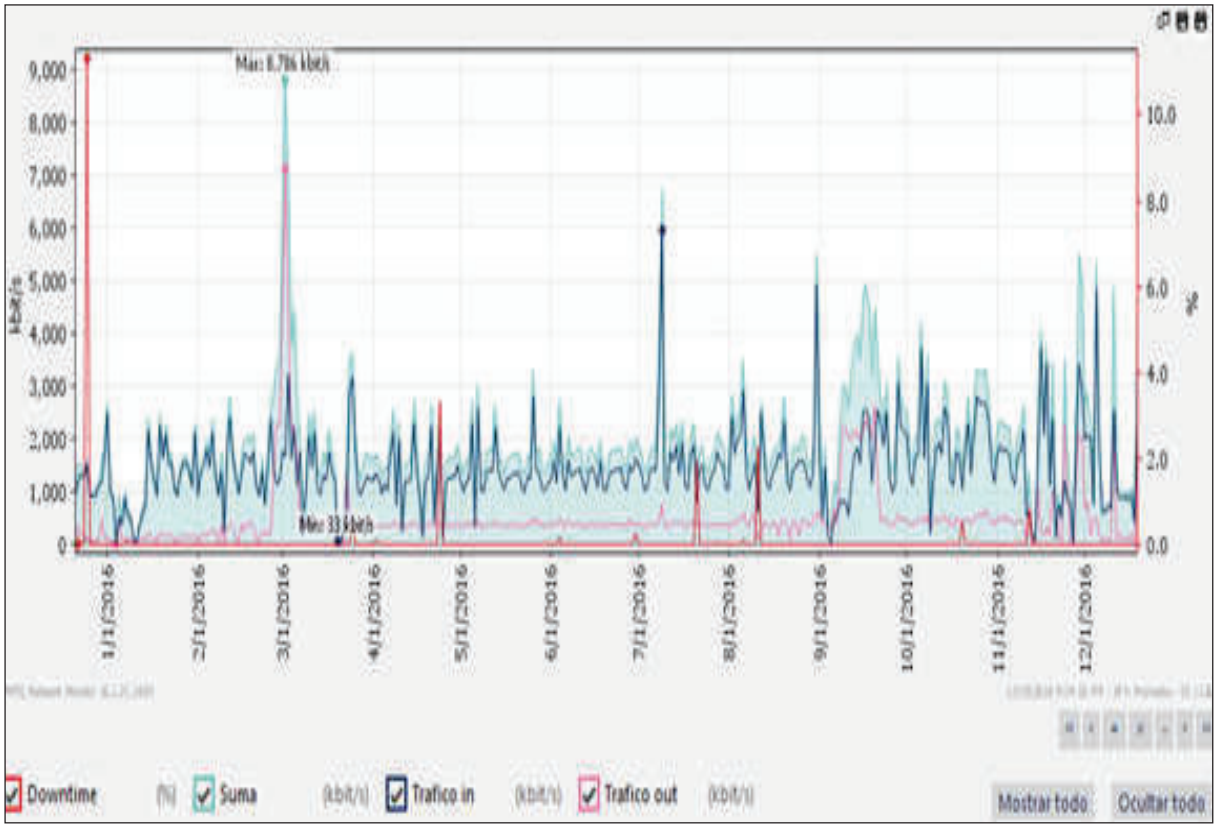

Figura 2.14 Monitoreo de la matriz del enlace de respaldo *Internet* de Telconet

- Valor máximo aproximado es 8786 Kbps, por tanto el porcentaje de uso es el 23,65%.

$$\frac{8786\ \text{Kbps}*100\%}{12000\ \text{Kbps}} = 73{,}22\%$$

- Valor mínimo aproximado es 33 Kbps,

$$\frac{8786\ Kbps + 33\ \text{Kbps}}{2} = 4409{,}5\ \text{K}bps$$

- El valor promedio es 3785 Kbps, por tanto el porcentaje de uso es el 36,75%.

$$\frac{4409{,}5\ \text{Kbps} * 100\%}{12000\ \text{Kbps}} = \ 36{,}75\%$$

Con los resultados anteriormente presentados podemos observar que no existe congestión en el enlace de respaldo WAN contratado, el porcentaje de uso es menor al 50%.

Como podemos observar existe tráfico circundante en el enlace de respaldo (configurado en modo activo), porque se utiliza con frecuencia exclusivamente para la descarga de actualizaciones, parches para los servidores y las estaciones de trabajo de la empresa ya que el sistema operativo principal es Microsoft *Windows Server* para los servidores, Microsoft *Windows* 7 *Professional* y actualizaciones del *antivirus* corporativo *Kaspersky*.

En caso que el enlace principal falle el de respaldo será el encargado de proporcionar acceso a *Internet* a la matriz de la empresa y otras tareas adicionales del enlace de respaldo serán postergadas.

2.6.1.1.2 Tráfico LAN

En esta sección se analiza el consumo de ancho de banda en la infraestructura interna (red LAN) de la matriz, utilizado por los principales servicios de red de la empresa, para verificar disponibilidad para incluir tráfico adicional requerido para el funcionamiento de Cisco ISE, sin afectar el correcto funcionamiento de la red evitando congestión que degrade la operación normal.

A continuación se presenta el análisis por cada servicio principal de la red de la empresa.

En la Figura 2.15 se muestra el tráfico generado en el Controlador de Dominio *Root* AD, servidor DNS, DHCP del 20 de noviembre al 20 de diciembre del 2016, cuyo valor máximo aproximado es 800 Kbps mientras que valor mínimo aproximado es 150 Kbps, dando como resultado un valor promedio de 475 Kbps.

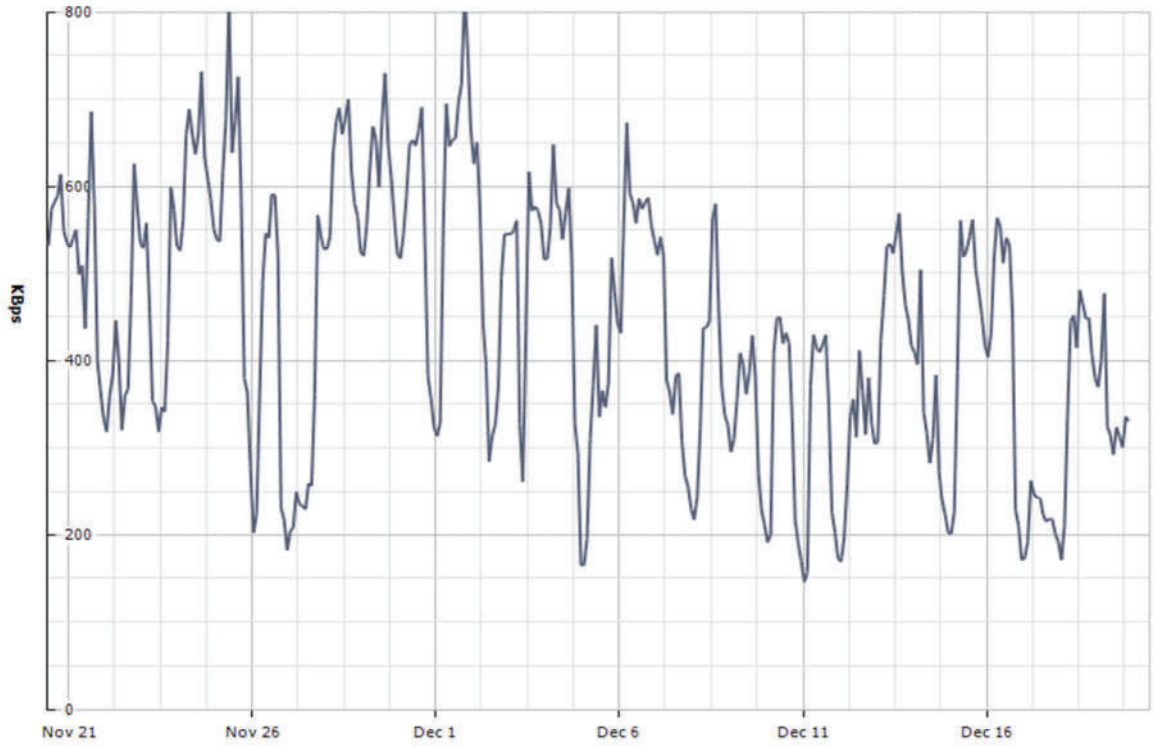

Figura 2.15 Tráfico generado en el Controlador de dominio AD *Root* de la matriz de la empresa petrolera

- Valor máximo aproximado es 800 Kbps
- Valor mínimo aproximado es 150 Kbps

$$\frac{\mathbf{800\ Kbps + 150\ Kbps}}{\mathbf{2}} = \mathbf{475\ Kbps}$$

Para el análisis del porcentaje de uso de las interfaces troncales se considera que las capacidades de los enlaces troncales entre las capas de distribución y acceso son de 2GBbps por cada enlace lógico (configurando *EtherChannel* con 2 interfaces físicas

GigabitEthernet para proporcionar redundancia y aumento en capacidad por puerto) pero el uso efectivo por puerto lógico es el 80% de sus capacidades teóricas. (2000000 Kbps*0,80=1600000 Kbps)

- El valor promedio es: 475 Kbps, por tanto el porcentaje de uso es el 0,03%.

$$\frac{475\ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = 0{,}03\%$$

En la Figura 2.16 se muestra el tráfico generado en el Controlador de Dominio *Child* AD entre 20 de noviembre al 20 de diciembre del 2016, donde el:

- Valor máximo aproximado es 4000 Kbps
- Valor mínimo aproximado es 490 Kbps,

$$\frac{4000\ Kbps + 490\ \text{Kbps}}{2} = 2245\ \text{K}bps$$

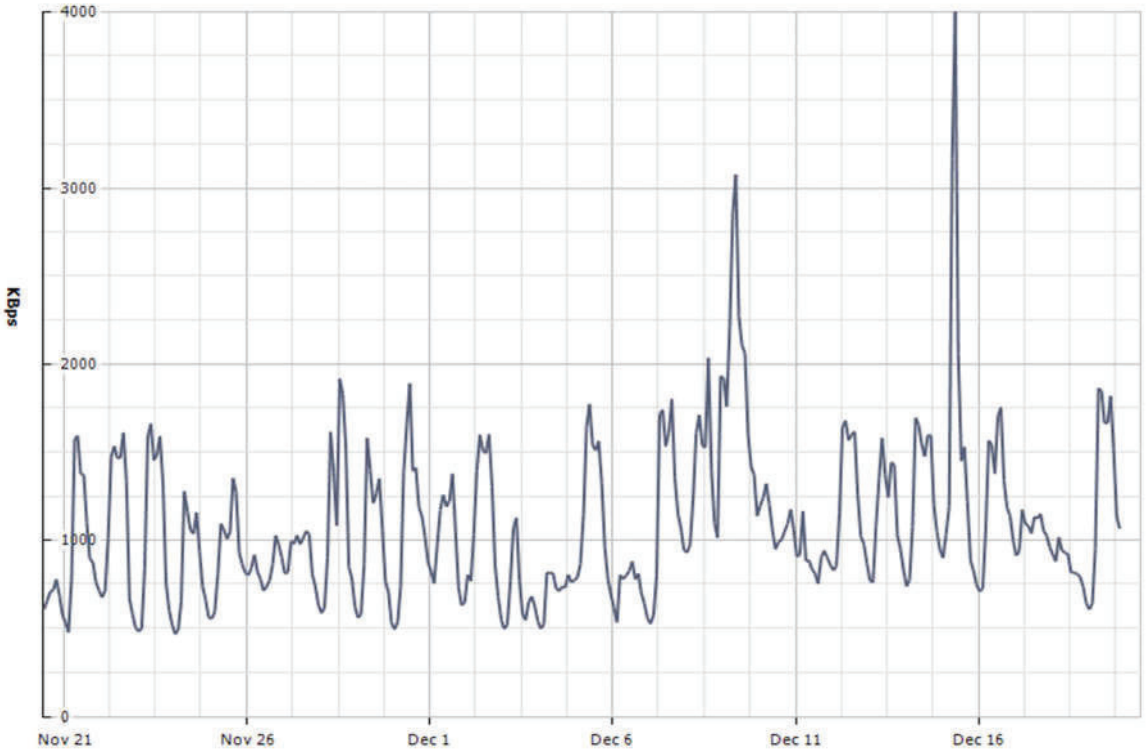

Figura 2.16 Tráfico generado en Controlador de dominio AD *Child* de la matriz de la empresa petrolera

- El valor promedio es 2245 Kbps., por tanto el porcentaje de uso es el 0,14%.

$$\frac{2245\ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = 0{,}14\%$$

Por los resultados presentados anteriormente, el tráfico de red circundante relacionado con el Controlador de dominio principal (*root*) y secundario (*child*), no satura el enlace disponible efectivo de 1600000, el porcentaje de uso es menor al 10%.

En la Figura 2.17 se muestra el tráfico generado en el Servidor Exchange CAS del 20 de noviembre al 20 de diciembre de 2016, cuyo valor máximo aproximado es 5000 Kbps, valor mínimo es 468,75 Kbps, obteniendo un valor promedio de 2734,25 kbps.

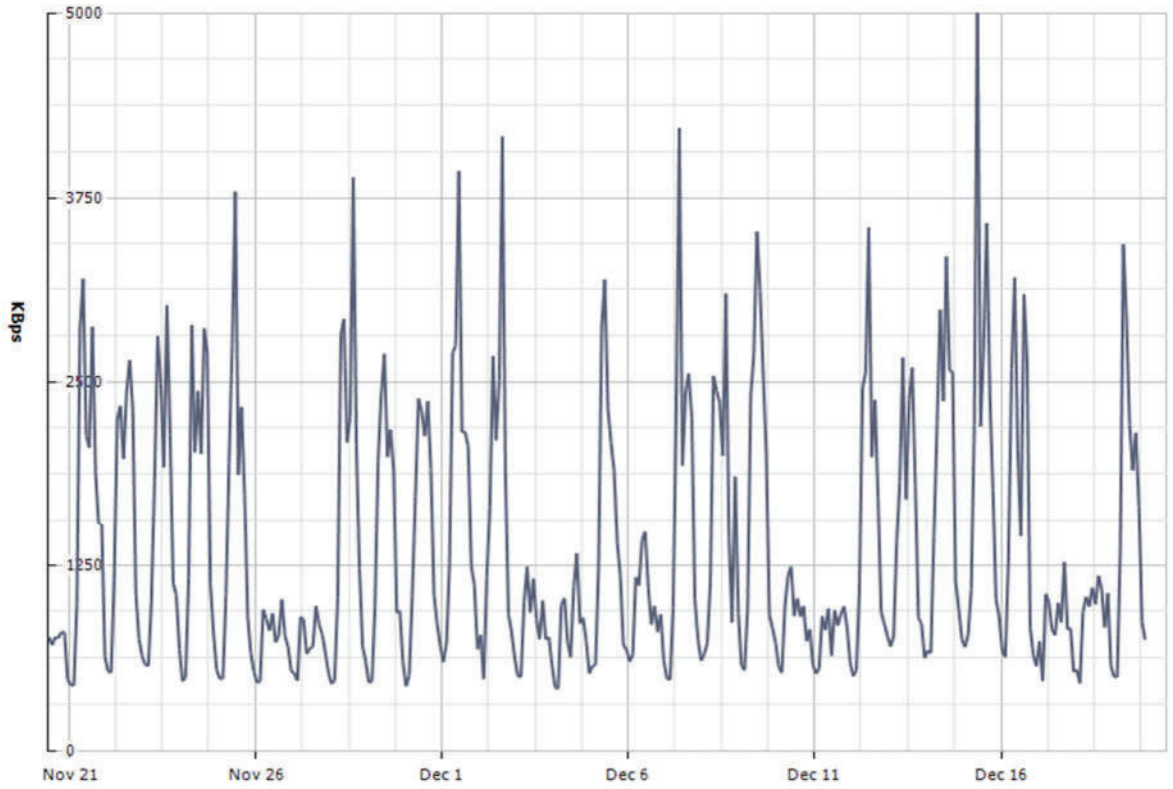

Figura 2.17 Tráfico generado en el servidor *Exchange* CAS de la matriz de la empresa petrolera

- El valor promedio es 2734,25 Kbps., por tanto el porcentaje de uso es el 0,17%.

$$\frac{2734{,}25\ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = 0{,}17\%$$

En la Figura 2.18 se muestra el tráfico generado en el Servidor *Exchange* EDGE, del 20 de noviembre al 20 de diciembre del 2016, cuyo valor máximo aproximado es 13750 Kbps y valor mínimo aproximado es 1250 Kbps, obteniendo un promedio de 7500 Kbps.

- Valor máximo aproximado es 13750 Kbps
- Valor mínimo aproximado es 1250 Kbps,

$$\frac{13750\ Kbps + 1250\ \text{Kbps}}{2} = 7500\ \text{K}bps$$

- El valor promedio es 7500 Kbps., por tanto el porcentaje de uso es el 0,47%.

$$\frac{7500\ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = 0{,}47\%$$

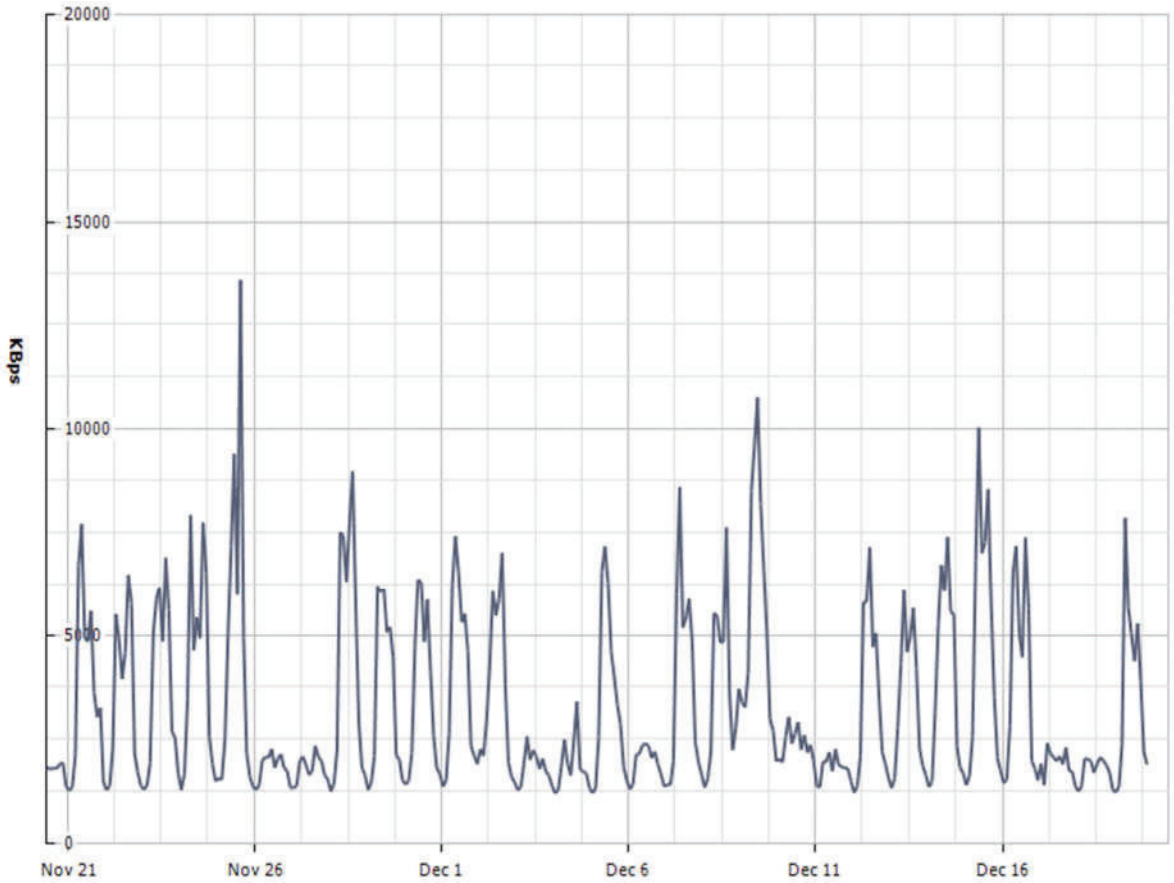

Figura 2.18 Tráfico generado en el servidor Exchange EDGE

En la Figura 2.19 se muestra el tráfico generado en el Servidor FTP comprendido entre el 20 de noviembre y 20 de diciembre del 2016.

- Valor máximo aproximado es 29062,5 Kbps
- Valor mínimo aproximado es 1200 Kbps,

$$\frac{29062{,}5\ Kbps + 1200\ \text{Kbps}}{2} = 15131{,}25\ \text{K}bps$$

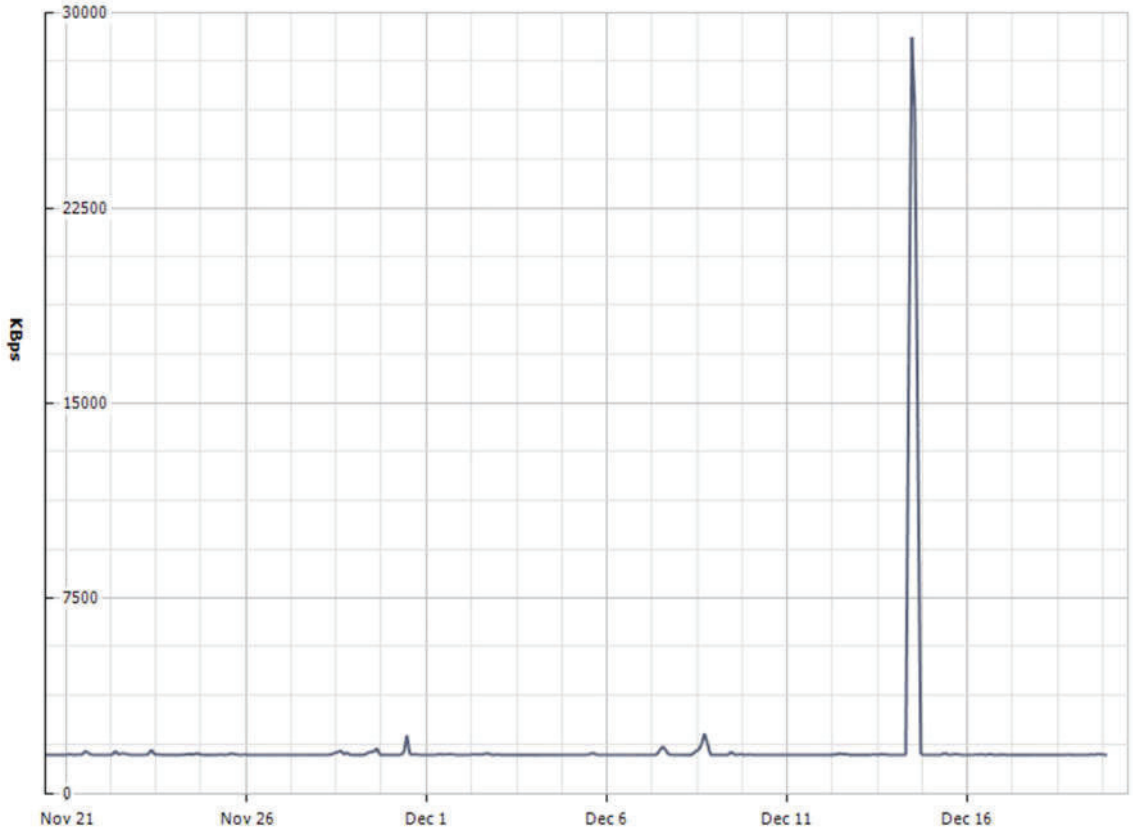

Figura 2.19 Tráfico generado en el servidor FTP de la matriz de la empresa petrolera

- El valor promedio es 2734,25 Kbps., por tanto el porcentaje de uso es el 0,95%.

$$\frac{15131{,}25\ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = 0{,}95\%$$

En la Figura 2.20 se observa el tráfico generado en el servidor *WEB* comprendido entre el 20 de noviembre y 20 de diciembre del 2016, cuyo valor máximo aproximado es

885,93 Kbps y valor mínimo aproximado es 75 Kbps, obteniendo un promedio de 480,47 Kbps.

- Valor máximo aproximado es 885,94 Kbps
- Valor mínimo aproximado es 75 Kbps,

$$\frac{885{,}94\ \ Kbps + 75\ \text{Kbps}}{2} = 480{,}47\ \text{K}bps$$

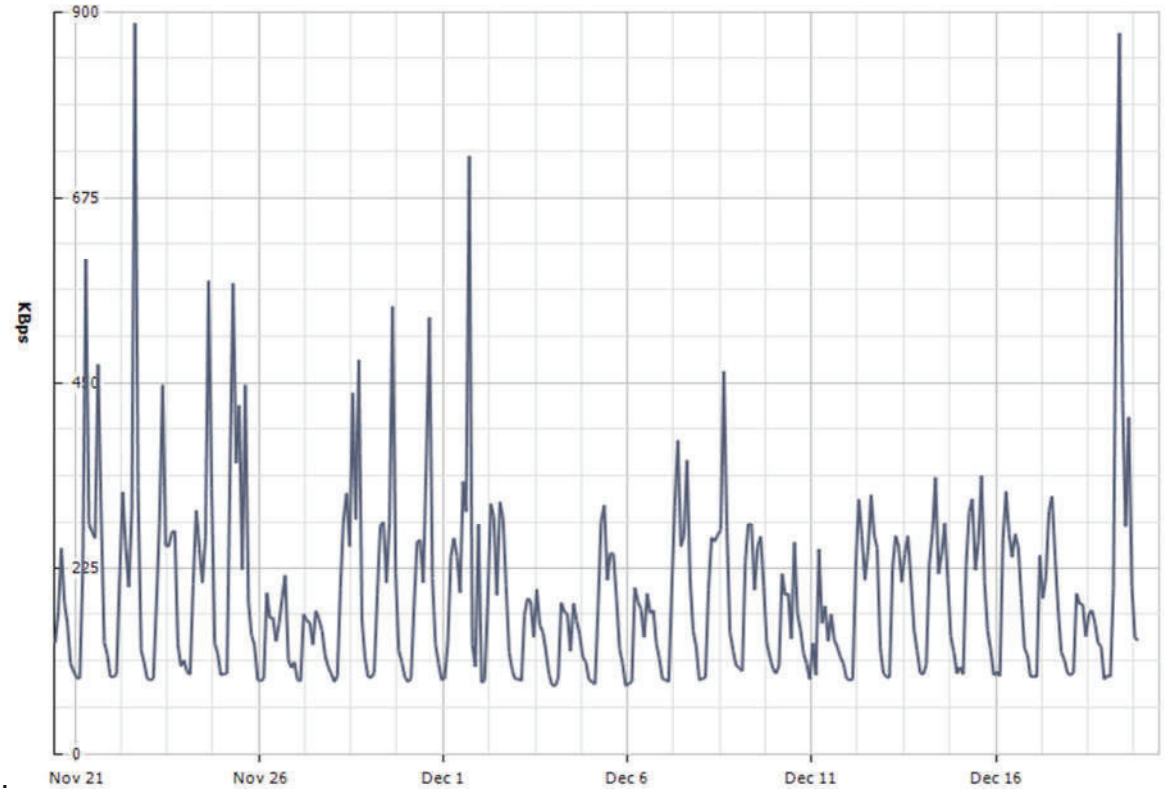

Figura 2.20 Tráfico generado en el servidor FTP de la matriz de la empresa petrolera

- El valor promedio es 2734,25 Kbps., por tanto el porcentaje de uso es el 0,18%.

$$\frac{480{,}47\ \ \text{Kbps} * 100\%}{1600000\ \text{Kbps}} = \ 0{,}18\%$$

Una vez analizadas las figuras de la captura del tráfico total entrante y saliente en los servidores conectados a un *switch* Cisco *Catalyst* 6500 (interfaces *GigabitEthernet*) ubicado en el *Datacenter* de la matriz obtenidas a través del *software* PRTG, se realiza

los cálculos respectivos de los valores de uso promedio y porcentaje de uso total de los enlaces troncales configurados con *Etherchannel* con capacidades teóricas de 2Gbps (la capacidad efectiva es 1600000) de los *switches* de la capa de distribución y acceso. En la Tabla 2.18, se observan los resultados del análisis de tráfico, donde podemos verificar que no existe congestión en la red actual, aun con tráfico adicional generado por el ISE.

MODELO	SERVICIO	VELOCIDAD DE LA TARJETA DE RED [Kbps]	VELOCIDAD MÁXIMA [Kbps]	VELOCIDAD MÍNIMA [Kbps]	VELOCIDAD PROMEDIO [Kbps]	PORCENTAJE DE USO [%] EN FUNCIÓN DE LA VELOCIDAD MÁXIMA (PEOR CASO)
ProLiant BL 460c G1	Servidor Exchange 2007 CAS - HUB	1000000	800,00	150	475,00	0,10
ProLiant DL360 G5	Servidor Exchange 2007 Edge	1000000	4000,00	490	2245,00	0,5
ProLiant BL 460c G1	Domain Controller Child	1000000	5000,00	468,75	2734,25	0,625
ProLiant BL 460c G1	Domain Controller Root, DNS, DHCP	1000000	13750	1250	7500	1,72
ProLiant BL 460c G1	Servidor FTP	1000000	29062,50	1200	15131,25	3,63
ProLiant BL 460c G1	Servidor WEB	1000000	885,94	75	480,47	0,11
ProLiant DL360 G5	Servidor NTP	1000000	3750,00	430	2090,00	0,47
ProLiant BL 460c G1	ISE (ADMIN, PSN, MON)	1000000	4009,00	1319	2664,00	0,50
		TOTAL	61257,44	5382,75	33319,97	7,66

Tabla 2.18 Análisis de tráfico LAN en la matriz de la empresa petrolera

La Tabla 2.19 muestra el porcentaje de utilización total de la capacidad de los enlaces troncales que interconectan la capa de distribución con la capa de acceso, Aún con la inclusión de la solución tecnológica Cisco ISE no se afecta la operación normal y no existe congestión en la red de la empresa. Cabe destacar que se realiza el análisis de tráfico considerando la inclusión de la configuración de *Etherchannels* en la topología de red de la empresa, que serán parte de la recomendación del presente proyecto. Sin la existencia de *Etherchanne*l el porcentaje de uso total de los enlaces troncales es del 7,66% (cuando la capacidad efectiva de los enlaces troncales es de 800000 Kbps).

CAPACIDAD REQUERIDA POR PUERTO TRONCAL [Kbps]	CAPACIDAD TEÓRICA POR ENLACE TRONCAL [Kbps]	CAPACIDAD EFECTIVA POR ENLACE TRONCAL [Kbps]	PORCENTAJE DE USO [%]
61257,44	2000000	1600000	3,83

Tabla 2.19 Uso total de las capacidades de los enlaces troncales de la matriz de la empresa petrolera

2.6.1.2 Zona Centro

En el Anexo B12 se muestra el tráfico total de consumo de los enlaces de datos, *Internet* e interno de los servicios locales de los bloques de la zona centro.

2.6.1.3 Zona Norte

En el Anexo B13 se muestra el tráfico total de consumo de los enlaces de datos, *Internet* e interno de los servicios locales de los bloques de la zona norte.

2.6.1.4 Zona Oeste

En el Anexo B14 se muestra el tráfico total de consumo de los enlaces de datos, *Internet* e interno de los servicios locales de los bloques de la zona oeste.

2.6.1.5 Zona Este

En el Anexo B15 se muestra el tráfico total de consumo de los enlaces de datos, *Internet* e interno de los servicios locales de los bloques de la zona este.

2.6.1.6 Zona del Litoral

En el Anexo B16 se muestra el tráfico total de consumo de los enlaces de datos, *Internet* de la zona litoral e interno de los servicios locales de los bloques de la Zona del Litoral.

2.7 LIMITANTES DEL SISTEMA DE AUTENTICACIÓN ACTUAL

Actualmente la empresa petrolera cuenta con un sistema de autenticación ACS de Cisco, que tiene las siguientes limitantes:

- Valida únicamente usuario y *hostname* / (802.1x)
- No valida el estado de salud del dispositivo
- No permite un adecuado control para el acceso de dispositivos BYOD
- No cubre las necesidades de crecimiento
- No automatiza las tareas de acceso ni facilita la operación / configuración de la red

2.7.1 POLÍTICAS DE SEGURIDAD DE RED DE LA EMPRESA PETROLERA

La empresa proporciona servicios a sus usuarios corporativos, invitados, entre otros; por tanto, es requirente implementar mecanismos de seguridad avanzados para control de usuarios y sus perfiles de autorización, pero principalmente políticas de seguridad restrictivas.

En esta sección se presentan las principales políticas de red definidas actualmente en la empresa, que posteriormente serán analizadas en el capítulo 3 para su respectiva redefinición o conservación.

2.7.1.1 Activos de riesgo

Es necesario definir los recursos sensibles de la empresa, que son propensos a ataques, como:

- Información confidencial de las principales áreas
- Equipos de conectividad
- Servidores Corporativos
- Las aplicaciones relacionadas con el sistema SCADA.

Mientras que las políticas de red se segmentan a dos grupos principales:

Red de negocios (usuarios corporativos):

- Los usuarios tendrán permisos de acceso relativos en función a su puesto.
- Una vez concedidos los permisos dependiendo de las actividades temporales a realizarse, el usuario es el único responsable del uso de las credenciales asignadas y de las operaciones que realice a través de las mismas.

Red de tecnologías (personal encargado de las TIC):

- Respaldar información sensible con la frecuencia y en el repositorio asignado
- Mantener copias de información actualizada
- Utilizar servidores virtuales o respaldos de servidores físicos
- Usar cortafuegos protege a la red local de ataques desde la red exterior
- Instalar *antivirus* y filtros anti-spam en las computadoras de los empleados como en los servidores
- Proporcionar redundancia de alimentación eléctrica con la utilización de UPS y generadores
- Determinar sitios permitidos y restringidos
- Actualizar en forma permanente tanto sistemas operativos y *software*
- Instalar mecanismos de seguridad perimetral

CAPÍTULO III

REDISEÑO DEL SISTEMA DE AUTENTICACIÓN E IMPLEMENTACIÓN A PEQUEÑA ESCALA [15] [16]

En este capítulo se presentará el rediseño de la red de la empresa, incorporando los principios recomendados según la arquitectura que define la tecnología Cisco *Borderless Network*, que son jerarquía, modularidad, flexibilidad y alta disponibilidad para proporcionar seguridad, redundancia y compatibilidad. Se incluye la configuración necesaria para cada capa (núcleo, distribución y acceso) tanto para la red inalámbrica como para la red cableada para cumplir con estos principios y que los dispositivos de la capa de acceso soporten Cisco ISE, considerando también los requerimientos técnicos actuales y futuros de la red de la empresa. Posteriormente se presentará las configuraciones para la implementación a pequeña escala de dos bloques de operación, como prototipo para realizar las pruebas de autenticación, perfilamiento, autorización, postura y remediación.

3.1 REDISEÑO DEL SISTEMA DE AUTENTICACIÓN DE LA EMPRESA [17] [18]

La solución elegida por la empresa para que realice autenticación, perfilamiento, autorización, contabilidad (*accounting*), postura y remediación es Cisco *Identity Services Engine* (ISE), que es una plataforma tecnológica de políticas de identidad y control de acceso, cuyas características, beneficios y funcionalidades fueron descritos en el capítulo 1.

El presente rediseño abarca la definición de nuevos perfiles tanto para usuarios como para servicios, políticas de red, requisitos mínimos, descripción de configuraciones y recomendaciones específicas para los equipos intermediarios (*switches* de núcleo, distribución y acceso), que deben ejecutarse para soportar la implementación de Cisco ISE. Aplicación obligatoria de políticas de red tanto a redes cableadas como inalámbricas.

3.1.1 REQUISITOS PARA LA IMPLEMENTACIÓN DE CISCO ISE [17] [19]

Cisco ISE utiliza exclusivamente los *switches* de la capa de acceso para la solicitud y envío de credenciales, que actúan como *Network Access Device (NAD)* manteniendo comunicación directa con los dispositivos finales (computadores, laptops, teléfonos IP, impresoras, y otros.) y les permiten conectarse a la red. La marca (Cisco), modelo y sistema operativo de interconectividad (IOS) de los *switches* de acceso deben ser compatibles con la versión 1.2 de Cisco ISE. Sin embargo, es necesario incluir ciertos cambios en la configuración de las capas de núcleo y distribución, inclusive en varios bloques debe ser segmentada la topología en un modelo de capas para cumplir con los principios de la arquitectura de Cisco y reemplazar los equipos con el objetivo de convalidar los equipos en función de los estándares de operación de la empresa (ver figura 3.1).

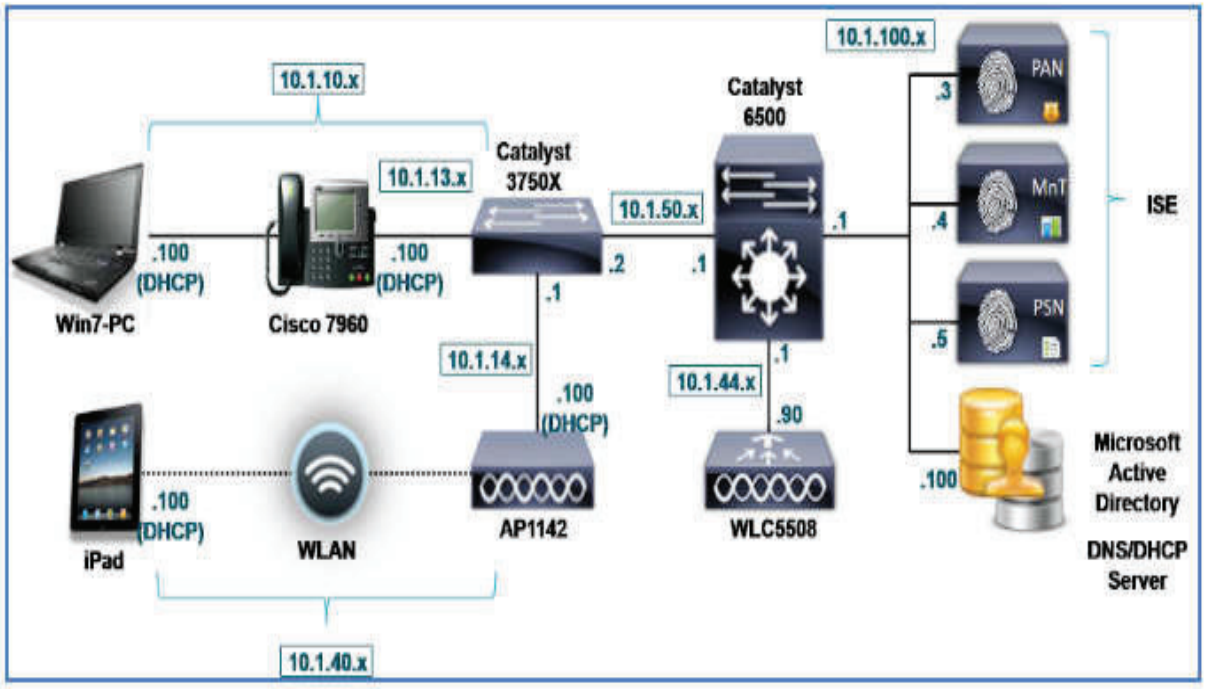

Figura 3.1 Topología Cisco ISE [20]

Por tanto, en el presente rediseño se considera la posibilidad de la adquisición de infraestructura y equipos para la empresa, dependiendo de los requerimientos, con el propósito de homologar los sistemas tecnológicos a la marca Cisco y disponer espacio

físico para la instalación del equipo (2 unidades de rack) por cada locación en los bloques en el que se instalará el equipo Cisco ISE. Con la adquisición y cambio de la actual conexión de los equipos y el cambio en la manera como se comunican, es necesario definir una nueva arquitectura de red, incluyendo topología lógica y física, considerando los principios de diseño según la arquitectura de Cisco. Este rediseño incluye:

- Determinación de la plantilla de configuración necesaria de los *switches* de acceso dependiendo del tipo de dispositivos finales y del bloque de operación.
- Definir un esquema de direccionamiento IPv4 general de toda la empresa incluyendo el necesario para los equipos CISCO ISE, redes adicionales para la VLAN de cuarentena (a la cual se redirigen los dispositivos que no cumplen con la postura), VLAN BYOD.
- Definir la matriz de riesgo para validación de las políticas actuales y generación de nuevas.
- Definir nuevos perfiles de usuarios enfocados en el uso actual de los servicios.

3.1.1.1 Rediseño de LAN multiservicios

La red de la empresa proporciona servicios de voz, datos, video, videoconferencia a usuarios que acceden a través de una conexión cableada e inalámbrica. El objetivo principal es la implementación de seguridad (a través de la autenticación de usuarios y dispositivos finales junto con la aplicación de nuevas políticas de red), alta disponibilidad, redundancia y compatibilidad. El uso de un modelo jerárquico en la red de la empresa permite un crecimiento modular de red, mejoramiento sustancial en la administración de la infraestructura, flexibilidad, tolerancia a fallas. Con la configuración de enlaces redundantes (puertos lógicos) proporciona una mejor asignación de ancho de banda a los enlaces troncales que soportan el tránsito de tráfico de varias VLAN, además es importante considerar adecuadamente el tipo de interfaces redundantes que se utilizan para la conexión entre la capa de núcleo con la de distribución, y la de distribución con la de acceso. En las mismas, por el requerimiento a nivel de ancho de banda y por alcance, se utilizará como medio de

transmisión fibra óptica. Con la inserción de enlaces redundantes a la topología resultante de la segmentación en capas disminuye la existencia de puntos críticos de nuestra red, aumentando considerablemente la confiabilidad y alta disponibilidad.

3.1.1.1.1 Rediseño de la arquitectura de la red LAN cableada

El dimensionamiento actual de los equipos de conectividad está basado en un análisis de la densidad de puertos requeridos, dependiendo del número de dispositivos finales en el que se incluyen estaciones de trabajo (computadores), teléfonos IP, impresoras, cámaras IP, incluyendo un 3 % de crecimiento anual en cada bloque de operación. El detalle del mismo se presenta en la Tabla 3.1.

ZONA	BLOQUE	USUARIOS REGISTRADOS	CRECIMIENTO 3 % EN CINCO AÑOS
ZONA DEL LITORAL	BLOQUE 1	120	138
ZONA DEL LITORAL	BLOQUE 6	150	173
ZONA OESTE	BLOQUE 7	700	805
ZONA CENTRO	BLOQUE 12	650	748
ZONA CENTRO	BLOQUE 15	720	828
ZONA OESTE	BLOQUE 18	730	840
ZONA OESTE	BLOQUE 21	620	713
ZONA ESTE	BLOQUE 31	850	978
ZONA NORTE	BLOQUE 43	1600	1840
ZONA NORTE	BLOQUE 63	1200	1380
MATRIZ	QUITO	400	460
ACCESO INALÁMBRICO	VLAN INVITADOS	300	345
TOTAL		**8040**	**9248**

Tabla 3.1 Dimensionamiento de usuarios

Actualmente las marcas de los equipos de conectividad existentes en todas las oficinas y campamentos de los bloques de operación a nivel nacional de la empresa son Cisco, Hirschmann, Ntron y otras; la variedad de marcas es producto de fusión de bloques pertenecientes a otras empresas (ver tabla 3.2).

ÁREA	MARCA DE EQUIPO	MODELO	TIPO
INFRAESTRUCTURA	3COM	3CR17333-91	*SWITCH*
INFRAESTRUCTURA	3COM	3C1647OB	*SWITCH*
INFRAESTRUCTURA	3COM	3C16471B	*SWITCH*
INFRAESTRUCTURA	3COM	3C16471B	*SWITCH*
INFRAESTRUCTURA	D-LINK	DES-1008D	*SWITCH*
INFRAESTRUCTURA	3COM	3CFSU08	*SWITCH*
INFRAESTRUCTURA	NETGEAR	FS608	*SWITCH*
INFRAESTRUCTURA	HP	13FSU08	*SWITCH*
INFRAESTRUCTURA	3COM	3C16794	*SWITCH*
INFRAESTRUCTURA	3COM	3C16794	*SWITCH*
INFRAESTRUCTURA	CNET	18-1SGH800CFB	*SWITCH*
INFRAESTRUCTURA	3COM	3C16700A	*HUB*
INFRAESTRUCTURA	3COM	3C16785	*SWITCH*
INFRAESTRUCTURA	DLINK	DES-1008D	*SWITCH*
INFRAESTRUCTURA	DLINK	DES-1008D	*SWITCH*
INFRAESTRUCTURA	N-TRON	105FX-SX	*SWITCH*
INFRAESTRUCTURA	N-TRON	405FX	*SWITCH*
INFRAESTRUCTURA	N-TRON	405FX	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XSDR22000-01	*SWITCH*
INFRAESTRUCTURA	3COM	2016	*SWITCH*
INFRAESTRUCTURA	D-LINK	DES-1008D	*SWITCH*
INFRAESTRUCTURA	LANTRONIX	XPRESS DR+	*SWITCH*
INFRAESTRUCTURA	D-LINK	DES-1005D	*SWITCH*
INFRAESTRUCTURA	N-TRON	304TX	*SWITCH*

Tabla 3.2 Descripción de *switches* de marcas diferentes del bloque 7

Estos equipos poseen características diferentes al actual estándar de la empresa, por tanto el primer paso es la estandarización de todos los equipos de todos los bloques a la marca Cisco, posteriormente los dispositivos actuales de la marca Cisco, deben ser catalogados para la verificación de la situación actual, características, modelo, versión de IOS, compatibilidad con ISE del equipo.

a. Compatibilidad de los equipos de conectividad con Cisco ISE v 1.2.

El catálogo de los equipos Cisco resultante permite analizar la compatibilidad de los mismos con Cisco ISE y cuáles equipos requieren una actualización de IOS para soportar Cisco ISE. A continuación se detalla la matriz de compatibilidad con Cisco ISE versión 1.2 de los equipos de conectividad en la capa de acceso, en la Tabla 3.3

MODELO DE *SWITCHES* COMPATIBLES	**VERSIÓN DE IOS RECOMENDADO** **VERSIÓN DE IOS MÍNIMO COMPATIBLE**
Catalyst 2960, ISR *EtherSwitch* ES2 (Catalyst 2960-S, Catalyst 2960-C LAN Base)	IOS v 12.2(55)-SE3
Catalyst 2960-SF, Catalyst 2960Plus	IOS v 15.0.2-SE (ED) LAN BASE
Catalyst 2960–XR, Catalyst 2960–X	IOS v 15.0.2-EX3 (ED)
Catalyst 3560-C Catalyst 3560-E, ISR *EtherSwitch* ES3 Catalyst 3560-X	IOS v 15.0.2-SE2 (ED)
Catalyst 3750-G	IOS v 12.2(55)-SE3
Catalyst 3750-E Catalyst 3750-X	IOS v 15.0.2-SE2 (ED) IP BASE
Catalyst 3850, 3650	IOS XE 3.2.2 SE
Catalyst 4500 Supervisor Engine 7-E, 7L-E	IOS-XE v 3.4.0 SG (ED)
Catalyst 4500 Supervisor Engine 6-E, 6L-E	IOS v 15.1.2 SG (ED)
Catalyst 6500 (Supervisor 32/Supervisor 720)	IOS v 12.2(33)-SXJ5 (MD)

Tabla 3.3 Matriz de compatibilidad con Cisco ISE versión 1.2 [21]

Para la verificación de compatibilidad del modelo del equipo de conectividad y la versión de IOS con el ISE, se compara con la Matriz de Compatibilidad del ISE versión 1.2, en el que se basa este rediseño (En el Anexo C1 se presenta el detalle completo de la matriz de compatibilidad para *switches*, WLC, ASA, dispositivos finales para Cisco ISE versión 1.2). A continuación, en la tabla 3.4, se indica los modelos de los

switches de acceso existentes en los bloques y su compatibilidad para la ejecución de autenticación a través del ISE.

EQUIPO-MODELO	SOPORTE ISE
WS-C2940-8TF-S	NO
WS-C2950-24	NO
WS-C2950C-24	NO
WS-C2950G-12-EI	NO
WS-C2960G-8TC-L	SI
WS-C2960-8TC-L	SI
WS-C2960C-8TC-L	NO
WS-C2960CG-8TC-L	NO
WS-C2960G-24TC-L	SI
WS-C2960S-24PS-L	SI
WS-C2960S-24TS-L	NO
WS-C2960S-24TS-S	SI
WS-C2960S-48LPS-L	SI
WS-C2960G-48TC-L	SI
WS-C3550-24-FX-SMI	NO
WS-C3560-8PC	SI
WS-C3560-8PC-S	SI
WS-C3560-24PS	NO
WS-C3560-24PS-S	SI
WS-C3560G-24TS	SI
WS-C3560G-24TS-S	SI
WS-C3560G-24PS	SI
WS-C3560X-24P-S	SI
WS-C3560G-24PS-E	SI
WS-C3560G-24PS-S	SI
WS-C3560G-48PS-S	SI
WS-C3560G-48PS	SI
WS-C3560X-48P-L	SI
WS-C3560G-48TS-S	SI
WS-C3560G-48TS	SI
WS-C3750G-12S-E	NO
WS-C3750G-12S-S	NO
WS-C3750X-24P	SI
WS-C3750X-24T-S	SI
WS-C3750G-48PS	SI
WS-C3750G-48PS-S	SI
WS-C3750G-48TS	SI
WS-C3750G-48TS-S	SI
IE-3000-8TC	NO

Tabla 3.4 Modelo de los equipos de conectividad en la capa de acceso vs compatibilidad ISE

b. Actualización IOS de los switches de acceso.

En los *switches* de acceso con soporte para Cisco ISE se realiza la actualización de IOS, la versión de la actualización es **15.(02)SE6** que soporta Cisco ISE 1.2.0.899, con la posibilidad de soporte a una actualización a la versión 1.4 (máxima versión de actualización hasta la fecha en Cisco ISE). Por ejemplo:

Para el *switch* Cisco 2960S-48TS-L, le corresponde la versión de IOS:

- c2960s-universalk9-mz.**150-2.SE6**.bin

Para el *switch* Cisco WS-C3560X-24P-L, le corresponde la versión de IOS:

- 15.0.2-SE2 (ED)

Para el *switch* Cisco WS-C3750X-24P-L, le corresponde la versión de IOS:

- 15.0.2-SE2 (ED) IP BASE

Los equipos que serán actualizados y que soportan Cisco ISE son

- Catalyst 2960
- Catalyst 3560
- Catalyst 3750

Los equipos que no son compatibles aún con la actualización de IOS serán reemplazados, para permitir compatibilidad y estandarización entre los dispositivos de conectividad y el ISE.

En la Tabla 3.5 se detalla las características principales incluyendo la versión de IOS recomendada de los equipos de conectividad de la capa de núcleo, distribución y acceso de la matriz, los bloques 1 y 6.

La información de los bloques restantes de la empresa petrolera se presentará en el Anexo C2.

MODELO SWICTH	UBICACIÓN	TIPO DE CAPA	COMPATIBLE	VERSIÓN DE IOS MÍNIMO RECOMEDADA PARA CISCO ISE
WS-C3750X-48P	MATRIZ	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C3750X-48P-S	MATRIZ	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C3750X-48P-S	MATRIZ	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C3750X-48P-E	MATRIZ	DISTRIBUCIÓN	NO APLICA	15.0.2-SE2 (ED) IP BASE
WS-C2960G-8TC-L	MATRIZ	ACCESO	SI	15.0.2-SE (ED) LAN BASE 4
WS-C6509-E	MATRIZ	NUCLEO	NO APLICA	12.2(33)-SXJ5 (MD)
WS-C3750X-48P-S	BLOQUE 1	DISTRIBUCIÓN	NO APLICA	15.0.2-SE2 (ED) IP BASE
WS-C2960S-48LPS-L	BLOQUE 1	ACCESO	SI	12.2(55)-SE3
WS-C3750G-48TS-S	BLOQUE 1	ACCESO	SI	12.2(55)-SE3
WS-C3750X-48P-S	BLOQUE 1	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C2960CG-8TC-L	BLOQUE 1	ACCESO	NO (REEMPLAZADO POR WS-C2960G-8TC-L)	15.0.2-SE (ED) LAN BASE 4
WS-C2960S-48LPS-L	BLOQUE 6	ACCESO	SI	12.2(55)-SE3
WS-C3750X-24P-L	BLOQUE 6	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C3750X-48P-S	BLOQUE 6	DISTRIBUCIÓN	NO APLICA	15.0.2-SE2 (ED) IP BASE
WS-C3750X-48PF-L	BLOQUE 6	ACCESO	SI	15.0.2-SE2 (ED) IP BASE
WS-C3560X-24P-L	BLOQUE 6	ACCESO	SI	15.0.2-SE2 (ED)

Tabla 3.5 Compatibilidad de los *switches* del bloque 1, bloque 6 y la matriz de la empresa [21]

c. Dimensionamiento de los switches en la capa de núcleo, acceso y distribución.

El detalle de los equipos reemplazados y trasladados se detalla en el Anexo C3 , con respecto a los *switches* de acceso no fue necesario la adquisición de nuevos equipos, ya que gracias al inventario realizado se determinó la existencia de equipos compatibles en buenas condiciones de la marca Cisco en varios bloques sin uso.

Los cuales a través de este rediseño serán trasladados a bloques que los requieran y previa verificación de compatibilidad, entrarán en operación junto con el ISE (ver tabla 3.6).

LUGAR	DENSIDAD DE PUERTOS DISPONIBLE	USUARIOS	*SWITCHES* EN LA CAPA DE ACCESO	*SWITCHES* EN LA CAPA DE DISTRIBUCIÓN	MODELO DE EQUIPOS EN LA CAPA DE DISTRIBUCIÓN
MATRIZ	674	460	23	4	WS-C3750X-48P-E
BLOQUE 1	256	138	7	2	WS-C3750X-48P-S
BLOQUE 6	235	173	9	2	WS-C3750X-48P-S
BLOQUE 7	894	805	53	1	WS-C4510R (ENGINE 6-E)
BLOQUE 12	788	748	48	1	WS-C4510R+E
BLOQUE 15	834	828	38	1	WS-C4507R-E
BLOQUE 18	858	840	42	3	WS-C3750G-48TS-S
BLOQUE 21	736	713	33	3	WS-C3750G-48PS-S
BLOQUE 31	984	978	70	1	WS-C4503-E
BLOQUE 43	1862	1840	83	1	WS-C4503-E
BLOQUE 63	1390	1380	34	1	WS-C4510R+E

Tabla 3.6 Dimensionamiento de equipos de conectividad (*switches* de acceso y distribución) de la empresa

d. Esquema de direccionamiento IP para la empresa.

En la tabla 3.7 se detalla la asignación de direccionamiento en IPV4 para la empresa.

BLOQUE	USUARIOS REGISTRADOS	NÚMERO DE HOSTS VÁLIDOS POR SUBRED	DIRECCIÓN DE RED	VLAN ID
BLOQUE 1	138	254	172.31.43.0/24	120 (VLAN NEGOCIOS)
BLOQUE 6	173	254	172.31.42.0/24	120 (VLAN NEGOCIOS)
BLOQUE 7	805	1022	172.31.36.0/22	120 (VLAN NEGOCIOS)
BLOQUE 12	748	1022	172.31.32.0/22	120 (VLAN NEGOCIOS)
BLOQUE 15	828	1022	172.31.28.0/22	120 (VLAN NEGOCIOS)
BLOQUE 18	840	1022	172.31.24.0/22	120 (VLAN NEGOCIOS)
BLOQUE 21	713	1022	172.31.20.0/22	120 (VLAN NEGOCIOS)
BLOQUE 31	978	1022	172.31.16.0/22	120 (VLAN NEGOCIOS)
BLOQUE 43	1840	2046	172.31.8.0/21	120 (VLAN NEGOCIOS)
BLOQUE 63	1380	2016	172.31.0.0/21	120 (VLAN NEGOCIOS)
QUITO	460	512	172.31.40.0/23	120 (VLAN NEGOCIOS)
GENERAL (VLAN INVITADOS)	345	254	172.31.200.0/23	201 (VLAN 8021X)
GENERAL (VLAN INVITADOS)	345	254	172.31.202.0/23	202 (VLAN BYOD)
VLAN TELEFONÍA	5150	8194	192.168.0.0/19	50 (VLAN TELIP)
GENERAL (VLAN VIDEOC)	515	1022	192.168.32.0/22	50 (VLAN VIDEOC)
GENERAL (VLAN TEMPORAL)	206	254	192.168.38.0/24	170 (VLAN TEMPORAL)
GENERAL (VLAN SRVNETIO)	258	510	192.168.36.0/23	170 (VLAN SRVSNETIO)

Tabla 3.7 Tabla de asignación de direccionamiento IP

3.1.1.1.2 Rediseño de la arquitectura de la red LAN inalámbrica

En esta sección se presenta la arquitectura de la red inalámbrica, que principalmente la conforman controladoras de LAN inalámbrica (WLC) y AP localizados en la matriz y en los bloques 7, 12, 21, 31, y 63. Las WLC se encuentran conectadas a los *switches* multicapa de la capa de distribución, principalmente se proporciona el acceso inalámbrico a los usuarios de tipo corporativo que realizan inspección de campo, pero principalmente utilizada por los usuarios de tipo INVITADO o acceso temporal; siendo esta la razón principal de la implementación de la solución Cisco ISE para controlar eficazmente el acceso vía inalámbrica y el acceso tipo BYOD.

a. Dimensionamiento de equipos inalámbrica y compatibilidad con la WLC.

Los equipos que conforman la red inalámbrica son WLC y AP. Los AP existentes son administrados y compatibles con las WLC, y hasta la fecha no superan las capacitadas de uso del 50% de su capacidad máxima efectiva, proporcionando buen servicio a los usuarios actuales y con disponibilidad de crecimiento a nivel de usuarios sin la necesidad de incorporación de nuevos equipos. Las WLC serán configuradas como NAD del ISE, por tanto deben ser compatibles con la versión 1.2. En la tabla 3.8 se puede apreciar la compatibilidad de las WLC existentes en la empresa con los equipos Cisco ISE 1.2.

MODELO WLC	NÚMERO DE EQUIPOS	UBICACIÓN	COMPATIBLE CON CISCO ISE 1.2
AIR-WLC4402-12-K9	1	MATRIZ	SI
AIR-CT2504-K9	1	MATRIZ	SI
AIR-WLC2106-K9	1	BLOQUE 7	SI
AIR-WLC4402-12-K9	1	BLOQUE 12 EPF	SI
AIR-WLC2106-K9	4	BLOQUE 12 PAÑACOCHA	SI
AIR-WLC4402-12-K9	1	BLOQUE 12 PAÑACOCHA	SI
AIR-WLC2106-K9	1	BLOQUE 21	SI
AIR-WLC2106-K9	1	BLOQUE 31	SI
AIR-WLC2504	1	BLOQUE 63	SI

Tabla 3.8 Compatibilidad entre la WLC vs Cisco ISE 1.2

b. Esquema de direccionamiento IP.

La red inalámbrica se segmenta exclusivamente en dos segmentos de red, lo cuales se muestran en la tabla 3.9. Uno relacionado con el acceso exclusivo a las laptops de usuarios corporativos o invitados con acceso a los servicios de red y se bloquea el acceso a teléfonos inalámbricos inteligentes, *Tablets* (WLAN 8021X_NETIO), mientras que el segundo está orientado al uso de todos los dispositivos móviles que puedan utilizar un explorador *web* para ingreso de credenciales y registro de su dispositivo a través de su dirección MAC (WLAN BYOD_NETIO). La asignación de direccionamiento IP cambia en el segundo octeto, siendo X el número de bloque correspondiente. Cabe destacar que el acceso inalámbrico está únicamente habilitado en la matriz y en los bloques 7, 12, 21,21, 63.

BLOQUE	USUARIOS REGISTRADOS	USUARIOS REGISTRADOS + 3% DE CRECIMIENTO	DIRECCIÓN DE RED	VLAN ID
X (VLAN CORPORATIVOS - INVITADOS) LAPTOPS	300	345	10.X.200.0/23	201 (VLAN 8021X)
X (VLAN CORPORATIVOS INVITADOS) DISPOSITIVOS INTELIGENTES	300	345	10.X.202.0/23	202 (VLAN BYOD)

Tabla 3.9 Asignación de direccionamiento IP para las WLAN

3.1.1.1.3 Configuraciones para los switches en la capa de acceso

Una vez determinados los equipos de conectividad requeridos en cada bloque (tabla 3.6), para cumplir el requerimiento a nivel de densidad de puertos y compatibilidad de características de soporte de Cisco ISE, se debe considerar los elementos adicionales requeridos para su instalación, como racks, acometidas eléctricas, cableado estructurado (para las conexiones entre las capas de núcleo con distribución, distribución con acceso por la capacidad requerida y alcance se utilizará fibra óptica monomodo y para la conexión entre los *switches* de acceso y los dispositivos finales

se utilizará cableado con categoría 6A, por su capacidades y acorde a los estándares de calidad de la empresa petrolera).

Cabe recalcar que la fusión de bloques nuevos a la empresa proporcionó equipos de conectividad compatibles con el ISE, junto con racks inteligentes con PDU (Unidades de Distribución de Energía de Rack) montadas, UPS, entre otras.

Por tanto, los requerimientos adicionales están cubiertos, mientras que el servicio de instalación y certificación de cableado estructurado requerido, será proporcionado por una empresa externa (la empresa petrolera usa en todas sus instalaciones únicamente cableado certificado). A continuación se procederá con la configuración de la plantilla necesaria en los *switches* de acceso para su funcionamiento como dispositivo de acceso de red (NAD).

3.1.1.1.4 Plantilla de configuración de los switches de acceso con soporte para autenticación a través de Cisco ISE

Para obtener características adicionales, a las definidas por defecto respectivos a *switches* de acceso, debe instalarse la plantilla *SDM* [22] *Prefer* `ip-routing`, que permite realizar funcionalidades de enrutamiento limitadas por el modelo del *switch*.

A través del comando `sdm preder ip-routing` en el modo de configuración global (cada modelo de *switch* puede presentar diferentes opciones de plantillas SDM).

Para cumplir el objetivo del rediseño implementando redundancia se utiliza la tecnología *Etherchannel*, que permite agrupar puertos físicos del *switch* en un solo puerto lógico que suma las capacidades de los puertos físicos y proporciona enlaces redundantes, denominado *Port-Channel* para los puertos troncales, que serán los encargados del transporte de tráfico de varias VLAN.

---

22 SDM: Security Device Manager, es una herramienta de mantenimiento basada en una interfaz web desarrollada por Cisco.

Las configuraciones necesarias y exclusivas para la integración del *switch* con el Cisco ISE para la autenticación a través de 802.1x y MAB son: ACL (listas de control de acceso), *RADIUS (Remote Authentication Dial-In User Service*), *AAA(Authentication, Authorization and Accounting*) y configuración de puertos. La plantilla general y detallada para todos los *switches* de acceso, a los cuales se conectan los dispositivos finales y en los que se van a realizar la validación de autenticación, es la siguiente:

a. Configuración AAA en un switch.

Habilita las configuraciones AAA con el comando**,** en el modo de configuración global del *switch*.

```
aaa new-model
```

b. Creación y habilitación del grupo de servidores RADIUS.

El grupo de servidores RADIUS denominado IseRadius, cuyos puertos de escucha son 1812 y 1813, fue configurado en los equipos determinados como NAD, mientras el *appliance* Cisco ISE fue simulado a través de una máquina virtual sobre el *Hypervisor* VMWare ESXI, que cumple los tres roles al mismo tiempo de *Admin*, *Monitor* y *Policy Services*. Por tanto, en los NAD, en modo de configuración global se crea el grupo, y posteriormente se indica la dirección IP del servidor RADIUS, que en nuestro caso es el ISE (máquina virtual). La dirección IP del ISE es 10.15.150.57.

```
aaa group server radius IseRadius
server 10.15.150.57 auth-port 1812 acct-port 1813
deadtime 1
```

c. Configuración AAA para autenticación, autorización, accounting.

Esta configuración se realiza en todos los puertos del *switch*, por tanto se ejecuta en modo de configuración global.

```
aaa authentication dot1x default group IseRadius local
aaa authorization network default group IseRadius local
```

```
aaa authorization network auth-list group IseRadius local
aaa authorization auth-proxy default group IseRadius
aaa accounting update periodic 5
aaa accounting auth-proxy default start-stop group IseRadius
aaa accounting dot1x default start-stop group IseRadius
```

d. Configuración AAA server para autenticación, autorización y accounting.

Para facilitar la interacción entre los dispositivos de conectividad elegidos como NAD con los servidores de políticas externas (en este caso el ISE), se debe definir una contraseña que le permita conectarse con el ISE. Esta configuración se realiza en el modo de configuración global del *switch*.

```
aaa server radius dynamic-author
client 10.15.150.57 server-key 7 Shared&Secret
```

e. Configuración de DHCP snooping.

Se configura DHCP *Snooping* para evitar los ataques de agotamiento de direcciones IP y suplantación de identidad. Esta característica filtra los mensajes DHCP de *broadcast* en puertos "no confiables", construyendo y manteniendo una tabla de asociaciones DHCP *Snooping* (contiene direcciones MAC, direcciones IP, tiempo de arrendamiento, tipo de asociación, número de VLAN, la interfaz local "no confiable" de un *switch*). Se configura DHCP *Snooping* por *switch* (por interfaz) o por VLAN, en nuestro caso se ha configurado por rango de VLAN.

```
ip dhcp snooping VLAN 48-202
no ip dhcp snooping information option
ip dhcp snooping
ip device tracking probe use-svi
ip device tracking probe delay 10
ip device tracking
```

f. Habilitación de EPM logging.

Al habilitar los *logs* del módulo de aplicación de políticas (EPM), se generan *syslogs* relacionados con la autorización de la ACL descargable (DACL), y parte de este registro se puede correlacionar con Cisco ISE, para que pueda recibirlos y realizar *troubleshooting* más avanzado a través de sus funciones.

```
epm logging
```

g. Configuración de dominio

Para la habilitación del acceso remoto a través de SSH.

```
ip domain-name netiopet.com
```

h. Habilitación de 802.1x de forma global.

```
dot1x system-auth-control
```

i. Habilitar el envío de paquetes EAPOL[23] (Extensible Authentication Protocol over) como críticos.

```
dot1x critical eapol
```

j. Configuración Listas de control de acceso nombradas (ACL).

Configuración de ACL, las cuales serán asignadas de forma dinámica dependiendo del equipo a conectar en los puertos del *switch* de acceso.

- La ACL nombrada ACL-ALLOW permite todo el tráfico.

```
ip access-list extended ACL-ALLOW
 permit ip any any
```

- La ACL nombrada ACL-DEFAULT permite el tráfico por defecto.

```
ip access-list extended ACL-DEFAULT
```

---

[23] EAPOL: es un protocolo de autenticación de un puerto de red a través de 802.1x normalmente utilizado sobre la red cableada.

```
 permit udp any any eq bootps
 permit udp any any eq 5355
 remark DNS
 permit udp any any eq domain
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny ip any any log
```

- La ACL nombrada ACL-POSTURE-REDIRECT se encarga de la redirección del tráfico para postura, tanto para la red cableada con para la inalámbrica 8021x_NETIO

```
ip access-list extended ACL-POSTURE-REDIRECT
 deny udp any any eq domain
 deny udp any eq bootpc any eq bootps
 remark Denegar IPS de ISE
 deny ip any host 10.15.150.57
 remark Servidores
 deny ip any host 10.15.150.15
 remark Redirecccion todo trafico www y https
 permit tcp any any eq www
 permit tcp any any eq 443
 deny ip any any
```

- La ACL nombrada ACL-WEBAUTHE-REDIRECT se encarga de la redirección del tráfico hacia la autenticación vía *web*, para la red inalámbrica BYOD_NETIO para el registro de dispositivos de tipo invitado.

```
ip access-list extended ACL-WEBAUTH-REDIRECT
```

```
deny   ip any host 172.17.0.6
deny   ip any host 172.25.1.6
permit ip any any
```

- La ACL nombrada PERMIT_ALL_TRAFIC se encuentra permitiendo todo el tráfico.

```
ip access-list extended PERMIT_ALL_TRAFFIC
 permit ip any any
```

k. Configuración de logging en un switch.

Configuración de *logging* el cual está direccionado al Cisco ISE en el puerto 20514. (El VLAN ID de la VLAN Administrativa es 99)

```
ip radius source-interface Vlan99
logging origin-id ip
logging source-interface Vlan99
logging host 10.15.150.57
logging host 10.15.150.57 transport udp port 20514
```

l. Configuración del servidor SNMP en un switch.

Configuración de *snmp-server community, traps, host*. (El VLAN ID de la VLAN Administrativa es 99)

```
snmp-server community netioadm RW
snmp-server trap-source Vlan99
snmp-server source-interface informs Vlan99
snmp-server enable traps snmp authentication linkdown linkup
coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature
status
snmp-server enable traps mac-notification change move threshold
```

```
snmp-server host 10.15.150.57 version 2c netioadm mac-
notification snmp

snmp-server host 10.15.150.57 version 2c netioadm mac-
notification snmp
```

m. Configuración del servidor RADIUS con sus principales atributos.

```
radius-server attribute 6 on-for-login-auth

radius-server attribute 8 include-in-access-req

radius-server attribute 25 access-request include

radius-server dead-criteria time 30 tries 3

radius-server host 10.15.150.57 auth-port 1812 acct-port 1813 key
7 Shared&Secret

radius-server host 172.25.1.6 auth-port 1812 acct-port 1813 key
7 Shared&Secret

radius-server deadtime 1

radius-server key Password12

radius-server vsa send accounting

radius-server vsa send authentication
```

n. Configuración del servidor NTP[24] en un switch.

La generación de *logs* tanto en el *switch* como en el ISE, necesitan marcas de tiempo, se deben sincronizar todos los servidores de la red (AD, WLC, equipos Cisco ISE).

```
ntp server 10.15.99.254
```

o. Configuración de notificaciones por el cambio de la tabla de direcciones MAC en un switch.

La siguiente configuración permite el envío de notificaciones (logs) cuando existe un cambio sobre la tabla de direcciones MAC en el *switch*.

```
mac address-table notification change interval 0
```

---

24 NTP: NETWORK TIME PROTOCOL, ES UN PROTOCOLO DE INTERNET QUE SINCRONIZA LOS RELOJES DE LOS SISTEMAS INFORMÁTICOS.

```
mac address-table notification change
mac address-table notification mac-move
```

p. Configuración específica de los puertos del switch de acceso conectado a dispositivos finales de la empresa.

A continuación se presenta la configuración base para cada uno de los puertos de acceso, para que trabajen de acuerdo a los requerimientos de la empresa (datos, voz, video-conferencia). Todo dispositivo conectado a la red cableada recibe direccionamiento IP dentro de la VLAN 170 (temporal), independientemente del tipo, será autenticado, perfilado, escaneado si cumple o no la postura, únicamente si cumple las anteriores condiciones se redirigirá a la VLAN de usuarios o la VLAN de voz (dependiendo del tipo de dispositivo) con los permisos de acceso del usuario autenticado, si no cumple la postura debe realizar la remediación respectiva dependiendo del tipo de dispositivo.

```
interface range fa0/5-24
switchport access VLAN 170
 switchport mode access
 switchport voice VLAN 48
 ip arp inspection limit rate 2048
 authentication event fail action next-method
 authentication event server dead action authorize VLAN 90
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
```

```
authentication periodic
authentication timer reauthenticate server
authentication violation restrict
mab
snmp trap mac-notification change added
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 15
auto qos trust dscp
spanning-tree portfast
ip dhcp snooping limit rate 35 spanning-tree portfast
ip dhcp snooping limit rate 35
```

3.1.1.1.5 Configuraciones para los switches en la capa de núcleo y distribución

Se recomienda en estas capas configurar redundancia a nivel de equipo en la capa de distribución y conexión de enlaces redundantes, los *switches* son estandarizados a la marca Cisco, así que por defecto se encuentra activo el protocolo STP (*Spanning Tree*) para la prevención de lazos a nivel de capa 2. en el presente proyecto se configura *Multiple Spanning Tree* (MST[25]), el mismo crea por cada instancia (conjunto de VLAN) un análisis de lazos diferente para cada conjunto de VLAN dependiendo que *switch* está configurado como *root brigde*, para lograr el equilibrio de carga en los enlaces ascendentes del *switches* de núcleo-distribución y distribución-acceso, basadas en VLAN pares o impares, y sobre los enlaces redundantes la configuración de *EtherChannels* manualmente, que permite agrupar capacidades de dos puertos físicos en un puerto lógico (ver figura 3.2).

---

[25] MST: Protocolo propietario de Cisco, evita lazos en enlaces redundantes sobre la capa enlace de datos.

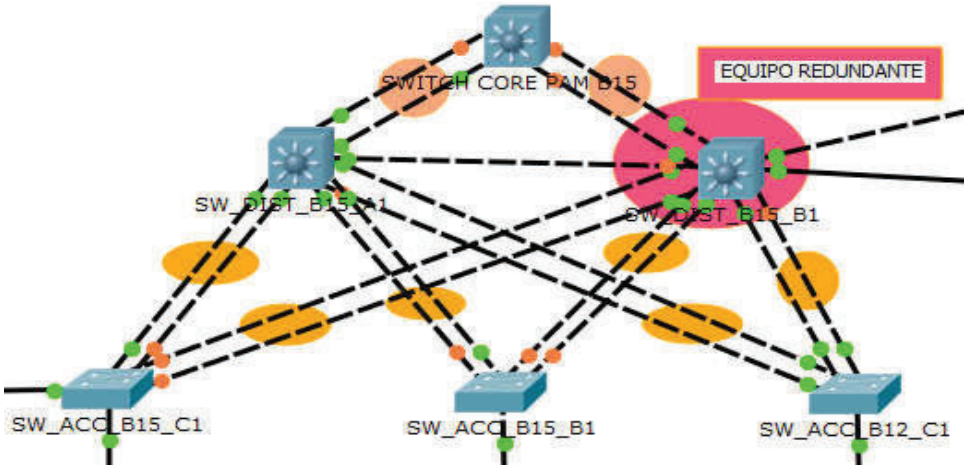

Figura 3.2 Topología con Redundancia con equipos y agregación de enlaces [11] [15]

Para activar los *EtherChannels* sobre los puertos *GigabitEthernet* 0/1 y 0/2 del *switch* de la capa de distribución y en los puertos *GigabitEthernet* 0/1 y 0/2 del *switch* de la capa de núcleo es necesario definir los mismos parámetros de operación, definición de la misma VLAN nativa, permitir el tránsito de las mismas VLAN, definición manual del modo del puerto troncal, y configuración del mismo número del *Portchannel* (el modo se define a través del comando `channel-group 1 mode on`), esta configuración debe ser la misma en los dos extremos del enlace.

```
interface range Giga0/1-2
 description EtherChannel entre DLS1y NÚCLEO B15
 switchport trunk native VLAN 777
 switchport trunk allowed VLAN 99,110,120,200,50
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
```

La configuración necesaria para la activación del *Portchanel* 1 es:

```
interface Port-channel1
 description Channel to sw NÚCLEO BL15
```

```
switchport trunk native VLAN 777
switchport trunk allowed VLAN 99,110,120,200,50
switchport mode trunk
switchport nonegotiate
```

Para la configuración de MST, se ocupa los siguientes comandos, en todos los *switches* parte de la topología:

```
Distribution1(config)#spanning-tree mst configuration
Distribution1(config-mst)#name region1
Distribution1(config-mst)#revision 10
Distribution1(config-mst)#instance 1 VLAN 777, 200, 201,202
Distribution1(config-mst)#instance 2 VLAN 50, 110, 120, 150
Distribution1(config-mst)#exit
```

Además, se define un *switch* raíz (conocido como *root bridge*) para el análisis de MST, ya que desde él se determina el flujo de tráfico y será la base para la determinación de que puertos pasarán a estado de bloqueo (no permite la circulación de tráfico pero seguirán recibiendo BPDU), y cuales a estado de envío (ver figura 3.3)

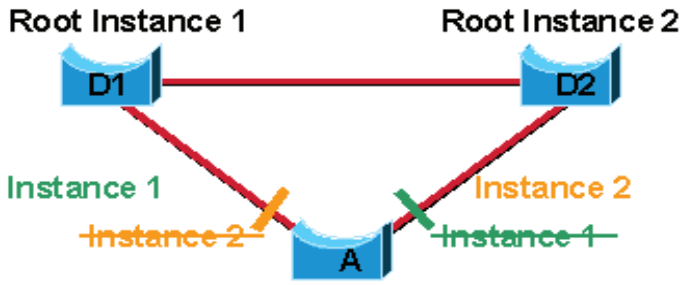

Figura 3.3 Topología con MST instancia 1 (VLAN impares), instancia 2 (VLAN pares) [11]

Los siguientes comandos permiten definir a un *switch* como *root* de la instancia 1 (VLAN 777, 200, 201, 202) para el protocolo STP, en este caso en modo MSTP+, en nuestra red será el *switch* de distribución 1 del bloque 15.

```
SW_DIST1_B15(config)#spanning-tree mst 0-1 root primary
```

```
SW_DIST1_B15(config)#spanning-tree mst 2 root secondary
```

La siguiente configuración es exclusiva para el *switch* definido como *root* de la instancia 2 (VLAN 50, 110, 120,150), en nuestra red será el *switch* de distribución 2 del bloque 15.

```
SW_DIST2_B15(config)#spanning-tree mst 2 root primary
SW_DIST2_B15(config)#spanning-tree mst 0-1 root secondary
```

Al tratarse de una red grande se segmentó a través de varias redes lógicas o virtuales (VLAN), dependiendo del propósito y servicios. Las VLAN resultantes se presentan en la tabla 3.10.

VLAN ID	NOMBRE	DESCRIPCIÓN
VLAN 120	Operaciones	Usuarios Autenticados por Red Cableada
VLAN 150	SRVS_NETIO	Granja de Servidores
VLAN 170	Temporal (CUARENTENA)	Usuarios conectados por Red Cableada pero deben cumplir la autenticación, perfilamiento, postura y remediación.
VLAN 201	8021X_NETIO	Usuarios conectados por Red inalámbrica pero deben cumplir la autenticación, perfilamiento, postura y remediación.
VLAN 202	BYOD_NETIO	Usuarios autenticados o invitados conectados por Red inalámbrica pero deben registrarse en el equipo Cisco ISE

Tabla 3.10 Segmentación de la red a nivel de VLAN

Se procede a la configuración del protocolo VTP[26], para la propagación de las VLAN creadas en el VTP server, y que serán aprendidas por cada *switch* configurado como cliente VTP. Configuración para el servidor VTP primario para MST 1, 2:

```
SW_DIST1_B15(config)# vtp version 3
SW_DIST1_B15(config)# vtp domain netiovtp
SW_DIST1_B15(config)# vtp mode server
```

[26] VTP: VLAN Trunking Protocol, es un protocolo utilizado para configurar y administrar VLAN en equipos de la marca Cisco.

```
SW_DIST1_B15(config)# vtp password mypassword
SW_DIST1_B15(config)# end
SW_DIST1_B15# vtp primary mst 1, 2
```

Un servidor de DHCP será el encargado de la asignación automática de direccionamiento IPv4 a los dispositivos finales (estaciones de trabajo, teléfonos IP, cámaras IP), el mismo está configurado a través de un rol instalado sobre *Windows Server Enterprise* 2008 R2, sobre el cual se crearán varios ámbitos dependiendo del requerimiento a nivel del número de VLAN configuradas en los *switches* que conforman la topología física de nuestra red, es decir un ámbito diferente por cada VLAN existente.

En cada ámbito de DHCP se define la dirección IP de la puerta de enlace predeterminada (*default-gateway*), esta dirección IP será la virtual asignada a la SVI de la VLAN respectiva, ya que para brindar redundancia de primer salto se configuró HSRP.

La configuración del *switch* multicapa que será HSRP activo es:

- Ingreso a la configuración específica de la SVI 99 y asignación de direccionamiento IP a la SVI 99

```
interface Vlan 99
ip address 10.1.99.253 255.255.255.0
```

- Configuración de la dirección IP virtual que comparten los *routers* (en este caso *switch* multicapa) dentro del grupo 99

```
standby 99 ip 10.1.99.254
```

- Asigna una prioridad (en este caso 120) a la interfaz del *router* (en este caso *switch* multicapa). El valor predeterminado es 100. El *router* (en este caso *switch* multicapa) con el valor más alto en prioridad será elegido como ACTIVO.

```
standby 99 priority 120
```

- Permite que el *router* (en este caso *switch* multicapa) se convierta en activo cuando su prioridad sea mayor a la de los demás *routers* (en este caso *switch* multicapa)

```
standby 99 preempt.
```

- Para la verificación de la configuración y estado de HSRP activo, se utiliza el siguiente comando:

```
RouterA#show standby

Gi0/1 – Group 99
Local state is Standby, priority 120
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 0.776
Virtual IP address is 10.1.99.254 configured
Active router is local
Standby router is 10.1.99.252, priority 120 expires in 9.568
```

La configuración de HSRP se puede realizar sobre una interfaz física o sobre una interfaz virtual del *switch* (SVI), como fue este caso.

- Para la verificación de la configuración y estado del *switch* multicapa como HSRP *stand-by (en reserva)*, podemos utilizar el mismo comando pero la información resultante es la siguiente:

```
RouterA#show standby

Gi0/1 – Group 99
Local state is Standby, priority 100
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 0.776
Virtual IP address is 10.1.99.254 configured
Standby router is local
Active router is 10.1.99.253, priority 100 expires in 9.568
```

3.1.1.1.6 Diagrama general de la empresa

En esta sección se presenta el diagrama de la red LAN de los 11 bloques de operación y la matriz de la empresa resultado del rediseño, en el mismo se incluye tanto la topología física como la topología lógica.

a. Topología física y lógica de la red

La topología física detalla la manera como se encuentran interconectados los dispositivos a través de medio físico, en relación a la red cableada las conexiones se realizan a través de fibra óptica y cable UTP de categoría 6A.

La topología lógica hace referencia a la manera cómo se comunican los dispositivos a través de medio físico; los enlaces redundantes pueden estar configurados como respaldos (es decir que pueden estar conectados pero no en uso hasta que el activo deje de funcionar) u operando en balanceo de carga (varios enlaces físicos agrupados en un puerto lógico a través de la tecnología *EtherChannel*).

Este tipo de conexiones se las realiza entre las capas de acceso-distribución y distribución-núcleo a nivel de la capa enlace de datos del modelo ISO/OSI, en los *switches* Cisco se ejecuta por defecto el protocolo *Spanning Tree* (STP) en modo PVST + (per VLAN STP+) para evitar lazos en los enlaces redundantes, pero en el presente rediseño se utiliza el modo MST.

El modo MSTP (*Multiple Spanning-tree Protocol*) está basado en el *standard* IEEE 802.1s[27], disponible desde Cisco IOS *Release* 12.2(25)SE y permite varias VLAN sean mapeadas a través de la misma instancia de S*panning-tree*, evitando así la creación de múltiples instancias de *Spanning-tree* para cada VLAN existente.

Este método proporciona rutas diferentes para el tráfico de datos para cada instancia, permitiendo tolerancia a fallas porque la caída de una instancia (ruta de reenvío) no afecta a la ruta utilizada por otras instancias. Si la ruta utilizada falla inmediatamente buscará una ruta de respaldo la cual pueda utilizar para restablecer la circulación de tráfico. La topología lógica resultante se muestra en la Figura 3.4 considerando el número de usuarios de cada bloque, y redundancia en los puntos críticos.

---

[27] 802.1s: Estandar IEEE Multiple Spanning Trees, es un estándar IEEE inspirado en la implementación del protocolo STP por instancias, es propietario de la marca Cisco.

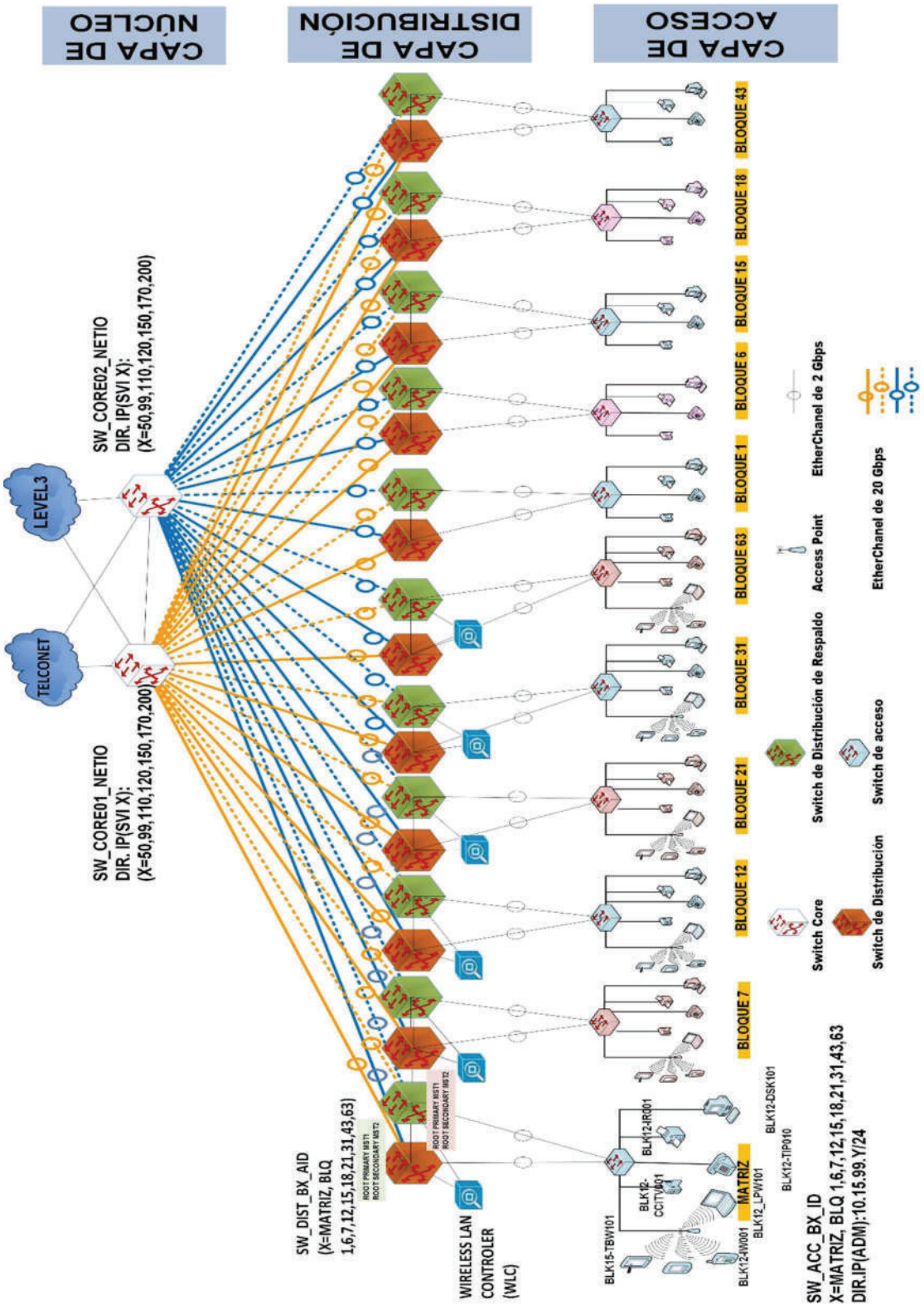

Figura 3.4 Topología física y lógica resultante del rediseño

3.1.1.2 Administración de la red

La herramienta utilizada para la administración y monitoreo centralizado de la empresa es PRTG *Network Monitor (Paessler Router Traffic Grapher*) versión 15.3.20.4114, instalada sobre una máquina de *Windows*, que permite colectar estadísticas de las máquinas, *software* y equipos detectados manualmente o automáticamente. Dentro de sus atributos se encuentra la capacidad de generar gráficas en tiempo real y reportes personalizados, que permite considerar el estado actual de la empresa y las aplicaciones recurrentes que ocupan mayor ancho de banda. Es un *software* propietario adquirido por la empresa, la licencia se encuentra activa y aún existen alrededor de 300 activas y disponibles para nuevos dispositivos. Por las razones expuestas, no será reemplazado.

Además con la inserción de los equipos Cisco ISE permite el monitoreo continuo en tiempo real de dispositivos de red catalogados, dispositivos finales y otros (ver figura 3.5).

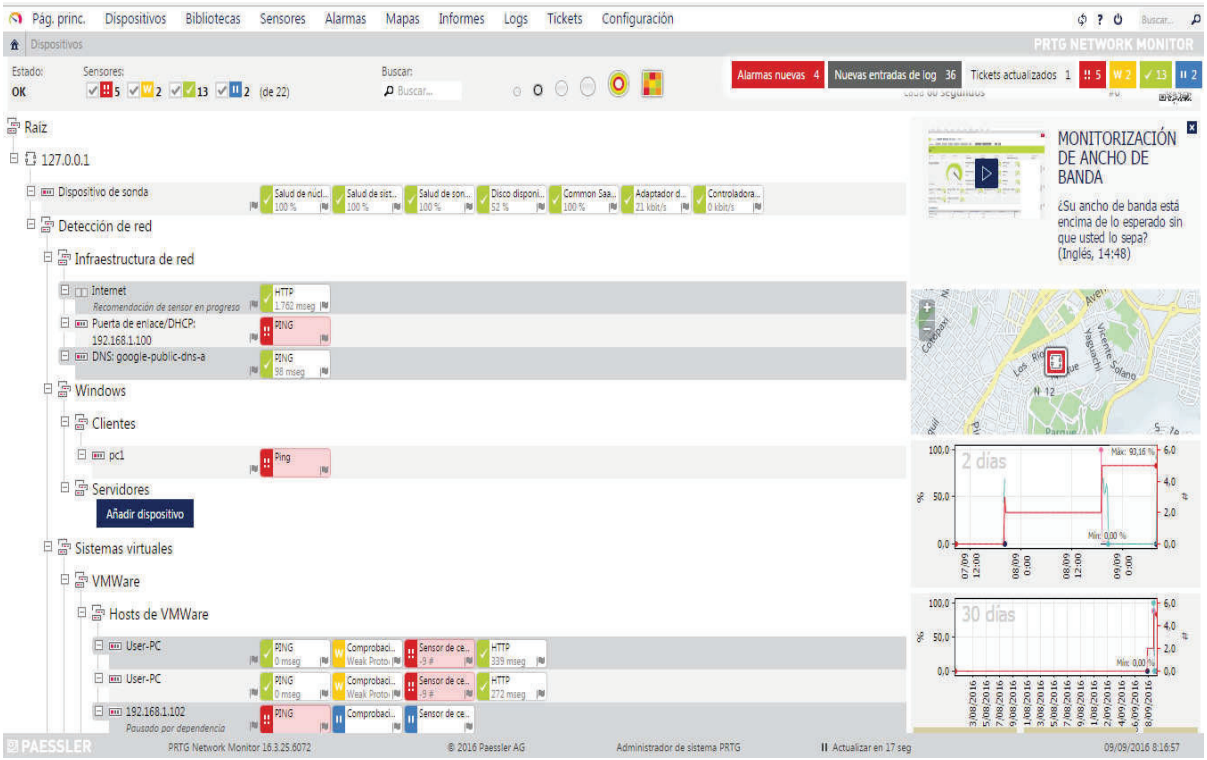

Figura 3.5 Monitoreo de equipos con PRTG

3.1.1.3 Seguridad de la red

Las innovaciones tecnológicas permiten el avance informático en el desarrollo y funcionamiento de servicios para los usuarios en las empresas, pero al mismo tiempo las técnicas de infiltración y ataque a redes mejoran con el fin de encontrar vulnerabilidades, pero los ataques no solo suelen ser de origen externo sino también de origen interno, consciente o inconsciente de los mismos usuarios internos de la empresa.

Por tanto, la seguridad de la red puede ser afectada por errores internos, debido a falta de procedimientos que rijan el modo de actuar con respecto a operaciones normales o a incidencias, es decir que la falta o mala definición de políticas de red en una empresa, puede ocasionar la operación incorrecta de la misma y en el peor de los casos la pérdida completa de servicios empresariales o captura de información confidencial. Por tanto, se prioriza la necesidad de articular mecanismos de seguridad y protección, este tema es muy amplio, pero los servicios de seguridad más significativos son la autenticación, el control de acceso, la confidencialidad y la integridad de datos. El alcance del presente proyecto es la autenticación (verificación de la identidad) relacionada con el control de acceso (protección contra el uso no autorizado de recursos disponibles).

Por esta razón, la empresa invierte recursos económicos para resguardar su red de amenazas, con la inserción de Cisco ISE, pero es necesario también la creación de estrategias de protección de los puntos sensibles y críticos, además de capacitar a sus empleados de los riesgos y las consecuencias existentes y la necesidad inherente de la ejecución correcta de las políticas de seguridad.

Dentro de una organización se requiere que los servicios proporcionados a los usuarios sean accesibles, seguros y orientados al perfil del usuario identificado. *Windows Server* permite la instalación de un rol que activa un servicio de directorio, denominado Directorio Activo (AD) cuya estructura organizada de identidades y funciones permite organizar, administrar y controlar los recursos de la red (usuarios, servidores, estaciones de trabajo, impresoras y otros). Además de permitir la

asociación de GPO (políticas de grupo) con unidades organizacionales (OU) de equipos, usuarios, es decir permitir o denegar el acceso a servicios dependiendo del grupo y/o tipo de usuario. La empresa cuenta con un AD montado sobre *Windows Server Enterprise* 2008 R2, y será utilizado como unidad de identidad externa para el ISE, que valida las credenciales (usuario-contraseña), políticas de seguridad, equipos vinculados al dominio de la empresa y otros. Los siguientes numerales han sido desarrollados en base a la norma ISO/IEC 27002:2005, se toma en cuenta los servicios en la matriz de la empresa, considerando que se replica el análisis de la matriz para los demás 10 bloques de operación de la empresa ubicados a lo largo del país.

3.1.1.3.1 Determinación de activos informáticos

Los recursos principales de la en la matriz de la empresa se muestran en la Tabla 3.11.

TIPO DE ACTIVO	DESCRIPCIÓN
RED	• Equipos de Cableado (Racks, Patch Panel, Bandejas, Escalerillas, y otras) • Equipos de Conectividad (*Switch*, *Router*, Firewall, WLC, AP) • Infraestructura (Planes, Documentación, y otras.) • Impresoras,Memorias portátiles, computadores de Escritorio y servidores. • Programas de administración y monitoreo Pozos Petroleros. • Programas de comunicación (correo electrónico, telefonía IP, Videoconferencia y Video streaming, y otras.) • Programas de manejo de proyectos • Programas de manejo, configuración y monitoreo Sistema SCADA. • Programas de producción de datos y reportes diarios, semanales, o por pedido. • Respaldos de configuraciones • Respaldos de garantías técnicas
TALENTO HUMANO	Personal que labora en las diferentes instalaciones por departamento y por bloque Nómina de trabajadores
FINANCIERO	Balances económicos, roles de pagos, ingresos, egresos. *Software* contable.
RESPONSABILIDAD SOCIAL	Informes anuales de inversión y resultados de proyectos medioambientales (beneficios a comunidades)
DEPARTAMENTOS VARIOS	Información confidencial interna por departamento. Productos institucionales (Investigaciones, Folletos, Fotos, y otras.)

Tabla 3.11 Activos de Información de la empresa

3.1.1.3.2 Determinación de posibles riesgos de seguridad

Esta sección es fundamental para el desarrollo y aplicación de las nuevas políticas de seguridad; o validar algunas de las actuales, al identificar las posibles fallas.

En la tabla 3.12 se presenta la valoración estimada para los niveles de privacidad, integridad y disponibilidad para los activos de información de la empresa descritos en la sección anterior.

NIVEL	VALORACIÓN DE RIESGO	DESCRIPCIÓN DEL RIESGO
PRIVACIDAD		
Bajo	1	Aquellos que se difunden a los usuarios de los diferentes departamentos de los diferentes bloques que utilizan los servicios que brinda la empresa
Mediano	2	Aquellos que los directivos comunican a determinadas personas (internas y externas), mediante la documentación pertinente (memos, informes y otras). Debe ejecutarse un control de su difusión.
Alto	3	Aquellos de uso único y exclusivo de los directivos de la Institución y que no pueden ser de dominio público.
INTEGRIDAD		
Bajo	1	Restablecer en máximo 2 días.
Medio	2	Restablecer máximo en cuestión de horas.
Alto	3	Restablecer máximo en cuestión de minutos
DISPONIBILIDAD		
Bajo	1	Se puede prescindir por unos días
Medio	2	Se puede prescindir por unas horas
Alto	3	Sin este, la empresa no puede operar normalmente

Tabla 3.12 Matriz de Riesgos de Seguridad

Se procede a establecer la magnitud de riesgos en los bloques de la empresa, correspondiente a cada activo relacionado con la información, sistema e infraestructura; es decir determinar el nivel de importancia que implica que dicho bien falle y la forma en que afecta a la operación normal de la red.

El detalle de los mismos se presenta en el Anexo C4. Los activos que obtengan valores mayores o iguales a 1.5; son aquellos que necesitan mayores márgenes de seguridad.

Tomando en cuenta los valores obtenidos en el Anexo C4 .; se indica que se debe poner mayor énfasis en la seguridad en los activos físicos y lógicos; en los activos de acceso a los servicios como datos, la telefonía IP y la video conferencia, ubicados en el perímetro de una red (dispositivos ubicados en la capa de acceso); así también en los activos de la documentación corporativa (datos como los: contratos, acuerdos, proyectos, inversiones, ganancias, informes, balances económicos, facturas, informes de situación actual de la empresa, reportes de riesgos, monitoreo, mantenimiento, y otros.); los mismos constituyen una parte indispensable para el funcionamiento en general de la empresa.

En consecuencia se procede a realizar la identificación de amenazas con su respectiva valoración (niveles), descritos en la tabla 3.13.

Dentro de la identificación de amenazas se distinguen tres grupos: aquellas originadas por la criminalidad común y motivación política; sucesos de origen físico; y sucesos derivados de la impericia de usuarios y decisiones institucionales.

ANÁLISIS		**PROBABILIDAD DE AMENAZA**		
		CRIMINALIDAD Y POLÍTICA	**SUCESOS DE ORDEN FÍSICO**	**IMPERICIA DE USUARIOS**
Magnitud de Daño	Datos e Información	8.5	6.3	7.8
	Sistemas e Infraestructura	6.5	7.5	9.2
	Personal	5.4	6.1	7.6

Tabla 3.13 Análisis de Riesgo

Con respecto a los datos mostrados en la Tabla 3.13, se debe considerar que el riesgo resultante en cada caso, se valora de acuerdo al siguiente criterio:

- Bajo Riesgo = 1 – 3
- Medio Riesgo = 3 – 6
- Alto Riesgo = 7 – 10

En base a los resultados obtenidos en cada bloques de operación y matriz, los sistemas e infraestructura y los datos e información; frente a las acciones que puedan tomar los usuarios frente a la infraestructura de red (impericia de los usuarios).

Por tanto, se pone más énfasis en cuanto al control de acceso de los usuarios, promoviendo conferencias de concientización a los funcionarios de la empresa por el personal de tecnologías acerca de los riesgos de seguridad y necesidad imperiosa de la ejecución de las políticas de red de la empresa.

3.1.1.3.3 Determinación de la matriz de riesgos de la instalación del nuevo sistema de autenticación

En este numeral se presenta la matriz de riesgos de la instalación de la plataforma tecnológica Cisco ISE sobre la infraestructura de la empresa resultante de este rediseño (ver tabla 3.14).

Tomando en cuenta que todo dispositivo será autenticado, no solo computadoras de los usuarios corporativos, sino también cámaras, impresoras, teléfonos IP, entre otros; provocando al inicio un retardo en tiempo hasta que sean comprobadas las credenciales del usuario, del dispositivo utilizado para la conexión para posteriormente ejecutar las políticas de postura, remediación y autorización.

Además se considera, que el cambio debe necesariamente incorporar una correcta capacitación del oferente al área de tecnología y a los usuarios corporativos de la empresa. Porque la empresa puede contar con la mejor tecnología disponible pero si no conocen como utilizarla y ejecutar sus políticas correctamente, la misma es inútil.

EVENTO	PROBABILIDAD DE OCURRENCIA 1-3	RIESGO (IMPACTO) 1-3	EXPOSICION PROBABILIDAD POR IMPACTO
Recolección errónea de información y requisitos de campo por parte de Operaciones TI	1	2	2
Diseño defectuoso por parte de los Especialista.	1	2	2
Listado faltante de equipos, materiales	1	2	2
Retraso en el ingreso y seguimiento a la orden de compra	1	2	2
Poca colaboración de otros departamento en la provisión de información a personal de TI	1	1	1
Falta de stock de equipos en fábrica	2	3	6
Entrega de equipos incompletos o por partes	2	2	4
El sistema de Autenticación ACS de Cisco tiene más de 5 años funcionando en la red	3	3	9
El sistema de Autenticación ACS de Cisco cumplió su EOL y EOS	3	3	9
Existen locaciones en las que no se está realizando autenticación para acceder a la red y no se puede seguir implementando el sistema de Autenticación ACS de Cisco debido a que ya cumplió el EOL y EOS	3	3	9
El soporte técnico para el sistema de Autenticación ACS de Cisco tiene un costo demasiado elevado	3	1	3
Equipos de Acceso a la red (*switches*) antiguos o descontinuados no soportan la configuración de Autenticación ISE	1	3	3
Falta de colaboración de personal de Operaciones de TI.	1	1	1
Falta de permisos de Gerentes de Campo	1	2	2
Rechazo de usuarios al cambio tecnológico	1	1	1
Problemas de adaptación de usuarios al nuevo sistema de Autenticación Cisco ISE	1	1	1
Limitaciones de espacio, energía, accesorios en rack de los centro de computo	2	2	4
Problema de inventarios durante la ejecución.	2	1	2
Falta de capacitación y auto capacitación continua del personal de TI	2	2	4
Falta de Mantenimiento programado de equipos que puede disminuir la vida útil de los mismos.	2	3	6

RANGO	PROBABILIDAD DE OCURRENCIA / RIESGO/ PROBABILIDAD	RIESGO
1	BAJO	1 a 3
2	MEDIO	4 a 6
3	ALTO	7 a 9

Tabla 3.14 Matriz de riesgo de la implementación de la plataforma Cisco ISE

A través de estos resultados se determina en qué áreas en específico es necesario redefinir las políticas de seguridad.

3.1.1.3.4 Lineamientos Generales para la definición de Políticas de Seguridad

Es importante la definición correcta de políticas de seguridad a ser concientizadas y ejecutadas por todos los usuarios de la red de la empresa, cabe destacar que son diferentes para cada área y tipo de usuario.

A continuación se describen las políticas de seguridad que fueron discriminadas dependiendo de los criterios anteriormente descritos, de los resultados de las encuestas realizadas al director y un subordinado de cada área y finalmente bajo la revisión y aprobación de cada director de área y del Jefe de Tecnologías de la empresa (La encuestas se encuentran en el Anexo C5).

El conjunto de políticas de seguridad informática propuestas y sanciones respectivas serán revisadas en conjunto con los directores de cada departamento, entre los más importantes tenemos Planificación, Talento Humano (unidad ejecutora de las sanciones respectivas) junto con el Jefe Nacional de Sistemas; y aprobadas por la Dirección General de la empresa.

a. Políticas de seguridad AT (Área de Tecnologías)

- Respaldar información sensible con la frecuencia y en el repositorio asignado para el área de operación por el Administrador de tecnologías.
- Al mantener copias de información actualizada, el tiempo de recuperación después de un incidente será mínimo.
- Se puede utilizar programas que se encarguen de realizar el respaldo físico o en línea automáticamente, pero de manera periódica.
- Utilizar servidores virtuales o respaldos de servidores físicos.
- Al existir algún fallo en el *hardware* del servidor local, la réplica de respaldo permite que las operaciones de la empresa puedan continuar con normalidad.

- Usar cortafuegos (firewalls) protege a la red local de ataques desde la red exterior, los mismos pueden ser implementados en *hardware* y *software*.
- Instalar *antivirus* y filtros anti-spam en las computadoras de los empleados como en los servidores, en nuestro caso al tratarse de una empresa con más de 8.000 usuarios se recomienda el uso de una consola de Administración del *Antivirus* corporativo, para que la misma se encargue de la instalación, actualización de la base de datos de virus, administración y monitoreo de manera remota y centralizada.
- Proporcionar redundancia de alimentación eléctrica con la utilización de UPS (Sistema de Alimentación Ininterrumpida), logrando que los equipos sensibles como por ejemplo servidores, equipos de conectividad posean suministro eléctrico por un período de tiempo determinado por la capacidad del UPS, en caso de un corte o problema con la alimentación eléctrica.

  En este tiempo disponible se utiliza para apagar o desconectar los dispositivos de manera segura.

  Por tanto, se debe estimar correctamente las capacidades de carga que debe soportar el UPS, además se debe tomar en cuenta que la capacidad total (efectiva) que se puede utilizar del UPS es el 80% de la capacidad nominal.
- Determinar sitios permitidos y restringidos, para este fin se utilizan los filtros de contenido que evitan que los usuarios puedan visitar sitios en *Internet* que impliquen un riesgo de seguridad para la empresa.
- El personal de Infraestructura es responsable de la administración, configuración y soporte brindado en bases de datos Microsoft SQL.
- El personal de Infraestructura es responsable de la administración del licenciamiento de Microsoft SQL.
- El personal del Departamento de TI es responsable de coordinar con el área de infraestructura, los trabajos de diseño e implementación de bases de datos de Microsoft SQL
- La divulgación y control de este documento es responsabilidad del área de infraestructura.

b. Políticas de seguridad UC (Usuarios Corporativos)

- El(los) administrador(es) de la red, usuarios de estaciones de trabajo y usuarios en general deberán actualizar en forma permanente tanto sistemas operativos y *software* que permita desarrollar de forma eficiente su trabajo.
- Es indispensable tener instalado un buen *software antivirus*, sin importar la marca o procedencia y actualizar su registro de virus continuamente.
- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares y otros.
- Cambiar de Claves de Acceso por lo menos cada 3 meses; aunque lo ideal es hacerlo mensualmente.
- Las carpetas compartidas, dentro de una red, deben tener una Clave de Acceso, la misma que deberá ser cambiada periódicamente.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.
- Verificar cualquier *software* que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
- No instalar copias de *software* pirata. Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad.
- Tomar precauciones con los contenidos de *applets* de Java, Java *Scripts* y Controles *ActiveX*, durante la navegación, así como con los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.
- Instalar un *Firewall* de *software* o cualquier sistema seguro para controlar los puertos del sistema.
- No almacenar información importante en su sistema. Si un intruso la captura, puede borrar esos archivos y eliminar toda prueba, para posteriormente usar los datos obtenidos. Es recomendable mantener esta información en un *pen drive*, con su respectivo respaldo.

- ❖ No se debe confiar en los archivos gratuitos que se descargan de sitios *web* desconocidos, ya que son una potencial vía de propagación de virus.
- ❖ Configurar el sistema para que muestre las extensiones de todos los archivos.
- ❖ De ninguna manera se debe ejecutar archivos con doble extensión.
- ❖ No contestar los mensajes *SPAM* (correo basura), ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, y otros.
- ❖ En el caso del administrador(es) de la red, tener precaución si algún servidor no reconoce su nombre, clave de acceso o servicio de correo, podría ser que ya esté siendo utilizado por algún intruso; a menos que haya un error en la configuración, la cual deberá ser verificada.
- ❖ La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o re-inicios continuos, inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, son evidencias de que el equipo está siendo controlado por un hacker que ha ingresado al sistema.
- ❖ Borrar constantemente las cookies, archivos temporales e historial, en la opción Herramientas, Opciones de *Internet*, del navegador.
- ❖ En cuanto a los servicios físicos de red, como *faceplate*, cable o cualquier tipo de equipo localizado en oficinas y demás dependencias, se deberá informar al departamento indicado, en caso de que estos estén dañados o averiados.

c. Políticas de seguridad UE (Usuarios Externos)

- ❖ El o los usuario(s) externo(s) deben comunicarse con anterioridad (por lo menos 7 días de anticipación) al responsable interno del proceso a realizarse en el X bloque el X día del X mes del X año, indicando las actividades, por tanto debe llenar un formulario de solicitud de servicio, el mismo se encuentra definido en el Anexo C6, con los campos requeridos para la creación del usuario.

- Los usuarios externos tendrán permisos de acceso relativos a la función que desempeñarán, el permiso por defecto es acceso a *Internet* limitado.
- Una vez concedidos los permisos dependiendo de las actividades temporales a realizarse, el usuario es el único responsable del uso de las credenciales asignadas y de las operaciones que realice a través de las mismas.
- Para que el usuario pueda conectarse a la red de la empresa deber ser autenticado, perfilado, y cumplir ciertos requerimientos de *software*.

d. Servicios que se prestan a las dependencias.

Considerando los servicios corporativos que proporciona la red de la empresa, se definen las siguientes condiciones:

- Los permisos de acceso para cada usuario (privilegios) fueron limitados por los jefes de cada área junto con el área de tecnologías para permitir exclusivamente los servicios necesarios para cumplir las tareas respectivas por departamento.
- El jefe de departamento de cada área, puede solicitar el bloqueo de acceso a *Internet*; acceso o bloqueo de un servicio adicional realizando una solicitud al departamento competente y al administrador de la red.
- Los usuarios corporativos o usuarios externos temporales de la red tienen pleno derecho de llamar al administrador o a sus subalternos, si presentan algún problema en cuanto a la operación de la red.
- Cabe destacar que la red cuenta con equipos de autorización, proporcionando un acceso restringido a los servicios corporativos dependiendo del tipo de privilegios de usuario y monitoreando accesos autorizados y no autorizados, de manera que el usuario accederá exclusivamente a los servicios autorizados dependiendo de su perfil.
- Todo empleado tiene la facultad de informar a quien corresponda si el técnico a cargo de la red no cumple con sus obligaciones, en cuanto al soporte.
- De manera similar la o las personas que intenten acceder a la red o a servicios de red no autorizados, se someterán a las sanciones respectivas notificadas por el área de tecnologías y ejecutadas por el área de Talento Humano.

e. Tipo de acceso a los equipos de red

Los equipos de red están conformados por *switches, routers*, *access points*, WLC, ASA, y otros. Y el acceso se delimita de la siguiente manera:

- El acceso físico a los equipos de red será exclusivo para el administrador de la red o subalterno del área de tecnologías de la sección de administración de la red y los técnicos de las empresas encargadas de los mantenimientos preventivos pero con la respectiva autorización interna previa a la ejecución (para la revisión técnica de la situación física de la red en algún bloque o matriz de la empresa, se deberá informar de manera escrita previamente al jefe de dicho departamento).
- Si se suscitare un daño parcial o general en la red; se realizará inmediatamente una auditoría externa, en base a los resultados se determinará si existe o no responsables; los implicados enfrentarán las sanciones estipuladas.

f. De los accesos permitidos

Una vez determinados estos parámetros se pueden definir los niveles de acceso, como se indica a continuación:

- Está permitido el acceso a páginas web cuyo contenido esté enfocado a fines laborales o de análisis comercial.
- Queda prohibido el acceso a todas aquellas páginas relacionadas con compras en línea, pago de valores adicionales, descargas de datos de forma continua, páginas de chat, redes sociales y aquellas con contenido obsceno o de entretenimiento.

g. De los impedimentos de acceso

Bajo ningún concepto se podrán instalar equipos que no los haya registrado el administrador de la red, la intromisión será sancionada. Gracias a la incorporación de Cisco ISE y su monitoreo en tiempo real se obtiene reportes continuos de todo dispositivo conectado a la red, NAD conectado (muestra información detallada, como

su *hostname* (nombre asignado al equipo de conectividad) relacionado con el bloque en el que encuentra y puerto en el que se encuentra conectado, y la dirección MAC.

h. Obligaciones

Es obligación del administrador de la red realizar por lo menos dos revisiones mensuales al *software* y *hardware* de la red en todas las dependencias de la empresa, y de encontrarse algún daño se deberá notificar como máximo a las 48 horas de encontrado, con el fin de acortar el máximo posible los daños en la red.

3.1.1.1.1 Sanciones generales

En el caso de ir en contra o no acatar las políticas expuestas en los LINEAMIENTOS GENERALES y DE LOS ACCESOS PERMITIDOS; la institución se encargará de aplicar las sanciones respectivas (Talento Humano), o si el caso lo amerita la empresa tendrá la obligación de imponer ante los organismos de ley las demandas pertinentes.

3.1.1.1.2 Seguridad perimetral de la red

Debido a que la red de datos se encuentra conectada al *Internet*, a través de dos ISP (TELCONET y *LEVEL* 3, como principal y respaldo respectivamente), la información que se maneja es sensible y vulnerable, por lo tanto la empresa cuenta con equipos de seguridad perimetral, que se encargan del control de acceso desde redes externas, así como desde el interior de la red, a través de la definición de conjunto de reglas que se establecen para permitir o denegar el flujo de tráfico interno y externo.

El filtrado de paquetes analiza parámetros como dirección de origen y destino, protocolo, puerto de origen y destino, otros. Ofrecen defensa de diferentes capas, a fin de proteger la red, permitiendo la inspección del protocolo de sitio a sitio y acceso seguro remoto VPN, previene de intrusos en línea, proporcionando servicio avanzado de *firewall* para aplicaciones. Los equipos más importantes adquiridos previamente por la empresa para protección tanto interna como externa, los podemos observar en la tabla 3.15.

MODELO DE FIREWALL	UBICACIÓN
CISCO ASA5505	MATRIZ
CISCO ASA5520	MATRIZ
CISCO ASA5510	BLOQUE 7
PIX-501	BLOQUE 12 EPF
CISCO ASA 5510	BLOQUE 12 EPF
PIX 515E	BLOQUE 12 PAÑACOCHA
CISCO ASA 5510	BLOQUE 21
PIX 515E	BLOQUE 21
CISCO 5525	BLOQUE 63

Tabla 3.15 Modelos de *firewall* de la empresa

3.1.1.1.3 Definición de perfiles de usuarios (perfiles de acceso)

Para la definición y ejecución de permisos de acceso se utiliza un servidor de directorio activo *root* y *child*, en el cual se definen grupos de usuarios, y sobre ellos, cuentas de usuarios vinculados, junto a directivas de grupo (GPO - grupo de políticas de grupo) se configura exclusivamente cuáles son los permisos otorgados sobre el sistema operativo dependiendo del tipo de usuario corporativo o invitado. Los servicios que proporciona la empresa son:

- Servidor *Exchange* 2010 *Mailbox*
- Servidor *Exchange* 2010 CAS *HUB (Client Access Server)*
- Servidor de Archivos
- Servidor SQL 2008
- *Domain Controller Child*
- *Domain Controller Root*
- DNS Perimetral
- Servidor de impresión
- Servidor MS SCCM
- Servidor MS WSUS
- Servidor *BlackBerry Enterprise Server*

- MS *Key Management Service*
- Servidor SCOM *Reporting Services*

En general, todo usuario corporativo independientemente del bloque al que pertenezca tiene acceso al servicio de correo. Los usuarios corporativos (empleados o directivos) se dividen en las siguientes áreas de trabajo junto a los servicios específicos que requieren y se encuentran autorizados:

a. Gerencia.

Única área que cuenta con todos los permisos a todos los servicios de la empresa, sin ninguna restricción. Incluye acceso a *Internet* ilimitado. Esta área se asigna al grupo UCEspecialesL1.

b. Staff de Gerencia.

Esta área tiene acceso a *Internet* limitado (páginas restringidas, sin acceso a redes sociales), correo institucional, repositorio de almacenamiento asignado. Esta área se asigna al grupo UCEspecialesL2.

c. Proyectos Especiales.

Esta área no tiene acceso a *Internet*, pero si tiene acceso al correo institucional, repositorio de almacenamiento asignado. Se establecerán permisos adicionales dependiendo del proyecto. Esta área se asigna al grupo UEEspecialesL1.

d. Soporte Técnico y Operativo.

Esta área si tiene acceso a *Internet* limitado, tiene acceso a correo institucional, repositorio de almacenamiento asignado, credenciales de acceso a los servidores de la empresa. Esta área se asigna al grupo ATecnologíaL1.

e. Soporte y Servicios Corporativos.

Esta área no tiene acceso a *Internet*, tiene acceso a correo institucional, repositorio de almacenamiento asignado, credenciales de acceso a los servidores del bloque local

en el que encuentre. Cabe recalcar que los permisos son únicamente locales, no podrán acceder al de otros bloques. Esta área se asigna al grupo ATecnologíaL2.

f. Exploración.

Esta área no tiene acceso a *Internet*, no se asignan permisos de acceso a otros servicios que no sean del bloque al que pertenece, tienen acceso a correo institucional, repositorio de almacenamiento asignado, credenciales de acceso a los servidores del bloque local en el que se encuentren. Más bien sus permisos están relacionados con la red de control SCADA. Esta área se asigna al grupo UCControlL1.

g. Desarrollo.

Esta área no tiene acceso a *Internet*, no se asignan permisos de acceso a otros servicios que no sean del bloque al que pertenece, tienen acceso a correo institucional, repositorio de almacenamiento asignado, credenciales de acceso a los servidores del bloque local en el que se encuentren. Más bien sus permisos están relacionados con la red de control SCADA. Esta área se asigna al grupo UCControlL2.

h. Operaciones.

Esta área no tiene acceso a *Internet*, no se asignan permisos de acceso a otros servicios que no sean del bloque al que pertenece, tienen acceso a correo institucional, repositorio de almacenamiento asignado, credenciales de acceso a los equipos de monitoreo y control del bloque local en el que se encuentren. Esta área está conformada por los empleados en general de empresa, se asigna al grupo UCEspecialesL3.

i. Offshore.

Esta área tiene acceso a *Internet* restringido, no se asignan permisos de acceso a otros servicios que no sea el acceso a correo institucional, repositorio de almacenamiento asignado.

Esta área se asigna al grupo UEEspecialesL2.

3.1.2 DISEÑO DE LA ARQUITECTURA DE LA PLATAFORMA CISCO ISE

En esta sección, se detalla la arquitectura de control de acceso de *Cisco Identity Service Engine - ISE* elegida para la red de la empresa (basada en la recomendación de diseño de Cisco ISE según el número de dispositivos finales que debe autenticar), la misma distribuye sus operaciones en roles que cumplen funciones específicas relacionadas con AAA.

El mismo nodo puede desempeñar varios roles a la vez (utilizado en redes pequeñas) o uno en específico (utilizado en redes medianas y grandes), en nuestro caso se trata de una red grande con más de 8000 usuarios (cada usuario normalmente tiene más de un dispositivo final).

En la figura 3.6 se indica la arquitectura recomendada de Cisco ISE para redes grandes en relación al número de dispositivos finales y cuando su topología es de tipo estrella (matriz-sucursales), que será la elegida en el presente proyecto.

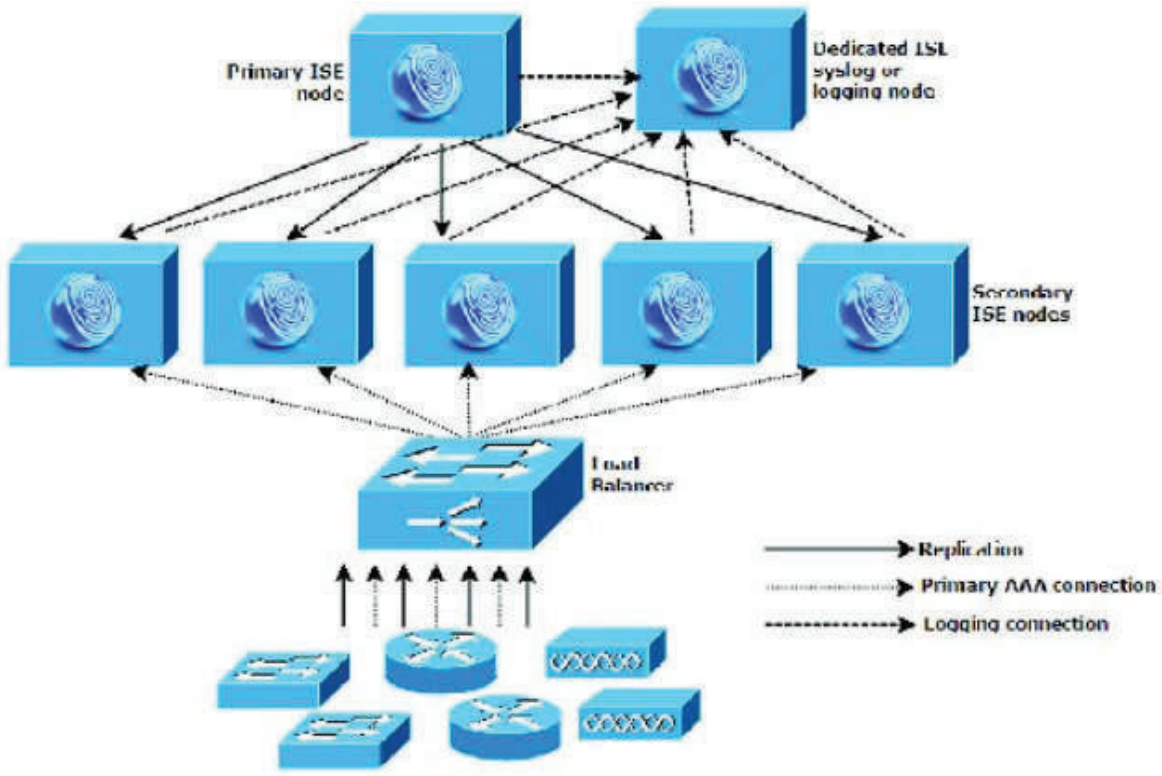

Figura 3.6 Arquitectura Cisco ISE para redes medianas y grandes [22]

Cada equipo cumple un rol en específico, Administrador-ADM, Monitoreo-MON, Políticas de servicio (PSN); tomando como base el análisis de la topología de red, dimensionamiento de usuarios, ubicación geográfica de cada bloque, y considerando la carga que soportará el equipo (ver tabla 3.16) y siguiendo las recomendaciones de diseño de Cisco, se adopta el modelo de redundancia ADM(Primario)+MON(Secundario), ADM(Secundario)+MON(Primario), un PSN de respaldo centralizado con 5 nodos PSN en 5 bloques en las zonas con mayor número de usuarios, en resumen este modelo soporta 2 nodos Administrador-ADM (Primario-Secundario), 2 nodos Monitoreo-MON (Primario-Secundario) y 5 nodos Políticas de servicio-PSN.

TIPO DE IMPLEMENTACIÓN	NÚMERO DE NODOS/PERSONAS	PLATAFORMA DEL DISPOSITIVO	NÚMERO MÁXIMO DE NODOS DE POLÍTICAS DE SERVICIO	NÚMERO DE DISPOSITIVOS FINALES ACTIVOS
Pequeña	Nodos independientes o redundantes (2) con roles de Administración, Servicio de políticas y Monitoreo habilitados.	Cisco ISE 3300 Series (3315, 3355, 3395)	0	Máximo de 2,000 dispositivos finales
		Cisco ISE 3415	0	Máximo de 5,000 dispositivos finales
		Cisco ISE 3495	0	Máximo de 10,000 dispositivos finales
Mediana	Administración y Monitoreo de personas en nodos únicos o redundantes. Máximo de 2 nodos de Administración y Monitoreo.	Cisco ISE-3355 or Cisco SNS 3415. Equipo de Administración y Monitoreo	5	Máximo de 5,000 dispositivos finales
		Cisco ISE 3395 or Cisco SNS 3495. Equipo de Administración y Monitoreo	5	Máximo de 10,000 dispositivos finales
Grande	Nodo / nodos de Administración dedicada. Máximo de 2 nodos de Administración.	Cisco ISE 3395. Equipo de Administración y Monitoreo	40	Máximo de 100,000 dispositivos finales
	Nodo / nodos dedicados de Monitoreo. Máximo de 2 nodos de Monitoreo.	Cisco SNS 3495. Equipo de Administración y Monitoreo	40	Máximo de 250,000 dispositivos finales

Tabla 3.16 Recomendaciones de dimensionamiento de Cisco ISE [22]

3.1.2.1 Descripción de equipos Cisco ISE

Una vez definida la arquitectura de la plataforma Cisco ISE, es necesario determinar los tipos de equipos (rol y modelo) dependiendo del número de dispositivos que simultáneamente pueden autenticar y el rol que deben realizar.

- Rol ADM
- Rol PSN
- Rol MON

Con la información detallada en la tabla 3.16, se determina la arquitectura (conexión, números de equipos máximo de cada rol y modelo de equipo de rol ADM-MON), para la elección del modelo del equipo de rol PSN, se utiliza la tabla 3.17, que proporciona una guía de elección de equipo de Cisco ISE del nodo *Policy Service*, que debe ser adquirido dependiendo del número de dispositivos finales activos.

Form Factor	Platform Size	Appliance	Maximum Endpoints
Physical	Small	Cisco ISE-3315	3,000
		Cisco SNS-3415	5,000
	Medium	Cisco ISE-3355	6,000
	Large	Cisco ISE-3395	10,000
		Cisco SNS-3495	20,000
Virtual Machine	Small/Medium/Large	Comparable to physical appliance	3,000 to 20,000

Tabla 3.17 Recomendaciones de dimensionamiento del nodo *Policy Service* [22]

Por tanto, la ubicación y modelos de los equipos de Cisco ISE que se utilizan en el presente rediseño, se indican en la tabla 3.18.

N°	UBICACIÓN	CAMPO	NUMÉRO DE USUARIOS CONSIDERANDO CRECIMIENTO	ROL CISCO ISE	MODELO ISE
1	BLOQUE 07	OESTE	805	PSN	Cisco ISE-3315
2	BLOQUE 18	OESTE	840		
3	BLOQUE 21	OESTE	713		
4	BLOQUE 15	CENTRO	828	ADMINISTRATOR (1)	Cisco ISE-3315
				MONITOR (2)	Cisco ISE-3395
				PSN	Cisco ISE-3315
5	BLOQUE 12	CENTRO	748		
6	BLOQUE 31	ESTE	978	PSN	Cisco ISE-3315
7	BLOQUE 43	NORTE	1840		
8	BLOQUE 63	NORTE	1380	PSN	Cisco ISE-3315
9	MATRIZ	QUITO	460	ADMINISTRATOR (2)	Cisco ISE-3315
				MONITOR (1)	Cisco ISE-3395
10	BLOQUE 1	LITORAL	138	PSN (C)	Cisco ISE-3355
11	BLOQUE 6	LITORAL	173		

Tabla 3.18 Descripción modelo y roles de los equipos Cisco ISE que conforman la solución de control de acceso

3.1.2.2 Topología resultante del rediseño de autenticación con la plataforma Cisco ISE

En la figura 3.7 se presenta el esquema de implementación resultante del rediseño de autenticación a través de la plataforma Cisco ISE.

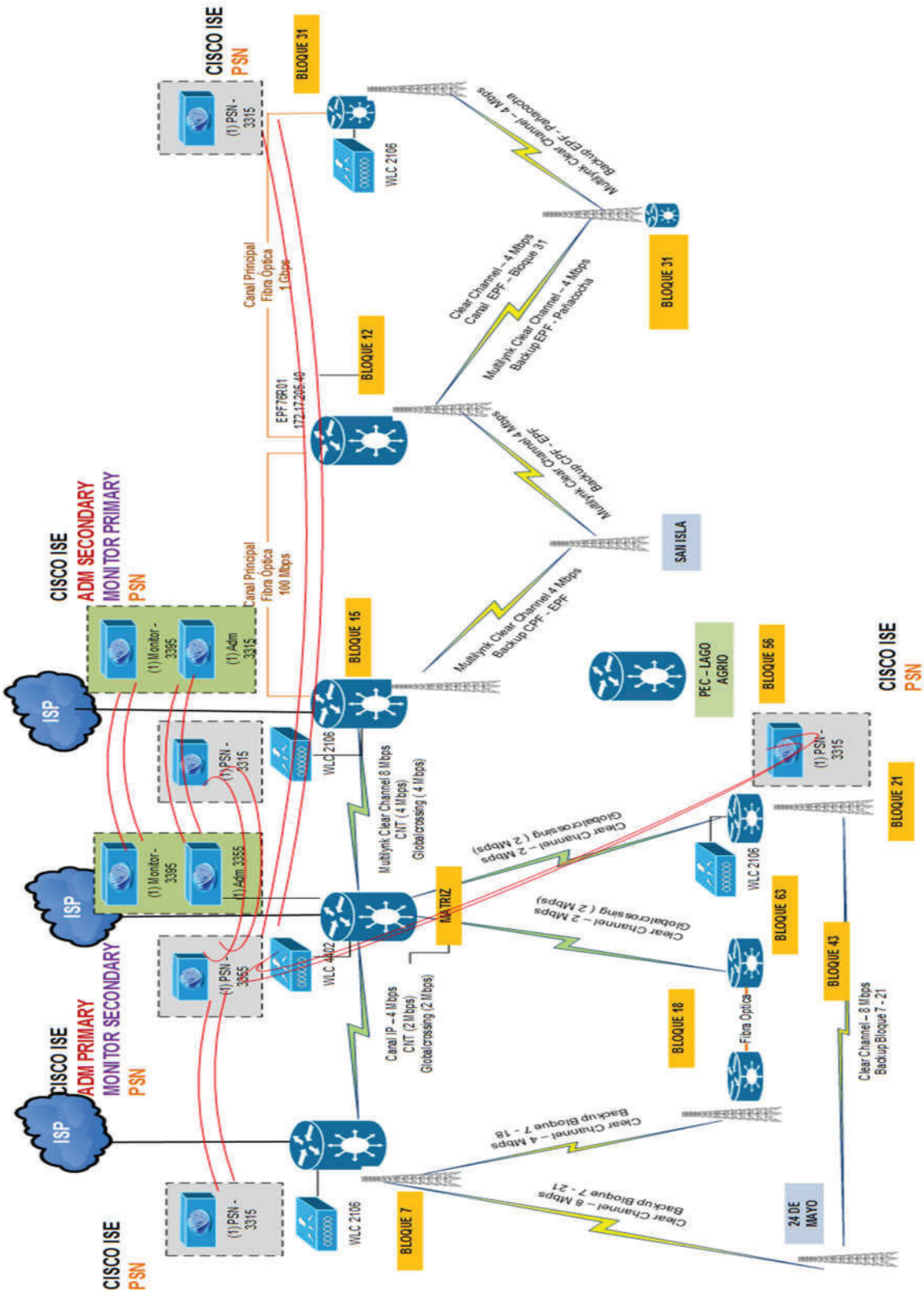

Figura 3.7 Esquema de implementación de Autenticación con Cisco ISE

3.1.2.3 Políticas de seguridad definidas en Cisco ISE

El ISE permite monitorear clientes y dispositivos conectados a nuestra red corporativa, a manera de una localidad centralizada con el rol *Monitoring* (*appliance* Cisco ISE 3395) permite realizar el *accounting* de los usuarios y dispositivos que intentar acceder a la red cuando logran o no autenticarse en el ISE que valida las credenciales de los usuarios de los grupos configurados en el *Active Directory* (AD) de la empresa (ver figura 3.8). El perfilamiento permite determinar de qué tipo de dispositivo se trata, analizando el tráfico que genera el dispositivo bajo ciertos criterios basados en ciertas características activadas en el ISE, prueba DHCP, HTTP, RADIUS, DNS, *traps* y *queries* SNMP, *scans* Nmap y Cisco IOS *NetFlow*.

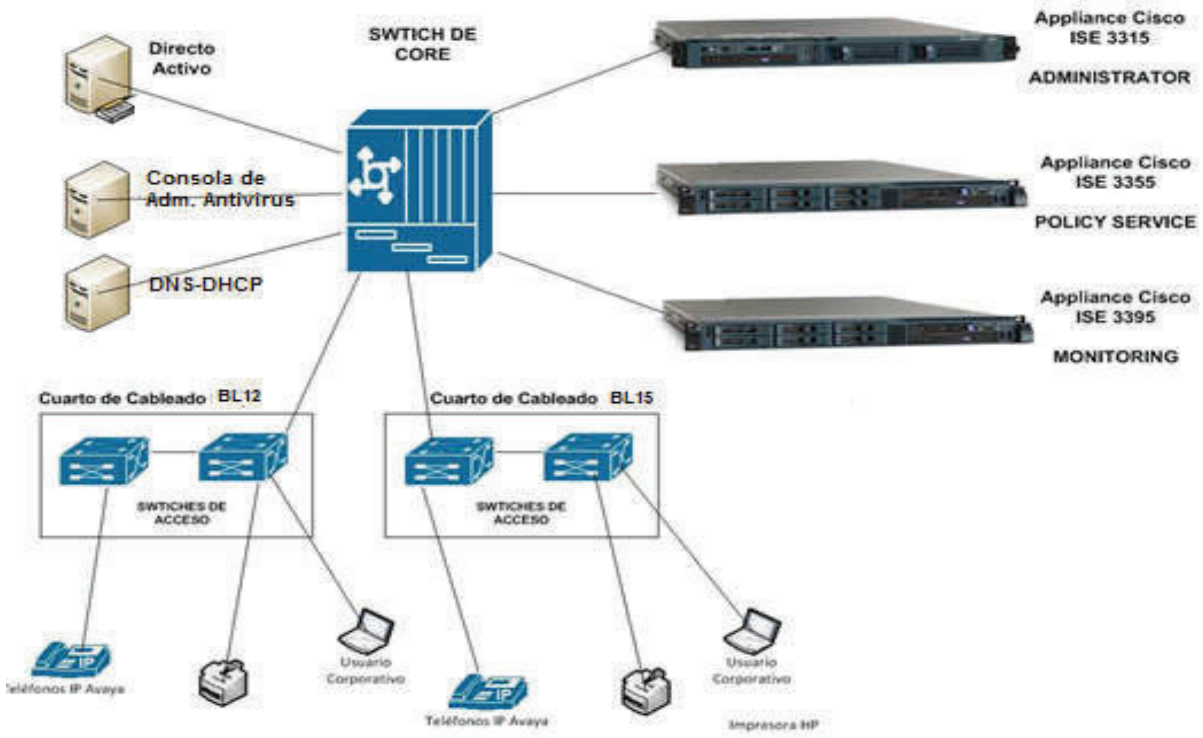

Figura 3.8 Diagrama de conexión de endpoints con los equipos Cisco ISE

En esta sección se explica la ejecución de las políticas para "*Authentication*", *"Authorization", "Profiling" y "Posture"* que se implementarán en los *appliance* Cisco ISE, lo que permitirá la correcta operación del sistema de autenticación ISE en la red de la empresa. Cada política incorpora un control independiente junto con una

ejecución restrictiva y sucesiva, que implica que el incumplimiento de una, restringe la revisión de la siguiente (ver figura 3.9). El detalle de la configuración y control de acceso basado en políticas definidas en el ISE, se describen en la sección 3.2.3.2.7 .

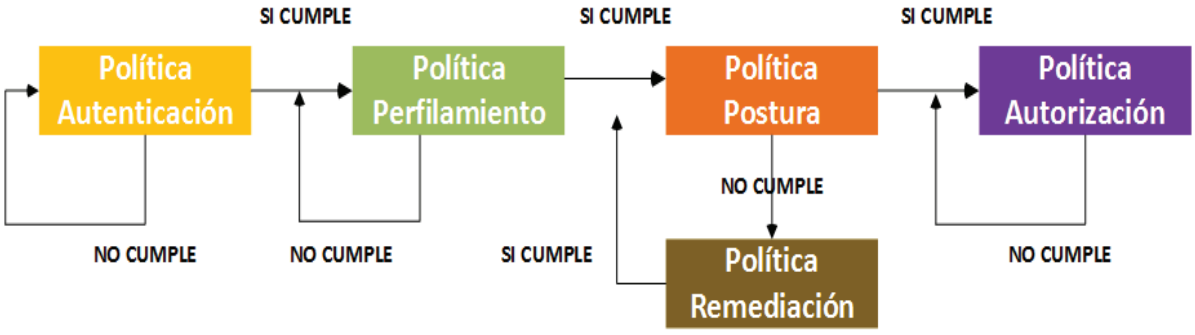

Figura 3.9 Orden de ejecución de políticas en el Cisco ISE

Gracias al control explícito de ingreso de credenciales que se envían encriptadas al NAD y posteriormente al ISE para verificación a través de la entidad de identidad externa (AD), se verifica al usuario, a continuación se verifica el dispositivo, su perfil, postura, si no lo cumple se direcciona para la ejecución de la remediación, y finalmente se asignará finamente el acceso a la red, con los permisos de acceso a los servicios basado en el tipo de usuario logeado. Previa a la implementación, la mejor práctica para probar la nueva solución es la realización de pruebas en un ambiente controlado.

3.2 IMPLEMENTACIÓN DEL PROTOTIPO

En esta sección se describirán los procedimientos necesarios para la implementación de un prototipo de la red que simulará dos secciones de dos bloques de la empresa, una vez que se hayan configurado los dispositivos y servicios involucrados, integrando componentes de *hardware* y *software* se ejecutarán las políticas de autenticación, autorización y perfiles tanto para la red cableada como inalámbrica, con la remediación respectiva, y BYOD para el acceso tipo INVITADO.

3.2.1 TOPOLOGÍA LÓGICA Y FÍSICA

La topología física y lógica que presentará el prototipo se muestra en la figura 3.10.

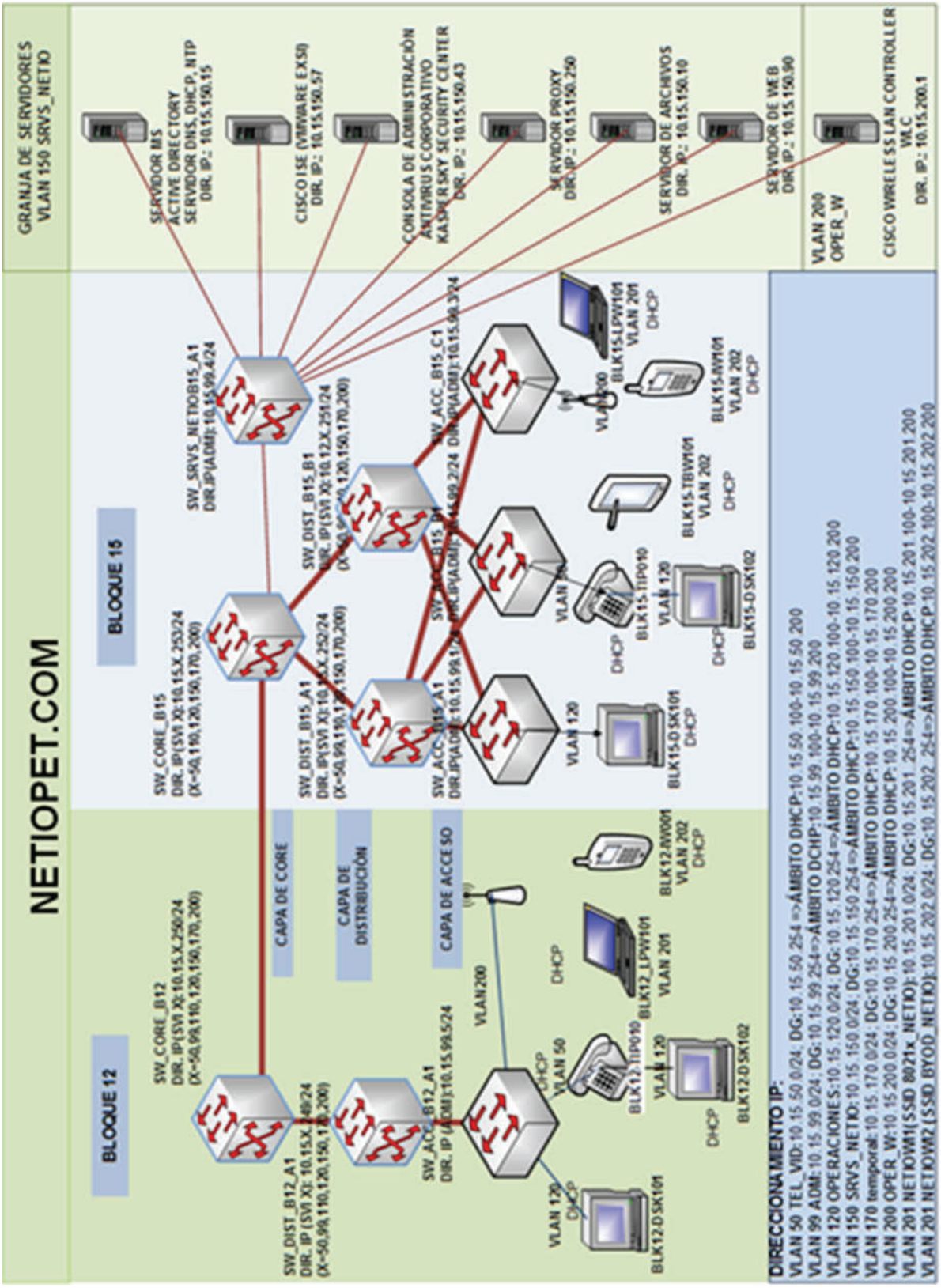

Figura 3.10 Topología Física del Prototipo

Para el desarrollo del prototipo se implementará el esquema de direccionamiento IP y VLAN; que se detalla en la tabla 3.19.

VLAN ID	DESCRIPCIÓN	DEFAULT GATEWAY (IP VIRTUAL-HSRP)	RANGO DE ASIGNACIÓN DIRECCIONAMIENTO IP	SERVIDOR DNS	SERVIDOR PROXY
48	TELEFONÍA IP Y VIDEO	10.15.48.254	10.15.48.1 A 10.15.51.254 (DHCP)	10.15.150.15	10.15.150.250
99	ADMINISTRACIÓN	10.15.99.254	10.15.99.1 A 10.15.99.254 (ESTÁTICO)	10.15.150.15	10.15.150.250
108	SERVICIO L3	10.15.108.254	10.15.108.1 A 10.15.111.254	10.15.150.15	10.15.150.250
120	USUARIOS	10.15.120.254	10.15.120.1 A 10.15.123.254 (DHCP)	10.15.150.15	10.15.150.250
150	SRVS DE TI	10.15.150.254	10.15.150.1 A 10.15.150.254 (ESTÁTICO)	10.15.150.15	10.15.150.250
170	TEMPORAL DE OPERACIÓN	10.15.170.254	10.15.170.1 A 10.15.170.254 (DHCP)	10.15.150.15	10.15.150.250
200	RED INALÁMBRICA ADM	10.15.200.254	10.15.200.1 A 10.15.200.254 (DHCP -ESTÁTICO)	10.15.150.15	10.15.150.250
777	VLAN NATIVA	NO APLICA	NO APLICA	10.15.150.15	10.15.150.250
201	WIRELESS 1 8021x	10.15.201.254	10.15.201.1 A 10.15.201.254 (DHCP)	10.15.150.15	10.15.150.250
202	WIRELESS 1 BYOD	10.15.202.254	10.15.202.1 A 10.15.202.254 (DHCP)	10.15.150.15	10.15.150.250

Tabla 3.19 Esquema de direccionamiento IP para las VLAN en el Prototipo.

3.2.2 INSTALACIÓN Y CONFIGURACIÓN DE DISPOSITIVOS

Para la implementación del prototipo se instalarán y configurarán los equipos de conectividad, dispositivos finales, servidores (habilitación de servicios o roles que sean necesarios, que incluyen Directorio Activo, Entidad Certificadora (CA), DNS, DHCP,

NTP) para probar el funcionamiento de la autenticación a través de Cisco ISE y con ello, el control de acceso a servicios corporativos.

3.2.2.1 Configuraciones de dispositivos finales

Se encuentran en la capa de acceso e interactúan directamente con los usuarios, para el desarrollo del prototipo se utilizarán cuatro computadoras de escritorio, dos laptops, dos teléfonos IP, dos *Smartphones* (marca Sony y IPhone) y una *tablet* (marca Samsung).

Las computadoras de escritorio reciben los siguientes nombres BLK12-DSK101, BLK12-DSK102, BLK15-DSK101 y BLK15-DSK102, basados en la norma de etiquetado de la empresa (dependiendo del bloque, el tipo de dispositivo y la numeración correspondiente), las *laptops* BLK12-LPW101 y BLK15-LPW101, las cuales tendrán instalado el sistema operativo *Windows* 7, 8 o 10.

El servidor DHCP permitirá a cada computador obtener de forma automática una dirección IP, máscara de subred, puerta de enlace predeterminada y dirección DNS inicialmente de la VLAN temporal (VAN 170), luego del proceso de autenticación correcto le asignará una dirección IP, máscara de subred, puerta de enlace predeterminada y dirección del servidor DNS, se utilizarán dos teléfonos IP físicos de marca Panasonic (BLK12-TELIP101, BLK12-TELIP101 respectivamente), dos *Smartphones* (BLK12-SF101, BLK15-SF101) y una *tablet* con el sistema operativo *Android* (BLK12-TB101), finalmente todos los dispositivos anteriormente descritos obtienen su direccionamiento IP de forma dinámica a través de un servidor DHCP dedicado.

3.2.2.1.1 Configuración de computadoras de escritorio

Las computadoras que se utilizarán en el prototipo serán de marca Intel, Compaq; las especificaciones generales de estos dispositivos se encuentran en el Anexo C7. La configuración de cada computador que se conectará de manera cableada a la red de la empresa, se detalla continuación:

- Debe iniciar sesión como usuario tipo Administrador, para realizar cambios en el Sistema Operativo. Iniciar el servicio ***Detección automática de redes cableadas***, ingresar a la consola de Administración del Equipo (clic derecho en el icono de equipo, elegir Administrar), ingresar a Servicios, elegir servicio Detección automática de redes cableadas, clic derecho sobre el servicio y elegir Propiedades, posteriormente elegir el inicio en Automático y posteriormente en Iniciar, cuando el Servicio se encuentre iniciado, hacer clic en Aplicar y Aceptar (ver Figura 3.11).

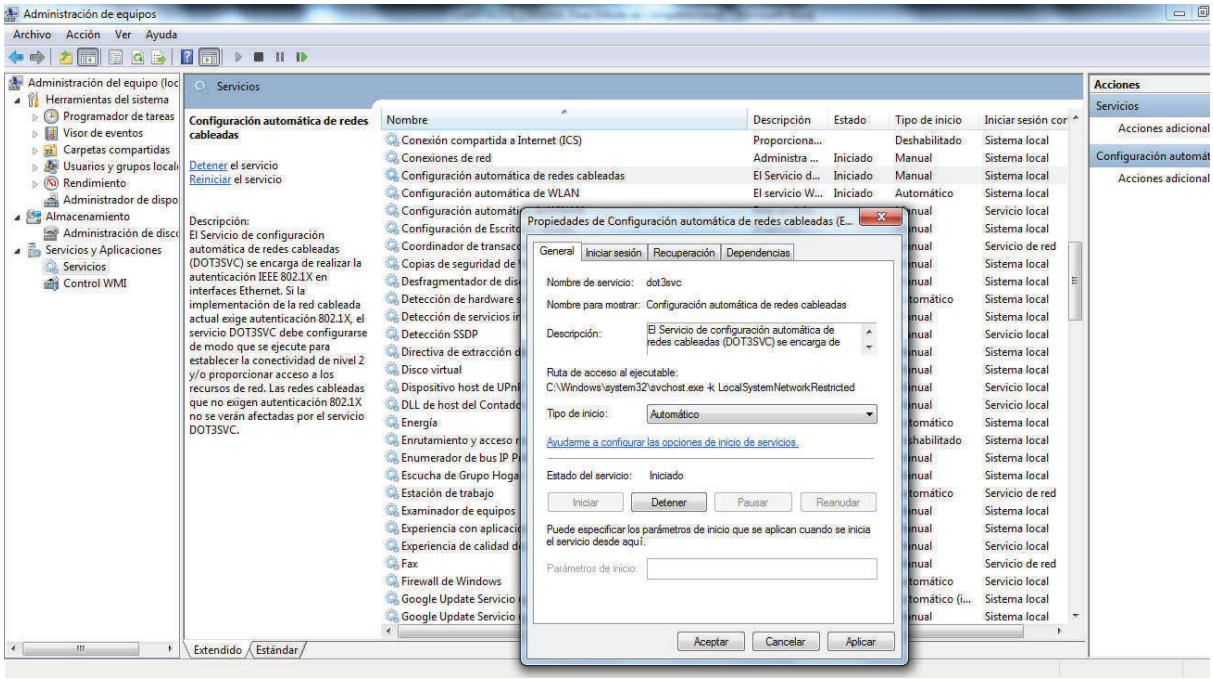

Figura 3.11 Activación de servicio de detección automática de redes cableadas

- A continuación ingresar a Panel de Control e ingresar a Redes y Recursos Compartidos, luego a Cambiar configuración del adaptador, hacer clic derecho sobre la tarjeta de red cableada, y clic en Propiedades. Al activar el servicio anteriormente descrito aparecerá una nueva pestaña de configuración en la tarjeta de red, ***Autenticación***.
- Hacer clic en el recuadro junto a Habilitar autenticación 802.1x, luego elegir Microsft EAP protegido (PEAP) como método de autenticación de red, y hacer clic en Configuración. Aparecerá una nueva ventana en la que se elegirá el

método de autenticación a Contraseña segura (EAP-MSCHAP v2), luego hacer clic en configurar y activar el recuadro para usar automáticamente como usuario y contraseña las ingresadas al inicio de sesión y luego clic en aceptar.

- En la pestaña de autenticación, ingresar a configuración adicional, en la nueva ventana activar la casilla de Especificar modo de autenticación y definirla a ***Autenticación de usuario o equipos***, finalmente hacer clic en aceptar.
- En la ventana de propiedades de Conexión de área local, Propiedad de protocolo de *Internet* versión 4, seleccionar Obtener una dirección IP automáticamente, así mismo seleccionar Obtener la dirección del Servidor DNS automáticamente y finalmente Clic en Aceptar.
- Instalar el programa *nacagentsetup-win*, que será el encargado de la revisión de cumplimiento o no de la postura.
- A continuación las computadoras deben ser registradas en el Directorio Activo, al dominio ***netiopet.com***, el nombre de cada computadora depende del bloque o campo en el que se encuentre, y el tipo de equipo, por ejemplo a una computadora de escritorio en el bloque 12, el nombre asignado será BLK12-DSK101 (ver figura 3.12)

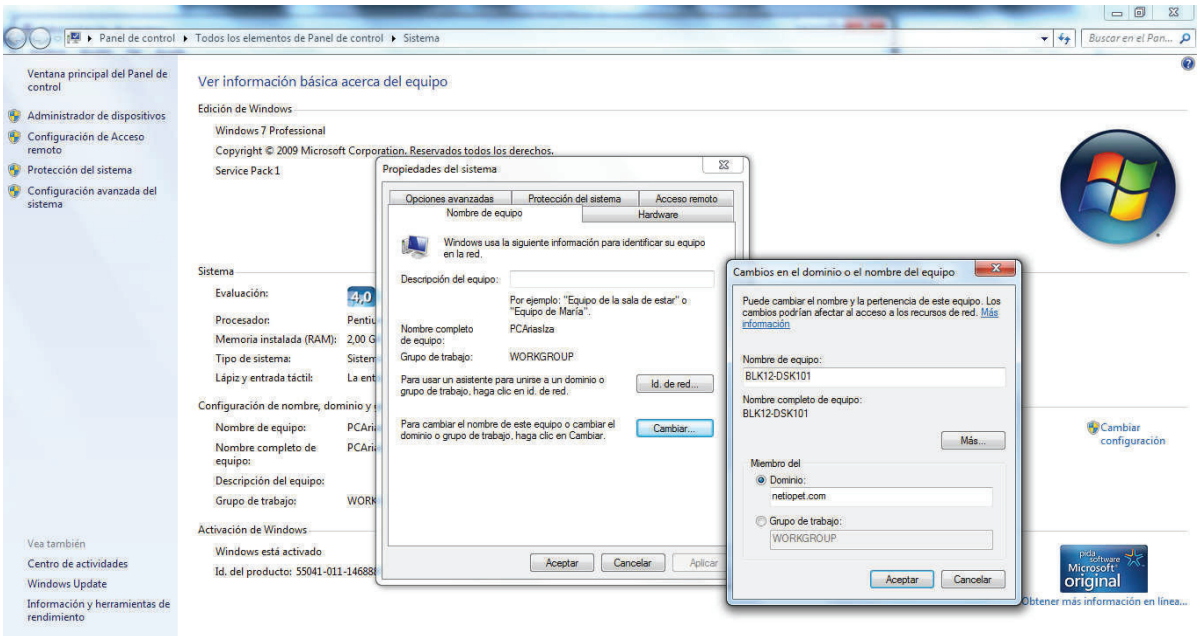

Figura 3.12 Vinculación del computador al dominio netiopet.com

- Al hacer clic en aceptar, el computador probará conexión al *Active Directory* con el nombre de dominio netiopet.com, de manera que el servidor de DNS debe estar correctamente definido y alcanzable para que pueda realizar la traducción correspondiente y localizar al AD, posteriormente solicitará un usuario definido en el AD y una contraseña que posea permisos para agregar equipos al AD, si las credenciales y permisos son válidos aparecerá un mensaje que el equipo se unió correctamente al dominio. Y posteriormente le pedirá un reinicio del equipo.
- Después del reinicio, el sistema le pedirá ingresar credenciales de un usuario normal registrado en el AD para iniciar sesión.

3.2.2.1.2 Configuración de las laptops

Las laptops que se utilizarán en el prototipo serán de marca Dell, COMPAQ; las especificaciones generales de estos dispositivos se encuentran en el Anexo C8 .

- Debe iniciar sesión como usuario tipo Administrador, para realizar cambios en el Sistema Operativo.
- Instalar el programa *nacagentsetup-win*, que será el encargado de la revisión de cumplimiento o no de la postura.
- A continuación ingresar a Panel de Control e ingresar a Redes y Recursos Compartidos, luego a Cambiar configuración del adaptador, hacer clic derecho sobre la tarjeta de red cableada, y clic en Propiedades.
- En la ventana de propiedades de Conexión de área local, Propiedad de protocolo de *Internet* versión 4, seleccionar Obtener una dirección IP automáticamente, así mismo seleccionar Obtener la dirección del Servidor DNS automáticamente y finalmente Clic en Aceptar.
- Posteriormente, es necesario crear un perfil de red inalámbrica, ya que es necesaria la configuración de parámetros específicos de conexión hacia las redes inalámbricas 8021x_NETIO y BYOD_NETIO, pero también está disponible la detección automática de la configuración de la red inalámbrica. El acceso depende de las políticas de red de la empresa, en las mismas se definen el tipo de acceso, permisos, y dispositivos permitidos. Para este fin, ingresar a

Panel de Control, Centro de redes y recursos compartidos, Administrar redes inalámbricas, y clic en Agregar, y elegir crear un perfil de red manualmente, e ingresar los datos indicados en la figura, a continuación clic en Siguiente, y el perfil está creado (ver figura 3.13).

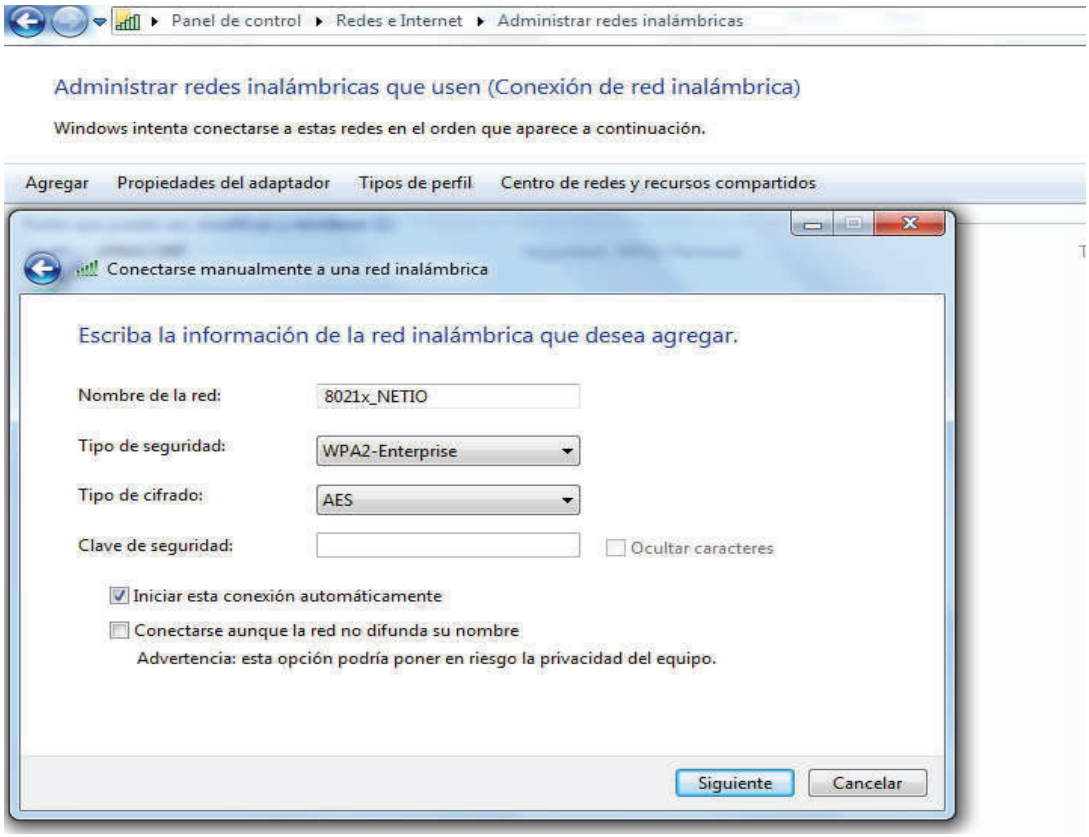

Figura 3.13 Creación del perfil de la WLAN 8021x_NETIO

- Para hacer cambios en el mismo, hacer clic derecho y elegir propiedades, y clic en la pestaña Seguridad.
- Elegir Microsft EAP protegido (PEAP) como método de autenticación de red, y hacer clic en Configuración:
- Aparecerá una nueva ventana en la que se elegirá el método de autenticación a Contraseña segura (EAP-MSCHAP v2), luego hacer clic en configurar y activar el recuadro para usar automáticamente como usuario y contraseña las ingresadas al inicio de sesión y luego clic en aceptar.

- En la pestaña de autenticación, ingresar a configuración adicional, en la nueva ventana activar la casilla de Especificar modo de autenticación y definirla a Autenticación de usuario o equipos, finalmente hacer clic en aceptar, el mismo procedimiento se realizará para la red inalámbrica BYOD_NETIO.

a. Configuración específica para la red inalámbrica con SSID 8021x_NETIO

Para la conexión a la red inalámbrica 8021x_NETIO (configurada para acceso exclusivo de laptops, a través de 802.1x excluyendo todo dispositivo móvil como por ejemplo teléfonos inteligentes, entre otros) es necesario que la laptop se encuentre registrada en el AD.

- A continuación las *laptops* deben ser registradas en el Directorio Activo, al dominio ***netiopet.com***, el nombre de cada laptop depende del bloque o campo en el que se encuentre, y el tipo de equipo, por ejemplo en el bloque 15, el nombre asignado será BLK15-LPW101.
- Al hacer clic en aceptar la *laptop* probará conexión al *Active Directory* con el nombre de dominio netiopet.com, de manera que el servidor de DNS debe estar correctamente definido y alcanzable para que pueda realizar la traducción correspondiente y localizar al AD, posteriormente solicitará un usuario definido en el AD y una contraseña que posea permisos para agregar equipos al AD, si las credenciales y permisos son válidos aparecerá un mensaje que el equipo se unió correctamente al dominio. Y posteriormente le pedirá un reinicio del equipo.
- Después del reinicio, el sistema le pedirá ingresar credenciales de un usuario normal registrado en el AD para iniciar sesión.

3.2.2.1.3 Configuración de los Smartphones y tablet

Los teléfonos inteligentes o *Smartphones* y la *tablet* que se utilizarán en el prototipo serán de marca Sony y Samsung con sistema operativo *Android*; las especificaciones generales de estos dispositivos se encuentran en el Anexo C9. Es necesario que la configuración de la tarjeta de red inalámbrica requerida en estos dispositivos se

encuentre funcionando correctamente y que obtenga direccionamiento IP de manera automática.

3.2.2.1.4 Configuración de teléfonos IP

Los teléfonos IP que se utilizarán en el prototipo serán de marca Panasonic; las especificaciones generales de estos dispositivos se encuentran en el Anexo C10.

La configuración de cada teléfono IP puede ser realizada de dos maneras, usando un navegador *Web*, conectándose a la dirección IP del mismo (para este tipo de acceso el teléfono IP debe estar reseteado y acceder a la dirección IP por defecto) o utilizando el menú de configuración del teclado.

En este caso, se utilizará el menú de configuración del teclado, las principales opciones que se pueden configurar a través del teclado son:

- La opción número 1 permite especificar si el direccionamiento IP será estático o dinámico mediante DHCP.
- Se configurará que reciba el direccionamiento mediante DHCP.

A través de un navegador *Web*, las principales opciones a configurar son:

- **Nombre de la cuenta:** Identifica la extensión desde la cual proviene una llamada, se puede colocar el número de extensión, nombre de la persona que utiliza el teléfono, departamento, y otros.
- **SIP server:** Dirección IP del servidor de telefonía IP.
- **SIP User ID:** Número de extensión, indicado en el archivo *sip.conf*.
- ***Authenticate ID*:** Número de extensión, indicado en el archivo *sip.conf*.
- ***Authenticate Password*:** Valor correspondiente al campo secret del archivo *sip.conf.*
- ***Name*:** Valor correspondiente al campo *callerid* del archivo *sip.conf*.

En la figura 3.14 se observa los parámetros generales a configurar en los teléfonos IP.

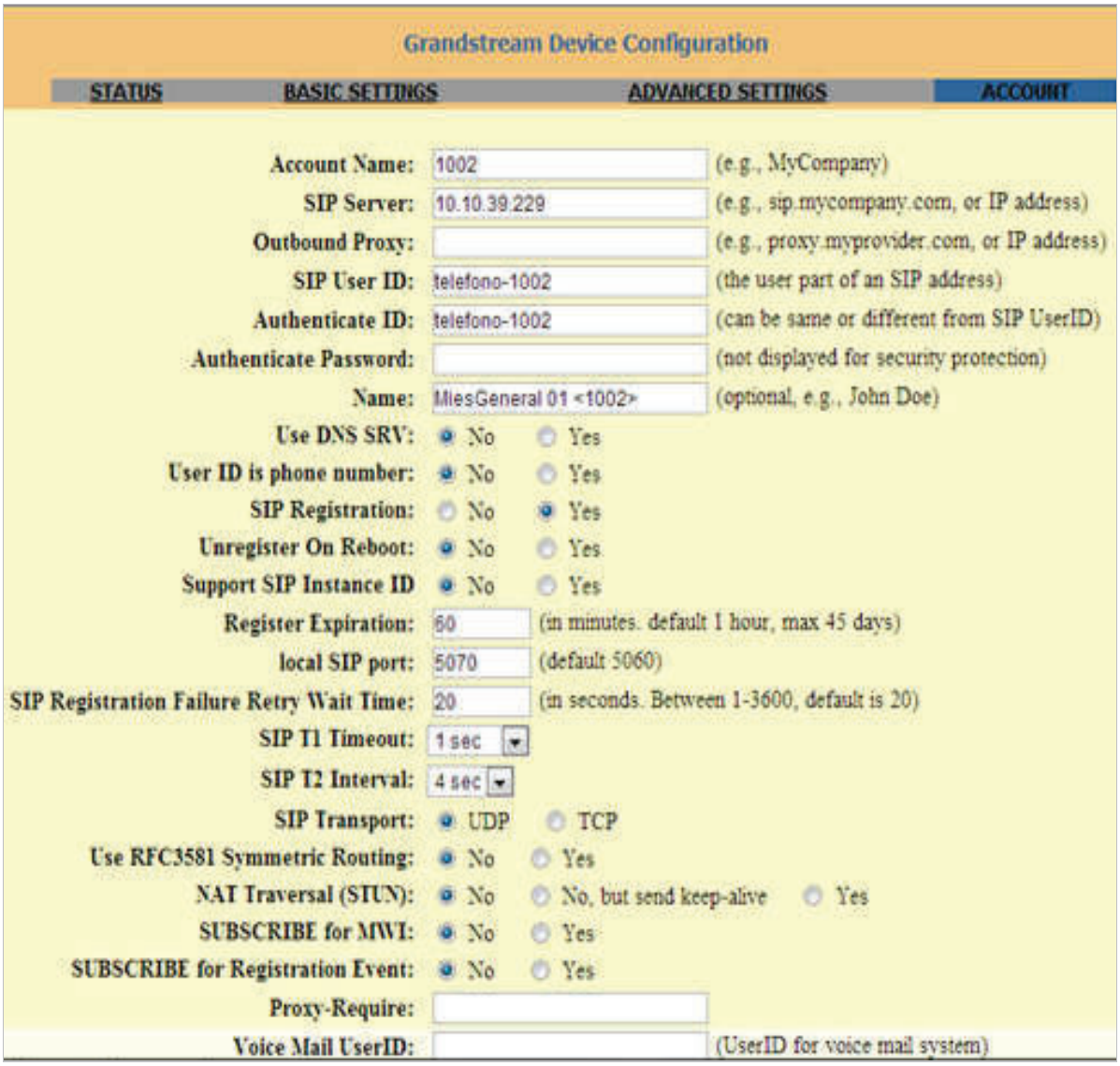

Figura 3.14 Interfaz *Web* de configuración de un teléfono IP

3.2.2.2 Configuración de equipos de conectividad (NAD)

En el desarrollo del prototipo se realizará la configuración de los equipos de conectividad de cada una de las 3 capas según las recomendaciones de arquitectura de Cisco (núcleo, distribución y acceso) como son: 5 *switches* de capa 3 (multicapa), 5 *switches* de capa 2. Además de un *Wirelless* LAN *Controller (WLC)* y 2 *Access Point*.

Las especificaciones técnicas de estos equipos respectivamente, se describen en el Anexo C11.

3.2.2.2.1 Configuración para Switches de la capa de acceso

Los *switches* multicapa que se utilizarán en el prototipo serán de marca Cisco, dos de los *switches* corresponden a la serie *Catalyst* 3760, asignados a la capa de núcleo, los tres restantes son *switches* que corresponden a la serie *Catalyst* 3560 POE-8, asignados a la capa de distribución.

Los cinco *switches* de capa 2 asignados a la capa de acceso corresponden a la serie *Catalyst 2960-S*; el archivo de configuración de los *switches* que conforman el prototipo se encuentra en el Anexo C12.

Básicamente los parámetros comunes a configurarse son los siguientes:

- Asignación de nombres a equipos y dispositivos de red *(Hostnames)*
- Encriptación de claves (consola, líneas VTY, acceso privilegiado)
- Configuración del dominio, servidor NTP
- creación usuario para acceso remoto únicamente a través de SSH
- Creación de VLAN (definición servidor y clientes VTP)
- Asignación de puertos a las respectivas VLAN
- Asignación de puertos troncales (VLAN permitidas, definición de la VLAN nativa)
- Configuración de `dhcp snooping` para evitar ataque de DHCP)
- Configuración de *STP* a *Rapid-PVST+*
- Configuración de una dirección IP para la interfaz de administración (SVI Administración)
- QoS básico de capa 2
- Definición del *default-gateway*.

Mientras que las configuraciones específicas para un *switch* de la capa de núcleo son:

- Asignación de una dirección IP para permitir la conexión *inter*-VLAN en las SVI en los *switches* multicapa
- Configuración de Redundancia de último salto a través del protocolo HSRP

- Configuración del protocolo de enrutamiento OSPF
- Configuración de *PortChannels* para los puertos troncales
- Configuración de retransmisión de información de direccionamiento por DHCP (`ip helper address` por *SVI*)
- Parámetros de Calidad de Servicio
- *Inter*-VLAN *routing*

Configuración específica para *switch* de distribución:

- Asignación de una dirección IP para permitir la conexión *inter*-VLAN a las SVI de los *switches* multicapa
- Configuración de Redundancia de último salto a través de protocolo HSRP
- Configuración de *PortChannels* para los puertos troncales
- Configuración de retransmisión de información de direccionamiento por DHCP (`ip helper address` por SVI)

Configuración específica para *switch* de acceso:

- Debe estar cargado la plantilla *SDM PREFER* `ip-routing`
- Configuración de *PortChannels* para los puertos troncales
- Las configuraciones del *switch* se basan básicamente en *ACL*, *RADIUS, AAA*, configuración de puertos, que son los parámetros principales que se requieren definir para la integración con el *Cisco ISE*.
- La plantilla general y detallada para todos los *switches* de acceso, a los cuales se conectan los dispositivos finales y en los que se van a realizar la validación de autenticación, ya fue detallada en la sección 3.1.1.1.3.

3.2.2.2.2 Configuración de la controladora de la LAN inalámbrica (WLC)

La controladora de la red inalámbrica (administración centraliza de puntos de acceso inalámbricos compatibles), mejor conocida como *Wireless* LAN *Controller* (WLC) que se utiliza en el prototipo será de la marca Cisco modelo 4400.

a. Configuración inicial

La WLC requiere de una configuración inicial a través del puerto de consola, en la que se define los parámetros principales de direccionamiento IP de la interfaz de administración y del puerto de servicio para activar el acceso vía *web*. El puerto que conecta a la WLC con el *switch* en la capa de distribución, debe estar configurado en modo troncal (`switchport mode trunk`).

Las configuraciones restantes se pueden realizar vía *web* apuntando a la dirección IP del puerto de servicio o de la interfaz de administración. Un requisito indispensable para la sincronización y vinculación correcta entre la WLC y el ISE es la definición de un servidor NTP, por tanto en la WLC se debe colocar correctamente la hora, fecha y la zona (ver figura 3.15).

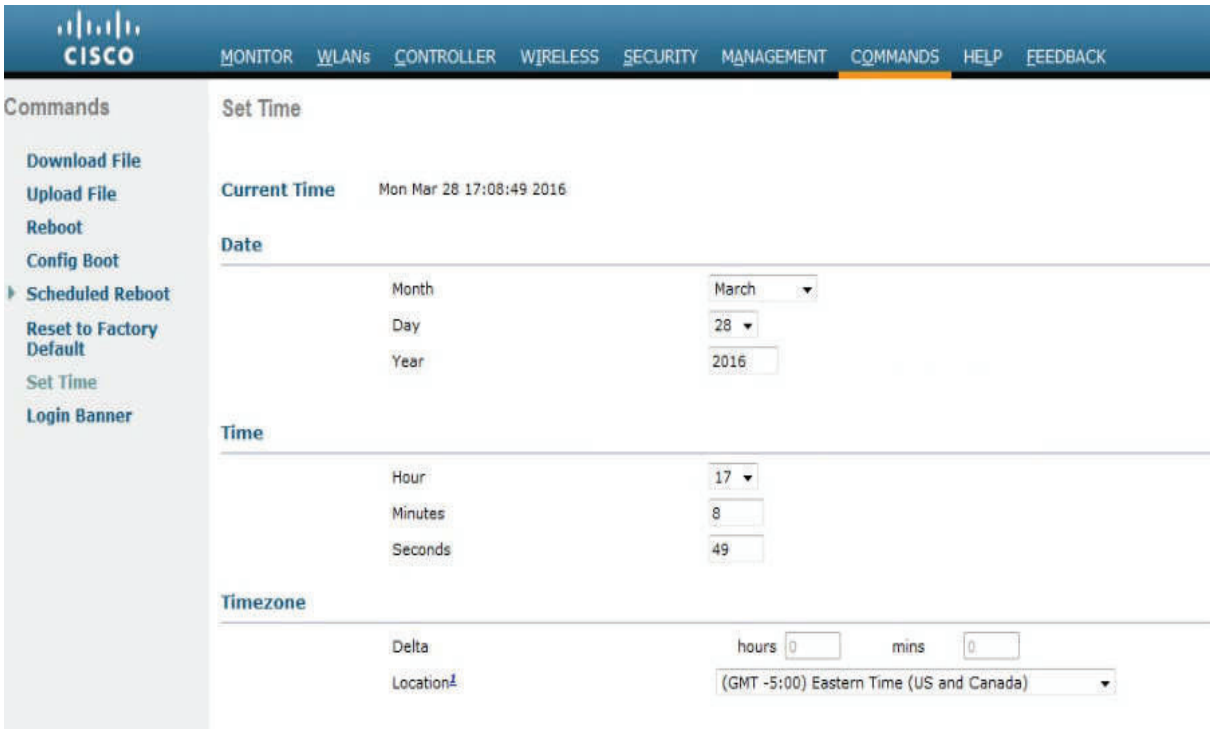

Figura 3.15 Configuración de fecha, hora y zona horaria en la WLC

Para la configuración de la WLC, se ingresa a la pestaña *CONTROLLER*, en la sección izquierda elegir *NTP Server*, e ingresar la dirección IP del servidor NTP configurado en la red (ver figura 3.16).

Figura 3.16 Configuración servidor NTP en la WLC

b. Configuración de redes inalámbricas en la WLC

En la WLC se configuran dos segmentos de red identificados con dos SSID (8021x_NETIO y BYOD_NETIO) cada uno de estos con su respectiva seguridad.

- La WLAN 8021x_NETIO permite acceso restringido a los servicios de red exclusivo a *laptops* de usuarios corporativos e invitados con credenciales dentro del AD y del ISE.
- La WLAN BYOD_NETIO permite acceso a teléfonos inteligentes, *Tablets y laptops* al acceso a *Internet*, aunque los permisos a servicios corporativos pueden ser modificados bajo solicitud expresa del usuario y aprobado por directivos de la empresa junto con el área de tecnologías.

Una vez creada cada WLAN, se puede editar su configuración por defecto, en la pestaña general, se configura la interfaz relaciona, su estado activo o inactivo y si debe difundir su SSID. Esta configuración se presenta en la Figura 3.17.

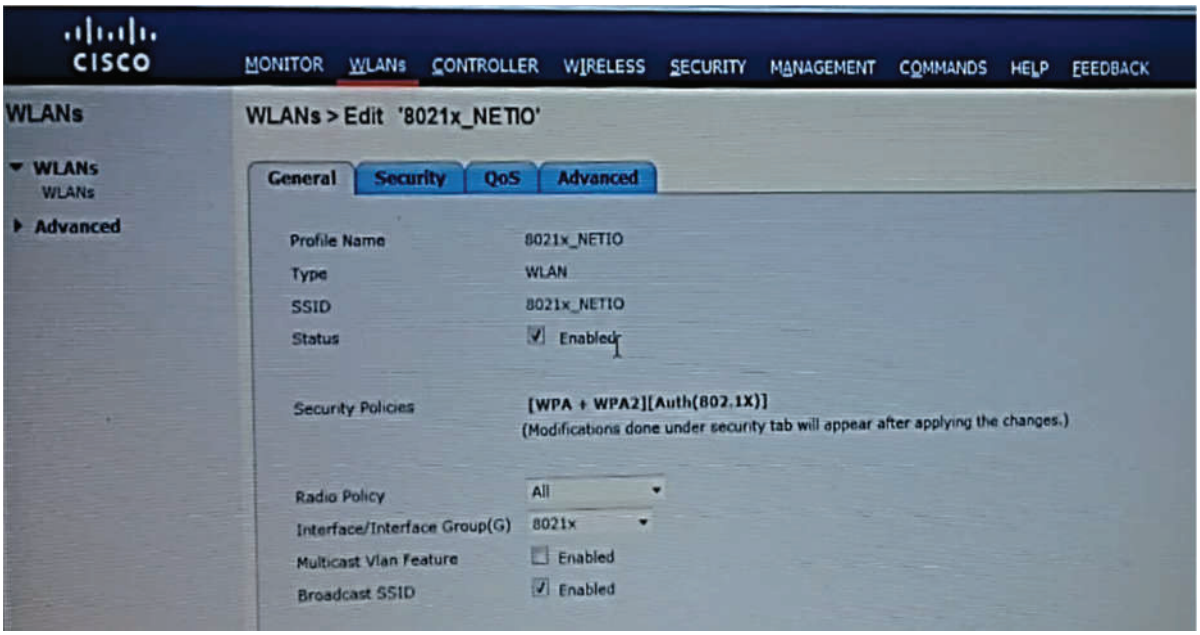

Figura 3.17 Configuración general de la WLAN

Posteriormente se define la seguridad, en nuestro caso se define en WPA-WPA2, tipo de encripción AES y la interfaz, en este caso la WLAN 802.1x (ver figura 3.18)

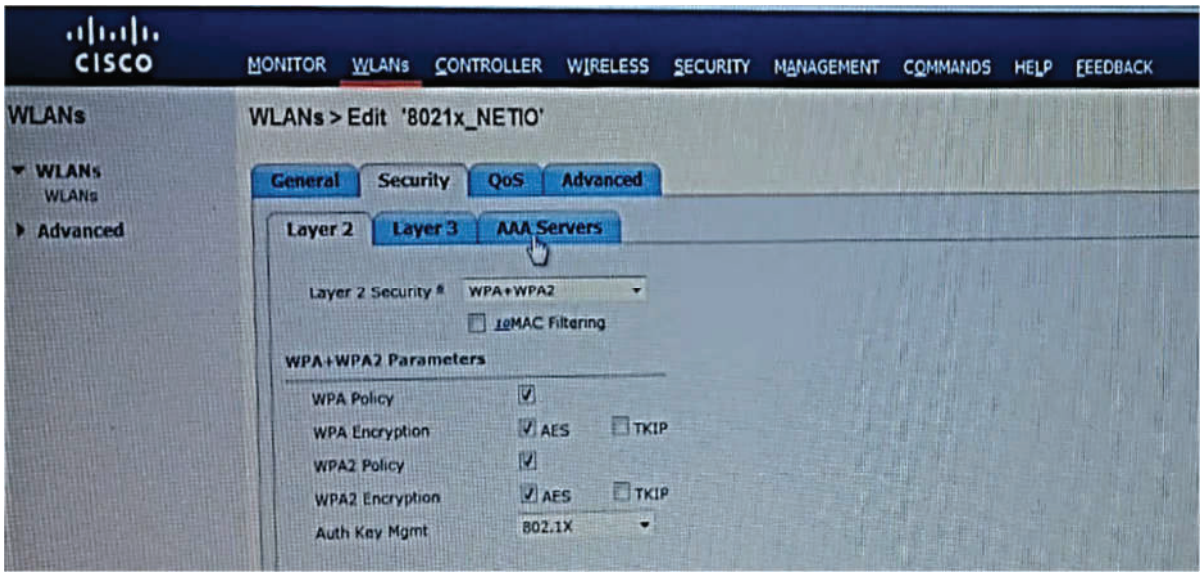

Figura 3.18 Configuración *Security* WLAN en capa 2

Con respecto al servidor AAA, podemos definir la dirección IP del equipo Cisco ISE, en este caso 10.15.150.57:1812 para los servidores de autenticación y 10.15.150.57:1813 para los servidores de contabilización *accounting* (ver figura 3.19).

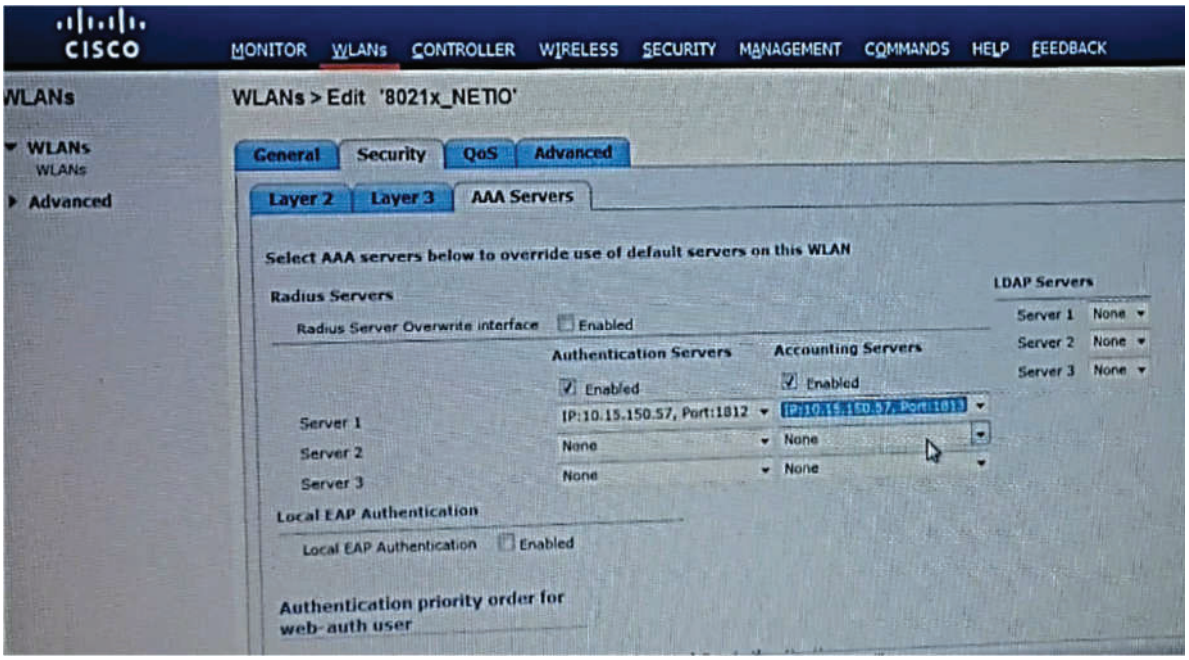

Figura 3.19 Configuración *Security* WLAN para servidores AAA

Para realizar configuraciones específicas acerca de varios servicios, incluidos los mecanismos de seguridad, se ingresa a la pestaña *Advanced*. El principal cambio que debe realizarse es la habilitación del NAC con la opción RADIUS NAC, que impica que el control de acceso estará bajo la responsabilidad del servidor RADIUS configurado en este caso en el ISE (ver figura 3.20).

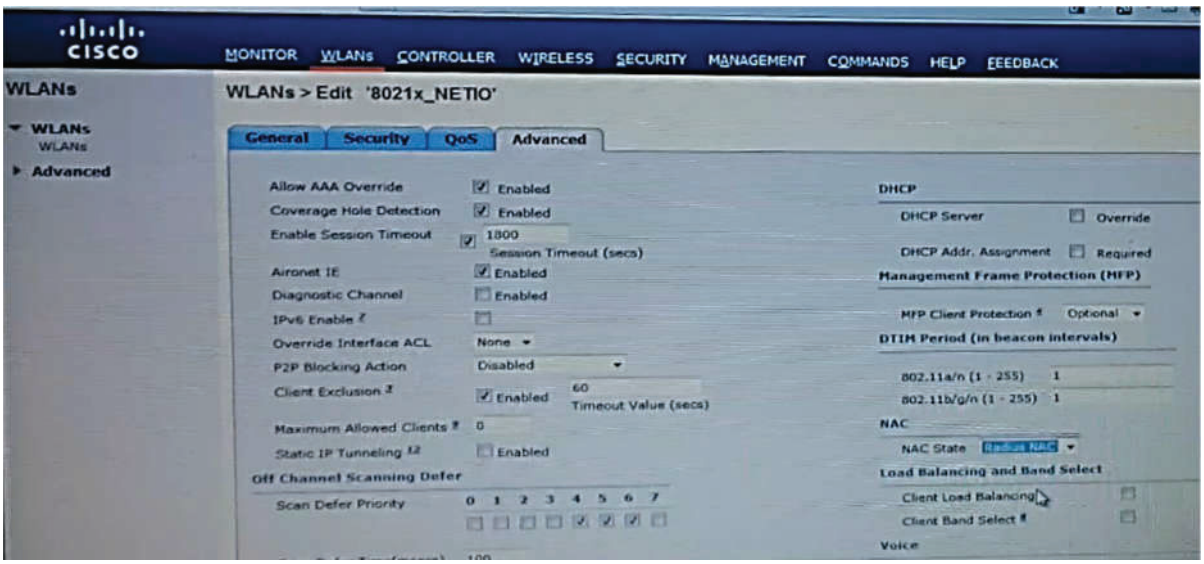

Figura 3.20 Configuración *Advanced* de la sección WLAN

c. Configuración de interfaces para cada WLAN creada

Se crea dos interfaces de tipo dinámicas, las cuales serán utilizadas para asociarlas a los dos SSID, una para 8021x_NETIO y la restante para BYOD_NETIO. Las mismas se crean y configuran en la interfaz *web* de la WLC, en la pestaña *CONTROLLER*, en la sección Interfaces, crear una nueva interfaz y luego elegir *Edit* para editarla (ver figura 3.21).

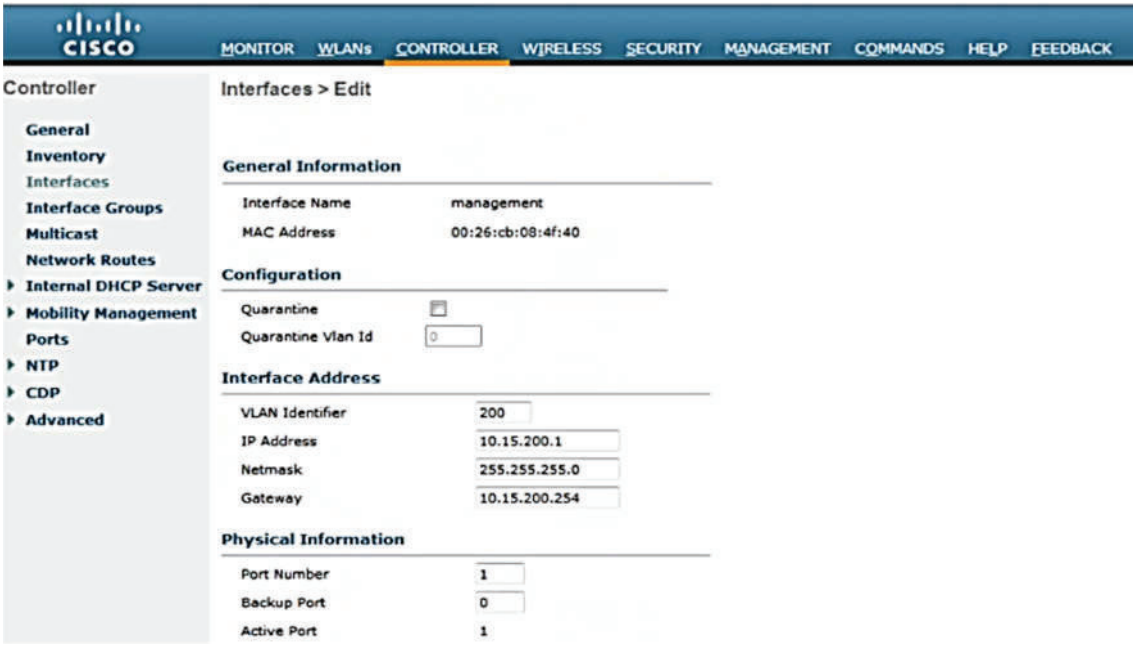

Figura 3.21 Configuración interfaces en la WLC

Para verificar las interfaces configuradas en la WLC, ingresamos en la pestaña *CONTROLLER*, en la sección Interfaces (ver figura 3.22).

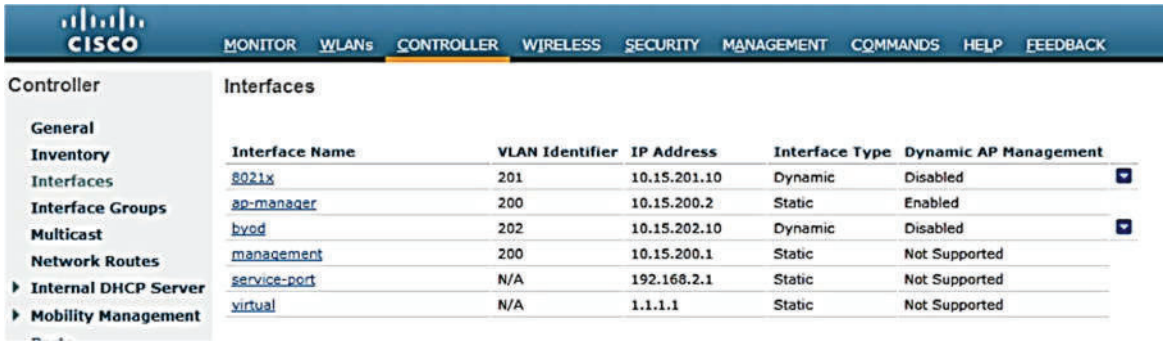

Figura 3.22 Verificación de configuración interfaces en la WLC

d. Configuración de ACL en la WLC

En las WLAN se configura listas de control de acceso (ACL) para limitar el tráfico dependiendo del direccionamiento IP origen-destino, protocolo de capa transporte, puerto origen-destino. Las ACL configuradas en las WLC ubicadas en los bloques de operación de la empresa se presentan en la figura 3.23, las mismas se crearon para limitar los accesos dependiendo del cumplimiento de los parámetros de autenticación, autorización, postura y remediación de Cisco ISE, relacionados con el acceso.

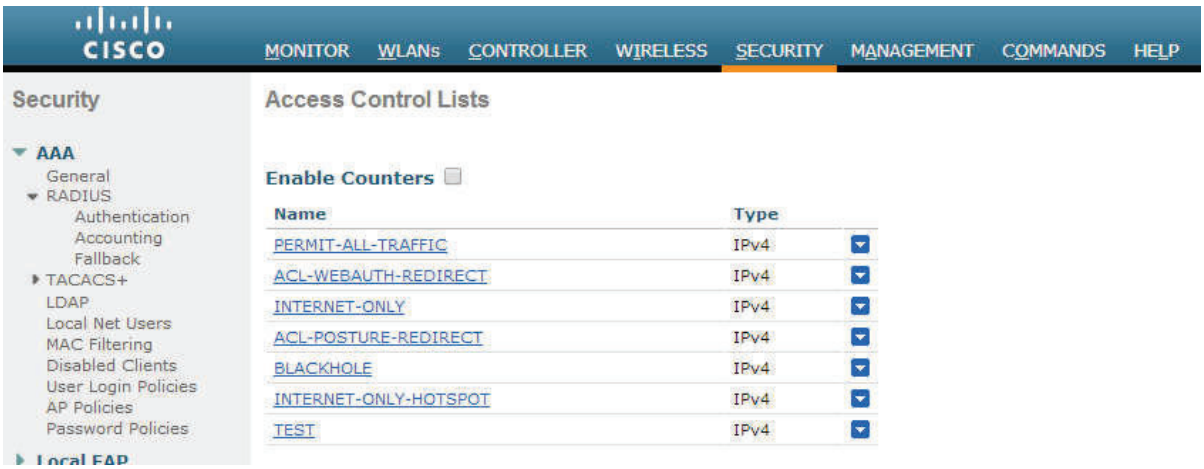

Figura 3.23 ACL configuradas en la WLC

- La ACL *PERMI-ALL-TRAFIC* permite todo tipo de tráfico de tipo `any any`.
- La ACL ACL-*WEBAUTH-REDIRECT* permite la redirección a un explorador *web* con un portal cautivo que solicita el ingreso de credenciales del usuario corporativo o invitado que se conecta a la red inalámbrica con SSID BYOD_NETIO para el registro o verificación del dispositivo que intenta conectarse a la red.
- La ACL *INTERNET-ONLY* bloquea el acceso a los servicios corporativos de la empresa, únicamente se permite el acceso a *Internet*.
- La ACL ACL-*POSTURE-REDIRECT* redirecciona a los dispositivos que no cumplen la postura al agente NAC, para que pueda revisar y descargarse agentes que le permitan instalar remotamente los parámetros faltantes para cumplir la postura, es decir que se ejecute el proceso de remediación.

- La ACL *BLACKHOLE* permite el acceso solo a dispositivos registrados en el ISE, caso contrario todo acceso será bloqueado.
- La ACL *INTERNET-ONLY-HOTSPOT* permite realizar *hotspot*, solo los dispositivos que previamente fueron registrados y asignados como *hotspot* autorizados dentro del ISE, caso contrario será bloqueado inmediatamente este dispositivo.

A continuación se presenta la configuración específica de la ACL *PERMIT_ALL_TRAFIC.*

❖ Configuración de la ACL *PERMIT_ALL_TRAFIC* en la WLC.

Para la creación de las ACL es necesario ingresar a la pestaña *Security*, en la sección *General*, crear la lista de acceso correspondiente y editarla, en este caso la ACL *PERMIT_ALL_TRAFIC* permite todo tipo de tráfico en específico sin ninguna restricción (ver figura 3.24).

La configuración de las ACL restantes, se presenta en el Anexo C13.

Figura 3.24 ACL sin restricción- permite todo el tráfico

3.2.2.2.3 Configuración de puntos de acceso inalámbrico (AP)

La configuración detallada de los *AP* (Cisco *Aironet* serie 1240) utilizados en el desarrollo del prototipo se encuentra en el Anexo C14.

3.2.2.3 Configuración de servidores corporativos

En el desarrollo del prototipo se instalarán y configurarán los servidores indicados en la tabla 3.20 , que simulan los servicios principales de la empresa.

SERVIDOR	SERVICIOS/ROLES	SISTEMA OPERATIVO
AD/CA/DNS/DHCP	DNS/DHCP/AD,CA	Microsoft *Windows Server* 2008 R2
FTP	Compartición de archivos	Microsoft *Windows Server* 2008 R2
CONSOLA DE ADMINISTRACIÓN *ANTIVIRUS* CORPORATIVO	Consola de Administración del *Antivirus* Kaspersky	Microsoft *Windows Server* 2008 R2
WWW	Servidor Web Corporativo	Microsoft *Windows Server* 2008 R2
PROXY	Acceso a *internet* controlado	*Open*Suse 7
NTP	Sincronización, servidor de tiempo de red	*Switch* Cisco Multicapa (C3560-IPSERVICESK9-M)

Tabla 3.20 Servidores a implementarse en el prototipo

3.2.2.3.1 Direccionamiento IP de los dispositivos del prototipo.

Los dispositivos finales, equipos de conectividad y servidores mantendrán el esquema de direccionamiento IP mostrado en la Tabla 3.21.

HOSTNAMES	ADMINISTRACIÓN	GERENCIA	OPERACIONES	SRV_NETIO	TEL_VID	TEMPORAL	OPER_W	
	VLAN ADM	VLAN 108	VLAN120	VLAN150	VLAN48	VLAN170	VLAN200	DEFAULT GATEWAY
SW_DIST_B12_A1 (Cisco Catalyst 3560-8PC)	10.15.99.250	10.15.108.250	10.15.120.250	10.15.150.250	10.15.48.250	10.15.170.250	10.15.200.250	10.15.99.254
SW_NÚCLEO_B12 (Cisco Catalyst 3760)	10.15.99.251	10.15.108.249	10.15.120.249	10.15.150.249	10.15.48.249	10.15.170.249	10.15.200.249	10.15.99.254
SW_ACC_B12_A1 (Cisco Catalyst 2960)	10.15.99.5	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	10.15.99.254
SW_ACC_B15_C1 (Cisco Catalyst 2960)	10.15.99.4	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	10.15.99.254
SW_ACC_B15_B1 (Cisco Catalyst 2960)	10.15.99.2	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	10.15.99.254
SW_ACC_B15_A1 (Cisco Catalyst 2960)	10.15.99.3	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	10.15.99.254
SW_DIST_B15_B1 (Cisco Catalyst)3560-8PC	10.15.99.252	10.15.110.251	10.15.120.251	10.15.150.251	10.15.48.251	10.15.170.251	10.15.110.251	10.15.99.254
SW_DIST_B15_A1 (Cisco Catalyst 3560-8PC)	10.15.99.253	10.15.110.252	10.15.120.252	10.15.150.252	10.15.48.252	10.15.170.252	10.15.110.252	10.15.99.254
SW_NÚCLEO_B15 (Cisco Catalyst 3760)	10.15.99.254	10.15.110.253	10.15.120.253	10.15.150.253	10.15.48.253	10.15.170.253	10.15.110.253	10.15.99.254
SERVIDOR DNS DHCP AD	NO APLICA	NO APLICA	NO APLICA	10.15.150.15	NO APLICA	NO APLICA	NO APLICA	NO APLICA
SERVIDOR CONSOLA ADMINISTRACIÓN ANTIVIRUS KASPERSKY	NO APLICA	NO APLICA	NO APLICA	10.15.150.43	NO APLICA	NO APLICA	NO APLICA	NO APLICA
SERVIDOR FTP	NO APLICA	NO APLICA	NO APLICA	10.15.150.5	NO APLICA	NO APLICA	NO APLICA	NO APLICA
SERVIDOR DE ARCHIVOS	NO APLICA	NO APLICA	NO APLICA	10.15.150.10	NO APLICA	NO APLICA	NO APLICA	NO APLICA
SERVIDOR WEB	NO APLICA	NO APLICA	NO APLICA	10.15.150.90	NO APLICA	NO APLICA	NO APLICA	NO APLICA
MV CISCO ISE	NO APLICA	NO APLICA	NO APLICA	10.15.150.57	NO APLICA	NO APLICA	NO APLICA	NO APLICA
B15-DSK100	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA
B15-DSK101	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA
B12-DSK100	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA
B12-DSK110	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA
B12-LPW200	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA
B15-LPW210	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA	DHCP	NO APLICA	NO APLICA

Tabla 3.21 Esquema de direccionamiento IP para los dispositivos del prototipo

3.2.2.3.2 Configuración del servidor de telefonía IP sobre Asterisk

Para implementar telefonía IP en el prototipo se utilizará *Asterisk* en la versión 1.8, sobre el sistema operativo Linux en la distribución CentOs. Este servidor se configuró con la dirección IP 10.15.150.5, en la VLAN 50 - SRV_NETIO.

3.2.2.3.3 Configuración del servidor FTP

Para la implementación del servicio FTP en el prototipo se instalará el rol Servidor FTP en el Sistema Operativo Microsoft *Windows Server* 2008 R2, para lo cual se requiere que se encuentre instalado el sistema operativo base y activar el rol respectivo. El servidor FTP se configuró con la dirección IP 10.15.150.5/24 dentro de la VLAN SRV_NETIO con VLAN ID 150. Los pasos generales para su instalación son los siguientes:

Ingresar al Administrador del Servidor > Roles > Anadir, Elegir Servidor FTP y finalmente clic en Instalar.

3.2.2.3.4 Configuración del servidor DNS

Para la implementación del servicio DNS en el prototipo se instalará el rol DNS en el Sistema Operativo Microsoft *Windows Server* 2008 R2, para lo cual se requiere que se encuentre instalado el sistema operativo base y activar el rol respectivo.

El servidor DNS se configuró con la dirección IP 10.15.150.15/24 dentro de la VLAN SRV_NETIO con VLAN ID 150. Los pasos generales para su instalación son los siguientes:

1. Ingresar al Administrador del Servidor > Roles > Anadir, Elegir Servidor DNS y finalmente clic en Instalar.
2. Al término de la instalación se procede a configurar tanto la zona de resolución directa como de resolución inversa, para llevar a cabo esta tarea es necesario ingresar a Herramientas administrativas y posteriormente elegir Servidor DNS.

3.2.2.3.5 Configuración del servidor DHCP

Para la asignación automática de parámetros como direcciones IP, máscara de subred, puerta de enlace, y otros; se implementará en el prototipo un servidor DHCP con la dirección IP 10.15.150.15/24 dentro de la VLAN SRV_NETIO con VLAN ID 150. Para la implementación del servicio DHCP en el prototipo, se instalará el rol Servidor DHCP en el Sistema Operativo Microsoft *Windows Server* 2008 R2, para lo cual se requiere que se encuentre instado el sistema operativo base y activar el rol respectivo. A continuación se mencionan los pasos generales para el funcionamiento del servidor DHCP en el prototipo.

- Instalar el rol DHCP en la consola del Administrador del Servidor
- Configurar los ámbitos necesarios para cada VLAN (ver Figura 3.25Figura 3.25 Consola de administración servidor DHCP)

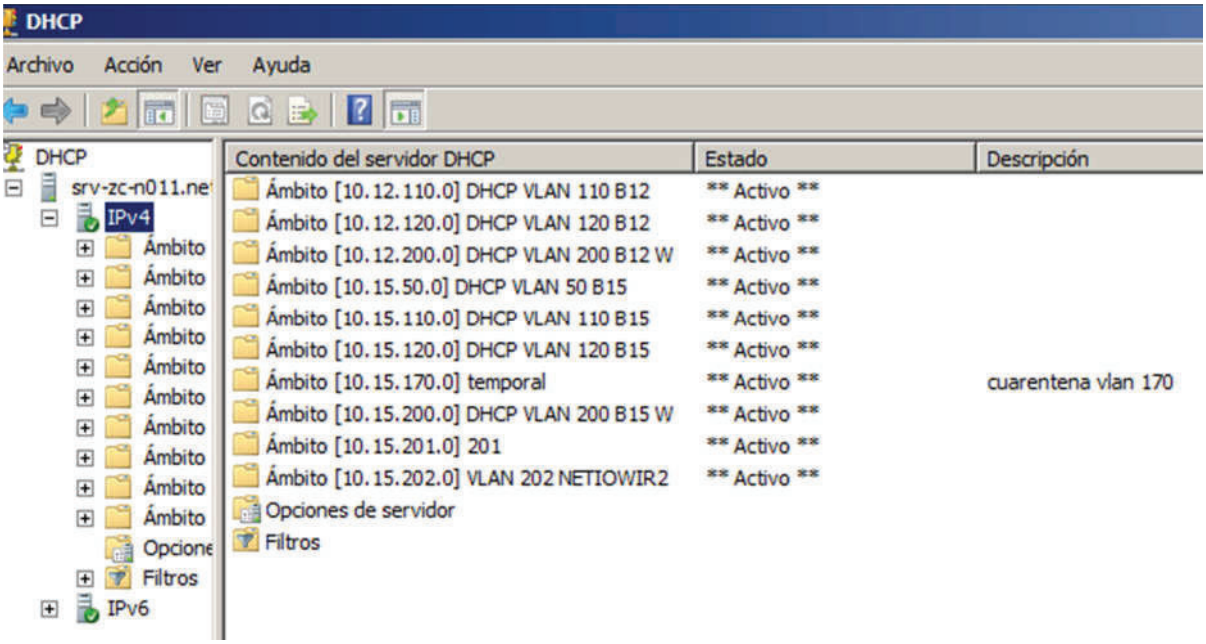

Figura 3.25 Consola de administración servidor DHCP

- Configurar los clientes para realizar las pruebas respectivas. (Inicio → Panel de Control → Redes e *Internet* → Centro de redes y recursos compartidos → Cambiar configuración del adaptador → Clic sobre Conexión de área local →

Clic derecho Propiedades → Protocolo de *internet* versión 4 → Seleccionar Obtener una dirección IP automáticamente, así mismo Seleccionar Obtener la dirección del Servidor DNS automáticamente y finalmente Clic en Aceptar).

- Verificar que los *switches* de núcleo y distribución se encuentren realizando la retransmisión de *broadcas*t y *unicast* de *DHCP* sobre los puertos denominados como confiables.

a. Pruebas de funcionamiento del Servidor DHCP

Para probar el funcionamiento del servidor DHCP se ejecutó el comando *ipconfig* desde un cliente *Windows*, se obtuvieron los resultados mostrados en la figura 3.26.

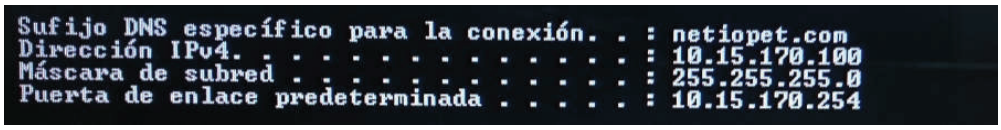

Figura 3.26 Pruebas desde un cliente DHCP

3.2.2.3.6 Configuración del servidor HTTP

La implementación del servidor de web corporativo, brindará los servicios de HTTP únicamente a usuarios autenticados de la empresa. Para el funcionamiento del servidor de *web* se utilizará XAMPP, es una distribución de Apache gratuita que contiene MariaDB, PHP y Perl.

a. Instalación y configuración XAMPP

Este servidor se configuró con la dirección IP 10.15.150.90/24 dentro de la VLAN SRVS_NETIO con VLAN ID 150. Los pasos que se deben seguir para su instalación y configuración se indican a continuación.

- Ejecutar el programa descargado de la página oficial, y esperar a que se instalen sus dependencias automáticamente.
- Editar el archivo de configuración con el respectivo nombre de usuario y *password* definidos al momento de crear la base de datos.

- ❖ Iniciar el servidor.
- ❖ Conectarse al servidor vía *web* para configurar los parámetros restantes y finalizar el proceso de instalación y configuración.

3.2.2.3.7 Instalación y configuración de la consola de administración del Antivirus Corporativo

Al ser una empresa reconocida e importante en el país, es vulnerable a ataques internos como externos, por esa razón es necesario la implementación de un *antivirus* corporativo, en este caso *Kaspersky.*

Para su instalación es necesario seguir los siguientes pasos:

- Descargar el instalador de KSC (http://www.kaspersky.com/*product-updates*/*security-center*).
- Verificar el cumplimiento de los requisitos para la instalación (SO *Windows Server* 2008, mínimo memoria RAM 1024 GB, espacio libre en disco duro).
- Ejecutar el instalador como administrador.
- Al ejecutar el instalador, aparece el asistente de instalación de Kaspersky *Security Center*, donde elegimos la opción "Instalar el Servidor de administración de Kaspersky *Security Center*".
- La instalación y configuración detallada de la consola de administración del *antivirus* se encuentra en el Anexo C15.

3.2.2.3.8 Instalación y configuración del Directorio Activo

Para la implementación del Directorio Activo en el prototipo se instalará el rol *Active Directory* en el Sistema Operativo Microsoft *Windows Server* 2008 R2, para lo cual se requiere que se encuentre instado el sistema operativo base y activar el rol respectivo. El Directorio Activo, mejor conocido como AD, se configuró con la dirección IP 10.15.150.15/24 dentro de la VLAN SRV_NETIO con VLAN ID 150.

La instalación y configuración detallada del servidor se puede encontrar en el Anexo C16.

Básicamente los pasos generales para su instalación son los siguientes:

- Instalar el rol AD en la consola del Administrador del Servidor
- Definir el nombre del domino a netiopet.com
- Definir nueva Unidad Organizativa
- Para obtener una mejor administración personalizada se crea una nueva Unidad Organizativa denominada NETIO*,* y sobre esta se creará el árbol de directorio de la empresa.
- Crear nuevas Unidades Organizativas para Usuarios, Equipos dentro de la OU NETIO
- Para la posterior creación de Usuarios, Grupos y Equipos de la empresa
- Crear las GPO – Política de Grupo (*Group Policy Object*) y vincularlas a las OU (Unidad Organizativa) respectivas.

3.2.2.3.9 Instalación y configuración de Entidad Certificadora

Para la implementación de la Unidad Certificadora del Directorio Activo en el prototipo, se instalará el rol en el Sistema Operativo Microsoft *Windows Server* 2008 R2, para lo cual se requiere que se encuentre instalado el sistema operativo base y activar el rol respectivo.

La Unidad Certificadora del Directorio Activo, mejor conocido como CA, se configuró con la dirección IP 10.15.150.15/24 dentro de la VLAN SRV_NETIO con VLAN ID 150. La misma es requerida para la compartición de certificados entre el Directorio Activo y el ISE.

3.2.3 CONFIGURACIÓN DE CISCO ISE

La implementación del Cisco ISE en el prototipo se lo realizará como máquina virtual en VMware ESXi (es una plataforma de virtualización que se instala como un sistema

operativo completo, producido por VMware Inc, tiene su propio entorno de configuración, gestión, administración de máquinas virtuales).

3.2.3.1 Instalación de Cisco ISE como máquina virtual (*software*)

El *Hypervisor VMware* EXSI, se configuró con la dirección IP 10.15.150.50/24 dentro de la VLAN SRV_NETIO con VLAN ID 150 con el usuario administrador *root* y la contraseña.

Para la creación, administración, gestión de máquinas virtuales del *hypervisor*, se utiliza la herramienta *VMware vSphere Client*, en la misma se ingresa con la dirección IP asignada al *hypervisor*, el usuario administrador y la contraseña respectiva.

Sobre la máquina virtual del *hypervisor* se creó una máquina virtual para el Cisco ISE, con los siguientes parámetros de operación recomendados:

- Espacio en disco mínimo 200GB *ThickProvisionning*
- Capacidad de memoria RAM mínimo 4 GB
- Mínimo número de núcleos es 4
- Mínimo 1 interfaz de red

La máquina virtual de Cisco ISE versión 1.2 tiene la dirección IP 10.15.150.57/24.

La instalación y configuración detallada del Cisco ISE se puede encontrar en el Anexo C17.

Básicamente los pasos generales para su instalación son los siguientes:

- Instalación de la imagen OS de Cisco ISE versión 1.2, junto con las dependencias.
- Configuración inicial.- *Hostname*, direccionamiento IP, Máscara de subred, Default Gateway, dominio, servidor DNS, servidor NTP, *timezone*, usuario administrador, contraseña, habilitación acceso vía SSH.

- Al finalizar la configuración de estos parámetros, realizará pruebas de conectividad.
- Si las mismas son exitosas, el sistema preguntará si desea guardar los cambios y reiniciará el sistema operativo.
- Después del reinicio se debe revisar si todos los servicios de Cisco ISE están activos y corriendo, con el comando `show application status ise`. A continuación podemos ocupar la interfaz gráfica del ISE para la configuración restante.
- Accedemos a través de un explorador *web* (de preferencia Microsoft *Windows Explorer* con Adobe *Flash Player* actualizado a la última versión disponible), colocando la dirección IP asignada al ISE, en nuestro caso 10.15.150.57, ingresamos el usuario y contraseña configurados previamente. (Ver figura 3.27).

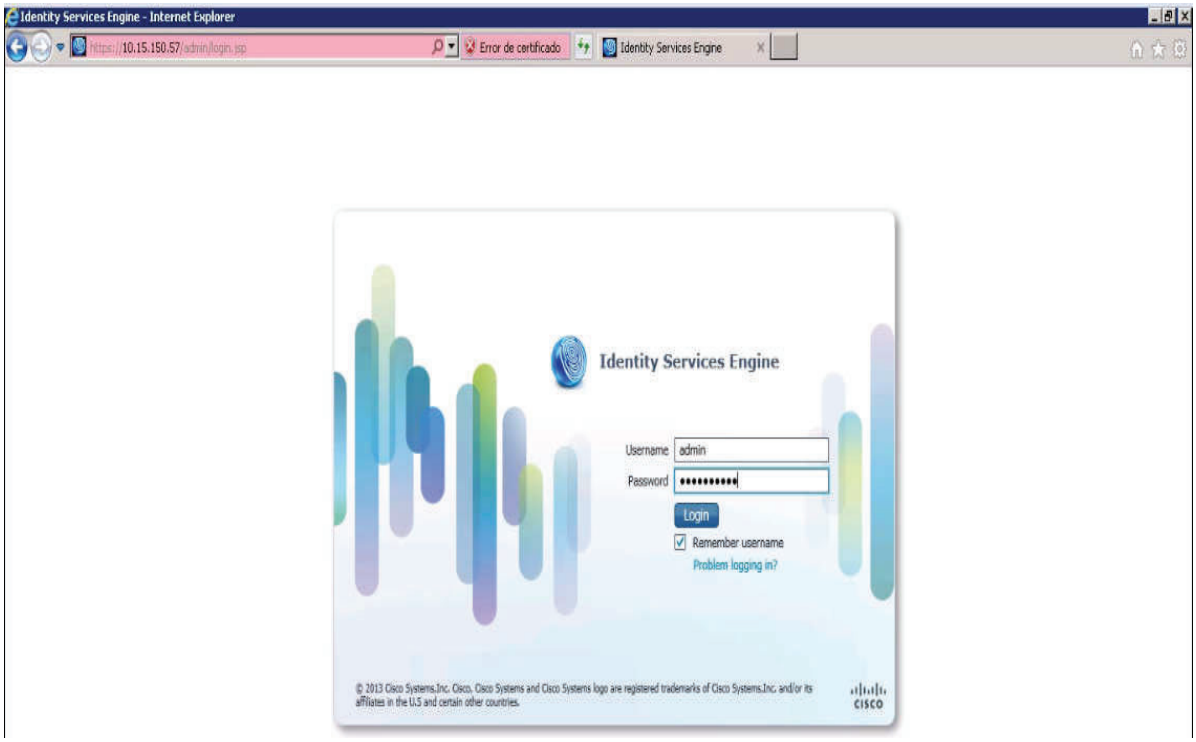

Figura 3.27 Interfaz web de configuración de Cisco ISE

3.2.3.2 Configuración Cisco ISE vía interfaz WEB

A continuación, se presenta la ventana de home de Cisco ISE (ver figura 3.28), donde encontramos la barra de menú tenemos las opciones disponibles de configuración de Autenticación, Perfilamiento, Autorización, y Postura.

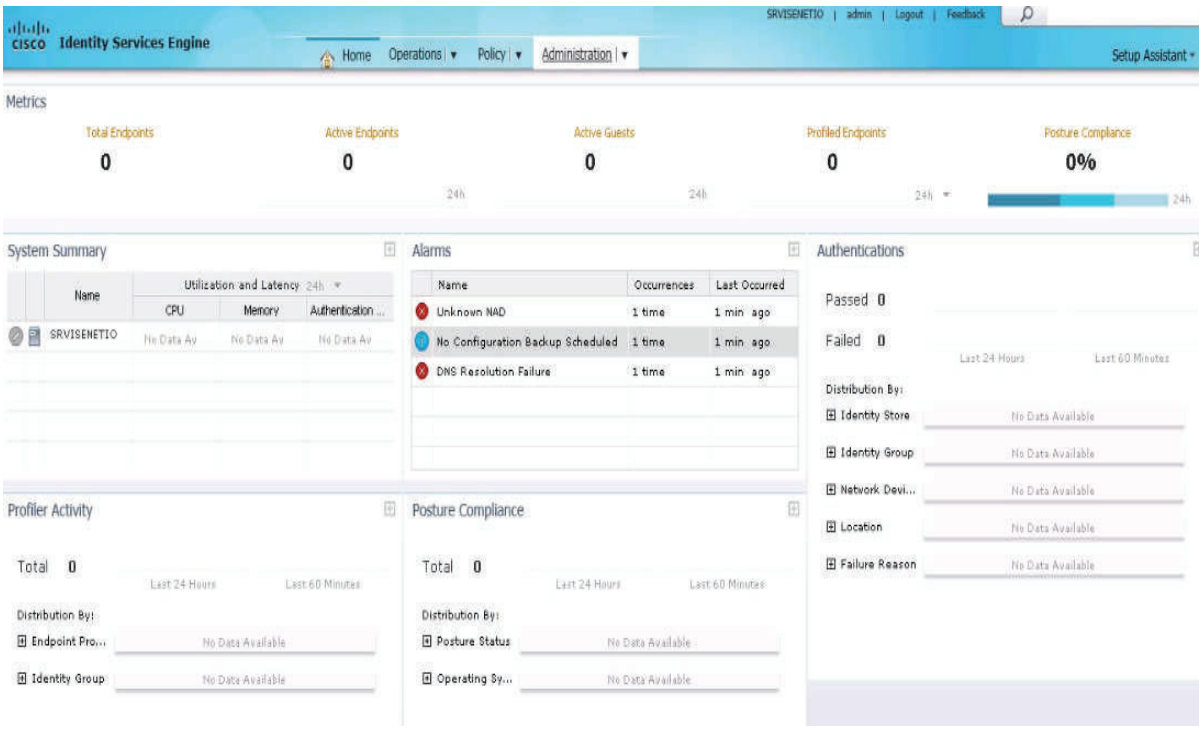

Figura 3.28 Pantalla principal de configuración de Cisco ISE

3.2.3.2.1 Configuración roles Admin-Monitor-Police Services

Configuración *Deployment*, cada dispositivo está asignado a su propio rol como es *Admin, Monitor y Policy Services* .En la configuración del ISE del presente prototipo se asignan los tres roles simultáneamente al mismo dispositivo considerando en este caso el alcance del prototipo (ver figura 3.29).

Figura 3.29 Configuración roles *Admin-Monitor-Police Services*

3.2.3.2.2 Sincronización NAD, Cisco ISE, WLC, Directorio Activo, servidor NTP

Para la sincronización completa con AD, equipos de conectividad, y otros, es necesario definir los parámetros de funcionamiento como servidor *PROXY* (descarga de parches y perfiles por defecto), servidor NTP para la correcta sincronización con el AD y los NAD (ver figura 3.30).

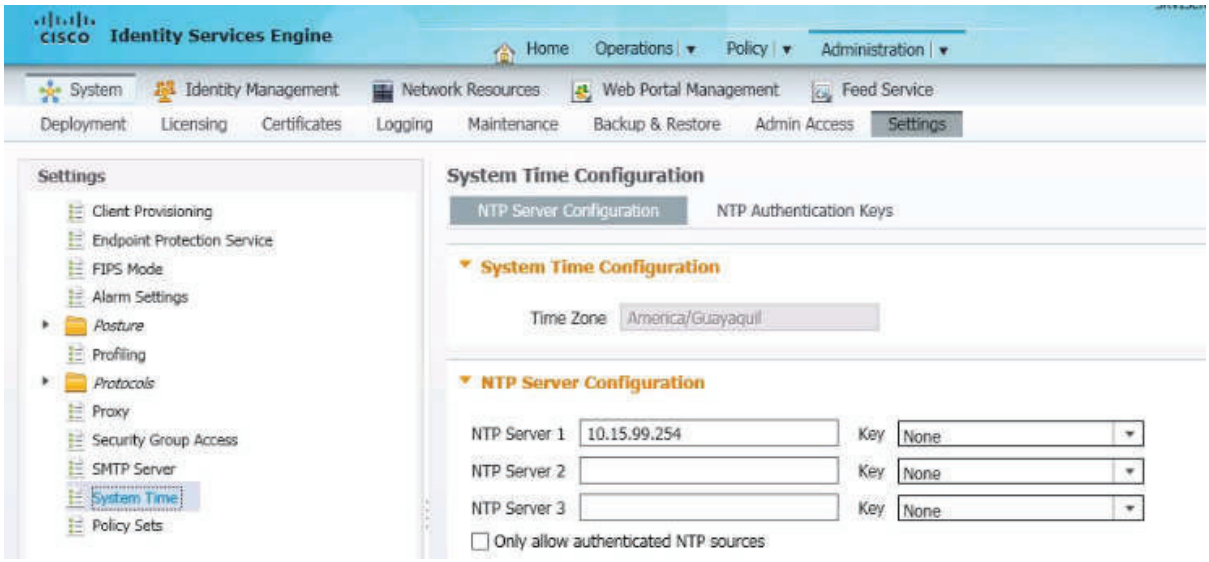

Figura 3.30 Configuración y sincronización con un servidor NTP.

3.2.3.2.3 Configuración de certificados entre Cisco ISE y Active Directory (CA)

A continuación se deben instalar los certificados correspondientes al servidor AD (CA) y Cisco ISE para realizar su unión y configurar el AD como unidad de identidad externa dentro del ISE.

Para la Creación del certificado CA se realiza los siguientes pasos:

- Abra una ventana del navegador a http://10.15.150.15/certsrv e ingrese
- Haga clic en Descargar certificado de CA, cadena de certificados o CRL (para el método de codificación, elegir DER).
- Haga clic en Descargar certificado de CA y selecciona Guardar Archivo y OK
- Este archivo se guarda como certnew.cer (ver figura 3.31)

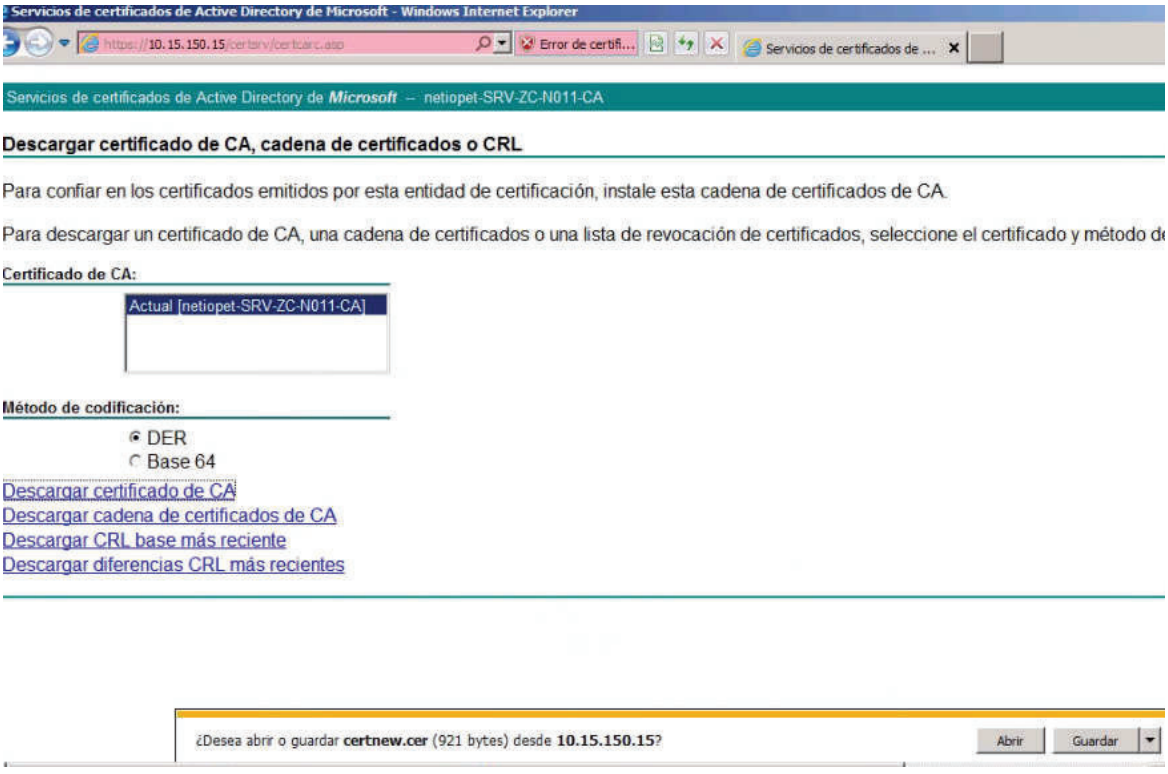

Figura 3.31 Generación de certificados digitales en la CA

A continuación se configuración el certificado en ISE *Administration Primary*. En el Cisco ISE, ingresar a Administración --> *System* --> *Certificates* --> *Certificate Store*, se evaluará la CA en el Cisco ISE (ver figura 3.32).

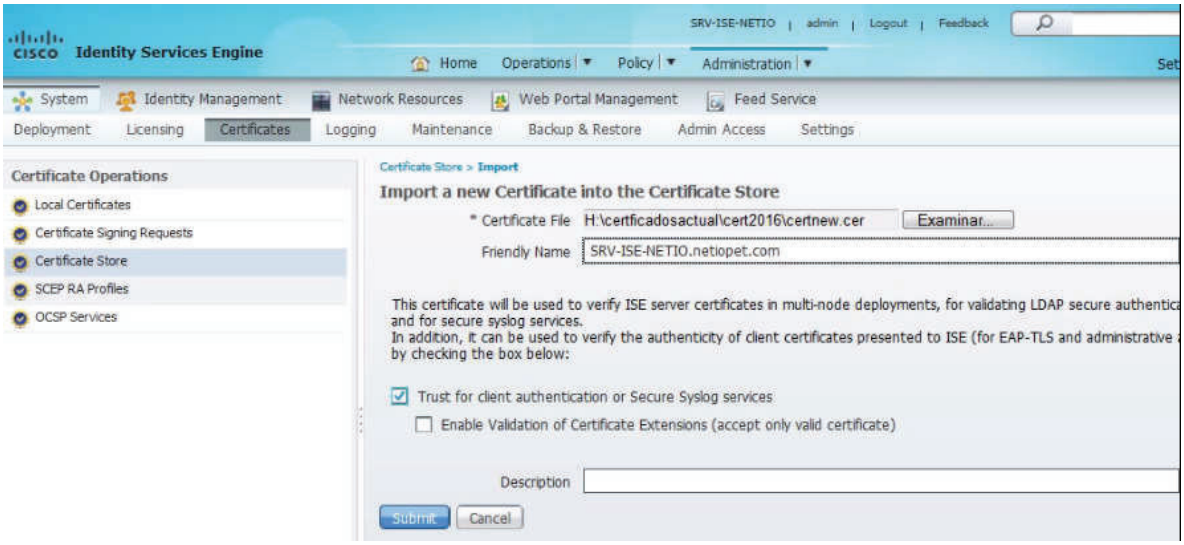

Figura 3.32 Importación de certificado digital del AD en el ISE

3.2.3.2.4 Integración de Cisco ISE con el Directorio Activo (AD)

Una vez configurados los certificados tanto en la CA del AD y el ISE se procede con la intergración del AD con el ISE (*Join*), esta tarea se realiza en el ISE en *Administration → External Identity Sources → Active Directory → connection* y se ingresa los datos del dominio (`netiopet.com`), un nombre abreviado que se utilizará en el ISE como *Identity Store Name* (`AD1`) (ver figura 3.33).

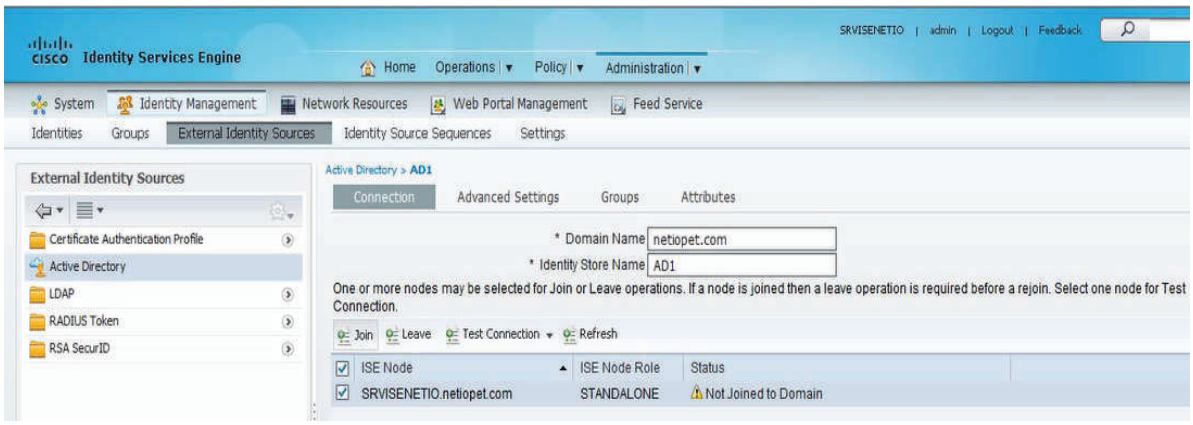

Figura 3.33 Integración de Cisco ISE con AD

A continuación se procederá con un *Test Connection* para probar que se tiene acceso al AD, posteriormente se procede con la Integración o *Join* en el *AD*, y el sistema solicitará el ingreso del usuario Administrador (que tenga permiso de interación en el AD) y la contraseña del *Active Directory*. Si las credenciales y permisos son correctos el proceso responderá con Completed, como lo indica la figura 3.34.

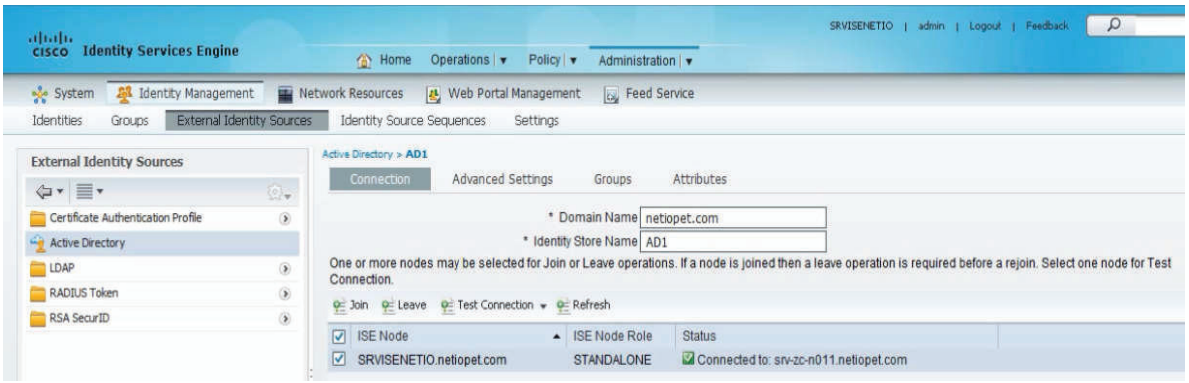

Figura 3.34 Vinculación de Cisco ISE con AD (sincronización con entidad de identidad)

3.2.3.2.5 Configuración de grupos del AD en cisco ISE.

Agregamos 2 grupos a Cisco ISE de acuerdo a nuestras necesidades como son:

a. Configuración de User Identity Groups

La configuración de grupos de identidad de usuarios se lo realiza para identificar las categorías de usuarios que se utilizarán para las diversas solicitudes de acceso a la

red como es el caso invitado. En la creación de cada uno de los grupos de identidad de usuarios es necesario *Name, Description*. Los grupos creados son Invitados, Empleados, los otros grupos son creados por *default*.

b. Configuración de grupos de identificación de dispositivos finales (Endpoint Identity Groups.)

La configuración de grupos de identidades de puntos finales se lo realiza para identificar las categorías de dispositivos finales, dependiendo de los requerimientos de la red se pueden realizar cambios o crear nuevos *endpoints* con un patrón específico de reconocimiento o dejarlo por defecto, ya que Cisco provee una lista completa de dispositivos y marcas (ver figura 3.35).

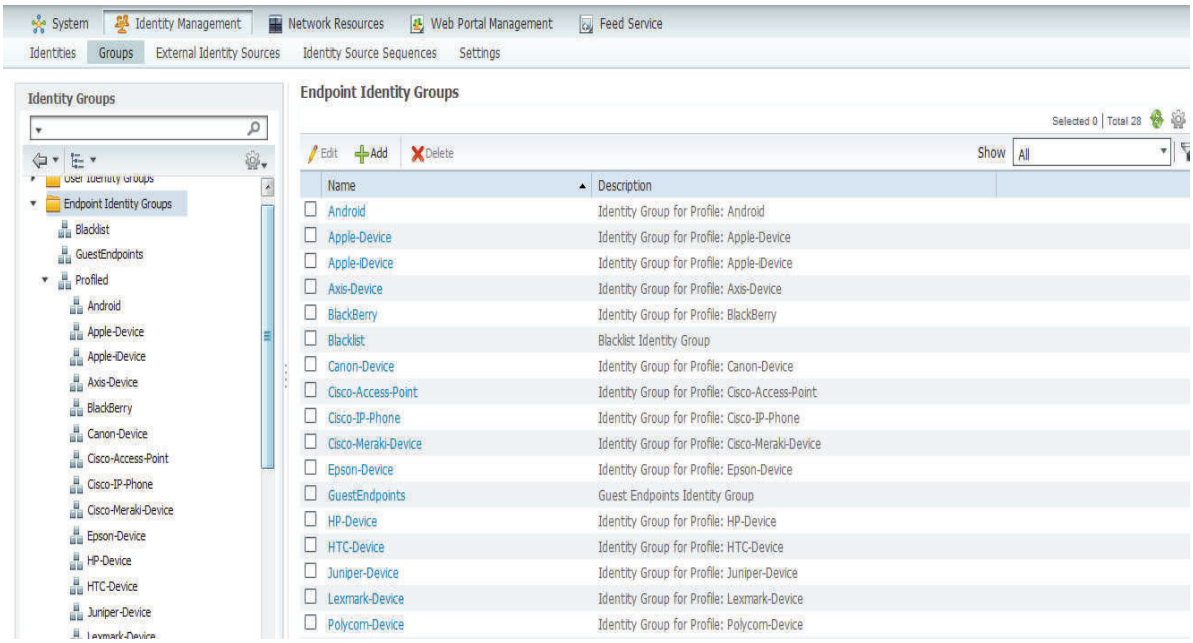

Figura 3.35 Grupos predefinidos para identidad de dispositivos finales (*endpoints*)

3.2.3.2.6 Configuración de Entidades de fuentes de Identidad (Identity Source Secuence)

Para la validación de credenciales se define una entidad de identidad (AD encargado de almacenar información de cuentas de usuario, registro de equipos, entre otros) con la cual se compara el ingreso de credenciales correctas para el proceso de autenticación.

La primera opción configurada es el AD y Local (base de datos local de registro del ISE) como segunda opción.

Por tanto, la secuencia de búsqueda y comparación de la credenciales de las cuentas de usuario y objetos, es el AD y luego localmente, en caso de no encontrarlos, el acceso será bloqueado o requerirá un registro previa autorización de las autoridades pertinentes (ver figura 3.36).

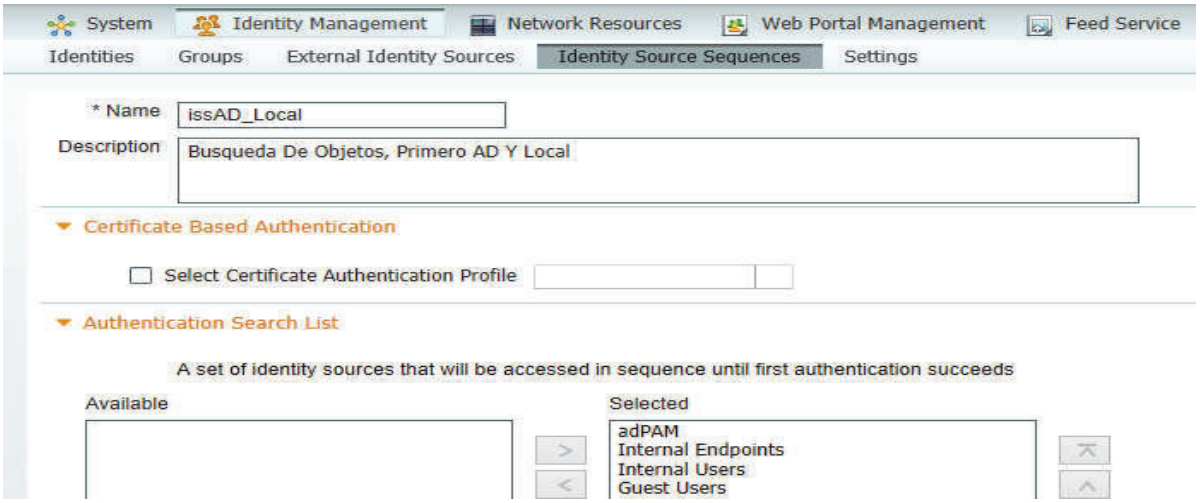

Figura 3.36 Secuencia de fuentes de identidad

En este caso un alias del AD fue definido como *adPAM (referencia directa al AD corporativo)*, mientras que *Internal Endpoints, Internal Users, Guest Users* serán los registros almacenados localmente en el ISE.

3.2.3.2.7 Configuración de Políticas tipo Authentication

- Esta configuración se realiza en *Policy→Authentication*
- Las políticas de autenticación están basadas en tipos de autenticación hacia la red ya sea por:
  - *wired* (conexión cableada)
  - *wireless* (conexión inalámbrica).
- En nuestro caso se configuraron tres tipos de autenticación (ver figura 3.37):

- Autenticación de dispositivos *wired* (*wired*_MAB)
- Autenticación corporativos *wired* (*wired*_802.1x)
- Autenticación corporativos *wireless* (*wireless*_802.1x) con protocolos permitidos (*default Network Access*).

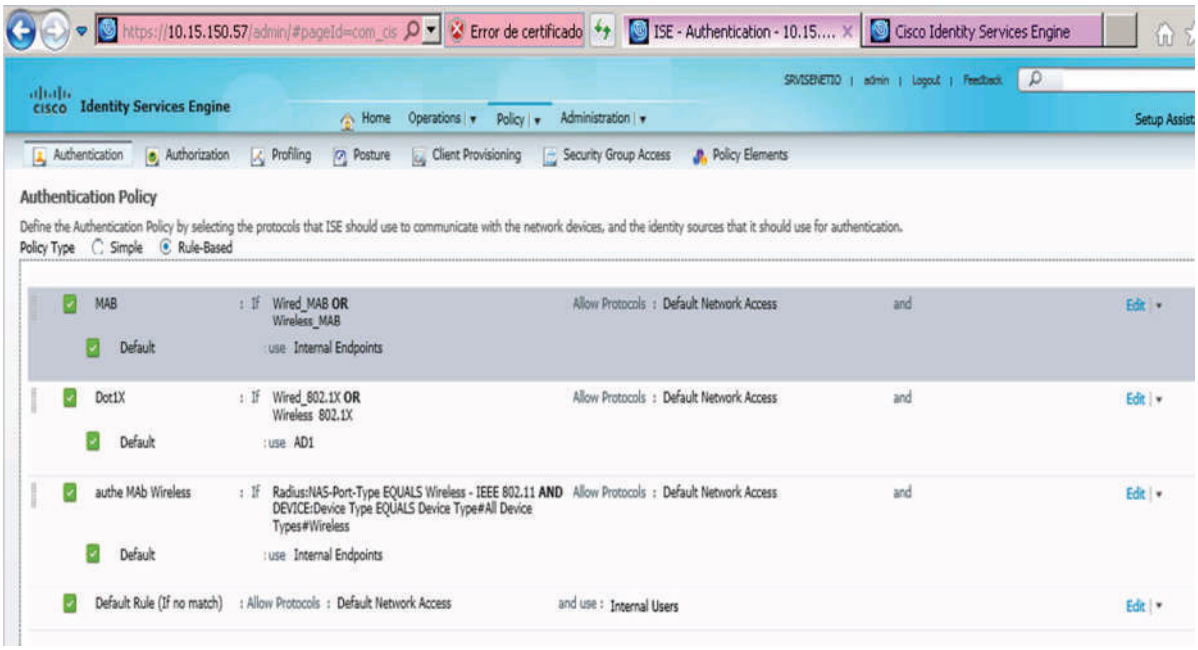

Figura 3.37 Políticas de autenticación configuradas en el ISE

a. Políticas de autenticación (Authentication Policy) para regla Default Network Access

En la regla *Default Network Access* habilitamos la opción de Enable EAP con lo cual validamos al usuario y sus credenciales.

La configuración específica se presenta en la figura 3.38.

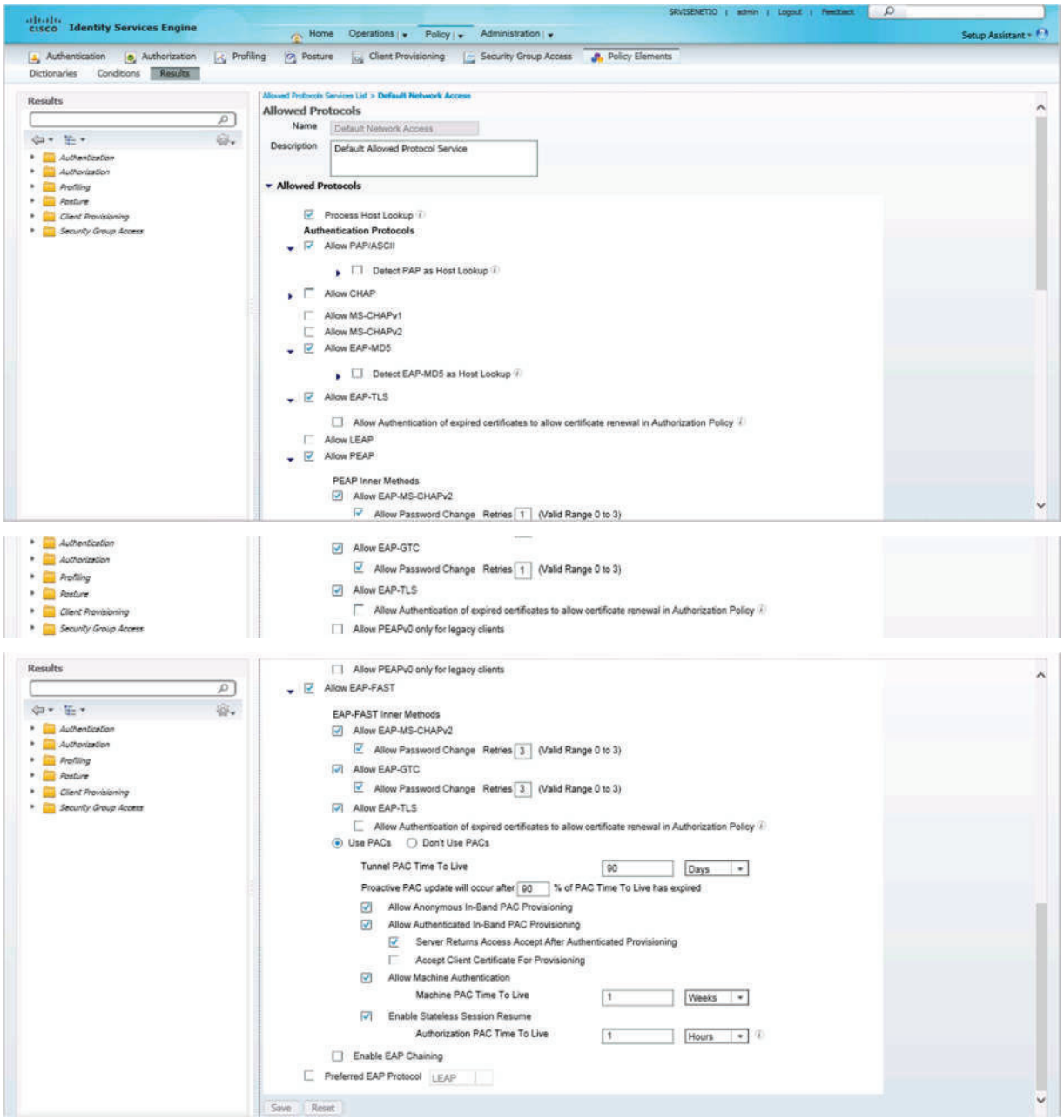

Figura 3.38 Configuración de política de autenticación *Default Network Access*

3.2.3.2.8 Configuración de Políticas tipo Authorization.

Las políticas de autorización son las encargadas de dar permisos a los equipos a diferentes roles como es el caso de la asignación a una VLAN X (VLAN usuarios Autenticados – VLAN OPERACIONES), dichas políticas están basadas en condiciones

y permisos. Para cada tipo de dispositivo se tiene una política de autorización como se indica en la figura 3.39.

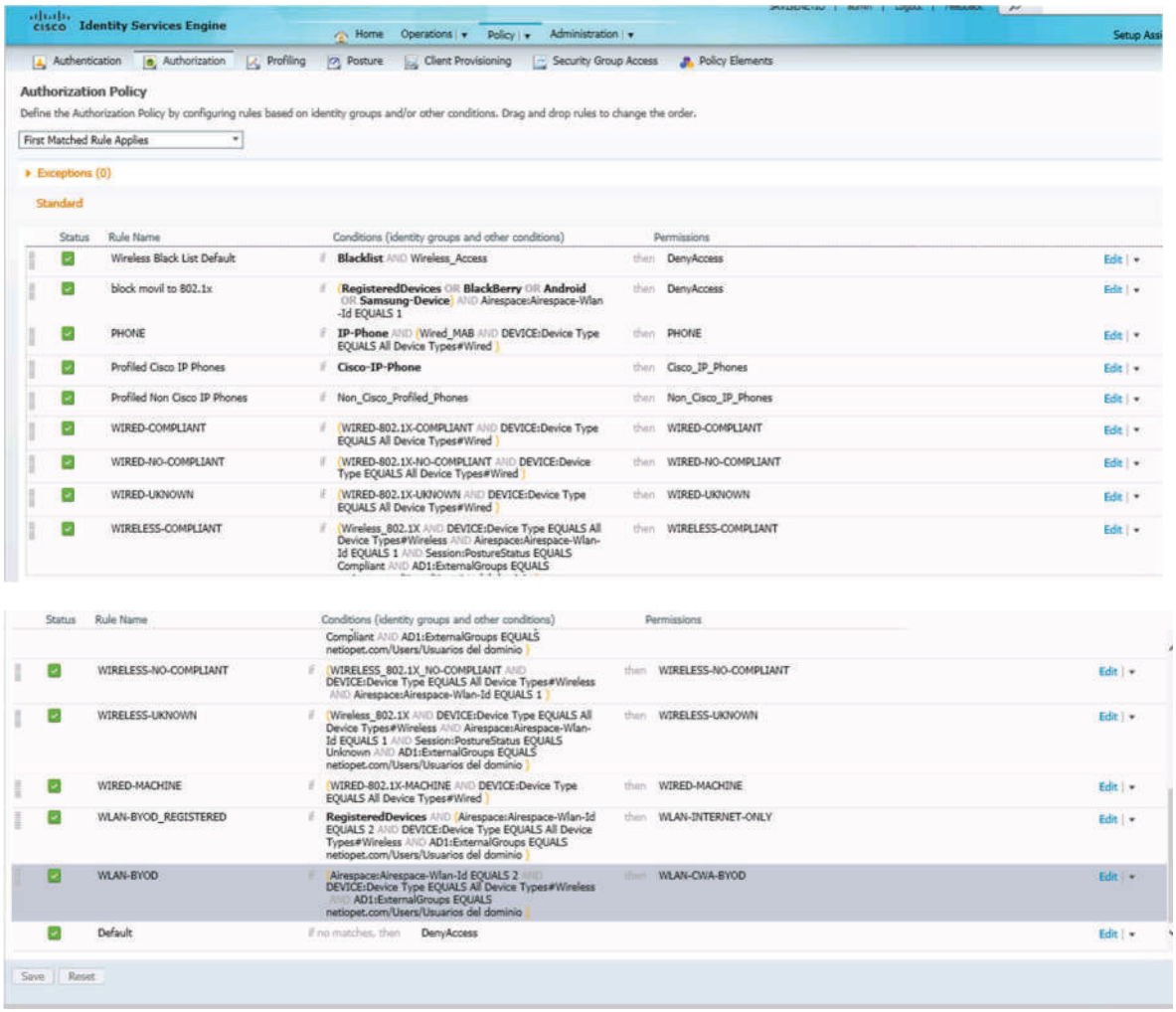

Figura 3.39 Configuración de políticas tipo *Authorization*

a. Política de autorización para equipos no permitidos (Bloqueo)

Estas políticas son realizadas para el bloqueo de equipos no permitidos tanto en la red (ver figura 3.40):

- *Wireless* NEIO_8021X
- *Wireless* NETIO_BYOD

- *Wired (*Dispositivos que se registren en la *Blacklist* a través de su dirección MAC*).*

Figura 3.40 Política tipo autorización de bloqueo

- Wireless Black List Default, indica que los equipos que se encuentren regustrados en la Lista Negra su acceso será denegado.
- Block movil to 802.1x, indica que Dispositivos registrados ó de perfil BlackBerry ó Android ó dispositivo tipo Samsung y que se encuentren en a red inalámbrica con SSID 802.1x (Airespace-Wlan-Id EQUALS 1) su acceso será denegado.

b. Política de autorización para usuarios Wired Corporativos

Estas autorizaciones están creadas para el acceso a usuarios *Wired* Corporativos (ver figura 3.41).

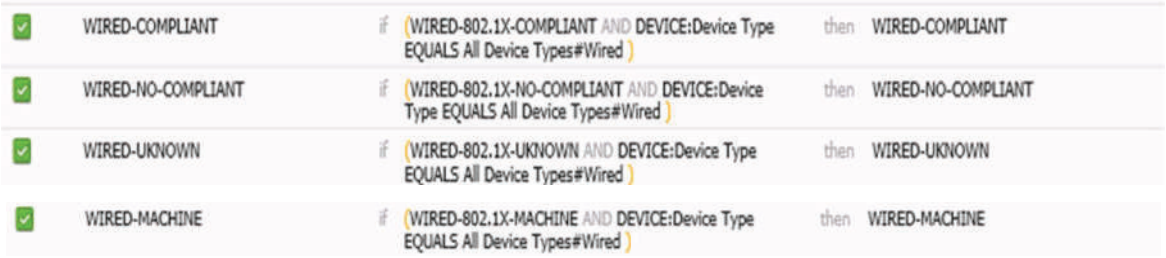

Figura 3.41 Política de autorización para dispositivos conectados a través de la red cableada

- La política *WIRED-COMPLIANT*:
  - Verifica un dispositivo conectado a través de una red cableada.
  - Valida las credenciales en el AD, enviadas a través del puerto del *switch* al ISE, si las mismas son correctas.
  - Se ejecuta la política ACL *PERMIT_ALL_TRAFFIC*.
  - Asigna el direccionamiento IP dentro de la VLAN OPERACIONES, asignada para todos los usuarios (ver figura 3.42).

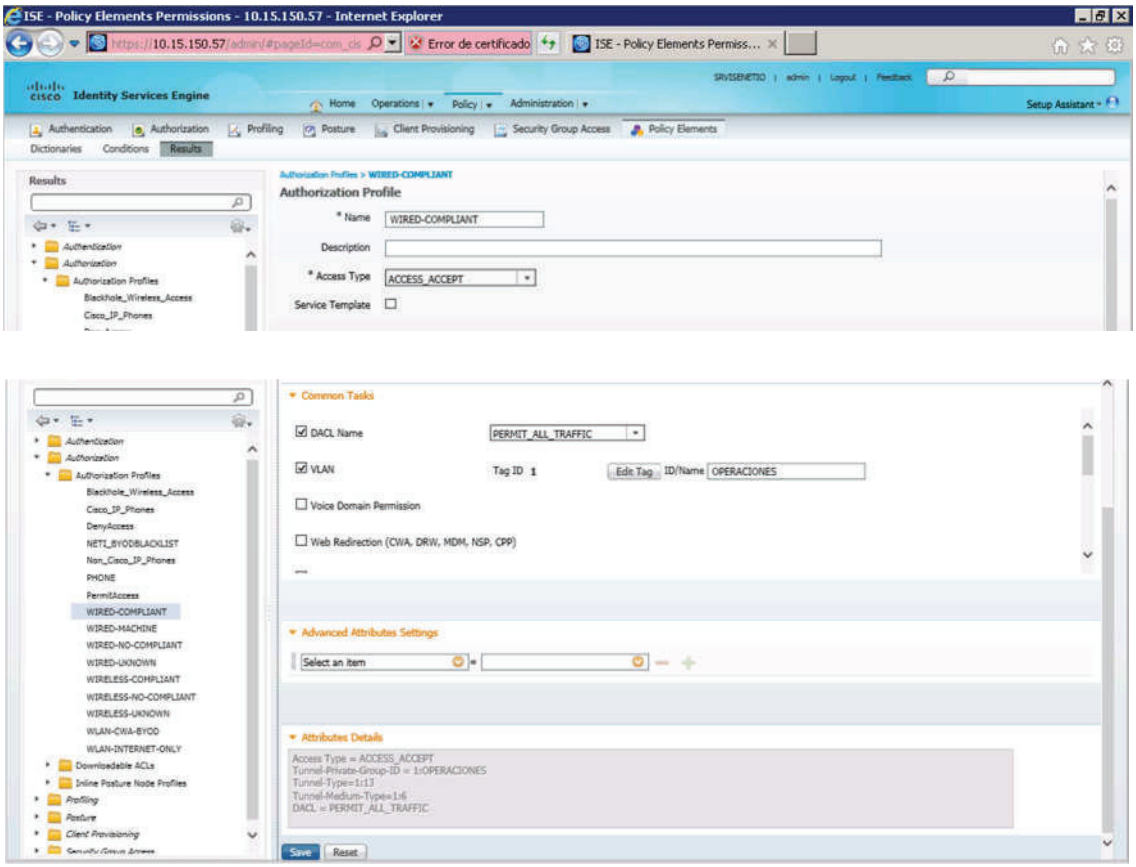

Figura 3.42 Configuración de política de autorización WIRED_COMPLIANT

La ACL que se encuentra asignado es *PERMIT_ALL_TRAFIC* en la cual tiene acceso hacia los todos los equipos de la red (ver figura 3.43).

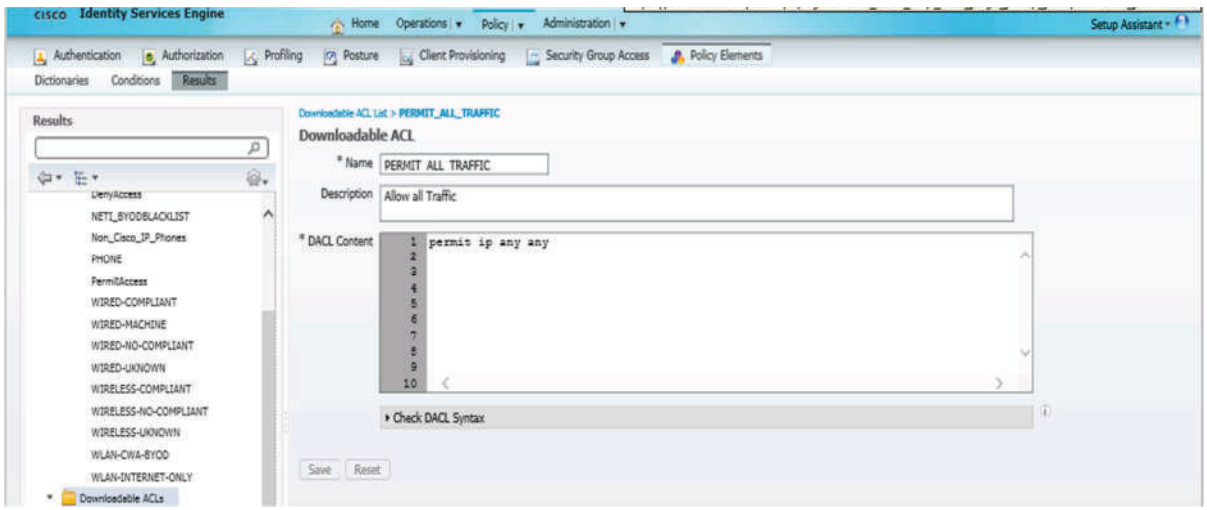

Figura 3.43 Configuración ACL PERMIT_ALL_TRAFIC

La configuración de las políticas de autenticación restantes, se presentan en el Anexo C18.

c. Política de autorización para Teléfonos alámbricos Corporativos

Esta política de autorización filtra el acceso de los teléfonos IP *Wired* Corporativos registrados (catalogados en el ISE o en el AD), se compara específicamente la dirección MAC del teléfono IP conectado a los puertos de acceso. Solo los dispositivos con las direcciones MAC catalogadas tienen acceso (ver figura 3.44).

Figura 3.44 Política de Autorización exclusiva para teléfonos IP

Cuando el perfil de autorización PHONE (creado para el control de tráfico de los teléfonos IP) se cumple, es decir el equipo está catalogado se asigna al dispositivo una dirección IP dentro de la VLAN de voz (VLAN ID 50), aplicando la ACL PERMIT_ALL_TRAFIC con lo cual garantizamos el acceso a la red de telefonía únicamente a los teléfonos IP catalogados en el ISE.

d. Política de autorización para usuarios Wireless Corporativos

Estas políticas de autorización están creadas para el acceso de los usuarios Wireless Corporativos a la WLAN con SSID 8021x_NETIO, que recibe un identificador Airespace-Wlan-Id igual a 1 (ver figura 3.45).

Figura 3.45 Política de autorización para usuarios con acceso inalámbrico a la WLAN 8021x_NETIO

Estas políticas de autorización están creadas para el acceso de los usuarios Wireless Corporativos a la WLAN con SSID BYOD_NETIO, que recibe un identificador Airespace-Wlan-Id igual a 2 (ver figura 3.46).

Figura 3.46 Política de autorización para usuarios con acceso inalámbrico a la WLAN 8021x_NETIO

El detalle de la configuración de las políticas creadas para cada WLAN se encuentra en el anexo C18.

3.2.3.2.9 Configuración de Políticas tipo Posture

Las políticas de postura verifican la instalación de aplicativos en el sistema operativo del dispositivo (parches, *antivirus*, entre otros) que intenta acceder a la red. Si la postura no se cumple, no se concede el acceso a los servicios de red, aun cuando el usuario fue autenticado correctamente.

a. Política de postura para verificación de instalación de antivirus Kaspersky

Se crea una nueva política de postura y se define el parámetro que se debe verificar su instalación, en este caso se configura Kasperky_Instalación, que verifica la instalación del *antivirus* corporativo Kaspersky. Política creada para la verificación de instalación para usuarios del NETIO, tanto para usuarios *Wired* como *Wireless* (para la WLAN 8021x_NETIO) (ver figura 3.47).

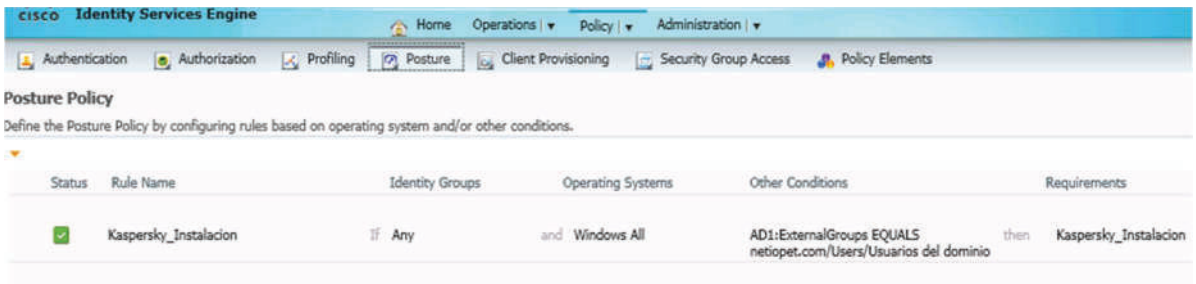

Figura 3.47 Lista de políticas de tipo postura

3.2.3.2.10 Configuración Política tipo Remediación

La política creada para la verificación de instalación de *antivirus* para usuarios del NETIO, tanto para usuarios *Wired* como *Wireless* (SSID 8021x_NETIO), revisa si tiene o no instalado el *antivirus*, si no lo tiene instalado el agente del NAC le permitirá descargar un archivo (AGENTE DEL *ANTIVIRUS*) para que después de instalarse se comunique con la Consola de Administración del *Antivirus* corporativo Kaspersky (Servidor con la dirección IP 10.15.150.43/24) y se realice la instalación remota del *Antivirus* (ver figura 3.48).

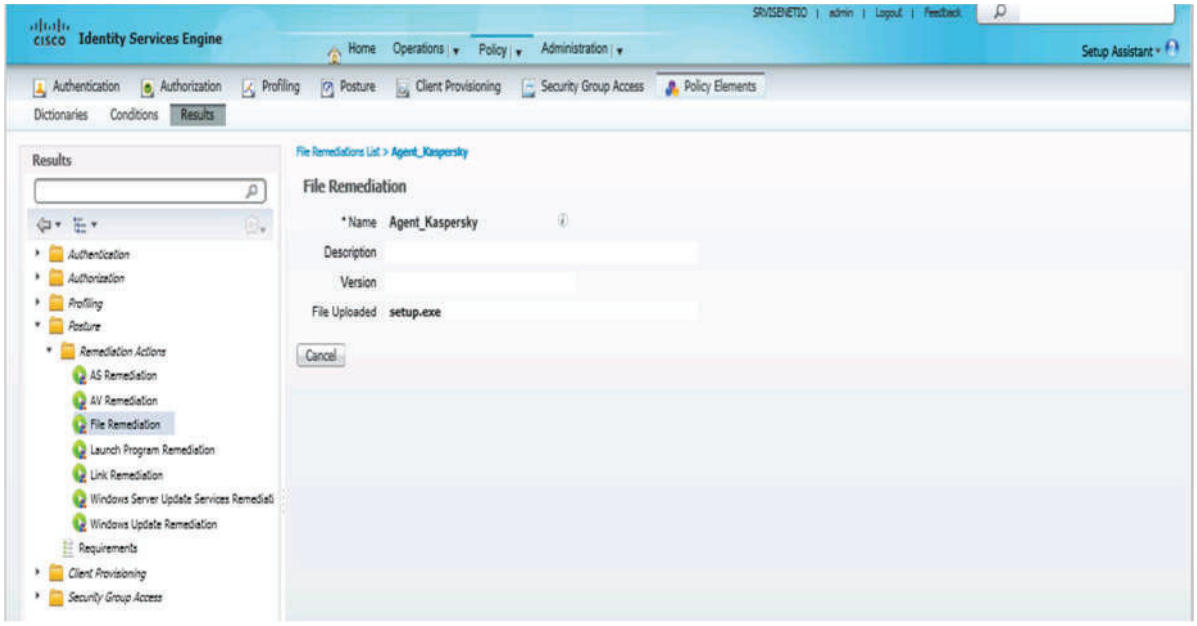

Figura 3.48 Configuración de la política de remediación *Agent_Kaspersky*

3.2.3.2.11 Políticas de Aprovisionamiento de clientes.

Determina la política de aprovisionamiento del cliente para determinar en qué usuarios se instalará el agente NAC.

a. Recursos de cada regla de aprovisionamiento

A continuación en la figura 3.49, se presenta la lista de recursos de aprovisionamiento configurados por defecto en el ISE.

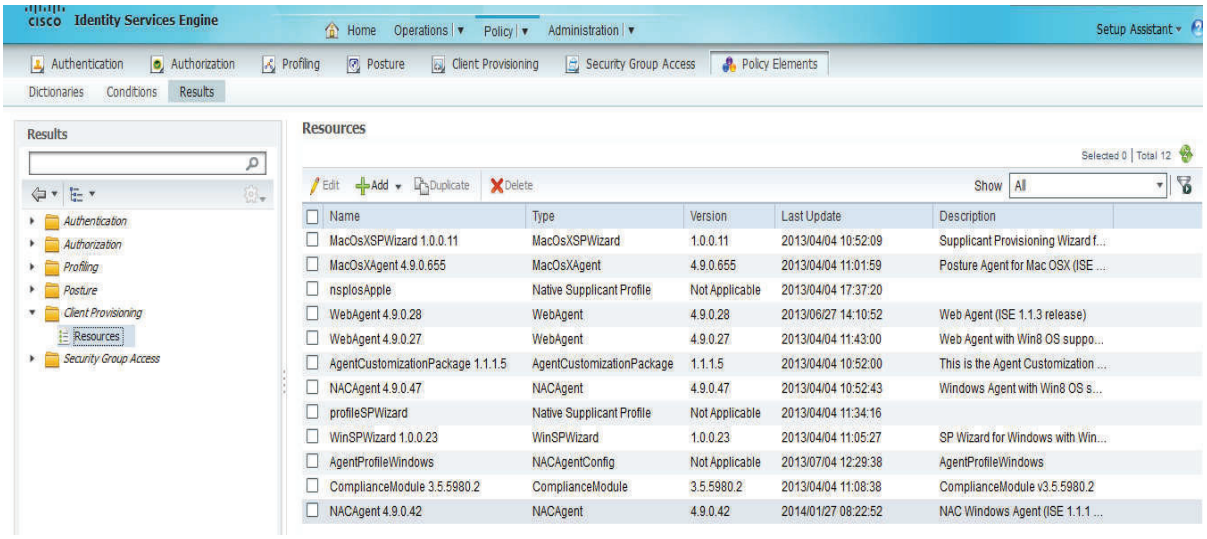

Figura 3.49 Lista de Recursos de aprovisionamiento configurados por defecto en el ISE

b. Políticas de Aprovisionamiento de clientes Wired y Wireless 8021x (WLAN 8921x_NETIO).

Determina la política de aprovisionamiento del cliente para usuarios. En la figura 3.50 se presenta la configuración de la política de aprovisionamiento del cliente para usuarios de la red *Wired* (conexión cableada) y *Wireless* (con al WLAN 8021x_NETIO), la misma verifica la instalación del *antivirus* a través de la ejecución del agente NAC, si no lo tiene instalado pasa directamente al proceso de remediación a una VLAN enjaulada con solo permisos exactos para instalar el *software* respectivo para cumplir la postura.

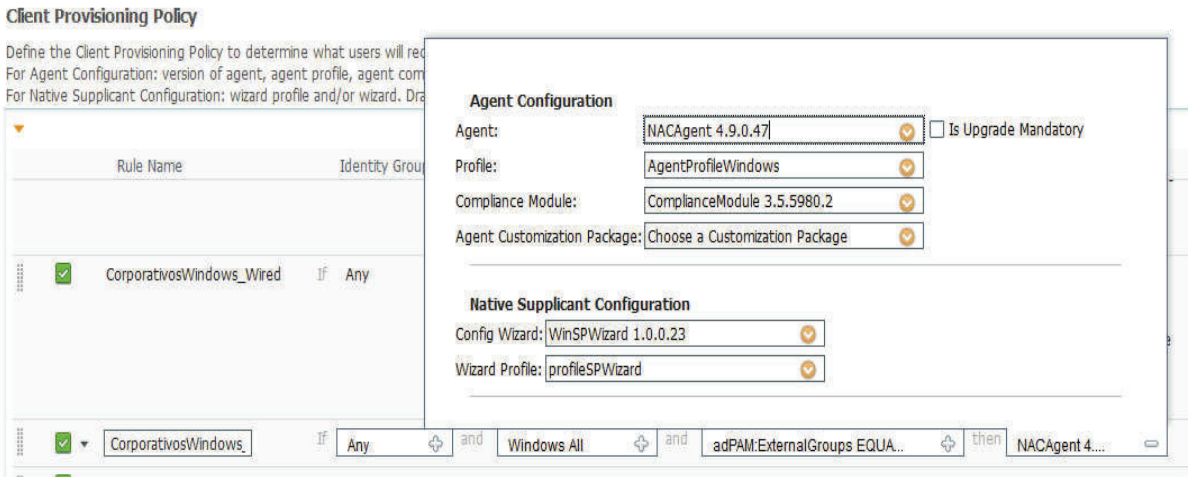

Figura 3.50 Política de aprovisionamiento para usuarios de la red WLAN 8021x_NETIO

3.2.3.2.12 Configuración de Sponsor Groups.

Se crean los grupos de *Sponsor* para la creación de usuarios invitados, *activeguest*. Estos usuarios serán creados en el Cisco ISE y no en el AD.

Cada uno de estos grupos con sus diferentes privilegios (ver figura 3.51).

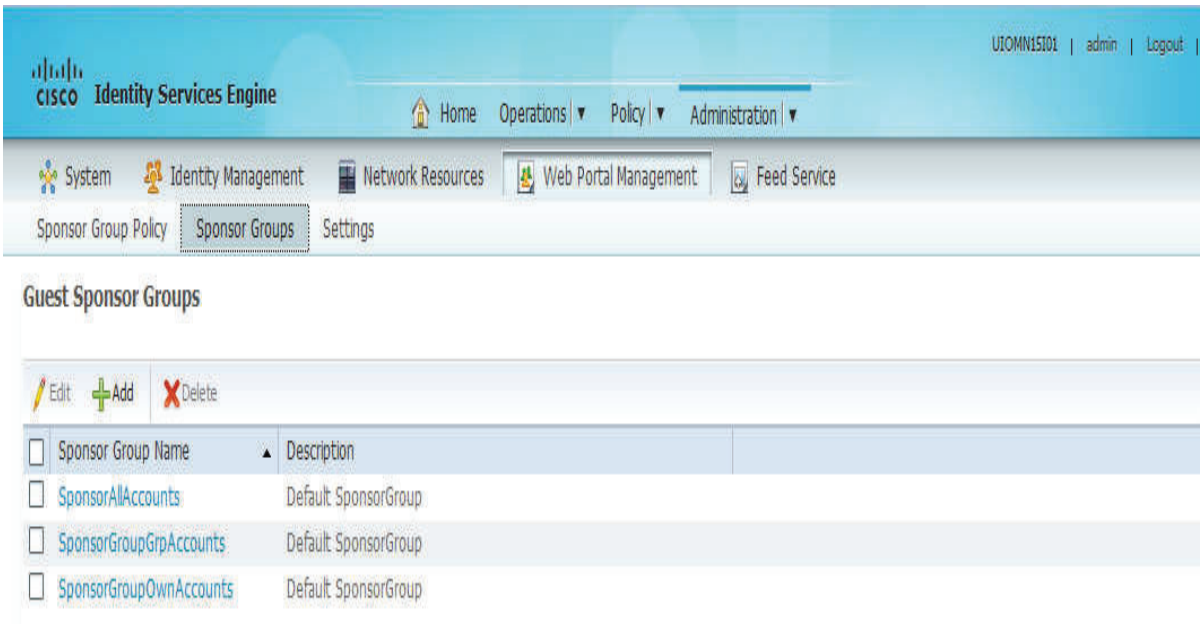

Figura 3.51 Lista de grupos de tipo Sponsor en el ISE

3.2.3.2.13 Configuraciones del portal Web.

Para que los dispositivos inalámbricos de los usuarios registrados en el AD y Cisco ISE puedan conectarse a la red inalámbrica con SSID BYOD_NETIO, requieren que su dispositivo sea registrado en el Cisco ISE.

Además del ingreso de credenciales de usuario correctas tanto del AD, o usuarios locales creados en el Cisco ISE, es necesario para el registro del equipo abrir un explorador web (de preferencia *Internet* Explorer).

A continuación, se redirigirá a un portal cautivo que solicitará nuevamente las credenciales del usuario (ver figura 3.52).

Figura 3.52 Portal cautivo para usuarios en la WLAN BYOD_NETIO

Si las credenciales son correctas, registrará la MAC del dispositivo, y le solicitará una descripción del equipo.

Y el equipo quedará registrado y posteriormente puede actualizar la página web y tener acceso a los permisos definidos en la red inalámbrica con SSID BYOD_NETIO.

3.2.3.2.14 Configuración de dispositivos de red en el ISE como NAD

Se configuran los dispositivos que trabajarán como clientes RADIUS (*switch*es, WLC, y otros) que se encargan de la retransmisión de credenciales de los endpoints al ISE.

Se lo configura en *Administration→Network Resource→Network Devices*

a. *Configuración cliente RADIUS en un Switch de acceso.*

Para la configuración de un *switch* de acceso como cliente RADIUS y autenticado como NAD en el ISE, es necesario crear un perfil cliente RADIUS. Los parámetros

solicitados son *Name, Description, IP addrress, Location, Device Type, Radius, snmp comunity*.

Y una contraseña compartida entre el ISE y el *switch* (ver figura 3.53).

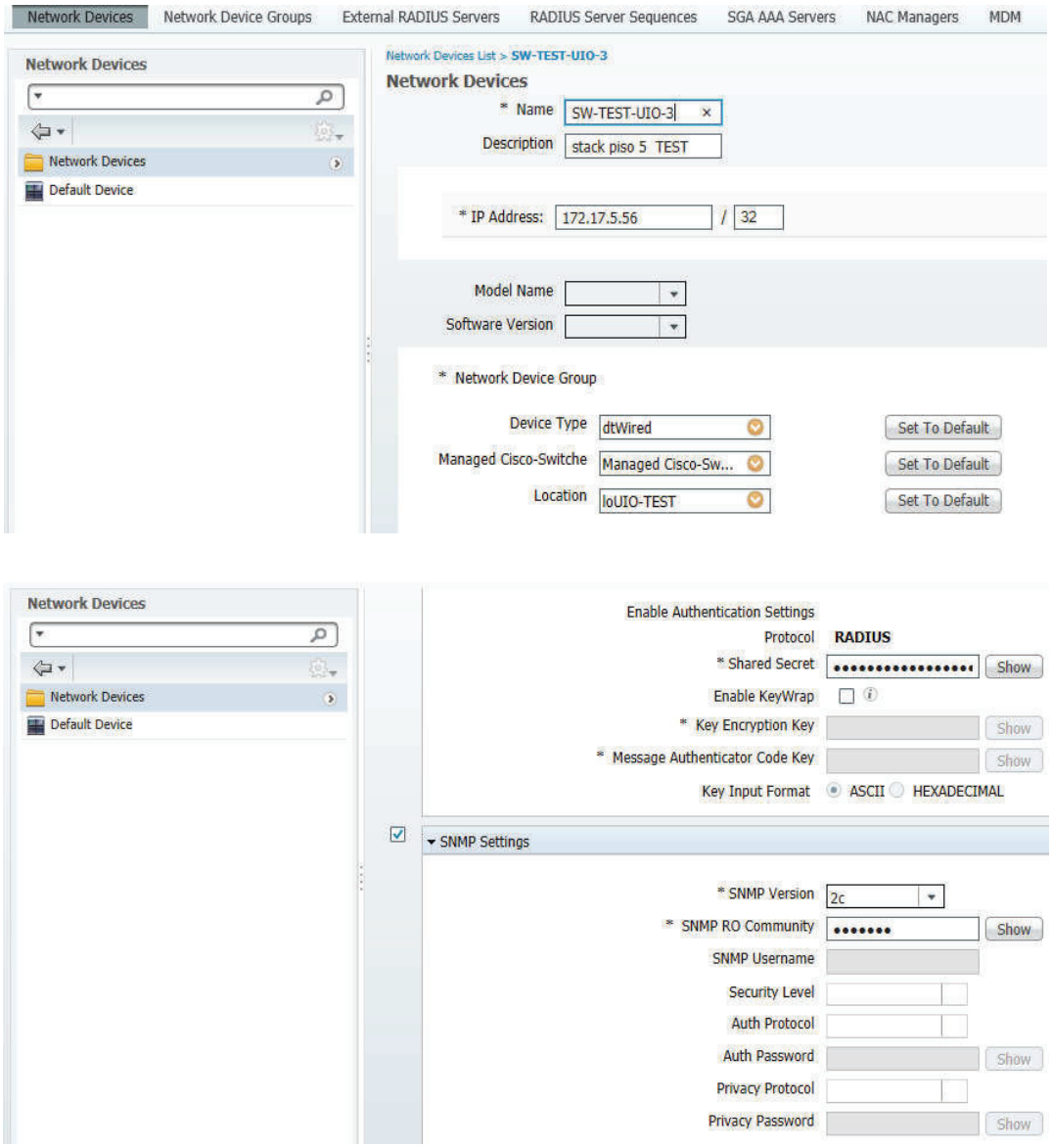

Figura 3.53 Configuración del *switch* de acceso como NAD reconocido por el ISE

c. Configuración cliente RADIUS en la WLC

Para la configuración de una WLC como cliente RADIUS y autenticado como NAD en el ISE, es necesario crear un perfil cliente RADIUS.

Los parámetros solicitados son *Name, Description, IP addrress, Location, Device Type, Radius, snmp comunity*. Y una contraseña compartida entre el ISE y la WLC (ver figura 3.54).

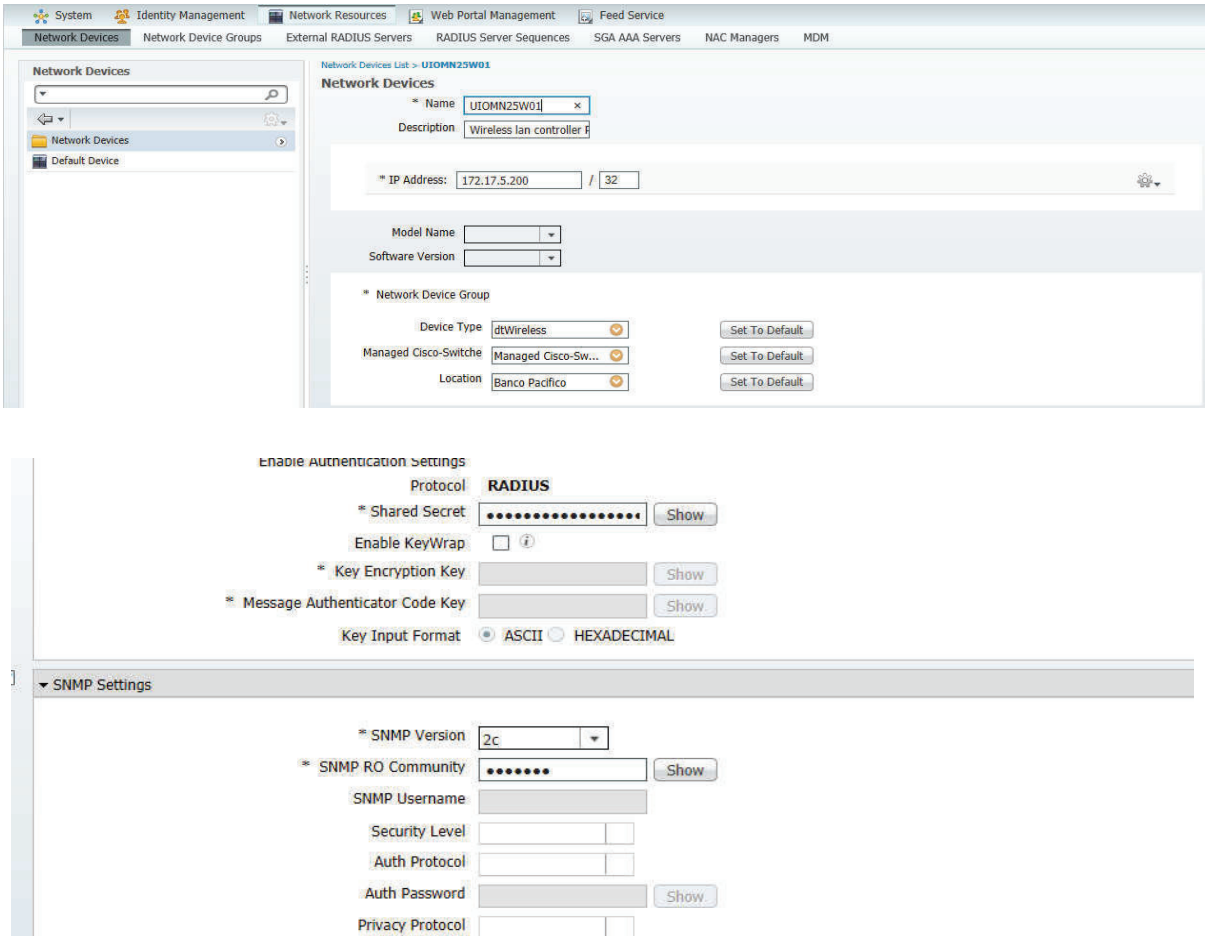

Figura 3.54 Configuración de la WLC como NAD reconocido por el ISE

3.2.3.3 Definición general de control de acceso para la red de la empresa

En resumen, el esquema general de control de acceso para la red de la empresa, independiente del tipo de conexión (cableada o inalámbrica), se describe en la figura 3.55, permitiendo un control de acceso basado en la detección de tipo de equipo para la ejecución de la respectiva política para ingreso de credenciales, cumplimiento estricto de postura, y concesión de permisos dependiendo del tipo de conexión y tipo de usuario autenticado.

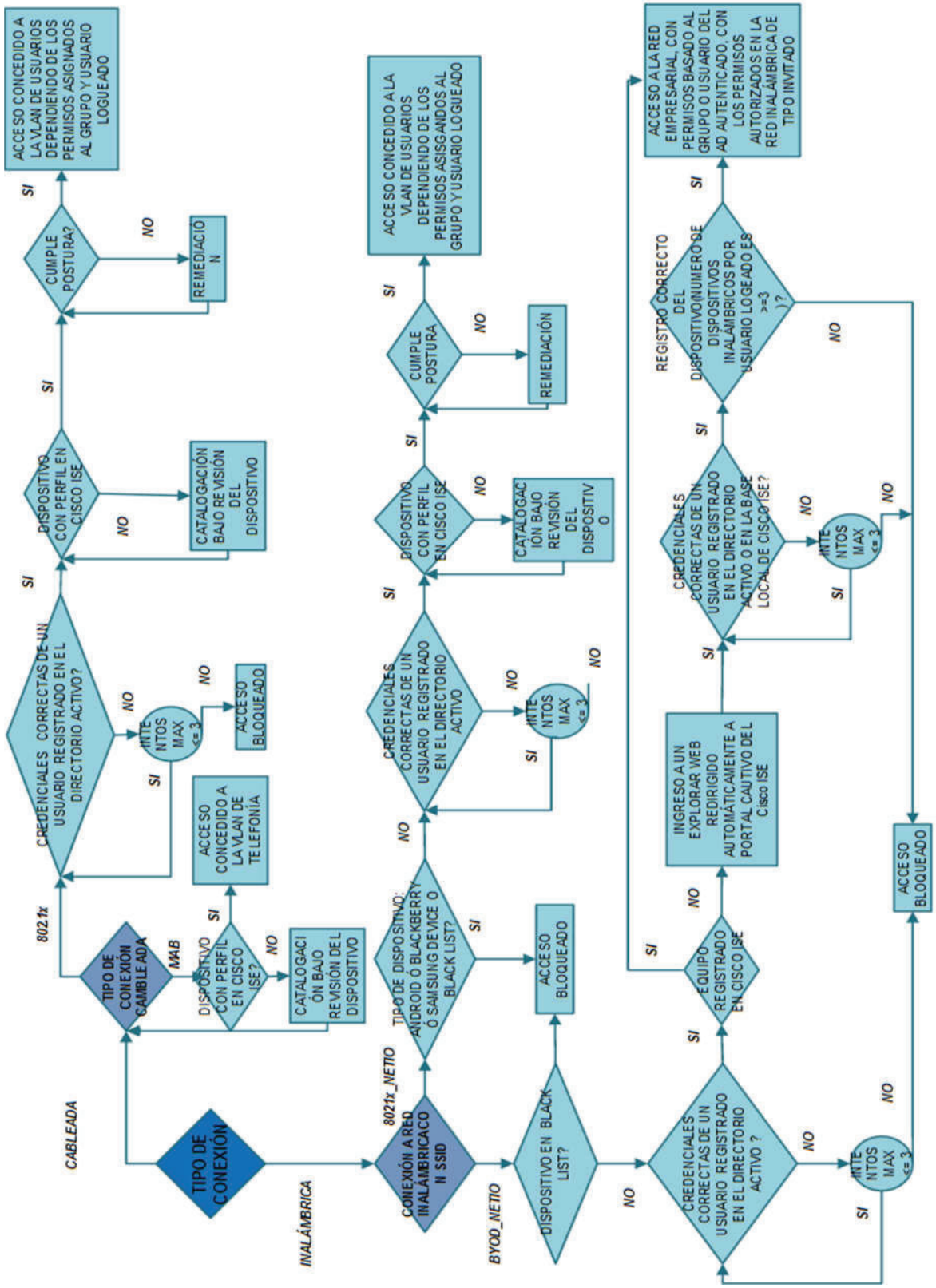

Figura 3.55 Control de acceso basado en AAA

3.2.3.4 Análisis de latencia antes y después de la gestión de autenticación a través de Cisco ISE

Para el análisis de latencia antes de la implementación de Cisco ISE, únicamente se toma en consideración el ingreso de credenciales para iniciar sesión y que el computador reciba direccionamiento IP (aproximadamente 90 segundos), mientras que al implementar autenticación a través de Cisco ISE, se debe considerar los tiempos en Autenticación, vinculación al AD o registro en el ISE, perfilamiento, postura, remediación si es necesario y autorización.

Los resultados de análisis de la latencia en la red cableada (tanto en computadoras como en teléfonos IP) con autenticación basada en Cisco ISE, los resultados de análisis de la latencia en la WLAN 8021X_NETIO (tanto en *laptops* como en dispositivos móviles) con autenticación basada en Cisco ISE y los resultados de análisis de la latencia en la WLAN BYOD_NETIO (tanto en *laptops* como en dispositivos móviles) con autenticación basada en Cisco ISE se detalla en la tabla 3.22.

Podemos definir que el tiempo adicional que incorpora la implementación de equipamiento de la plataforma de autenticación Cisco ISE es justificado con el mejoramiento de seguridad de acceso tanto para usuarios como para sus dispositivos, promoviendo el BYOD.

Todo dispositivo conectado a un puerto de acceso o que intenta acceder a la WLAN corporativa registrado o no, será obligatoriamente escaneado y se ejecutarán las políticas de:

- Autenticación (verificación de usuario)
- Perfilamiento (verificación del tipo de dispositivo)
- Postura (verificación de parámetros de operación en el dispositivo)
- Remediación (instalación de parámetros faltantes en el dispositivo para cumplir la postura)
- Autorización (después de la verificación del usuario y dispositivo se asignan de permisos de acceso respectivos)

TIPO DE DISPOSITIVO	TIPO DE USUARIO	PERFIL DETECTADO	TIPO DE CONEXIÓN	¥INCULADA AL DOMINIO	AUTENTICACIÓN [s]	PERFILAMIENTO [s]	POSTURA [s]	REMEDIACIÓN [s]	AUTORIZACIÓN [s]	TIEMPO REQUERIDO PARA ACCESO A SERVICIOS [s]
COMPUTADOR DE ESCRITORIO	CORPORATIVO	SI	CABLEADA	SI	30	30	30	0	30	120
	INVITADO REGISTRADO	SI	CABLEADA	SI	30	30	30	1080	30	1200
	INVITADO NO REGISTRADO	SI	CABLEADA	NO	300	30	30	1080	30	1470
TELEFONO IP	REGISTRADO	SI	CABLEADA	SI	30	30	NO APLICA	NO APLICA	30	90
	NO REGISTRADO	SI	CABLEADA	NO	90	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	120
ANY	ANY	SI	CABLEADA	NO	90	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO	90
ANY	ANY	NO	CABLEADA	NO	90	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO	90
LAPTOP	CORPORATIVO	SI	INALÁMBRICA (802.1x, METID)	SI	30	30	30	0	30	120
	INVITADO REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	SI	30	30	30	1080	30	1200
	INVITADO NO REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	NO	90	30	30	1080	30	1260
SMARTPHONE	REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60
	NO REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	NO	90	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	120
TABLET	REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60
	NO REGISTRADO	SI	INALÁMBRICA (802.1x, METID)	NO	90	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	120
ANY	ANY	SI	INALÁMBRICA	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60
ANY	ANY	NO	INALÁMBRICA	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60
LAPTOP	CORPORATIVO	SI	INALÁMBRICA (BYOD_METID)	SI	30	30	30	0	30	120
	INVITADO REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	SI	30	30	30	1080	30	1200
	INVITADO NO REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	NO	90	30	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS	120
SMARTPHONE	REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	NO	30	30	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS	60
	NO REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	NO	90	30	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS	120
TABLET	REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	NO	30	30	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS	60
	NO REGISTRADO	SI	INALÁMBRICA (BYOD_METID)	NO	90	30	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS	120
ANY	ANY	SI	INALÁMBRICA	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60
ANY	ANY	NO	INALÁMBRICA	NO	30	30	BLOQUEADO	BLOQUEADO	BLOQUEADO	60

Tabla 3.22 Resumen de latencia en la red cableada e inalámbrica con la implementación de Cisco ISE

3.3 PRUEBAS DE FUNCIONAMIENTO

El desarrollo del prototipo permite probar perfiles de usuarios, políticas de seguridad, niveles de acceso definidas en el rediseño de los servicios implementados en el prototipo, en ellos está el servidor DNS, servidor DHCP, servidor AD, servidor FTP, servidor HTTP, pero cabe destacar que el prototipo se enfoca en las pruebas de autenticación, perfilamiento, autorización, postura y remediación, tanto para la red cableada (computadores de escritorio, teléfonos IP) como para la red inalámbrica (*laptops, Smartphones, tablets*).

En esta sección se presentará las pruebas realizadas con el prototipo y los resultados que se obtuvieron del desarrollo del mismo.

3.3.1 PRUEBAS DE CONEXIÓN A TRAVÉS DE LA RED CABLEADA

Para las pruebas sobre la red cableada existen dos tipos de conexiones disponibles a través de 802.1x y MAB, en la primera se pueden verifican credenciales como nombre de usuario y contraseña y/o identificación del dispositivo con el que se desea conectar a la red cableada, mientras que la segunda opción únicamente se realizará una verificación de la dirección MAC del dispositivo (autenticación), si la misma se encuentra en la lista de dispositivos registrados y permitidos se le concederá acceso caso contrario será denegado, a continuación se procede con la determinación de tipo de dispositivo (perfilamiento), luego dependiendo del tipo de dispositivo se valida si el mismo cumple con los parámetros definidos, por ejemplo que se encuentre instalado el *antivirus* (postura) y si los cumple se le concede acceso a la red empresarial limitado por los permisos asignados dependiendo del tipo de usuario, si la postura no se cumple, el dispositivo es trasladado a una VLAN de cuarentena hasta que instale o active los parámetros de operación faltantes (remediación).

3.3.1.1 Estación de trabajo usuario corporativo

Se presentan las pruebas realizadas sobre una computadora de escritorio de un usuario corporativo que cuenta con todos los aplicativos y *antivirus* corporativo.

3.3.1.1.1 Pruebas de autenticación

Verificación de la autenticación de usuarios y dispositivos.

Cuando un computador se enciende e inicia el proceso de arranque y búsqueda de un servicio de DHCP, el puerto del *switch* se encuentra configurado para asignar temporal direccionamiento IP en la VLAN temporal con ID 170 (VLAN de cuarentena), cuando lo obtiene e intenta iniciar sesión en el computador, ingresa su nombre de usuario y contraseña, estas credenciales de usuario son enviadas al *switch* y posteriormente al ISE, va a aparecer la pantalla de *login*, si las credenciales del usuario son correctas (se verifica coincidencia con los registros del AD) ingresa al *home* del usuario.

3.3.1.1.2 Pruebas de perfilamiento

Todos los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, con la identificación del dispositivo ejecuta las políticas correspondientes, en este caso reconoce al dispositivo como computador y la marca en este caso HP, a través del puerto fa0/16 del *switch* denominado SW_ACC_B15_A1 (ver figura 3.56).

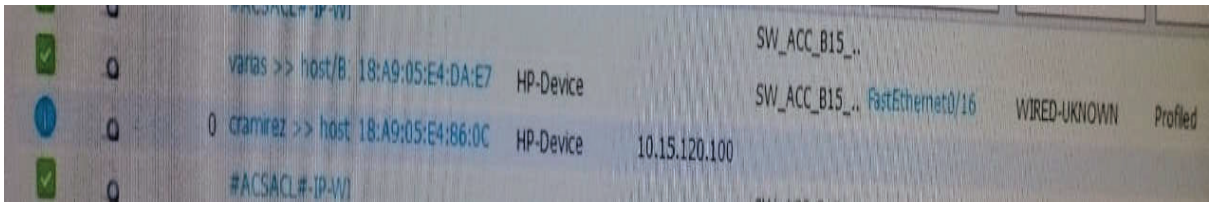

Figura 3.56 Captura de Cisco ISE de perfilamiento del dispositivo

3.3.1.1.3 Pruebas de postura

Una vez validada la identidad del usuario, y determinado el tipo de dispositivo, se procede con el escaneo de aplicativos instalados en el computador, en este caso la política determina que debe estar instalado el *antivirus* corporativo Kaspersky, por tanto arranca el agente de aprovisionamiento, agente NAC (ver figura 3.57).

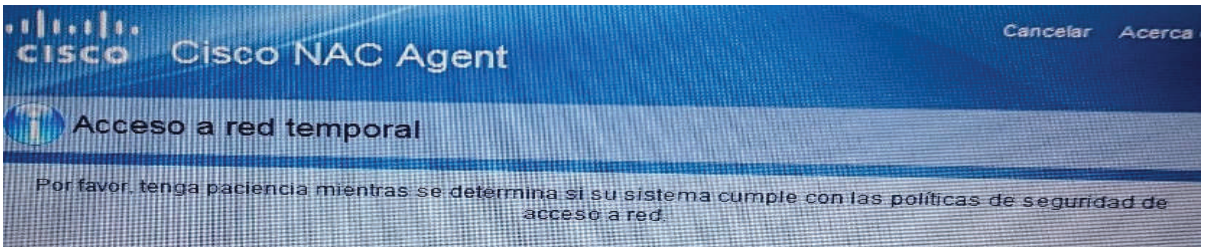

Figura 3.57 Análisis del sistema operativo del cliente de aprovisionamiento

Como se trata de un computador de la empresa posee todos los aplicativos de las políticas de red. Por tanto cumple con la postura y no es necesario la ejecución de la remediación (ver Figura 3.58).

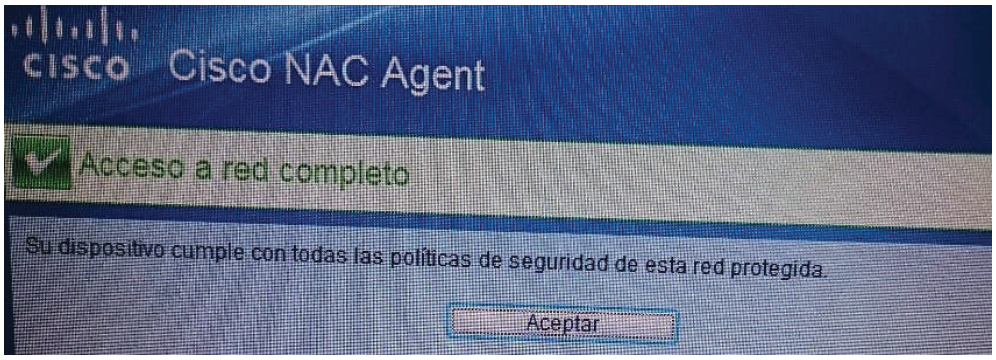

Figura 3.58 Respuesta de Agente de NAC de cumplimiento de postura.

3.3.1.1.4 Prueba de remediación

Como el dispositivo cumple con la política de postura, no es necesario realizar la política de remediación, por tanto pasa directamente a la revisión de la política de autorización.

3.3.1.1.5 Prueba de autorización

Se determinará que a los usuarios y dispositivos se les asigne los permisos correctos de acceso a los recursos de red. Se realizaron 2 pruebas, una con un usuario earias (del grupo Proyectos con permisos exclusivo de mail corporativo, servidor web) el mismo tuvo acceso sin inconvenientes a estos servicios, mientras que al servidor ftp fue denegado confirmando así la correcta asignación de permisos.

3.3.1.2 Estación de trabajo usuario invitado

Se presentarán las pruebas realizadas sobre una computadora de escritorio de un usuario invitado que no cuenta con todos los aplicativos y *antivirus* corporativo.

3.3.1.2.1 Pruebas de autenticación

Verificación de la autenticación de usuarios y dispositivos. El usuario invitado debe comunicarse con anticipación con el área de tecnologías para solicitar la creación de una cuenta de usuario invitado temporal y la asignación de los permisos pertinentes dependiendo de la tarea que va a realizar.

3.3.1.2.2 Pruebas de perfilamiento

Todos los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, en este caso un computador de la marca Compaq.

3.3.1.2.3 Pruebas de postura

Como se trata de un computador de un usuario invitado registrado temporalmente en el AD, su computador no cumple con la política de la instalación del *antivirus* corporativo, de manera que el agente NAC al terminar el escaneo determina el incumplimiento de la política de postura, por tanto debe ejecutar remediación.

3.3.1.2.4 Prueba de remediación

Como el dispositivo escaneado no cumple con la política de postura, debe ejecutar la política de remediación, por tanto el agente NAC proporciona la opción de descarga del agente del *antivirus*, para proceder con la instalación remota a través de la consola de Administración del *antivirus* corporativo.

Cuando ejecute la política de postura y se confirme la instalación del *antivirus*, pasará a la verificación de la política de autorización (ver figura 3.59).

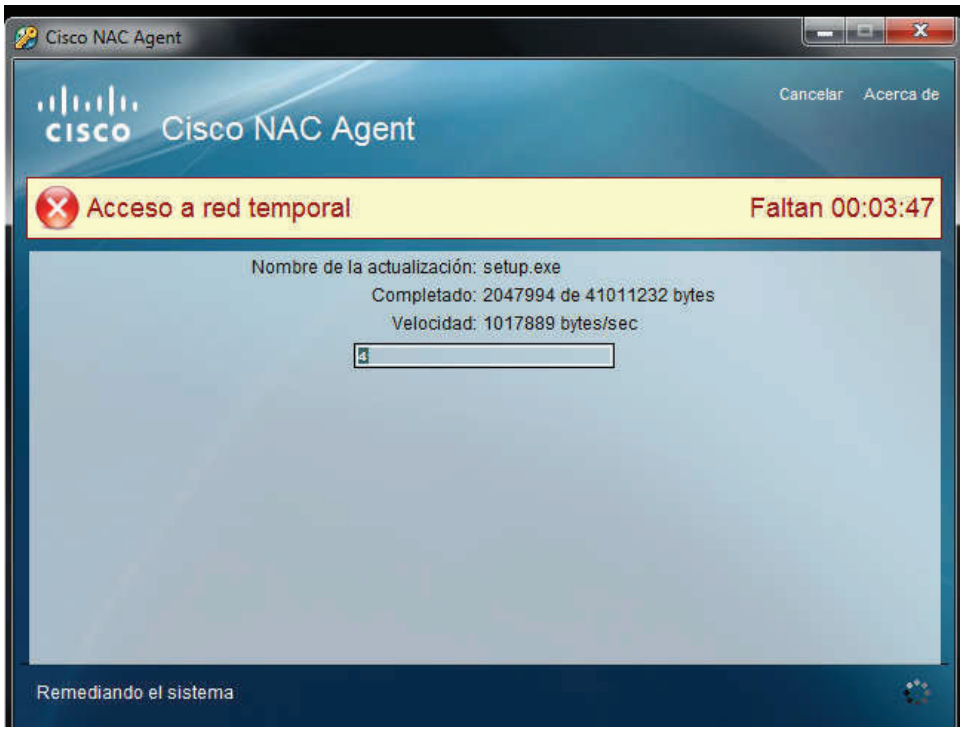

Figura 3.59 Agente de aprovisionamiento para ejecución de remediación

3.3.1.2.5 Prueba de autorización

Se ha determinado que al usuario autenticado y dispositivo se asigne los permisos correctos de acceso a los recursos de red. En este caso, el usuario es de tipo invitado por tanto al ejecutar la política de autorización se realizan las pruebas respectivas y se confirma que el usuario únicamente tiene acceso a *Internet* y el resto de servicios corporativos está bloqueado.

3.3.1.3 Teléfono IP registrado

Se realizarán las pruebas de las políticas definidas sobre un teléfono IP de la empresa registrado en el ISE a través de su dirección MAC. Cisco ISE determina el tipo de dispositivo a través de varios parámetros, pero se consideró que el óptimo para verificar la identidad del dispositivo era a través de su dirección MAC ya que la marca del teléfono utilizado en el prototipo es Grandstream, pero no fue reconocida de manera nativa por el ISE.

3.3.1.3.1 Pruebas de autenticación

Verificación de la autenticación del dispositivo, en este caso un teléfono IP conectado a un puerto de un *switch* de acceso revisa la dirección MAC del dispositivo y envía al ISE para su verificación, que en este caso es correcta. Por tanto se asigna directamente a la VLAN de voz.

3.3.1.3.2 Pruebas de perfilamiento

Todos los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, en este caso Cisco ISE no determina la marca Panasonic, por tanto fue necesario la definición de un nuevo perfil de tipo PHONE (se comprobó la coincidencia de los primeros dígitos de la dirección MAC de los teléfonos IP corporativos así que se creó un nuevo perfil, que verifique este parámetro).

3.3.1.4 Teléfono IP no registrado

Se realizarán las pruebas de las políticas definidas sobre un teléfono IP no registrado en el ISE.

3.3.1.4.1 Pruebas de autenticación

Verificación de la autenticación de usuarios y dispositivos.

Por el tipo de dispositivo no se envían credenciales sino se verifica la dirección MAC, como el dispositivo no está registrado, no coincide con ninguna entrada en el ISE, por tanto se bloquea el acceso.

3.3.1.4.2 Pruebas de perfilamiento

Los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, en este caso se determina que se trata de un teléfono IP, el perfil tipo PHONE.

3.3.2 PRUEBAS DE CONEXIÓN A TRAVÉS DE LA RED INALÁMBRICA

Las pruebas de acceso respectivas a la red inalámbrica, serán divididas en dos secciones cada una relacionada a una WLAN en específico, cada una con propiedades y permisos de acceso diferentes. Según las políticas de red, la WLAN 8021x_NETIO permite acceso exclusivo a las *laptops* a los servicios de la empresa a usuarios corporativos, mientras que la WLAN BYOD_NETIO permite el acceso a *Internet* a todo dispositivo móvil que contenga credenciales de usuario dentro del dominio de la empresa y su dispositivo sea registrado en el ISE a través de un portal cautivo.

3.3.2.1 Red inalámbrica con *SSID* 802.1X_NETIO

En este caso, se realizará la prueba de acceso con *laptops* de un usuario corporativo, un usuario invitado y dispositivos móviles.

3.3.2.1.1 Laptop usuario corporativo

Se realiza la prueba de acceso a través de una *laptop* de usuario corporativo, por tanto la misma consta con aplicativos y *antivirus* corporativo.

a. Pruebas de autenticación

Verificación de la autenticación de usuarios y/o dispositivos. En este caso se valida las credenciales del usuario corporativo.

b. Pruebas de perfilamiento

Los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, en este caso lo reconoce como Compaq-*device* (que es la marca exacta de la *laptop*).

c. Pruebas de postura

Se ejecuta la política de postura y se verifica la instalación del *antivirus* corporativo. Si la cumple para directamente a la revisión de la política de autorización si no la cumple de ejecutar la política de remediación.

d. Pruebas de remediación

No se ejecuta ya que la política de postura se cumple.

El computador tiene instalado el *antivirus Kaspersky* y activo *Windows Defender*.

e. Pruebas de autorización

Se realizan las pruebas de acceso a los servicios corporativos, en este caso el usuario autenticado pertenece al grupo Gerente por tanto tiene acceso a todos los servicios de red.

3.3.2.1.2 Laptop usuario invitado

Se realiza la prueba de acceso a través de una *laptop* de usuario invitado, por tanto no consta con aplicativos ni *antivirus* corporativo.

a. Pruebas de autenticación, perfilamiento, postura, remediación y autenticación

Verificación de la autenticación de usuarios y/o dispositivos.

Como se trata de un usuario invitado, el mismo debe comunicarse con anticipación para la creación de una cuenta de usuario de tipo invitado y los permisos requeridos.

Los dispositivos IP mediante revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico.

En este caso, se verifica que se trata de una *laptop* y el ISE la detecta como ACER-*device*.

Se ejecuta el agente de aprovisionamiento y se determina que el *antivirus* corporativo no se encuentra instalado.

Por tanto debe ejecutarse la política de remediación y posteriormente dependiendo del tipo de usuario, la verificación de los permisos concedidos de acceso, en este caso únicamente acceso a *Internet*.

3.3.2.1.3 Teléfono inteligente registrado y no registrado

Un teléfono inteligente y una *tablet* intentan conectarse a la WLAN 8021x_NETIO.

a. Pruebas de autenticación, perfilamiento y autorización

Mediante la revisión de tráfico y comportamiento serán asociados a un tipo de dispositivo específico, por tanto determina que se trata de dispositivos móviles, aun cuando se autentique el usuario correctamente existe un política de autorización de bloqueo para los dispositivos móviles hacia esta red, de manera que se bloquea el acceso al dispositivo.

3.3.2.2 Red inalámbrica con *SSID* BYOD_NETIO

Esta WLAN permite el acceso a todo dispositivo que intente conectarse inalámbricamente y posea credenciales de usuario corporativo o invitado en el AD de la empresa.

Luego de conectarse a la red se solicita un registro obligatorio del dispositivo en el ISE, que guarda el registro de la dirección MAC con un identificador que proporciona el usuario, se limita el registro hasta 3 dispositivos.

Cuando el dispositivo se encuentre registrado obtendrá los permisos de acceso asignados dependiendo del usuario y hacia esta WLAN.

3.4 ANÁLISIS DE RESULTADOS

Según las pruebas realizadas con el prototipo, se puede determinar que el diseño de la red multiservicios con:

- Autenticación (acceso a la red empresarial únicamente a usuarios registrados en el AD o en el Cisco ISE)
- Perfilamiento (detección específica del tipo de dispositivo y acceso exclusivo a los configurados en el Cisco ISE según las políticas de la empresa)

- Autorización (basado exclusivamente en los permisos de acceso de acuerdo a los grupos definidos en el *Active Directory* como en el permisos de los usuarios locales del Cisco ISE)
- Postura (únicamente los dispositivos que cumplan los parámetros de configuración del sistema operativo definidos por las políticas de red tendrán acceso)
- Remediación (dispositivos que pertenezca a la red empresarial, pero no cumplen con la postura definida por las políticas de red pueden remediar su sistema para cumplirla pero únicamente si las revisiones anteriores fueron exitosas)

Se convierte en una red robusta con respecto a la seguridad de acceso y verificación de identidades de usuario y dispositivos, tal como fue propuesto en el capítulo No.3, es factible para la transmisión de los tres servicios: datos, voz y video sobre la misma infraestructura de red.

La tabla 3.23 describe un resumen de las pruebas realizadas, y los resultados obtenidos en cada tipo de conexión de cada tipo de dispositivo (computador de escritorio, *laptop*, teléfono IP, *Smartphone, tablet*) y nos permite verificar el cumplimiento de las políticas de acceso de la empresa, permitiendo un acceso seguro a los servicios de la red de la empresa.

Esta plataforma no exige únicamente la autenticación de un usuario para la concesión de acceso sino que valida tanto usuarios y dispositivos, que los mismos cumplan con los parámetros de operación definidas por las políticas de red de la empresa y verifica que se asignen al usuario los permisos correspondientes dependiendo del tipo de usuario y grupo del AD.

Cabe señalar que en la Tabla 3.23, se presenta un resumen de todas las pruebas realizadas de autenticación, perfilamiento, postura, remediación y autorización y resultados obtenidos tanto para la red cableada como para la red inalámbrica (ver Anexo C19).

TIPO DE DISPOSITIVO	MARCA	TIPO DE USUARIO	PERFIL DETECTADO	TIPO DE CONEXIÓN	VINCULADA AL DOMINIO	AUTENTICACIÓN	RESULTADO	PERFILAMIENTO	POSTURA	REMEDIACIÓN	AUTORIZACIÓN
									SI	NO	REVISIÓN TIPO USUARIO Y GRUPO Y ASIGNACIÓN DE PERMISOS RESPECTIVOS
COMPUTADOR DE ESCRITORIO	DELL	CORPORATIVO	SI	CABLEADA	SI	SI	PERMIT	COMPUTADOR [MARCA REGISTRADA]	NO [DEBE REALIZAR REMEDIACIÓN]	INSTALACIÓN REMOTA APLICATIVO	REVISIÓN TIPO USUARIO Y GRUPO Y ASIGNACIÓN DE PERMISOS RESPECTIVOS
	DELL	INVITADO REGISTRADO	SI	CABLEADA	SI	SI	PERMIT	COMPUTADOR [MARCA REGISTRADA]			
	COMPAQ	INVITADO NO REGISTRADO	SI	CABLEADA	NO	NO	DENY HASTA QUE SE VINCULE AL DOMINIO	COMPUTADOR	BLOQUEADO	BLOQUEADO	BLOQUEADO
	PANASONIC	REGISTRADO	SI	CABLEADA	SI	SI	PERMIT	PHONE	NO APLICA	NO APLICA	ACCESO A LA VLAN DE TELEFONÍA
TELEFONO IP	PANASONIC	NO REGISTRADO	SI	CABLEADA	NO	SI	DENY (DISPOSITIVO NO PERMITIDO)	PHONE	BLOQUEADO	BLOQUEADO	BLOQUEADO
											REVISIÓN TIPO USUARIO Y GRUPO Y ASIGNACIÓN DE PERMISOS RESPECTIVOS
	COMPAQ	CORPORATIVO	SI	INALÁMBRICA (802.1x_NETIO)	SI	SI	PERMIT	LAPTOP [MARCA REGISTRADA]	SI	NO	
LAPTOP	COMPAQ	INVITADO REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	SI	SI	PERMIT	LAPTOP [MARCA REGISTRADA]	NO [DEBE REALIZAR REMEDIACIÓN]	INSTALACIÓN REMOTA APLICATIVO	REVISIÓN TIPO USUARIO Y GRUPO Y ASIGNACIÓN DE PERMISOS RESPECTIVOS
	COMPAQ	INVITADO NO REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	NO	SI	DENY HASTA QUE SE VINCULE AL DOMINIO, O REGISTRE LA LAPTOP	LAPTOP [MARCA REGISTRADA]	BLOQUEADO	BLOQUEADO	BLOQUEADO
	SONY	REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	NO	SI	DENY (DISPOSITIVO NO PERMITIDO)	DISPOSITIVO MOVIL	BLOQUEADO	BLOQUEADO	BLOQUEADO
SMARTPHONE	IPHONE	NO REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	NO	SI	DENY (DISPOSITIVO NO PERMITIDO)	DISPOSITIVO MOVIL	BLOQUEADO	BLOQUEADO	BLOQUEADO
	SAMSUNG	REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	NO	SI	DENY (DISPOSITIVO NO PERMITIDO)	DISPOSITIVO MOVIL	BLOQUEADO	BLOQUEADO	BLOQUEADO
TABLET	SAMSUNG	NO REGISTRADO	SI	INALÁMBRICA (802.1x_NETIO)	NO	SI	DENY (DISPOSITIVO NO PERMITIDO)	DISPOSITIVO MOVIL	BLOQUEADO	BLOQUEADO	BLOQUEADO
	COMPAQ	CORPORATIVO	SI	INALÁMBRICA (BYOD_NETIO)	SI	SI	PERMIT	DISPOSITIVO MOVIL [COMPAQ]	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
LAPTOP	COMPAQ	INVITADO REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	SI	SI	PERMIT	DISPOSITIVO MOVIL [COMPAQ]	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
	COMPAQ	INVITADO NO REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	NO	SI	DENY HASTA QUE SE REGISTRE LA LAPTOP	DISPOSITIVO MOVIL [COMPAQ]	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
	SONY	REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	NO	SI	PERMIT	DISPOSITIVO MOVIL (SONY)	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
SMARTPHONE	IPHONE	NO REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	NO	SI	DENY HASTA QUE REGISTRE EL DISPOSITIVO MOVIL	DISPOSITIVO MOVIL (IPHONE)	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
	SAMSUNG	REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	NO	SI	PERMIT	DISPOSITIVO MOVIL (SAMSUNG)	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
TABLET	SAMSUNG	NO REGISTRADO	SI	INALÁMBRICA (BYOD_NETIO)	NO	SI	DENY HASTA QUE REGISTRE EL DISPOSITIVO MOVIL	DISPOSITIVO MOVIL (SAMSUNG)	NO APLICA	NO APLICA	DEBE REGISTRAR EL DISPOSITIVO A TRAVES DEL PORTAL CAUTIVO DEL ISE HASTA UN MÁXIMO DE 3 DISPOSITIVOS
ANY	ANY	ANY	SI	CABLEADA	NO	NO	DENY (3 INTENTOS FALLIDOS Y SERÁ BLOQUEADO)	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO
ANY	ANY	ANY	NO	CABLEADA	NO	NO	DENY (3 INTENTOS FALLIDOS Y SERÁ BLOQUEADO)	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO
ANY	ANY	ANY	SI	INALÁMBRICA	NO	NO	DENY (3 INTENTOS FALLIDOS Y SERÁ BLOQUEADO)	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO
ANY	ANY	ANY	NO	INALÁMBRICA	NO	NO	DENY (3 INTENTOS FALLIDOS Y SERÁ BLOQUEADO)	BLOQUEADO	BLOQUEADO	BLOQUEADO	BLOQUEADO

Tabla 3.23 Resumen de pruebas de acceso desde diferentes tipos de dispositivos finales

- ❖ Observaciones:
  - Dispositivo sin perfil, no tendrá acceso hasta que se registre su perfil dentro de los definidos por defecto o se puede crear uno nuevo personalizado.
  - Los permisos de acceso a la WLAN BYOD dependen de las ACL configuradas en el ISE y la WLC, y del tipo de usuario.

3.5 BENEFICIOS DIRECTOS

- ❖ El rediseño implementa una red redundante, flexible, de alta disponibilidad, ya que el cableado y demás componentes pasivos y activos que conforman este sistema se han dimensionado de forma adecuada y garantizan la transmisión correcta de la información a nivel de capa física y se determinó los puntos críticos en donde es requerido redundancia a nivel de equipos como de enlaces.
- ❖ La implementación de Cisco ISE permite de forma adecuada y segura el acceso a los servicios de la red empresarial exclusivamente a usuarios configurados en el AD o usuarios locales del Cisco ISE.
- ❖ Los equipos activos de núcleo, distribución y acceso definidos permiten implementar los servicios planteados, pues como se indica en el desarrollo del prototipo se necesitan algunas características como manejo de VLAN, AAA, SNMP, *logs* EPM, enrutamiento entre otras. Sus equipos deberán manejar similares características para que exista compatibilidad y soporte con el Cisco ISE recomendado.
- ❖ El rediseño presenta una infraestructura escalable, lo que permite el crecimiento de usuarios y dependiendo de los requerimientos, la implementación de nuevos servicios.
- ❖ En cuanto a los servidores actuales de la empresa, y los enlaces troncales están en capacidad de soportar el tráfico generado por los usuarios y de ofrecer los servicios de DNS, DHCP, FTP, WWW y Telefonía IP, respectivamente, todas las horas del día, garantizando disponibilidad de cada uno de los servicios de la red corporativa, lo requerido será espacio en los racks y conexiones de red para la incorporación de los *appliance* de Cisco ISE.

- Además el diseño propuesto para la red, considera políticas de seguridad, tanto físicas como en el aspecto lógico, para asegurar la confiabilidad de la información y de cada uno de los dispositivos que conforman la red multiservicios.
- Todos los puertos de los *switches* de acceso se encuentran configurados con una plantilla que permite conectarse al ISE para la discriminación del dispositivo y la ejecución de las políticas respectivas, no es necesario crear configuraciones diferentes a cada puerto dependiendo del tipo de dispositivo.
- La implementación de la plataforma de autenticación Cisco ISE permite disminuir los huecos de seguridad, la creación de servicios recreativos, realizar *accounting*, llevar registro de los horarios de utilización, mejorar nivel de seguridad para los accesos de usuarios tipo contratistas, recibir notificaciones de comportamiento extraño, escanear intentos de ingreso de acceso fallido, entre otros.

3.6 BENEFICIOS INDIRECTOS

- Reducción significada en el tiempo de configuraciones específicas para cada dispositivo nuevo en la red, la inclusión de nuevos tipos de dispositivos finales a la red se limita al reconocimiento automático o manual del perfil y la determinación de las políticas asociadas.
- Reducción significativa en las tareas manuales de *helpdesk* (revisión, actualización de *Antivirus* y parches).
- La implementación de este tipo de plataforma, permite disminuir los tiempos muertos de productividad, por algún cambio de configuración con relación a instalación de aplicativos de cumplimiento de políticas de red, registro de usuarios invitados y monitoreo efectivo de las conexiones de los mismos.

CAPÍTULO IV

PRESUPUESTO REFERENCIAL

En este capítulo se presenta los costos referenciales de los elementos necesarios para la implementación de la autenticación a través de la plataforma de autenticación Cisco ISE en la red multiservicios, para los once bloques de operación de la empresa, considerando la homologación a la marca Cisco, así como los costos correspondientes a traslado, configuración, cambios en la infraestructura e instalación de la nueva plataforma de autenticación.

4.1 RED ACTIVA

La red activa de la empresa se encuentra conformada por los equipos de conectividad, equipos Cisco ISE (considerando los 3 roles por separado como fue detallado en la sección 3.1.2), licencias para *endpoints* (para el funcionamiento correcto del ISE en la empresa no basta con solo adquirir el equipo , sino que deben ser adquiridas también licencias por cada dispositivo final que será autenticado tanto en la red cableada como en la inalámbrica) junto con las garantías técnicas del equipo y soporte técnico, acometidas eléctricas adicionales para los nuevos equipos, racks adicionales, aire acondicionado, UPS, entre otros.

4.1.1 COSTOS REFERENCIALES DE LA RED ACTIVA

Se analizará aspectos técnicos y económicos de los equipos de la marca Cisco, determinando las características que permitan satisfacer los requerimientos actuales.

4.1.1.1 Dispositivos de Red (NAD)

Los dispositivos NAD (*Network Access Device*) permiten que los dispositivos finales (*endpoints*) puedan conectarse a los recursos de red, previo el envío de credenciales para validad su identidad, si las mismas son correctas ingresa a la red empresarial caso contrario será denegado el acceso.

4.1.1.1.1 Switches de la capa de acceso

Gracias a los resultados del inventario realizado sobre todos los equipos de conectividad de los bloques de operación y la matriz, se determinó la existencia de *switches* compatibles con el ISE en perfecto estado, pero sin uso. Los valores presentes en la columna NÚMERO DE *SWITCHES* de la Tabla 4.1 hacen referencia al número de equipos para la capa de acceso, que serán traslados a los bloques respectivos dependiendo de la densidad de puertos requerida (ver Anexos digitales C3 y C20).

En el presente rediseño se considera la reutilización de estos equipos, iniciando con el traslado de los equipos sin uso a bloques que los requieren (analizando la densidad de puertos requerida por bloque) y con la actualización de IOS, para el cumplimiento de los prerrequisitos para operación con el ISE (esta tarea pueda ser realizada por los técnicos del área de tecnologías de la empresa).

Por tanto, los costos asociados a los *switches* de acceso corresponden al traslado a los bloques requeridos, montaje en los racks respectivos, configuración e instalación de módulos de fibra y cableado necesario para la interconexión con la capa de distribución (conexión redundante a través de 2 módulos de fibra por *switch*).

La empresa de telecomunicaciones AKROS, cotizó dichos módulos en 248,00 USD (ver Tabla 4.1), y la proforma recibida se detalla en el Anexo D0 que incluye el costos de los módulos y la certificación respectiva.

BLOQUE DE INSTALACIÓN	NÚMERO DE *SWITCHES*	NÚMERO DE INTERFACES DE FIBRA	COSTO UNITARIO	COSTO TOTAL
BLOQUE 1	8	32	$ 248,00	$ 3968
BLOQUE 12	1	4	$ 248,00	$ 496
BLOQUE 15	32	128	$ 248,00	$ 15872
BLOQUE 21	1	4	$ 248,00	$ 496
BLOQUE 18	17	68	$ 248,00	$ 8432
BLOQUE 31	34	136	$ 248,00	$ 16864
BLOQUE 43	50	200	$ 248,00	$ 24800
TOTAL				$ 70928,00

Tabla 4.1 Costos de los módulos de fibra de los *switches* de acceso para cada bloque

4.1.1.1.2 Switches de la capa de distribución

Los *switches* de distribución permitirán la conexión de todos los *switches* de acceso de los bloques de operación y la matriz. Se analiza el *switch Catalyst WS-C4510R (ENGINE 6-E)*, cuyas características se desglosan en la tabla 4.2.

La propuesta económica se obtuvo de la empresa de telecomunicaciones INTCOMEX DEL ECUADOR S.A., esta información está disponible en el Anexo D1 .

ESPECIFICACIONES TÉCNICAS DE LOS *SWITCHES* DE LA CAPA DE DISTRIBUCIÓN	
INTERFACES	Tarjeta de línea de 48 Puertos RJ45 *Full Duplex* de 10/100/1000 Mbps; con características de Auto Negociación, Auto MDI/MDIX y *Autosensing*.
	4 Puertos SFP(*Small Form Pluggable*)
	Puerto de consola
RENDIMIENTO	Buffer de Memoria Basado en Puerto
	Throughput: 18 Mpps
	Velocidad de backplane: 24 Gbps
ESTÁNDARES	10 Base-T, 100BASE-TX, 1000Base-T, 1000 Base-SX
PROTOCOLOS SOPORTADOS	IEEE 802.3i (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab, IEEE802.3z, (Gigabit Ethernet), IEEE 802.3ad, (Agregación), IEEE 802.1d Protocolo Spanning Tree (STP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1q (Trunking), IEEE 802.1x (Autenticación**)**, IEEE 802.1p (Asignación de Prioridades). HSRP.
CARACTERÍSTICAS DE CONMUTACIÓN	Soporte Spanning Tree (STP, RSTP, MSTP).
	Soporte LACP (*Link Aggregation Control Protocol*), Agregación de enlaces.
CARACTERÍSTICAS DE ENRUTAMIENTO	Enrutamiento IP entre VLAN (SVI), soporte de protocolos de enrutamiento.
ADMINISTRACIÓN	Configuración CLI (*Command-line interface*) y vía web, Permitir acceso y configuración vía TELNET, SSH, Soporte SNMP v1, v2c, v3.
SEGURIDAD	Soporte de ACLs (listas de control de acceso) para impedir el acceso de usuarios no autorizados.

Tabla 4.2 Especificaciones Técnicas mínimas de los *Switches* de Distribución

La solicitud de la oferta económica tuvo dos objetivos, conocer una estimación económica de la inversión que consisten la adquisición de cinco *switches* para la capa de distribución y también revisar la opción de no adquirir un equipo completo sino otra

controladora para el *switch* actual de la capa de distribución de los bloques 1, 15, 31, 43, 63. La oferta económica se presenta en la tabla 4.3.

LUGAR	MODELO DE EQUIPOS EN LA CAPA DE DISTRIBUCIÓN	PRECIO UNITARIO	CONTROLADORA ADICIONAL EN EL *SWITCH* DE DISTRIBUCIÓN ACTUAL
BLOQUE 7	WS-C4510R (ENGINE 6-E)	$ 28.406,47	$ 19.995,00
BLOQUE 15	WS-C4507R-E	$ 28.406,47	$ 19.995,00
BLOQUE 31	WS-C4503-E	$ 28.406,47	$ 19.995,00
BLOQUE 43	WS-C4503-E	$ 28.406,47	$ 19.995,00
BLOQUE 63	WS-C4510R+E	$ 28.406,47	$ 19.995,00
	TOTAL	$ 142.032,35	$ 99.975,00

Tabla 4.3 Inversión económica en dispositivos en la capa de distribución

Las dos opciones nos permiten obtener redundancia, pero la primera opción nos permite la implementación de redundancia independiente del equipo. Para este caso los módulos de fibra por *switch* y *tranceivers* externos se incluyen en la propuesta de la empresa, como se visualiza en el Anexo D2 , para completar la conexión mediante hilos de fibra entre el nivel de acceso-distribución y distribución-núcleo.

El costo de cada *transceiver* es de 750,00 USD junto con su respectiva instalación, por tanto el costo de conexión de todos los puertos en redundancia al nuevo equipo es 16.500,00 USD.

4.1.1.1.3 Switches de la capa de núcleo

Los *switches* de núcleo contienen interfaces para la conexión con los *switches* de distribución; además permitirán la conexión del *firewall* corporativo y el *router* que provee los servicios del ISP y *Carrier*. Por la importancia de su funcionamiento ininterrumpido se propone la adquisición de uno adicional por redundancia y alta disponibilidad. En la tabla 4.4 se presentan las especificaciones técnicas del *switch* de la marca Cisco *WS-C6509-E.* La propuesta económica se obtuvo de la empresa de

telecomunicaciones INTCOMEX DEL ECUADOR S.A., se puede observar en el Anexo D2 .

ESPECIFICACIONES TÉCNICAS DEL *SWITCH* DE NÚCLEO		
INTERFACES	Puertos RJ45 10/100/1000Base-T; con características de Auto Negociación, Auto MDI/MDIX y Autosensing.	
	Puerto de consola	
RENDIMIENTO	Throughput: 27 Mpps	
	Velocidad de backplane: 36 Gbps	
PROTOCOLOS SOPORADOS	IEEE 802.3i (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab, IEEE802.3z, (Gigabit Ethernet), IEEE 802.3ad, (Agregación), IEEE 802.1d Protocolo Spanning Tree (STP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1q (Trunking), IEEE 802.1x (Autenticación), IEEE 802.1p (Asignación de Prioridades), IEEE 802.3x. HSRP	
	Soporte LACP (Link Aggregation Control Protocol), Agregación de enlaces	
	Soporte Spanning Tree (STP, RSTP, MSTP)	
	Compatibilidad con el protocolo IEEE 802.3x	
	Soporte del protocolo ARP(Address Resolution Protocol)	
	Manejo de redes virtuales (802.1 q)	
ENRUTAMIENTO CAPA3	Soporte de enrutamiento IPv4, estático, dinámico RIP V1,V2	
	Manejo de protocolos RIP V1,V2, OSPF, IGRP, BGP, IS-IS	
	Soporte de enrutamiento IPv6	
CALIDAD DE SERVICIO	Soporte 802.1 p (Asignación de prioridades al tráfico)	
	Manejo de WRR (Weighted Round-Robin)	
	Clase de servicio basada en puerto, ToS y prioridad de VLAN.	
	Manejo de DSCP (Differentiated Services Code Point)	
SEGURIDAD	Manejo de seguridad en puertos, IEEE 801.X. Autenticación en redes LAN, acceso limitado a determinados segmentos de la red.	
	Gestión segura mediante SSH (Secure Shell) (V1, V2)	
ADMINISTRACIÓN	Configuración CLI (Command-line interface) y vía web	
	Permitir acceso y configuración vía TELNET	
	Soporte SNMP v1, v2c, v3.	
	Soporte DHCP Snooping	
	COSTO TOTAL	**$ 33,650.00**

Tabla 4.4 Especificaciones Técnicas mínimas de los *switches* de Núcleo

4.1.1.2 Equipamiento Cisco ISE

En relación al rediseño realizado en el capítulo 3, se definió que los equipos requeridos son 2 nodos Administrador-ADM (Primario-Secundario), 2 nodos Monitoreo-MON (Primario-Secundario) y 5 nodos Políticas de servicio-PSN.

A continuación, en la tabla 4.5, se detalla el número, modelo de los equipos Cisco ISE requeridos y el precio respectivo.

N°	UBICACIÓN	NUMÉRO DE USUARIOS CONSIDERANDO CRECIMIENTO	ROL CISCO ISE	MODELO ISE	PRECIO
1	BLOQUE 07	805	PSN	Cisco ISE-3315	$ 8.243,44
2	BLOQUE 18	840			
3	BLOQUE 21	713			
4	BLOQUE 15	828	*ADMINISTRATOR* (1)	Cisco ISE-3315	$ 10.008,19
			MONITOR (2)	Cisco ISE-3395	$ 20.705,59
			PSN	Cisco ISE-3315	$ 8.243,44
5	BLOQUE 12	748			
6	BLOQUE 31	978	PSN	Cisco ISE-3315	
7	BLOQUE 43	1840			
8	BLOQUE 63	1380	PSN	Cisco ISE-3315	
9	MATRIZ	460	*ADMINISTRATOR* (2)	Cisco ISE-3315	$ 10.008,19
			MONITOR (1)	Cisco ISE-3395	$ 20.705,59
10	BLOQUE 1	123,6	PSN (C)	Cisco ISE-3355	$ 8.243,44
11	BLOQUE 6	154,5			
				TOTAL	$ 102.644,76

Tabla 4.5 Costo del equipamiento de Cisco ISE

4.1.2 COSTOS INDIRECTOS

Son aquellos costos que no se contemplan directamente para el funcionamiento de la red multiservicios; pero que son importantes para que se mantenga operativa. Estos

costos son la instalación y puesta en marcha de la red, servicios de la red, entre otros, para que se mantenga operativa durante 3 años o más.

4.1.2.1 Equipos UPS y Aire Acondicionado

Con respecto a capacidades disponibles en el UPS y aire acondicionado, no es necesario realizar alguna inversión adicional ya que los *Datacenters* y áreas de equipos cuentan con aire acondicionado de precisión y UPS con capacidades efectivas disponibles, aún con la justa consideración de un incremento relacionado con el ingreso de nuevo equipamiento.

4.1.3 COSTO TOTAL DE LA RED ACTIVA

Luego del análisis de las características técnicas y económicas de los elementos, el costo total de la red activa es de 236.269,76 USD, en la cual se incluyen licencias respetivas del ISE tanto para soporte de usuarios de la red cableada e inalámbrica. Los costos en detalle se presentan en el Anexo D2 .

4.2 RED PASIVA

La red pasiva incluye elementos de cableado estructurado, instalación, certificación, entre otros.

4.2.1 COSTO TOTAL DE LA RED PASIVA

El costo total de la red pasiva incluye elementos de cableado estructurado, instalación y certificación.

Pero el cableado estructurado actual de la empresa está en óptimas condiciones y está certificado, por tanto no es necesario reemplazarlo.

Sin embargo, es necesaria la instalación de las conexiones de fibra entre los *switches* trasladados e implementar redundancia a través de enlaces agregados.

El costo total de la red pasiva es de 113828USD, en la cual se incluyen los costos de la canaleta, bandejas de fibra, entre otros. Los costos en detalle se presentan en el Anexo D2 .

4.3 COSTOS ADICIONALES

Dentro de estos costos se encuentran los relacionados con la instalación de los equipos, licencias, capacitación de la infraestructura instalada.

4.3.1 COSTOS DE INSTALACIÓN Y PUESTA EN MARCHA

A parte de la instalación y puesta en marcha de los equipos, se incluye el transporte de los diferentes elementos de la red a los bloques que lo requieren, instalación de los equipos y configuración. La tabla 4.6 incluyen los valores correspondientes a este numeral.

DESCRIPCIÓN	COSTO
COSTO TRANSPORTE DE EQUIPOS	$ 16.500,00
SERVICIO DE INSTALACION Y CONFIGURACION	$ 69.050,00
TOTAL	$ 85.550,00

Tabla 4.6 Resumen de costos adicionales

4.3.2 LICENCIAS POR ENDPOINT

Con respecto a las licencias de los equipos de conectividad, se incluye en el precio del equipo, pero con respecto al equipamiento Cisco ISE se deben solicitar por separado dependiendo del número de dispositivos finales que se conectan a través de la red cableada e inalámbrica. El precio cambia dependiendo del número de usuarios que soporta simultáneamente (ver tabla 4.7).

NÚMERO DE PARTE	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
LICENCIAS BÁSICAS 2500				
L-ISE-BSE-2500-M=	Cisco ISE 2500 *EndPoint Base Migration License*	1	$ 3.913,41	$ 3.913,41
TOTAL				**$ 3.913,41**
LICENCIAS AVANZADAS 1500 (3 AÑOS)				
L-ISE-ADV3Y-1500=	Cisco ISE 1500 *EndPoint 3Year Advanced Subscription License*	1	$ 52.653,18	$ 52.653,18
TOTAL				**$ 52.653,18**

Tabla 4.7 Costos de licencia de *Endpoints* de Cisco ISE

4.3.3 SOPORTE Y CAPACITACIÓN

Estos gastos se generan a partir de la necesidad de la empresa por mantener un *software* actualizado (soporte) y personal capacitado en la nueva plataforma instalada, que permita a la red multiservicios operar de forma normal (ver tabla 4.8).

ELEMENTO	CANTIDAD	COSTO UNITARIO (USD)	COSTO TOTAL (USD)
Soporte de Administración, monitoreo.	1	$995,00	$ 2.190,00
Actualización licenciamiento	1	$ 2.550,00	$ 2.550,00
Capacitación para operar la red	1	$ 1.800,00	$ 3.600,00
		TOTAL (USD)	$ 8.340,00

Tabla 4.8 Costos relacionados con soporte y capacitación

4.4 COSTO TOTAL REFERENCIAL DEL REDISEÑO DE LA RED

El costo total del proyecto se calcula en base a los resultados que se obtuvieron tanto para la red pasiva, red activa y costos adicionales, como se muestra en la tabla 4.9.

ÍTEM	COSTO
Red Activa	$ 236.269,76
Red Pasiva	$ 113828,00
Costos adicionales	$ 150.456,59
TOTAL (USD)	**$ 500554,35**

Tabla 4.9 Costo total referencial del rediseño de la red

Considerando los resultados de la tabla 4.9, se requiere **500554,35 USD** para la implementación de la nueva plataforma de autenticación y servicios adicionales, para realizar la instalación en la red actual y dejarla operativa.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El uso de las directrices de diseño de la arquitectura Cisco *Borderless Network* permite gestionar, automatizar la seguridad y el control de accesos de forma centralizada, permitiendo la conexión (cableada o inalámbrica) de cualquier dispositivo promoviendo el BYOD, aplicaciones integradas como por ejemplo videoconferencia, compatibilidad con las últimas tendencias de seguridad como por ejemplo *Identity Services Engine* (ISE), que se encarga de la creación de políticas corporativas (AAA) y gestión centralizada para el control de acceso según el usuario, dispositivo, aplicación (o servicio) y ubicación.
- Un diseño jerárquico permite separar la red en 3 capas (núcleo, distribución y acceso), cada capa cumple funciones específicas, cabe recalcar que la separación no solo física sino también de manera lógica (como se comunican los dispositivos). Este modelo de red es el más utilizado con redes de gran tamaño donde los requerimientos son alta disponibilidad, confiabilidad, escalamiento y alto rendimiento (los *switches* de distribución y núcleo hacen que la información vaya a casi la velocidad del cable por sus ventajas de conmutación y porque el enrutamiento se realiza por *hardware*).
- El uso de capas independientes, permite agregar nuevos equipos, servicios sin realizar cambios significativos en la topología de red, mientras que la segmentación de funciones entre los *switches* en cada nivel hace que la administración sea más simple y la resolución de problemas sea más rápida.
- La implementación de redundancia a nivel de enlaces agregados (en los enlaces troncales si se requiere ancho de banda adicional se crea *Etherchannel*) y equipos minimiza la existencia de puntos críticos de red, y proporciona una rápida recuperación en caso de fallas, incorporando las opciones de configuración de protocolos que proporcionen tolerancia a fallos

como los son HSRP, GLBP y sobre capa 2 el protocolo STP, en nuestro proyecto se utiliza MST y HSRP.

- La plataforma de autenticación Cisco ISE brinda control sobre políticas de parches, actualizaciones, *antivirus* y prerrequisitos de sistemas operativos y aplicativos necesarios para acceder a la red corporativa.
- Cisco ISE permite la utilización obligatoria de las credenciales de Directorio Activo para el inicio de sesión única y asignación de listas de acceso para los recursos en red.
- Cisco ISE monitorea en tiempo real los accesos de usuarios invitados y su comportamiento en la red, teniendo la posibilidad de excluirlos de la red en cualquier momento.
- El tiempo de espera para el acceso a los servicios corporativos se incrementa con la inclusión de la plataforma de autenticación Cisco ISE (porque se encarga de validar credenciales de usuario y dispositivos, reconocer automáticamente del tipo de dispositivo conectado, revisar el cumplimiento de las políticas de postura y asignar las políticas de autorización dependiendo del perfil asignado al dispositivo final), sin embargo el tiempo adicional requerido se justifica claramente con el incremento de seguridad de acceso.
- La implementación de esta plataforma de autenticación no solo mejora el control de acceso de usuarios y dispositivos sino también la gestión, monitoreo, detección de amenazas en la red, generando un mecanismo de ejecución obligatoria de políticas de red y exclusión directa de dispositivos no registrados dentro del AD o del ISE.
- La realización de pruebas de compatibilidad de IOS y soporte de comandos de autenticación sobre los dispositivos de red proporciona seguridad en la determinación de dispositivos que serán los encargados de la entrega de credenciales recibidas de los dispositivos finales, a través de la red para ser entregados al ISE para su verificación.
- La implementación de un laboratorio de pruebas (prototipo) permite determinar la eficacia de las políticas configuradas de control de acceso, perfilamiento,

postura, remediación y finalmente autorización, tanto para la red cableada como para la red inalámbrica.

- La configuración de una plantilla general de autenticación por cada puerto de acceso de los *switches* de la capa de acceso permite generalizar el reconocimiento de cualquier dispositivo automáticamente y la asignación de un perfil determinado por el tipo de dispositivo, evitando una configuración diferenciada para cada puerto dependiendo del tipo de dispositivo, es decir es el ISE quien determina qué tipo de dispositivo es y ejecuta las políticas asociadas a su perfil, por tanto puede conectarse al mismo puerto un teléfono IP, o una cámara o un computador u otro dispositivo que el ISE de igual manera diferenciará el tipo de dispositivo, asignará el perfil correspondiente y ejecutará las políticas relacionadas con el tipo de perfil detectado.
- Cuando un dispositivo ha superado las políticas de autenticación, perfilamiento, postura, remediación si fuese necesario, recibe autorización de acceso a los servicio de red pero los permisos de acceso son limitados al tipo de usuario autenticado, es decir no basta con aprobar las políticas anteriores, el usuario no tendrá acceso total sino que los permisos asignados dependen exclusivamente del grupo y tipo de cuenta configurada en el AD o en el ISE.

5.2 RECOMEDACIONES

- Se debe realizar inventarios cada 6 a 12 meses para determinar el estado real de los equipos de conectividad, y si es necesario ejecutar garantías técnicas (cabe recalcar que para ejecutar el reemplazo del equipo o sus partes deben estar vigentes las garantías de los equipos).
- Se debe configurar seguridad de puerto de recepción y envío de mensajes de DHCP junto con la configuración de autenticación a través de Cisco ISE, para evitar la recepción automática de otro servidor de DHCP que el definido para la asignación de direccionamiento IP en la VLAN de cuarentena hasta que el dispositivo terminal cumpla cada política configurada en el ISE y se traslade a la VLAN de usuario corporativo con acceso a servicios de red.

- El usuario de vinculación entre el servidor de Directorio Activo (*AD*) y Cisco ISE debe ser de tipo administrador, para evitar inconvenientes de vinculación por falta de permisos por el tipo de usuario.
- Para obtener una amplia gama de tipos de perfiles de dispositivos finales de distintas marcas compatibles por el ISE, es recomendable instalar todos los parches del ISE antes de realizar alguna configuración. Pero si el dispositivo o la marca del mismo, no se encuentra en la lista de perfiles por defecto del ISE, se puede configurar un nuevo perfil manualmente definiendo un parámetro identificable en el dispositivo, como por ejemplo la dirección MAC.
- Se deben definir los tipos de dispositivos finales y marcas permitidas en la red de la empresa, para activar o crear los nuevos perfiles respectivos exclusivamente para estos dispositivos, el resto de equipos deben ser bloqueados por el ISE. Por tanto, se recomienda activar los perfiles exclusivamente de las marcas existentes en la empresa y no todos los disponibles, que es la configuración por defecto en el ISE.
- Se pueden definir las políticas para "*Authentication*", "*Authorization*", "*Profiling*", "*Posture*" y "*Remediation*" en el ISE, o también solo una de ellas, pero la configuración de las 5 políticas permite la correcta operación del sistema de autenticación ISE según las recomendaciones de diseño de Cisco relacionadas con el ISE.
- Se recomienda realizar una configuración de políticas por fases, es decir una política a la vez y hacer las pruebas respectivas de operación para posteriormente continuar la configuración de la siguiente política, es decir configurar primero la política de Autenticación probar su funcionamiento correcto y continuar con la configuración de la política de Perfilamiento y probarla y así sucesivamente, para al final no tener problemas derivados de la mala configuración de alguna de ellas, ya que las mismas trabajan de manera dependiente una de otra.
- Se recomienda determinar la línea base de la red de la empresa, y realizar pruebas de operación cada 2 meses, para la verificación del correcto funcionamiento.

REFERENCIAS BIBLIOGRÁFICAS

[1] L. Tangient, «Seguridad Informática SMR,» 20 Enero 2016. [En línea]. Available: https://seguridadinformaticasmr.wikispaces.com/TEMA+6+-+SEGURIDAD+EN+REDES. [Último acceso: 20 Marzo 2016].

[2] B. Plasencia, «Servidor AAA para Validación y Control de Acceso a Usuarios Hacia la Infraestructura del Ministerio de Defensa,» Universidad Técnica del Norte, Ibarra, 2012.

[3] C. Rosalba, «Seguridad Lógica,» 19 Mayo 2014. [En línea]. Available: http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20IV.pdf. [Último acceso: 15 Agosto 2016].

[4] C. Vásquez y W. Vaca, «Control de Acceso y Administración de Recursos de Red Mediante un Servidor AAA en el GAD Municipal de Urcuquí,» GAD Municipal Urcuquí, San Miguel de Urcuquí, 2012.

[5] Cisco, Systems, «How Does RADIUS Work,» Cisco Systems, Enero 19 2006. [En línea]. Available: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html. [Último acceso: 1 Marzo 2016].

[6] P. Correa, «Protocolos de Control de Acceso RADIUS,» CUJAE, 30 Enero 2015. [En línea]. Available: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjRz9eInZrPAhUHKx4KHSD8A54QFggsMAI&url=http%3A%2F%2Frevistatelematica.cujae.edu.cu%2Findex.php%2Ftele%2Farticle%2Fdownload%2F51%2F50&usg=AFQjCNHbJHM_M_fsOE5LRz9o1B. [Último acceso: 12 Febrero 2016].

[7] A. Valdivieso, «Diseño e Implementación de un Sistema de Autenticación y Politicas de Seguridad Mediante un Servidor AAA,» Escuela Politecnica Salesiana, Quito, 2015.

[8] L. Rosales, «Networkeando,» Cisco Systems, 18 Enero 2009. [En línea]. Available: http://networkeando.blogspot.com/2009/01/configurando-aaa-en-un-router.html. [Último acceso: 17 Enero 2016].

[9] M. Paredes, W. Urbina y N. Espinosa, «Implementación de un Plan Piloto de Seguridad Bajo de Protocolo IEEE 802.1x para el Departamento de Gestion Tecnológica del Ministerio de Telecomunicaciones,» Escuela Politécnica del Ejercito, Sangolqui, 2014.

[10] D. Esmoris, «Control de Acceso a las Redes,» Universidad Nacional de La Plata, 12 Abril 2015. [En línea]. Available: http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Esmoris.pdf. [Último acceso: 12 Abril 2016].

[11] Cisco, Systems, «Understanding Multiple Spanning Tree Protocol (802.1s),» Cisco Systems, 17 Abril 2007. [En línea]. Available: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html. [Último acceso: 1 Abril 2016].

[12] A. Corletti, «ISO-27001 Los Controles,» 1 Noviembre 2006. [En línea]. Available: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf. [Último acceso: 15 Enero 2016].

[13] Cisco, Systems, «Cisco Identity Services Engine Administrator Guide,» Cisco Systems, 1 Abril 2014. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html. [Último acceso: 15 Mayo 2016].

[14] Cisco, Systems, «Cisco Identity Services Engine,» Cisco System, 1 Junio 2015. [En línea]. Available: http://www.cisco.com/go/ise. [Último acceso: 26 Enero 2016].

[15] A. Bruno y S. Jordan, «Cisco Certified Design Associate 640-864,» Cisco Systems, San Francisco, 2011.

[16] Cisco, Systems, «Cisco TrustSec How-To Guide: ISE Profilinig Design Guide,» Cisco Systems, 16 Enero 2012. [En línea]. Available: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_30_ise_profiling.pdf. [Último acceso: 13 Marzo 2016].

[17] Cisco, Systems, «Cisco Identity Services Engine Hardware Installation Guide, Release 1.2,» Cisco Systems, 1 Enero 2015. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ise_vmware.html. [Último acceso: 12 Mayo 2016].

[18] D. Econ, «Diseño de topologías de red,» Econuba, 20 Abril 2015. [En línea]. Available: http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/briano/seoane/tp/2002_1/redes.htm. [Último acceso: 13 Julio 2016].

[19] C. Hyps, «Cisco ISE Profiling Design Guide,» Cisco Systems, 10 Febrero 2012. [En línea]. Available: https://communities.cisco.com/docs/DOC-68156. [Último acceso: 20 Julio 2016].

[20] Cisco, Systems, «Cisco ISE Profiling Design Guide,» Cisco Systems, 10 Julio 2015. [En línea]. Available: https://communities.cisco.com/docs/DOC-68156. [Último acceso: 1 Noviembre 2015].

[21] Cisco, Systems, «Cisco Identity Services Engine Network Component Compatibility, Release 1.2.x,» Cisco Systems, 24 Enero 2015. [En línea].

Available: http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/compatibility/ise_sdt.html. [Último acceso: 20 Octubre 2015].

[22] Cisco, Systems, «Cisco Identity Services Engine Hardware Installation Guide, Realease 1.2,» Cisco Systems, San Francisco, 2015.

ANEXOS

Anexo B

- Anexo B1
    - Anexo B1.1
    - Anexo B1.2
    - Anexo B1.3
- Anexo B2
- Anexo B3
- Anexo B4
- Anexo B5
- Anexo B6
- Anexo B7
- Anexo B8
- Anexo B9
- Anexo B10
- Anexo B11
- Anexo B12
- Anexo B13
- Anexo B14
- Anexo B15
- Anexo B16

Anexo C

- Anexo C1
- Anexo C2
- Anexo C3
- Anexo C4
- Anexo C5
- Anexo C6

- Anexo C7
- Anexo C8
- Anexo C9
- Anexo C10
- Anexo C11
- Anexo C12
- Anexo C13
- Anexo C14
- Anexo C15
- Anexo C16
- Anexo C17
- Anexo C18
- Anexo C19
- Anexo C20
- Anexo C21

Anexo D

- Anexo D0
- Anexo D1
- Anexo D2
    - Anexo D2.1

Los anexos se incluyen en el CD adjunto.