ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

"ESTUDIO DE LA TECNOLOGÍA CISCO IDENTITY SERVICES ENGINE (ISE) PARA MEJORAR LA SEGURIDAD DE LOS USUARIOS DE LA INFRAESTRUCTURA WLAN DE LA ESPOCH"

Trabajo de titulación presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTORES: OSCAR ALEXANDER MIRANDA SILVA
OSCAR PATRICIO MORALES RUEDA

TUTOR: ING. EDWIN VINICIO ALTAMIRANO SANTILLÁN Msc.

Riobamba-Ecuador
2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica: "ESTUDIO DE LA TECNOLOGÍA CISCO IDENTITY SERVICES ENGINE (ISE) PARA MEJORAR LA SEGURIDAD DE LOS USUARIOS DE LA INFRAESTRUCTURA WLAN DE LA ESPOCH", de responsabilidad de Oscar Alexander Miranda Silva y Oscar Patricio Morales Rueda ha sido minuciosamente revisado por los miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	FIRMA	FECHA
Ing. Washington Luna **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Franklin Moreno **DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Edwin Altamirano Msc. **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Alberto Arellano **MIEMBRO DEL TRIBUNAL**	_____	_____

Nosotros, Oscar Alexander Miranda Silva y Oscar Patricio Morales Rueda declaramos ser los autores del presente trabajo de titulación: "ESTUDIO DE LA TECNOLOGÍA CISCO IDENTITY SERVICES ENGINE (ISE) PARA MEJORAR LA SEGURIDAD DE LOS USUARIOS DE LA INFRAESTRUCTURA WLAN DE LA ESPOCH", que fue elaborado en su totalidad por nosotros, bajo la dirección del Ingeniero Edwin Altamirano, haciéndonos totalmente responsables de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio de la misma pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Oscar Alexander Miranda Silva

Oscar Patricio Morales Rueda

DEDICATORIA

El presente trabajo lo dedico en primer lugar a Dios que nos brinda la oportunidad de día a día ser mejores y vivir a plenitud, a mis padres Franklin y Nely por su apoyo y amor incondicional dándome ánimo y fuerza para concluir con mis estudios siendo ellos un pilar fundamental en mi carrera universitaria, pues al brindarme sus consejos y todo su amor me han enseñado a no darme por vencido jamás y siempre tener la convicción de ser mejor cada día, conservando siempre la humildad que creo que es el valor más importante en la vida universitaria, este logro se lo debo a ellos por siempre haber creído en mí y para ellos va dedicado este triunfo los amo papás. A mis hermanos por haberme brindado el apoyo necesario siempre contando con ellos para cualquier problema o adversidad que se ha puesto en mi camino, brindándome su apoyo incondicional y de esta manera poder afrontarlos de la mejor manera pues ellos han sido mis amigos y confidentes, por nunca dejarme desfallecer ante los problemas gracias Anthony y Stevens.

Alexander

Primero dar gracias a Dios por bendecirme y darme las fuerzas necesarias para no desmayar y seguir luchando cada día para cumplir esta meta. A mis padres Jorge y Lupe quienes me han brindado su amor y su apoyo incondicional en las buenas y en las malas, alentándome siempre y creer en mí.

Oscar

AGRADECIMIENTO

Agradezco a Dios por haberme permitido culminar una etapa más en mi vida como fue la universitaria. A mis padres quienes con su amor y apoyo me supieron brindar todo de sí para alcanzar esta meta añorada, se los agradezco con todo mí ser pues con su apoyo soy lo que soy, los amo. A mis hermanos que creyeron y confiaron en mí hasta el final gracias por siempre brindarme ese apoyo incondicional de hermanos.

También agradecerle al Ing. Edwin Altamirano y al Ing. Ángel Ordoñez que con sus enseñanzas y doctrinas pudimos culminar este trabajo de titulación.

Finalmente agradecer a mis profesores y amigos pues ellos también formaron parte fundamental de la vida universitaria.

Alexander

A Dios por la bendición de haber culminado esta etapa de mi vida, a mis padres y hermano, sabiendo que no hay forma de agradecerles por su sacrificio, para verme alcanzar mí meta.

Agradecimiento fraterno al Ing. Edwin Altamirano e Ing. Ángel Ordoñez quienes con sus conocimientos y consejos fueron una guía y ayuda para culminar tan arduo trabajo, a todos nuestros profesores que nos formaron para ser buenos profesionales y así culminar con éxito nuestra carrera.

Oscar

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación estudia de la tecnología Cisco IDENTITY SERVICES ENGINE (ISE) para mejorar la seguridad de los usuarios de la infraestructura de red de área local inalámbrica (WLAN) de la Escuela Superior Politécnica de Chimborazo (ESPOCH), se analizó una posible solución de control de acceso seguro y controlado en la infraestructura WLAN que posee la ESPOCH. Se estudió el manejo de políticas de autenticación y autorización según los perfiles: tipos de dispositivos, ubicación, grupos de usuarios, etc. Utilizando una controladora de LAN inalámbrica (WLC) encargada de automatizar el control de los puntos de acceso de una manera centralizada, que al integrarla con ISE, este, actúo como servidor RADIUS tanto de autenticación como autorización permitiendo el control del identificador de conjunto de servicios (SSID) de acuerdo a las políticas de seguridad propuestas usando el protocolo 802.1X, se contó con un repositorio externo Active Directory que fue el validador de usuarios y de certificados necesarios para poder acceder a la red inalámbrica. Mediante las políticas propuestas en el estudio se analizó la gran capacidad de esta tecnología al brindar diferentes tipos de soluciones para la seguridad a la red y a los usuarios específicamente, donde al tener un SSID esta tecnología a través de normas de seguridad se encarga de segmentar automáticamente la red al direccionar dinámicamente a una VLAN correspondiente para cada grupo de usuarios. Se concluyó que el contar con una infraestructura de red con equipos Cisco brinda un sinnúmero de ventajas en cuanto a la seguridad inalámbrica, que por el actual crecimiento de las redes y la información que se maneja en ellas se vuelve más importante el contar con políticas de seguridad bien establecidas. Se recomienda revisar el manual de usuario ante posibles problemas de instalación de ISE.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES DE COMPUTADORES>, <CISCO IDENTITY SERVICES ENGINE (ISE)>, <ACTIVE DIRECTORY>, <CONTROLADORA DE LAN INALÁMBRICA (WLC)>, <PROTOCOLO 802.1X>, <SERVIDOR RADIUS>, <RED DE ÁREA LOCAL INALAMBRICA (WLAN)>.

SUMMARY

The present graduation research work was a study of the Cisco ISE (Identity Services Engine) technology apply to improve the users safety of the WLAN (Wireless Local Area Network) infrastructure of ESPOCH (Escuela Superior Politécnica de Chimborazo) to analyze a possible safety and control the access to the ESPOCH's WLAN facility. The management of authentication and authorization policies was studied according to these profiles: device types, location, user groups, etc by using a WLC (Wireless LAN Contoller) that is responsible for automating the control of access point in a centralized way. It is integrated with an ISE, it acts as both authentication and authorization RADIUS server allowing the control of the SSID (Specifying Service Set Identifier), according to the proposed safety policies using the 802.1X protocol, an external active directory repository that was used as the evaluator of users and the certificates needed to access the wireless network. The policies proposed in the study analyzed the great capacity of this technology by providing different types of safety solutions to the network and users specifically. They were having an SSID, this technology through security standard is responsible for automatically segmenting the network by dynamically addressing corresponding VLAN for each user group. It was concluded that having a network infrastructure with Cisco equipment offers a number of advantages in terms of wireless safety, that the current growth of networks and the information that is used in them becomes more important to have well established policies. It is recommended to review the user manual for possible ISE installation problems.

Keywords: < ENGINEERING TECHNOLOGY AND SCIENCE>, <COMPUTER NETWORK>, <CISCO IDENTITY SERVICES ENGINE (ISE)>, <ACTIVE DIRECTORY>, <WIRELESS LAN CONTROLLER>, <802.1X PROTOCOL>, <RADIUS SERVER>, <WIRELESS LOCAL AREA NETWORK (WLAN)>.

INTRODUCCIÓN

Cisco Identity Services Engine (ISE) es una tecnología que permite a instituciones y organizaciones identificar y aplicar políticas de seguridad a las redes basadas en identidad de usuarios, tipo del dispositivo, comportamiento del dispositivo y algunos atributos más, lo cual conlleva a brindar una notable mejoría en la seguridad en cuanto a redes se trata, ya puede ser de forma cableada, inalámbrica o por medio de una Red Privada Virtual (VPN).

En el presente trabajo se realizó un estudio de la tecnología mencionada (ISE), con el fin de conocer su funcionalidad, se investigó el tema que trata sobre seguridad en las redes inalámbricas, controladoras inalámbricas (WLC), Active Directory (AD), protocolos de seguridad como es el 802.1X , que van de la mano con la tecnología ISE, específicamente las políticas de seguridad y como aplicarlas para mejorar la seguridad en las redes de datos, así como también la manera de cómo ponerlas a trabajar en conjunto para obtener resultados más satisfactorios, sabiendo que hoy en día el flujo de la información que circula por la red es muy vulnerable y accesible, y de esta manera brindar una solución más robusta para proteger estos datos e información.

Para culminar el trabajo de la mejor manera se aplicó la metodología analítica llevando a cabo las siguientes investigaciones: investigación bibliográfica, implementación y configuración de la tecnología propuesta, evaluación de resultados y su respectiva documentación. El estudio de esta tecnología es un aporte académico dirigido para todos los estudiantes y profesionales interesados en la seguridad de las redes inalámbricas.

ANTECEDENTES

La Escuela Superior Politécnica de Chimborazo maneja tres diferentes redes inalámbricas con distintos tipos de seguridad y varias políticas de acceso en el campus politécnico, el departamento encargado de brindar estas redes con sus respectivos permisos y privilegios es el DTIC (Dirección de Tecnologías de la Información y Comunicación) el cual por diferentes requerimientos y necesidades de personal administrativo, docente y estudiantil otorga acceso a cada una de las redes inalámbricas, así por consecuencia tenemos:

La red SSID: ESPOCH-PORTAL tiene como modo de ingreso portal cautivo la cual redirige a una página especial para poder ingresar a internet y navegar de forma normal, este modo de autenticación consiste en que los recursos de la red inalámbrica de la Espoch lleguen a las

personas adecuadas; con ello solo los miembros activos que pertenecen a la institución tendrán acceso a internet a través de la red inalámbrica. Por lo cual, la principal vulnerabilidad de esta red es: (SISTEMA DE AUTENTICACIÓN WIRELESS ESPOCH – SAWE. http://oldwww.espoch.edu.ec/Descargas/sawe.pdf)

- DNS tunneling, el gateway que captura las conexiones y las redirecciona en función del token permitiendo así las solicitudes DNS hacia la zona privada; de esta forma es posible encapsular el tráfico TCP/IP dentro de la solicitud DNS y eludir las restricciones del portal cautivo. (Seguridad en redes inalámbricas. http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf).

La red SSID: ESPOCH-OPEN es una red abierta que no requiere ningún tipo de autenticación para ingresar a ella, sin embargo, esta red tiene un ancho de banda limitado restringiendo de esta manera el ingreso a ciertas páginas web que no tienen relación con el ambiente académico y así garantizar que su uso se vea enfocado al correcto uso institucional, de tal manera al ser una red abierta es propensa a un sin número de posibles ataques, siendo los más frecuentes los siguientes:

- Ataque de Denegación de Servicio (DoS) consiste en cortar la comunicación entre un terminal y un punto de acceso. Esto se logra haciéndose pasar por el AP colocando su dirección MAC (se la obtiene por medio de un sencillo sniffer) y privarle la comunicación al terminal o terminales elegidos mediante el envío permanente de notificaciones de desvinculación. (Seguridad en redes inalámbricas. http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf)

- Ataque Man in the middle hace creer al cliente que será la víctima que el atacante es el AP y, al mismo tiempo, persuadir al AP de que el atacante es el cliente, para lo cual se necesita obtener el SSID de la red, dirección MAC del AP, así como también el de la víctima; una vez obtenidos estos datos la metodología es la misma que en el ataque de tipo DoS para cortar la conexión entre el cliente y el AP. (Seguridad en redes inalámbricas. http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf)

- Ataque ARP Poisoning la finalidad de este ataque consiste en acceder al contenido de la comunicación entre dos terminales conectados por medio de dispositivos inteligentes como un switch. Dicho ataque recurre a la modificación de la tabla ARP que mantienen en modo stateless todos los dispositivos de red. (Seguridad en redes inalámbricas. http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf)

La red SSID: EDUROAM como principal característica su autenticación viene dada por el protocolo 802.1x mediante servidor RADIUS, eduroam (sinéresis de education roaming) es el servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. Eduroam persigue el lema "abre tu portátil y estás conectado". El servicio permite que estudiantes, investigadores y personal de las instituciones participantes del sistema tengan conectividad vía internet dentro de su propio campus y así también cuando se encuentran en otras instituciones participantes, Eduroam comenzó en Europa y ha cobrado desarrollo en toda la colectividad de investigación y educación dando como resultado que hasta el momento se encuentra imperante en 74 países alrededor del mundo y de la misma manera posee ciertas vulnerabilidades siendo más frecuentes las mencionadas a continuación:

- En la fase de identificación el cliente manda el mensaje EAP-Identity sin cifrar, permitiendo a un atacante ver la identidad del cliente que está tratando de conectarse.
- De la misma forma el envío de la aceptación/denegación de la conexión se realiza sin cifrar, con lo que un eventual atacante puede reenviar este tipo de tráfico para generar ataques de tipo DoS.

FORMULACIÓN DEL PROBLEMA

¿Cómo mejorará la seguridad de la red inalámbrica en la Espoch mediante el uso de la tecnología Cisco Identity Services Engine (ISE)?

SISTEMATIZACIÓN DEL PROBLEMA

¿Disminuirá el porcentaje de intrusiones mediante la autenticación con ISE?

¿Qué aporta la tecnología en estudio en la infraestructura WLAN con ISE frente a la infraestructura WLAN sin ISE?

¿Cómo será la autenticación de las redes inalámbricas en cada punto de acceso con ISE?

JUSTIFICACIÓN TEÓRICA

La utilización de ISE permite un acceso seguro a la red, al administrador de la red le permitirá controlar y autorizar el acceso de los usuarios o grupos de usuarios a los diferentes servicios ofrecidos por el mencionado sistema. De igual manera, se podrá utilizar la estructura del

servidor AAA (Autenticación, Autorización y Auditoría) para gestionar el acceso a los equipos activos de la red para los usuarios que accedan a los recursos de que se encuentran en los grupos de Active Directory.

Gracias a esa falta de confianza de las redes inalámbricas es necesario un mecanismo que logre autenticar y autorizar los usuarios a la red, ya que debido a la proliferación de dispositivos que no son administrados y menos aún de confianza que están conectados a la red, surge la necesidad de que en cada dispositivo deba comprobarse el cumplimiento de la seguridad antes de que permita el acceso a los recursos de la red, esta comprobación varía de acuerdo a las políticas de seguridad brindadas por ISE las cuales implican, tipo de dispositivo, ubicación, estado de gestión y sistema operativo.

Debido a la escasez de seguridad en la infraestructura wlan se propone la integración de Cisco Identity Services Engine (ISE), para de esta manera mejorar la seguridad y administración de los usuarios y dispositivos respectivamente, los cuales se conectan a la red.

Mediante el presente documento se demostrará las bondades y ventajas además de versatilidad de ISE en las redes y así justificar una futura implementación por parte del DTIC a dichas redes, asegurando y recuperando el control de las redes sin fronteras. De esta manera quedará demostrado y justificado que es factible la utilización de ISE y que puede ser aplicado a mayor escala en todas las redes inalámbricas del campus politécnico.

JUSTIFICACIÓN APLICATIVA

El sistema de seguridad de red inalámbrica con protocolo 802.1X implementado ISE constará con el registro de tipo de dispositivo, identidad de usuario el cual, nos permitirá tener una mejor administración y dominio de la red asegurándose de que la seguridad de dicha red sea lo primordial al momento de la conectividad de los usuarios.

Para que este control se lleve a cabo ISE puede obtener información de identidad y validar su autenticidad utilizando varias fuentes, incluyendo su propia base de datos local, y lo haremos con 802.1X que es un estándar IEEE para la capa 2 de control de acceso a internet cableado e inalámbrico de redes. WPA2 Enterprise utiliza 802.1X más Extensible Authentication Protocol (EAP) para la autenticación, 802.1X puede utilizar la identidad del usuario o tipo de dispositivo, o se puede utilizar los dos, 802.1X ofrece la capacidad de permitir o negar la conectividad de red de capa 2, y asignar una VLAN con lo cual se llevarán los paquetes de autenticación EAP a través del punto del acceso que mantiene las credenciales de autenticación, este servidor tiene

en ejecución un protocolo RADIUS el cual es el servidor de autenticación, autorización y auditoria (AAA).

En donde la autenticación debería ser exitosa se permite entonces que el tráfico de datos atraviese el puerto virtual desde el puerto virtual del cliente de la Wlan.

Como parte final lo que se debe hacer es colocar la identidad y la información de contexto para trabajar a través de las políticas de ISE, con lo cual ofrece una vista centralizada de la que se puede administrar hasta 250.000 puntos finales, las políticas ISE dependen de las necesidades de la red para esto una vez que la política coincida con los permisos son aplicados a la red o al dispositivo como son denegar cualquier acceso a la red, permitir todos los accesos a la red, asignar Vlan al Switch. El ISE nos proporciona políticas basadas en: quién, qué, cuándo, dónde y cómo para el acceso a la red las cuales a su vez nos brindan parámetros de autorización como: miembros de grupo de Active-Directory, tiempos, fechas, coincidencia de perfil por tipo de dispositivo, localización, tipo de sistema operativo y demás con lo cual aseguramos una red confiable y de acceso seguro para los profesores y alumnos que se verán beneficiados pues ellos contarán con los privilegios que se aplicaron a esta red mediante la autenticación.

Esta solución permite a instituciones y organizaciones identificar y aplicar las políticas de seguridad de red basada en la identidad del usuario, tipo de dispositivo, comportamiento del dispositivo, y otros atributos como la postura de seguridad por tal motivo surge la necesidad de aplicar el ISE en la infraestructura wlan de la ESPOCH para precautelar y controlar el acceso a datos de los usuarios de la red garantizando un servicio de calidad y confiabilidad de la información que tengan los dispositivos conectados por lo cual surge la iniciativa de aplicar el BYOD (Bring Your Our Device) o traer tu propio dispositivo, lo que conlleva a un mejor desenvolvimiento de los profesores y estudiantes que utilice en la red inalámbrica.

OBJETIVOS

OBJETIVO GENERAL

Estudiar la tecnología Cisco Identity Services Engine (ISE) para mejorar la seguridad de los usuarios de la infraestructura WLAN de la Espoch.

OBJETIVOS ESPECÍFICOS

- Estudio del funcionamiento de ISE en combinación con el protocolo 802.1X para autenticación de la infraestructura wlan de la Espoch.

- Configurar el servidor RADIUS con ISE para obtener la autenticación, autorización y auditoria (AAA) estableciendo políticas de autorización de acceso a la infraestructura wlan de la Espoch.

- Realizar pruebas en la topología para garantizar el correcto funcionamiento de protocolo 802.1X con ISE en la infraestructura wlan de la Espoch.

- Proponer una guía de implementación y configuración de ISE para el DTIC de la Espoch.

CAPÍTULO I

1. MARCO TEÓRICO

1.1 Redes inalámbricas

1.1.1 Definición

Una red inalámbrica es un sistema de comunicación de datos que proporciona conexión inalámbrica entre equipos situados dentro de un mismo sector (interior o exterior) de cobertura. En lugar de utilizar el par trenzado, el cable coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas usando el aire como medio de transmisión.

Esta tecnología permite a los usuarios amplia movilidad, conexiones de red sin limitaciones ni costos ya que se elimina las conexiones cableadas y así brindar la facilidad a los usuarios de acceder desde cualquier punto dentro de la zona de cobertura que se encuentre una red inalámbrica.

Es de conocimiento popular la creciente demanda e implementación de todo tipo de redes inalámbricas en entornos empresariales, pequeños negocios y en el ámbito familiar; este tipo de redes ofrecen una amplia gama de ventajas frente a las típicas redes cableadas como las mencionadas anteriormente además de; facilidad de instalación, sencilla ampliación, entre otras.

Lo cual conlleva que gracias a estas peculiaridades las redes inalámbricas están experimentando el gran auge que atraviesan este momento.

1.1.2 Clasificación de las redes inalámbricas

En la figura 1-1 se observa la clasificación de las redes inalámbricas y su respectiva área de cobertura:

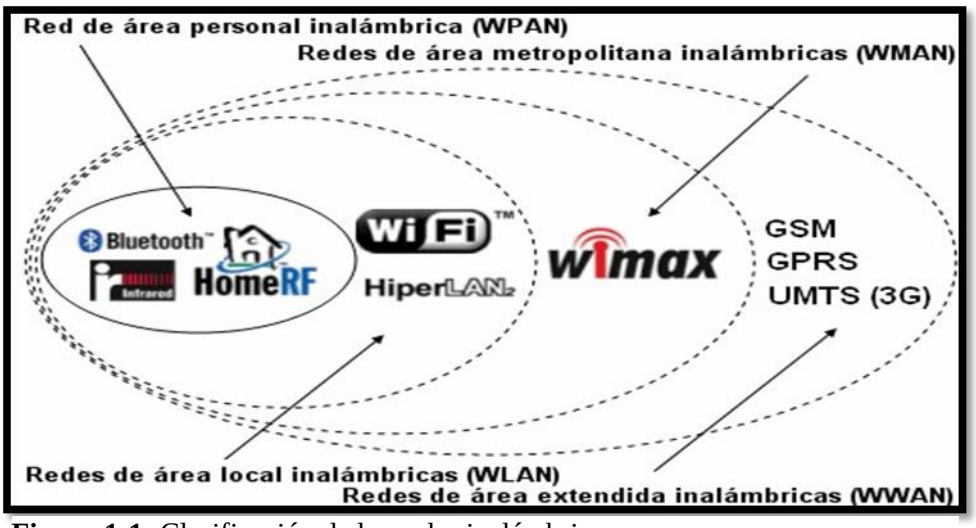


Figura 1-1: Clasificación de las redes inalámbricas
Fuente: (http://www.consernet.com.ve/site/wp-content/uploads/2014/08/funcionamiento-wimax.png)

1.1.3 Red de área local inalámbrica (Wireless Local Area Network WLAN)

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías:

- Wifi (o IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.

- HiperLAN2 (High Performance Radio LAN 2.0), estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz. (WLAN LAN inalámbrica. http://es.ccm.net/contents/817-wlan-lan-inalambrica).

1.1.4 Estándar IEEE 802.11 y sus variantes más comunes para WLAN

El estándar 802.11 en realidad es el primer estándar y permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o para especificar

componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad, como se observa en la tabla 1-1. (Introducción a Wi-Fi (802.11 o WiFi). http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi).

Tabla 1-1: Variantes del estándar 802.11

Estándar	Nombre	Descripción
802.11a	Wifi5	Trabaja en la frecuencia de 5 GHz y provee 8 canales de radio.
802.11b	Wifi	Trabaja en la frecuencia de 2,4 GHz y tiene alcance para 300 metros.
802.11c	Combinación de 802.11 y el 802.1d	Con sus características permite a los APs actuar como bridges (puentes)
802.11d	Internacionalización	Permite la comunicación en cualquier parte del mundo mediante el protocolo 802.11
802.11e	Mejora de la calidad del servicio	Se introdujo QoS para permitir mejores transmisiones de audio y vídeo sobre IP.
802.11f	Itinerancia	Maneja el protocolo IAPP que le permite a un usuario tener la movilidad para ir de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red.
802.11g		Trabaja en la frecuencia de 2,4 GHz y además es compatible con el estándar 802.11b.
802.11h		El estándar 802.11h tiene por objeto permitir la coexistencia con el estándar europeo HiperLAN 2.
802.11i		Este estándar mejora la seguridad por medio de la autenticación y la encriptación.
802.11r		Usaba señales infrarrojas por lo cual se ha vuelto un estándar obsoleto.
802.11m		Estándar recomendado para realizar mantenimiento a las redes inalámbricas.

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

1.2 Seguridad en redes inalámbricas (WLAN)

La seguridad en estas redes se convierte en algo primordial debido a su manera de ser transmitida, combinado con la carencia de una frontera física, significa que un dispositivo inalámbrico está emitiendo broadcast a su ámbito cercano, por esto, cualquier estación que este en la zona del nodo WLAN gozara de acceso íntegro a los datos.

Las formas primarias para asegurar una red son encriptar y autenticar, además hay que tener presente que así como la red debe autenticar a los usuarios, el usuario de igual manera debe verificar la red a la cuál va a acceder para de esta manera tratar de evitar ciertos tipos de ataques.

1.2.1 Métodos de seguridad en redes inalámbricas (WLAN)

Existen varias formas para brindar seguridad a una red inalámbrica, y estas se las pueden aplicar para que trabajen individualmente o agrupadas entre sí.

1.2.1.1 Identificador de conjunto de servicio (SSID, Service Set Identifier)

Un identificador de conjunto de servicio (SSID) es el nombre que identifica una red inalámbrica. Todos los dispositivos de una red deben conocer el SSID de la red inalámbrica o no podrán comunicarse entre ellos. Normalmente, la red inalámbrica transmite el SSID para permitir que los dispositivos inalámbricos se conecten a ella. En ocasiones, el SSID no se transmite por motivos de seguridad. Un SSID puede tener hasta 32 caracteres alfanuméricos. (¿Qué es un SSID? http://www.cryptoman.com/storage/Pubs/es/ntwk_guide/what-is-ssid-topic.html)

1.2.1.2 Control de acceso al medio (MAC, Media Access Control)

Mediante el filtrado MAC se puede determinar una lista de direcciones físicas de los adaptadores de red que pueden ingresar a la red inalámbrica a través de un punto de acceso.

1.2.1.3 Privacidad equivalente al cableado (WEP, Wired Equivalent Protocol)

WEP intenta proveer de la seguridad de una red con cables a una red Wireless, cifrando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace). El protocolo WEP está basado en el algoritmo de cifrado RC4, y utiliza claves de 64bits o de 128bits. (Seguridad en redes inalámbricas. http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf)

1.2.1.4 Estándar IEEE 802.1X

Se encarga del control de acceso y autenticación a la red, estableciendo una conexión punto a punto para transportar la información de identificación del usuario. La arquitectura IEEE 802.1X está formada por tres entes (Geier, 2008, pp. 33 - 40):

- El suplicante que se une a la red (cliente).
- El autenticador que hace el control de acceso (punto de acceso).
- El servidor de autenticación toma las decisiones de autorización (RADIUS).

1.2.1.5 Acceso Protegido Wi-Fi (WAP, Wi-Fi Protected Access)

WPA es una versión del protocolo 802.11i y del algoritmo TKIP (Temporal Key Integrity Protocol), provee una encriptación fuerte y utiliza una clave privada compartida, la cual cambia cada cierto tiempo. Los datos del usuario se chequean usando el protocolo 802.1X, en un servidor de autenticación como RADIUS (Stallings, 2005, p. 453).

1.2.1.6 Estándar IEEE 802.1i

El estándar IEEE 802.11i (WPA2), se basa en el cifrado TKIP, también admite AES (Advanced Encryption Standard) considerado como una técnica de encriptación de alta seguridad debido a que su algoritmo es complejo al tener claves robustas, utiliza CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), que surgió para remplazar a TKIP, y el cual es obligatorio en el estándar 802.11i (Lehembre, 2006, http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf). WPA2 define dos modos de trabajo:

- **WPA-Personal:** utiliza una clave compartida, llamada PSK (Pre-Shared Key) que está tanto en el punto de acceso como en el dispositivo del usuario.
- **WPA-Enterprise:** requiere de una arquitectura de autenticación 802.1X.

1.2.1.7 Red Privada Virtual (VPN, Virtual Private Network)

Esta red privada se la construye dentro de una infraestructura en una red pública, empleando diferentes protocolos se establece un canal seguro.

Las VPN suelen ser muy preciadas cuando se trata de preservar redes inalámbricas, puesto que actúan sobre todo tipo de hardware inalámbrico y sobrepasan las limitaciones que posee WEP.

1.3 Active Directory (AD)

1.3.1 Definición

El directorio activo es un servicio de directorio. El término de servicio de directorio se refiere a dos cosas: un directorio donde la información sobre usuarios y recursos esta almacenada, y un servicio o servicios te dejan acceder y manipular estos recursos. El directorio activo es una manera de manejar todos los elementos de una red, incluidos ordenadores, grupos, usuarios, dominios, políticas de seguridad y cualquier tipo de objetos definidos para el usuario.

Además de esto, provee de funciones adicionales más allá de estas herramientas y servicios, como se observa en la figura 2-1.

(Ordenadores y Portátiles, 2014, http://www.ordenadores-y-portatiles.com/directorio-activo.html)

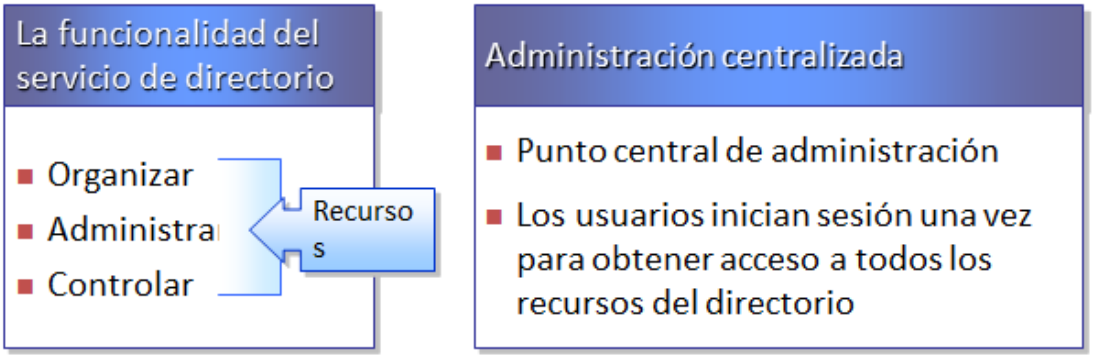


Figura 2-1: Definición de Active Directory
Fuente: (Marrias, Y, 2011, http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103)

1.3.2 Características de Active Directory

- Administración simplificada de usuarios y recursos de red
- Sistema de autenticación y autorización flexible y seguro
- Consolidación de directorios
- Infraestructura y aplicaciones habilitadas para el uso de directorios
- Escalabilidad sin complejidad
- Uso de los estándares de internet
- Un entorno de desarrollo eficaz
- Replicación y supervisión de confianza
- Listas de distribución de servicio de Message Queue Server

1.3.3 Estructura de Active Directory

El Active Directory está proyectado para acumular una cadena de objetos de manera ordenada y gradual.

Admite instaurar la estructura Organizacional para su administración, además que está diseñado para que varios servidores interactúen entre sí. Active Directory posee una estructura tanto física, como también una estructura lógica, como se observa en la figura 3-1.

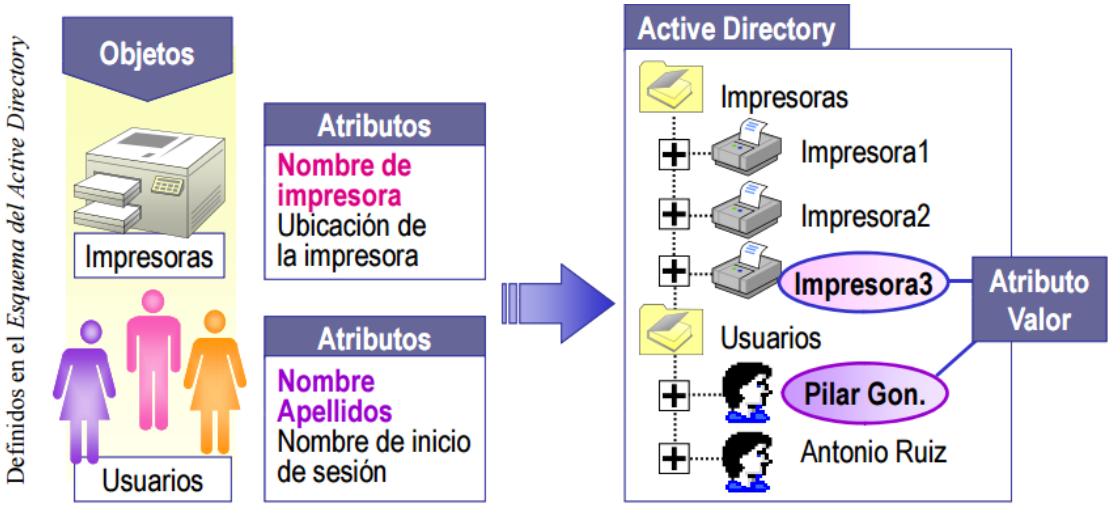


Figura 3-1: Organización de Active Directory
Fuente: (Siesquen, J, 2016, http://juliosiesquen.blogspot.com/2016/01/active-directory.html)

1.3.4 Estructura Lógica de Active Directory

Dentro de Active Directory podemos regular los recursos en una estructura lógica, y por medio de esta agrupación lógica, localizar un recurso se facilita pues la búsqueda puede ser por nombre o atributos y no solamente por su localización física.

En esta estructura lógica del Active Directory se encuentran: Objetos, Unidades Organizativas, Dominios, Arboles de dominios y finalmente Bosques.

1.3.4.1 Objeto

Es cualquier elemento u objeto que tenga existencia en el directorio, como puede ser un programa, archivo, carpeta, computador, impresora, router, usuario, contraseña o también un proxy.

1.3.4.2 Unidades Organizativas

Una OU es un objeto contenedor que nos permite estructurar los objetos en un domino en grupos lógicos administrativos.

Una OU puede abarcar objetos tales como: cuentas de usuarios, grupos, ordenadores, impresoras, aplicaciones, ficheros compartidos y en algunos casos otras OUs.

La jerarquía OU en un dominio es independiente de la estructura de otros dominios. Cada dominio puede implementar su propia jerarquía OU.

También se puede determinar permisos a las OU para autorizar la administración, como se observa en la figura 4-1. (Marrias, Y, 2011, , http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103)

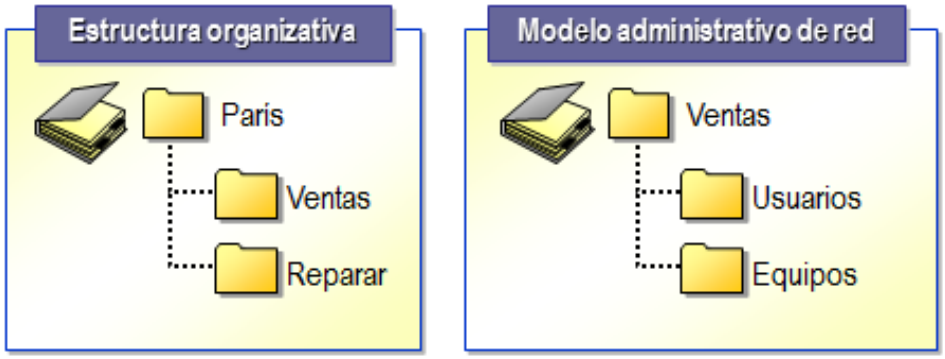


Figura 4-1: Jerarquía de las Unidades Organizativas
Fuente: (Marrias, Y, 2011, , http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103)

1.3.4.3 Dominios

Un dominio es una sucesión de normas para administrar una serie de recursos en una red, que pueden ser local y/o externa. En un dominio existe lo que se conoce como un servidor principal nombrado PDC (primary domain controller) el cual se encarga de asignar derechos, y gobierna recursos y usuarios.

1.3.4.4 Árboles de dominios

Está conformado por un grupo de dominios que permiten compartir diferentes tipos de recursos (servicios) entre sí.

1.3.4.5 Bosque

Es un conjunto de dos o más árboles que comparten una relación entre sí.

1.3.5 Active Directory y DNS

Active Directory (AD) emplea la relación DNS para designar nombres a los dominios, además AD utiliza DNS para ejecutar el dictamen de nombres cuando los nombres que poseen los host son convertidos a direcciones IP.

Cualquier servicio del directorio es un cúmulo de nombres. Sea cual sea el objeto que se encuentre dentro del directorio posee un nombre exclusivo y este podrá ser resuelto por el servicio. Ejemplo: espoch.edu.ec o Ise.espoch.edu.ec

1.3.5.1 DNS Domain Name Service

Como se observa en la figura 5-1 el DNS (Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar (pero que también pueden causar muchos conflictos puesto que los nombres son activos valiosos en algunos casos). (Marrias, Y, 2011,http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103)

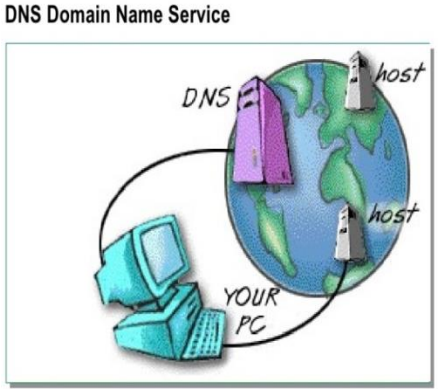


Figura 5-1: DNS Domain Name Service
Fuente: (Marrias, Y, 2011,http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103)

1.4 Cisco Wireless Lan Controller (WLC)

1.4.1 Definición

Las redes inalámbricas se han convertido en una necesidad en la actualidad. Muchos entornos corporativos requieren el uso de redes inalámbricas a gran escala. Cisco ha propuesto el concepto de Red Inalámbrica Unificada de Cisco (CUWN), lo que facilita el manejo de tales implementaciones a gran escala. El WLC es un dispositivo que asume una función central en el CUWN. Las funciones tradicionales de los puntos de acceso, tales como asociación o autenticación de los clientes de red inalámbrica, son realizadas por el WLC. Los puntos de acceso, llamados Lightweight Access Point (LAPs) en el entorno unificado, se registran con un WLC y hacen un túnel de los paquetes de datos y administración a WLCs, que luego conmutan los paquetes entre los clientes de red inalámbricos y la porción cableada de la red. Todas las configuraciones se hacen en el WLC. Los LAP descargan la configuración completa de los WLC y actúan como la interfaz inalámbrica a los clientes., como se observa en la figura 6-1 se puede apreciar la controladora inalámbrica. (Regulador del Wireless Lan (WLC), 2009, http://www.cisco.com/c/es_mx/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html)

Figura 6-1: Cisco 5508 Wireless Controller
Fuente: (http://www.cisco.com/c/en/us/support/wireless/5508-wireless-controller/model.html)

1.4.2 Características importantes

- Soporta 6,12 o 25 Access Point.
- Soporta IEEE 802.11a/b/g/d/h/n.
- Contiene módulos de conmutación Ethernet y Power-over-Ethernet (PoE) las opciones son compatibles con Cisco 2800, 3700 y los routers de la serie 3800.
- Estándares de seguridad:
    - Acceso protegido Wi-Fi (WAP).
    - IEEE 802.11i (WAP2 y una robusta red de seguridad [RSN]).
    - RFC 1321 MD5 Message-Digest Algorithm.
    - RFC 2104 HMAC: Hash con llave para la autenticación de mensajes.
    - Capa RFC 2246 Seguridad en el Transporte (TLS) PROTOCOLO DE LA VERSION 1.0.

- Encriptación:
  - WEP y Temporal Key Integrity Protocol Message Integrity Check (TKIP-MIC): RC4 de 40, 104 y 128 bits.
  - Nivel de sockets seguros (SSL) y TLS: RC4 de 128 bits y RSA de 1024 y 2048 bits.
  - Protocolo de autenticación de código (CCMP).

- Authentication, Authorization y Accounting (AAA):
  - IEEE 802.1x.
  - RFC 2865 RADIUS Authentication.
  - RFC 2866 RADIUS Accounting.
  - RFC 2867 RADIUS Tunnel Accounting.
  - RFC 2869 RADIUS Extensions.
  - RFC 3576 Dynamic Authorization Extensions to RADIUS.
  - RFC 3579 Soporte RADIUS para EAP.

- Voz a través de WLAN. (Olguín, A, 2011 p:11-12)

1.5 Cisco Identity Services Engine (ISE)

1.5.1 Definición

ISE (Identity Services Engine) de Cisco constituye la columna vertebral de la solución de política de seguridad de próxima generación basada en identidades, se introdujo por primera vez en 2011.

Cisco lo creó para ofrecer a las empresas un enfoque de sistemas integrados a sus requisitos de acceso y política de red. La solución ISE ofrece una visibilidad consolidada e integral de la red utilizando la identidad y la conciencia contextual. Esto incluye quién, qué, dónde, cuándo y cómo acceder a la red. La Figura 7-1 ilustra la naturaleza de políticas de ISE.

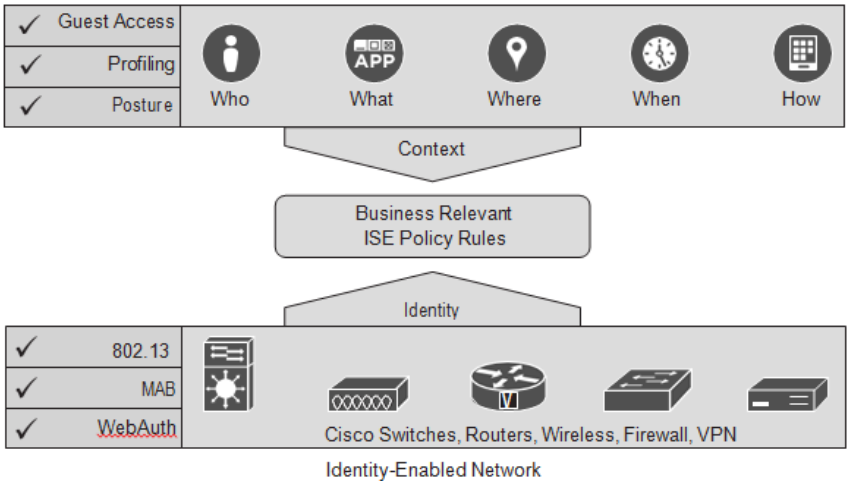


Figura 7-1: Visibilidad de ISE
Fuente: (Woland, A; Heary, J, 2013, p.10)

Vamos a dividir la información que se encuentra en la Figura 7-1 en sus partes constituyentes. Las dos partes principales son Contexto e Identidad.

La identidad proporciona el conocimiento del usuario o del dispositivo; esto nos da que el contexto extiende la cantidad de información que tenemos acerca de una identidad para proporcionar información adicional, como qué, dónde, cuándo y cómo.

La consolidación de la identidad y del contexto permite la creación de políticas relevantes para la red a administrar.

1.5.2 Tipos de autenticación en ISE

Ahora que ya sabe qué información desea incluir en sus políticas de ISE, debe averiguar cómo recopilar esos datos. Daremos un vistazo a cada uno de estos con algún detalle, empezando por la identidad.

La identidad se puede reunir de varias maneras usando la solución ISE. Los siguientes métodos son los más favorables, enumerados a continuación en la tabla 2-1.

Tabla 2-1: Tipo de autenticación de ISE

Tipos de autenticación en ISE	
1	802.1X
2	Autenticación VPN / RADIUS
3	Firewall de identidad de ASA
4	Autenticación Web
5	Bypass de autenticación MAC (MAB)
6	Acceso de invitado no autenticado / autenticado

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

1.5.2.1 802.1X

IEEE 802.1X es el estándar para el control de acceso de red basado en puertos. El protocolo utiliza Extensible Authentication Protocol (EAP), un marco de autenticación flexible definido en RFC-3748. El protocolo define tres componentes en el proceso de autenticación:

- **Suplicante**: El agente en el dispositivo / PC que se utiliza para acceder a la red. El suplicante se incorpora o se agrega al sistema operativo. El autenticador le solicita autenticación.
- **Autenticador:** El dispositivo que controla el estado de un enlace; Típicamente un switch cableado o una controladora LAN inalámbrica.
- **Servidor de autenticación**: Un servidor de segundo plano (backend) que autentica las credenciales proporcionadas por los solicitantes. Por ejemplo, la controladora LAN inalámbrica pasa las credenciales del solicitante a través de RADIUS a ISE para la autenticación.

1.5.2.2 Autenticación VPN / RADIUS

Utilizando ISE para autenticar sus clientes VPN, ISE conoce la identidad de sus usuarios VPN. Por ejemplo, Cisco ASA envía credenciales desde el cliente VPN a través de RADIUS a ISE para la autenticación.

1.5.2.3 Firewall de identidad de ASA

Cisco ASA admite firewall de identidad (IDFW). ASA puede utilizar ISE como un servidor de autenticación para este propósito. De esta forma, ISE aprenderá la identidad de todos los usuarios que pasen por el Cisco ASA habilitado para IDFW.

1.5.2.4 Autenticación Web

Proporciona autenticación a través de una página web, normalmente a través de una dirección URL del navegador del usuario. La funcionalidad incorporada del servidor de invitados de ISE proporciona este servicio de portal web. Por ejemplo, un usuario se conecta a una red inalámbrica sin autenticación, es decir, modo abierto, el navegador del usuario es redirigido a la página de inicio de sesión alojada por ISE.

ISE recopila las credenciales y realiza la autenticación.

1.5.2.5 Bypass de Autenticación MAC (MAB)

MAB confía en una dirección MAC para la autenticación. Una dirección MAC es un identificador globalmente único que se asigna a todos los dispositivos conectados a la red y, por lo tanto, a menudo se denomina una dirección ftftware o pftysical.

Debido a que es un identificador único global. Sin embargo, la capacidad de asignar su propia dirección MAC a su dispositivo significa que, por sí mismo, una dirección MAC no es una forma confiable de autenticación.

1.5.2.6 Acceso de invitado no autenticado / autenticado

ISE incluye una función de servidor invitado que proporcionará una página de bienvenida de usuario invitado y, opcionalmente, una página de acuerdo de usuario y / o una página que solicite información del usuario como su dirección de correo electrónico, empresa, y así sucesivamente.

A los huéspedes se les permite el acceso sin proporcionar información de identidad, que generalmente se denomina "acceso de invitado no autenticado". Esto es lo que se encuentra generalmente en laboratorios de universidades o en algún cibercafé que ofrece acceso gratuito a Internet, normalmente sólo permite el acceso a Internet y no otros privilegios dentro de ISE.

En casi todos los casos, el acceso a la red que recibe un invitado está severamente restringido en comparación con lo que recibe un empleado autenticado y normalmente sólo permite el acceso a Internet esto sucede más frecuentemente dentro de las empresas u organizaciones que tienen que proteger sus datos, archivos, e información en general.

1.5.3 Reglas de autorización de ISE

Una vez completada la autenticación, ISE realiza su aplicación de políticas, también conocida como autorización. ISE puede utilizar decenas de atributos de políticas para cada regla, consolidada para su autorización. A continuación se muestra algunos de los atributos de políticas más populares disponibles para su uso en ISE:

- Resultados de la evaluación de postura.
- Afiliación al grupo de Active Directory.
- Atributos basados en el usuario de Active Directory (nombre de la empresa, departamento, dirección, título del trabajo, etc.).

- Localización.
- Método de acceso (MAB, 802.1X, cableado, inalámbrico, etc.).
- Hora y fecha.
- Combinación de perfiles para con el tipo de dispositivo.
- Si el dispositivo ha sido registrado con ISE.
- Información sobre el certificado digital (comúnmente utilizada para determinar los activos corporativos y no corporativos).
- Cientos de atributos y valores de RADIUS.

1.5.4 Componentes de la solución ISE

Cada grupo tiene un papel distinto que desempeñar en la solución ISE. Se analizó los roles y funciones de estos grupos donde se encuentran detallados las características recomendadas por Cisco.

1.5.4.1 Componentes de Infraestructura

Los componentes de infraestructura soportados por ISE son numerosos, como se observa en la tabla 3-1. Estos dispositivos de infraestructura de red incluyen tanto dispositivos de marca Cisco como dispositivos que no son de Cisco. Sin embargo, los dispositivos de marca Cisco, previsiblemente, proporcionan más funcionalidad con una mejor integración en la solución ISE. (Woland, A; Heary, J, 2013)

Tabla 3-1: Componentes de infraestructura recomendados por Cisco

Switches de Acceso	Switches de Core	Switchs de Centro de Datos	Controladora Wireless	Routers	Firewall
Catalyst 3650X/3750 X	Catalyst 6500 Supervisor	Nexus 7000 Series	WLC 5500/2500	ISR G2 Models	ASA 5585 9.X
Catalyst 3850	Catalyst 4500 Supervisor 7-	Nexus 5500 Series	WLC 5760	ISR G3 Models	ASA 5500-X 9.x
Catalyst 4500/4500x			WiSM 2 for Catalyst 6500	ASR 1000 Models	

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

1.5.4.2 Componentes de las políticas

Cisco Identity Services Engine comprende el único componente de políticas de la solución ISE.Tener un único motor centralizado de política significa la potencia inherente a la solución ISE. ISE proporciona una solución de control de acceso basada en atributos altamente robusto y flexible y los combina en una única plataforma: autenticación, autorización y auditoria (AAA); además servicios de gestión de huéspedes.

Los administradores pueden crear y administrar centralmente directivas de control de acceso para usuarios y puntos finales de manera consistente y obtener visibilidad de extremo a extremo en todo lo que está conectado a la red. ISE descubre y clasifica automáticamente los puntos finales, proporciona el nivel adecuado de acceso basado en la identidad y proporciona la capacidad de aplicar el cumplimiento del punto final, comprobando la postura de un dispositivo.

ISE también ofrece capacidades avanzadas de aplicación, incluyendo SGA a través del uso de Security Group Tags (SGT), Security Group Firewalls como el Cisco ASA y Security Group ACLs (SGACL).

1.5.4.3 Componentes de puntos finales

Los puntos finales de red desempeñan un papel integral en la solución ISE total. Es el punto final que proporciona autenticación mediante 802.1X, MAB o autenticación web. También es el punto final que proporciona información de postura al ISE para asegurar que está en conformidad con las políticas de seguridad, siendo los siguientes componentes de punto final recomendados para brindar una mayor robustez a la plataforma de ISE:

- **802.1X Supplicant / Agent:** Un suplicante es básicamente un software que entiende cómo comunicarse a través del protocolo de autenticación extensible a través de LAN (EAPoL). Hay muchos suplicantes disponibles para su uso. Un suplicante está integrado en Windows y Mac OS-X. También está disponible a través de Cisco AnyConnect y otros agentes de software de suplentes de terceros. Cisco IP Phones, equipos de video, Impresoras y muchos otros dispositivos ahora vienen con suplicantes incorporados. Casi cualquier dispositivo que sea capaz de usar WiFi tendrá un suplicante nativo.
- **Agente de Cisco NAC**: para Windows, Mac OS X y Linux. Proporciona información de postura de host a ISE.

1.5.5 Personajes dentro de ISE

La arquitectura ISE tiene muchos personajes para ayudarlo a escalar a grandes redes y a un gran número de usuarios y dispositivos. ISE tiene una arquitectura altamente disponible y escalable que soporta implementaciones independientes y distribuidas. ISE tiene tres personajes principales. La persona o las personas de un nodo ISE determinan los servicios que proporcionará. Un nodo ISE puede asumir cualquiera o todos los siguientes personajes:

- Administración: Le permite realizar todas las operaciones administrativas en una implementación ISE de Cisco independiente o distribuida. El nodo Administración proporciona un solo panel para la gestión. Maneja todas las configuraciones y las políticas relacionadas con el sistema. Un nodo ISE dedicado al personaje de administración se conoce como Nodo de Administración de Políticas (PAN).
- Servicio de Políticas: Proporciona acceso a la red, postura, acceso de invitado, aprovisionamiento de clientes, portales web y servicios de creación de perfiles. Este personaje evalúa las políticas y toma todas las decisiones. Asumir este personaje puede tener más de un nodo. Cuando un nodo está dedicado a la persona del servicio de políticas, se le conoce como nodo de servicio de políticas (PSN). Normalmente, un despliegue distribuido tendría más de una PSN.
- Supervisión: Permite que ISE funcione como el colector de registros y almacene los mensajes de registro de todos los nodos de servicio de administración y políticas de su red. Este personaje proporciona herramientas avanzadas de supervisión y solución de problemas que puede utilizar para administrar eficazmente la red y sus recursos. Un nodo con este personaje agrega y correlaciona los datos que recopila para proporcionarle información significativa.

1.5.6 Licencias, Requisitos y Performance de ISE

En esta sección se analiza el modelo de licencia centralizado de ISE, los requisitos de hardware y máquina virtual así como también el rendimiento de un nodo ISE.

1.5.6.1 Licencia ISE

Sólo hay tres licencias y cada licencia se clasifica para usuarios y dispositivos autenticados simultáneamente. La Figura 8-1 muestra los tres tipos de licencia ISE: Base, Avanzado y Sólo

inalámbrico.Wireless License (Base & Advanced solamente para implementaciones inalámbricas licencia para 5 años).

Las licencias mostradas en la Figura 8-1 incluyen adicionalmente un recuento de usuarios. Por ejemplo, L-ISE-ADV3Y-100 = significa una licencia avanzada de 100 usuarios que es válida por 3 años.

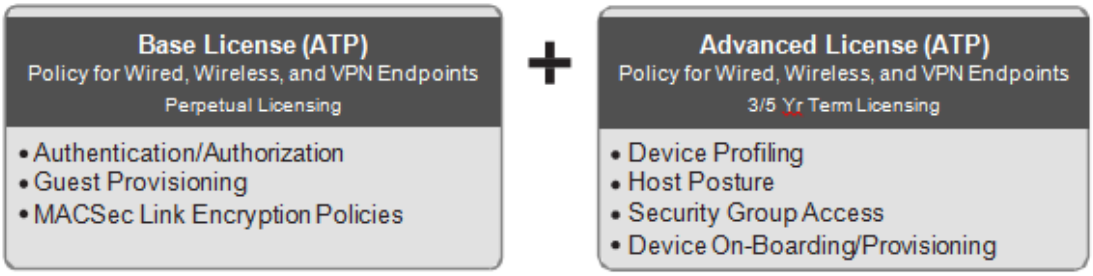


Figura 8-1: Licencias de ISE
Fuente: (Woland, A; Heary, J, 2013, p.23)

ISE viene en factores de dos formas: dispositivo físico y dispositivo virtual. El dispositivo físico viene con el hardware del servidor; El dispositivo virtual viene como un paquete de dispositivo virtual de VMware que se puede cargar en un servidor VMware ESX. El dispositivo físico viene en tres factores de forma: pequeño, medio y grande. La Tabla 4-1 y 5-1 proporcionan los detalles del hardware. (Woland, A; Heary, J, 2013)

Tabla 4-1: Detalles de Hardware A

Plataforma	**Cisco Identity Services Engine Dispositivo 3415 (Pequeño) UCS-C220-M3**	**Cisco Identity Services Engine Dispositivo 3495 (Grande)**
Procesador	Xeon E5-2609 4 core processor @ 2.4 GHz	2 x QuadCore Intel Xenon E5-2609 @ 2.4 GHz
Memoria	16 GB	32 GB
Disco Duro	1 x 600-GB SAS	2 x 600-GB SAS
RAID	No	Yes (RAID 0+1)
Ethernet NICs	4x 1 Gigabit NICs	4 x Integrated Gigabit NICs
		Dual Pwr, SSL Acceleration card

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Tabla 5-1: Detalles de Hardware B

Plataforma	Cisco Identity Services Engine Dispositivo3315 (Pequeño)	Cisco Identity Services Engine Dispositivo 3355 (Mediano)	Cisco Identity Services Engine Dispositivo 3395 (Grande)
Procesador	1 x QuadCore Intel Core 2 PU Q9400 @ 2.66 GHz (4 total cores)	1 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz (4 total cores)	2 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz (8 total cores)
Memoria	4 GB	4 GB	4 GB
Disco Duro	2 x 250-GB SATA HDD (250 GB total disk space)	2 x 300-GB SAS Drives (600 GB total disk space)	4 x 300-GB SFF SAS Drives (600 GB total disk space)
RAID	No	Yes (RAID 0)	Yes (RAID 0+1)
Ethernet NICs	4x Integrated Gigabit NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Para el dispositivo virtual, las especificaciones para el host de la máquina virtual (VM) deben tener un tamaño igual o superior a las especificaciones del dispositivo físico que se intenta igualar. Por ejemplo, si se desea tener un rendimiento similar al de un aparato físico mediano, se debe crear una máquina virtual con las especificaciones de un dispositivo mediano que se muestra en la Tabla 4-1.

VMware VMotion y la clonación sólo se admiten en versiones de ISE 1.2 o posterior.

Estos son los requisitos mínimos de espacio en disco para la implementación de producción en Virtual Machine de ISE:

- ISE independiente: 600 GB
- Administración: 200 GB
- Monitoreo: 600 GB
- Administración y monitoreo: 600 GB
- Servicio de administración, supervisión y políticas: 600 GB
- Servicio de políticas: 100 GB (se recomiendan 200 GB)

1.5.6.2 Performance de ISE

El rendimiento del ISE depende de varios factores y, lamentablemente, no es un cálculo directo o preciso. Depende del tipo de nodo, persona (s), complejidad de políticas, tipo de dispositivos, puntos finales y otras variables, como se muestra en la tabla 6-1 y 7-1.

Tabla 6-1: Performance de ISE

Plataforma	Puntos finales máximos	Perfilador de Eventos	Posturas de autenticaciones
Cisco Identity Services Engine Dispositivo 3395	3000	500 por Segundo	70 por Segundo
Cisco Identity Services Engine Dispositivo 3355	6000	500 por Segundo	70 por Segundo
Cisco Identity Services Engine Dispositivo 3395	10000	1200 por Segundo	110 por Segundo
Cisco Identity Services Engine Dispositivo 3415	5000		
Cisco Identity Services Engine Dispositivo 3495	20000		

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Tabla 7-1: Performance de ISE (Máximo por implementación)

Descripción	Número
Número máximo de puntos finales con separación de nodos de Administración, supervisión y servicio de políticas.	200,000
Número máximo de puntos finales con un solo nodo de Administración y supervisión.	10,000
Número máximo de puntos finales con un solo nodo de Administración, supervisión y servicio de políticas.	2000 para todas las plataformas 33x5, 5000 Para 3415, y 10.000 para 3495
Número máximo de nodos con Servicio de políticas con separación de nodos de Administración, supervisión y servicio de políticas.	40
Número máximo de nodos de servicio de políticas con un solo nodo de Administración	5

y supervisión.	
Número máximo de dispositivos de acceso a la red (NAD)	10,000

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Hay que tener presente que nunca se debe exceder el 80% de la capacidad declarada, y 50% o menos para el diseño. Esto le permite desarrollar crecimiento en la arquitectura, y asegura que tiene un buffer saludable en caso de que su entorno no refleje las métricas de rendimiento probadas y documentadas por Cisco. Estas especificaciones se muestran en la tabla 4-1 y 5-1 respectivamente. (Woland, A; Heary, J, 2013)

1.5.7 Estructura basada en políticas de ISE

ISE se basa en un conjunto de reglas impulsadas por políticas, para tomar decisiones. ISE tiene varios tipos de políticas diferentes que se consolidan en un conjunto de políticas.

Un conjunto de políticas es un agrupamiento de varias reglas de política diferentes, de ambas políticas de autenticación y autorización. Por consiguiente, se puede tener varios conjuntos de políticas que se procesan en orden, de arriba hacia abajo, por último, se puede tener reglas de excepción global en toda la implementación de ISE. Los siguientes tipos de reglas se pueden llamar dentro de un conjunto de directivas de ISE:

- Política de autenticación
- Política de autorización
- Política de creación de perfiles
- Política de Postura del Dispositivo
- Política de aprovisionamiento de clientes
- Política de acceso a grupos de seguridad
- Política de invitados

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1 Metodología de la investigación

En el presente capítulo se muestra las etapas a seguir para realizar la integración de Cisco ISE con la infraestructura de red de la Espoch administrada por el DTIC, así también la unión de AD con ISE en donde se crea una base de datos de los usuarios y grupos de usuarios para clasificar los diferentes permisos y limitaciones de acceso a la red.

Este proceso investigativo utilizará la metodología analítica llevando a cabo las siguientes investigaciones: investigación bibliográfica y de observación. Cada una de las cuales se aplicarán en el estudio a medida de cómo se obtenga la información. A continuación se describen de manera general los procesos a realizar.

Para realizar este estudio se empezará con una previa recopilación de fuentes bibliográficas y tecnológicas, en las cuales se inspeccionarán las características de las comunicaciones inalámbricas, así como también los componentes y características de ISE.

Se procederá con la reunión de información a través de una investigación de campo acerca de la infraestructura de red, para poder definir el perfil del funcionamiento actual de la red wlan que posee la Espoch, y comprobar que es factible la utilización de ISE, y aplicarla en la mencionada red inalámbrica, a la cual se le realizarán las respectivas pruebas, para comprobar su comportamiento y funcionamiento, de ésta manera obtener los resultados, conclusiones, recomendaciones y de esta forma se finalizará con la documentación del estudio de esta tecnología.

2.2 Diagrama de topología de la red

El modelo de diseño de red de la Espoch se basa en el modelo jerárquico, todos estos equipos se encuentran el en Data Center de la institución. Como a continuación se muestra el diagrama físico de la red, y sus respectivas capas las cuales son: capa de núcleo, figura 1-2, capa de distribución y acceso, figura 2-2 y figura 3-2.

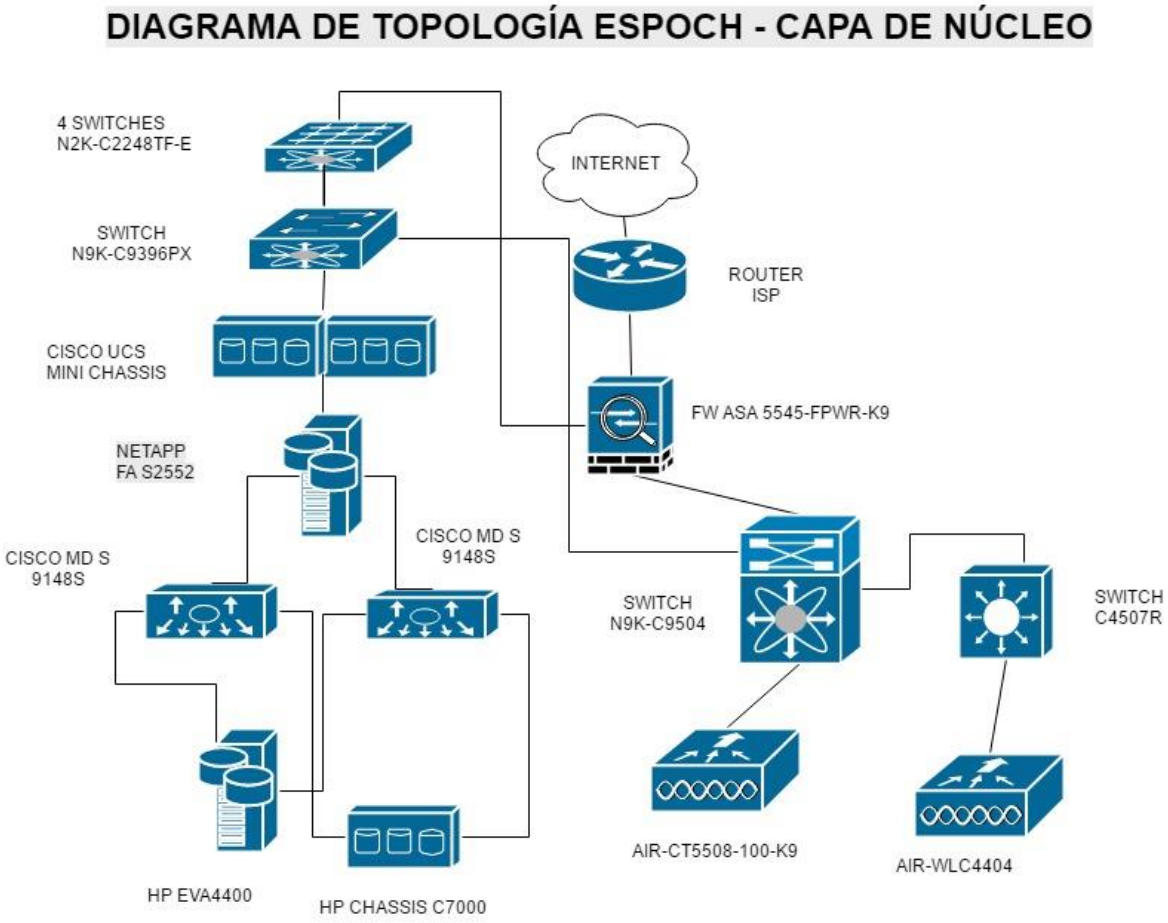


Figura 1-2: Topología Espoch-Capa de núcleo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

A continuación se enumeran los equipos existentes.

En la capa de Data Center como se muestra en la figura 1-2 se tiene:

- 4 Switchs stackables Cisco Nexus 2248 Fabric Extender.
- Switch Nexus 9396PX
- Cisco UCS Mini Chassis
- HP EVA4400
- HP Chassis C7000
- 2 Switch Cisco MDS Multicapa 9148S
- NetApp FA S2552

En la capa de Core como se muestra en la figura 1-2 se tiene:

- Router ISP
- FW ASA 5545

- Switch Nexus N9K-C9504
- Switch Catalyst C-4507
- Controladora inalámbrica AIR-CT5508-100-K9
- Controladora inalámbrica AIR-WLC4404

Desde el switch Nexus SC 9504 en la capa de Core se van interconectando hacia cada uno de los switch Catalyst 3850 que son de tipo stackable, para luego brindar la conexión hacia los switchs Catalyst 2960 en la capa de distribución y acceso, que a su vez se conectan con los APs encargados de difundir la red, como se muestra en la figura 2-2.

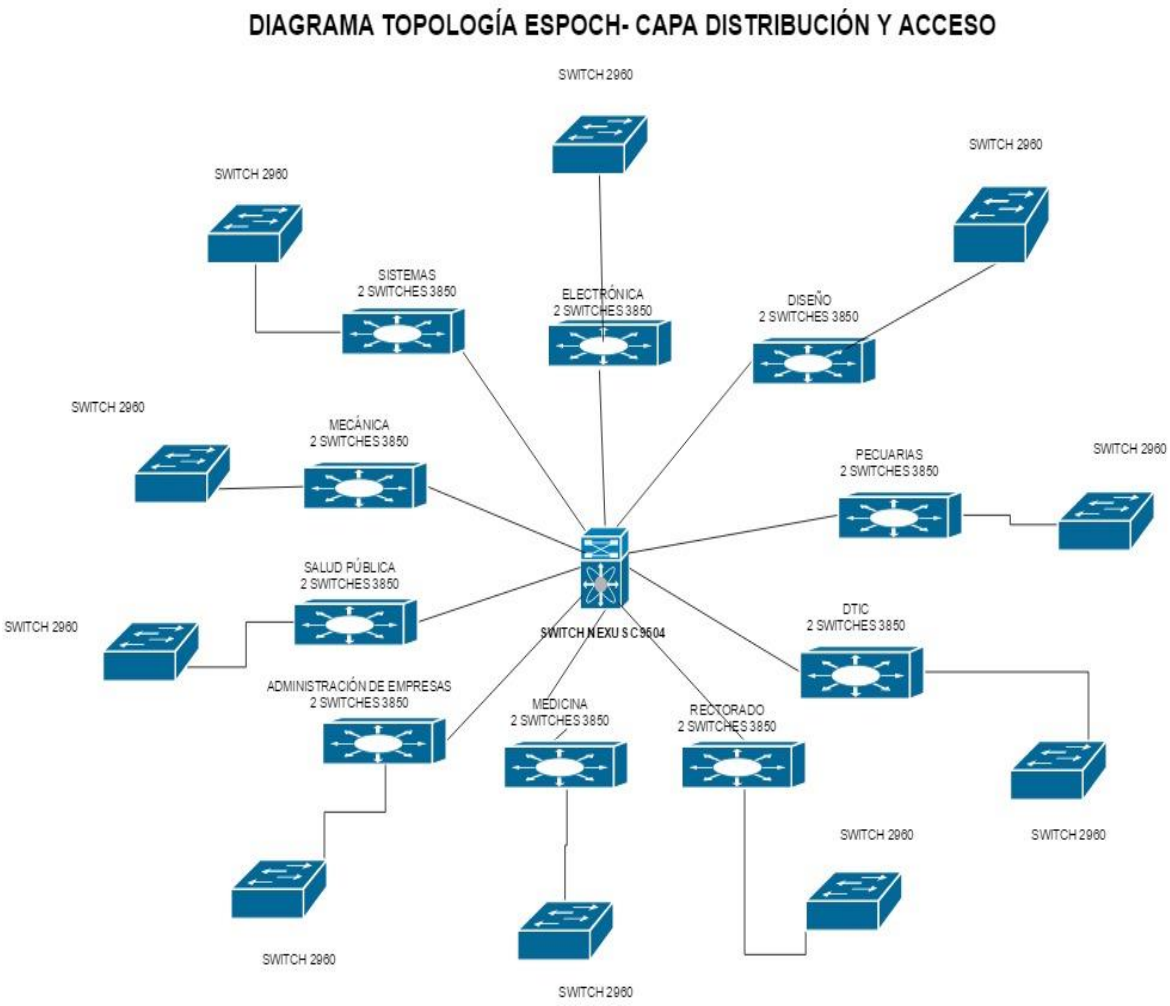


Figura 2-2: Topología Espoch-Capa distribución y acceso
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Desde la capa de Core con el switch Catalyst C4507R se van conectando en la capa de distribución los switches Catalyst 3850 los cuales son del tipo stackables, para luego dar la conexión hacia los switches Catalyst 2960 que pertenecen a la capa de acceso y se encuentran

sitiados para dar servicio en las diferentes facultades y dependencias como se muestran en la figura 3-2.

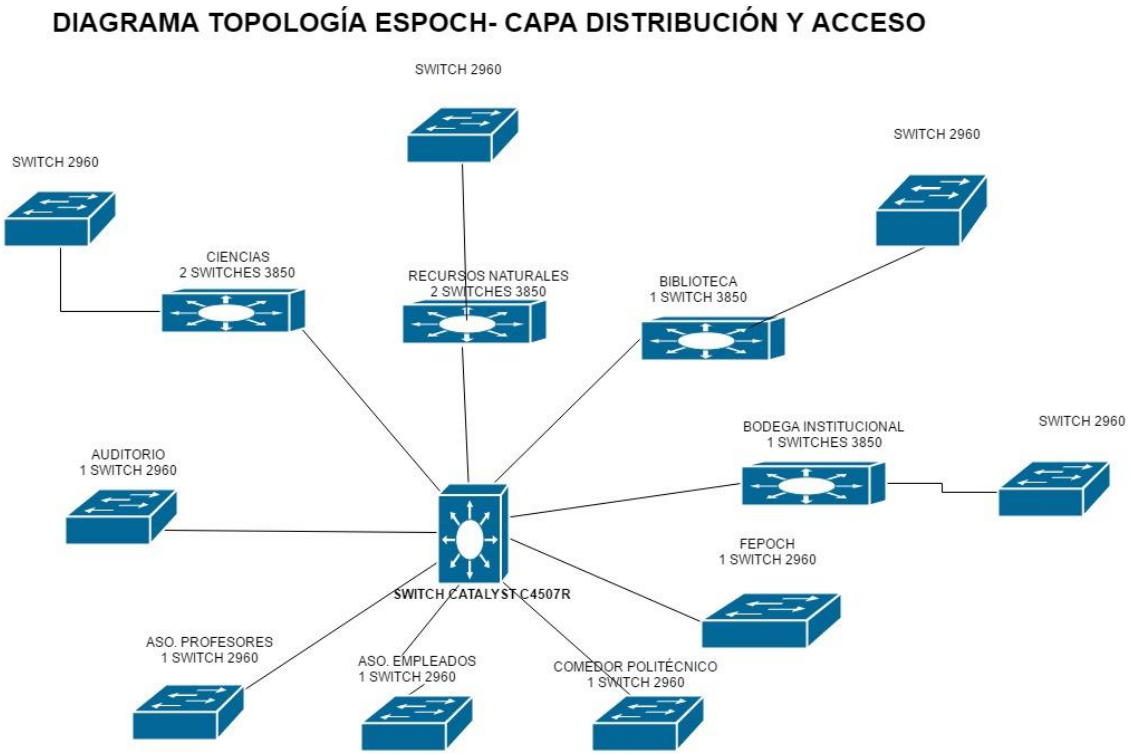


Figura 3-2: Topología Espoch – Capa Acceso
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

A continuación se enumeran los equipos existentes en la capa de distribución:

- Switch Catalyst 3850

A continuación se enumeran los equipos existentes en la capa de Acceso:

- Switch Catalyst 2960
- AIR AP 2700
- AP 1550 MESH

Dentro de la infraestructura que posee la Espoch se muestran los equipos con su versión de sistema operativo actual, y su rol en la misma, como se muestra en la tabla 1-2.

Tabla 1-2: Infraestructura para ISE

Componente	Versión de iOS	Rol
Switch Cisco Nexus N9K-C9504	v 7.0(3)|1(1)	Switch de Core
Switch Cisco Catalyst C-4507R	IOS 15.2.2 E5	Switch de Core
FireWall ASA Cisco 5545	ASA 9.2.1	Seguridad a la Red
WLC Cisco AIR-CT5508-100-K9	AirOS 8.0.140.0	Controla los puntos de acceso de manera centralizada
WLC Cisco AIR-WLC4404	AirOS 7.0.252.0	Controla los puntos de acceso de manera centralizada
Switch Cisco Catalyst 3850	IOS-XE 3.6.5E	Switch de distribución
Switch Cisco Catalyst 2960-S	IOS 15.0.2 SE	Switch de acceso
Switch Cisco Catalyst 2960-SF	IOS 15.0(2)SE7	Switch de acceso
AIR AP Cisco 2700	_____	Puntos de acceso
AP Cisco 1550 MESH	_____	Puntos de acceso

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.3 Justificación de equipos para compatibilidad de ISE

Los componentes de infraestructura soportados por Cisco ISE son numerosos. Estos dispositivos de infraestructura de red incluyen tanto dispositivos de marca Cisco como dispositivos que no son de Cisco, en el caso del Data Center de la Espoch se evidencia que su gran mayoría de equipos son de la marca Cisco, previsiblemente, proporcionan más funcionalidad con una mejor integración en la solución ISE.

Según (Cisco Systems, 2014), los equipos que se muestran a continuación en la tabla 2-2 son algunos de los equipos que poseen compatibilidad con ISE.

Tabla 2-2: Equipos recomendados por Cisco para ISE

Componente	Versión OS recomendada	Rol
Cisco Identity Services Engine	2.0	Servidor
Switches		
Catalyst 2960-S y 2960-C	IOS v 12.2(55)-SE5	
Catalyst 2960-SF y 2960Plus	IOS v 15.2.2-SE7	
Catalyst 2960-XR y 2960P-X	IOS v 15.2.2-EX5 (ED)	

Catalyst 3560-C, 3560-E, ISR EtherSwitch ES3 Catalyst 3560-X	IOS v 15.0.2-SE2 (ED)	Switch de acceso/core
Catalyst 3750-G	IOS v12.2(55)-SE5	
Catalyst 3750-E y 3750-X	IOS v 12.2.(55)SE5	
Catalyst 3850 y 3650	IOS XE 3.6.3	
Catalyst 4500-X	IOS 15.0.2 E5	
Catalyst 6500 (Supervisor 32/Supervisor 720)	IOS v 12.2.33-SJX9	
Nexus N9K-C9504	IOS v 7.0(3)|1(1)	
Inalámbricos		
Wireless LAN Controller (WLC) 2100, 4000, WiSM1 y WiSM2 Blade for 6500	AirOS 7.0.116.0	Controla los puntos de acceso de manera centralizada.
WLC 2500, 5500, 7500 y 8500	AirOS 8.0.121.0	
WLC 5760	IOS XE 3.6.3	
Routers		
WLC ISR (ISR2 ISM, SRE700 y SRE900)	7.3.112.0(ED)	Enrutamiento.
ISR 88X, 89X Series, 19x, 29x, 39x Series	15.3.2T(ED)	
Firewalls		
Cisco ASA 5500 y 5545	ASA 9.2.1	Seguridad a la red.
Access Point		
Cisco Series AP 3700, 3600, 3500, 2600	----------	Puntos de acceso.

Fuente: (Cisco Systems, 2014)

Si una infraestructura cumple con los requerimientos recomendados, estos son capaces de soportar las siguientes funciones:

- Bypass de Autenticación MAC (MAB): Utilización de la dirección MAC de un punto final que no puede autenticarse el mismo en la red.
- 802.1X: El estándar IEEE para la comunicación de credenciales de identidad mediante EAP (Extensible Authentication Protocol) a través de LAN.
- Autenticación web: Autenticación de usuarios que intentan acceder a la red a través de una página web. La autenticación web tiene dos modos de implementación:
    - Central Web Authentication (CWA): La opción más popular, controlada por ISE.

    - Autenticación Web Local (LWA): Realizada por el conmutador o el controlador de LAN inalámbrica (WLC) y no puede realizar CoA (descrito a continuación), modificar la VLAN del puerto o soporta sesión de identidad.
- Cambio de autorización (CoA): Atributo RADIUS que ISE emite a un dispositivo de acceso para forzar la reautenticación de la sesión. CoA forma la columna vertebral de la solución 802.1X ISE.
- VLAN: El dominio de difusión de la capa 2 que podría asignarse a los dispositivos entrantes.
- ACL descargable (dACL): Una lista de control de acceso que se envía desde ISE al dispositivo de acceso para restringir la sesión.
- Acceso de grupo de seguridad (SGA): la arquitectura SGA construye redes seguras estableciendo un dominio de dispositivos de confianza SGA usa la información de identidad del dispositivo de usuario adquirida durante la autenticación que clasificar los paquetes como han entrado a la red, esta clasificación de paquetes, es realizada por un etiquetamiento de paquetes que ingresan a una red basada en SGA, el etiquetamiento llama a un grupo de seguridad SGT (Security Group Tag) permitiendo que el dispositivo de red actúe sobre el SGT para controlar o restringir el tráfico.
- Sensor IOS: Habilita la funcionalidad de creación de perfiles integrada con los IOS de los switches Catalyst, hardware de WLCs, permitiendo hacerlo de forma local, en lugar de hacerlo en forma centralizada en un nodo de ISE.

Nota: Ciertos casos de uso avanzado, como los que implican la evaluación de la postura, la creación de perfiles y la autenticación web, no están disponibles de forma consistente con dispositivos que no pertenecen a Cisco o pueden proporcionar funcionalidad limitada y, por lo tanto, no se admiten con dispositivos que no sean de Cisco. Además, algunas otras funciones avanzadas, como la Centralized Web Authentication (CWA), el cambio de autorización (CoA), el acceso al grupo de seguridad y las listas de control de acceso descargables (dACL), sólo se admiten en los dispositivos Cisco.

2.4 Licencias y Servicios de Cisco ISE

Las licencias de Cisco ISE vienen dadas por cinco packs disponibles, los cuales se detallan a continuación en la tabla 3-2:

Tabla 3-2: Tipos de licencias de ISE

Pack de licencia Cisco ISE	Enfoque	Tipo Permanente o suscripción
Evaluación	Uso limitado del producto Cisco ISE para pruebas o evaluaciones de clientes de preventa	Temporal 90 días
Administración de Dispositivos	Levanta dispositivos de administración/TACACS+ soportado por dispositivos de networking	Permanente
Base	Provee alta seguridad de dispositivos y usuarios de acceso	Permanente
Plus	Proporciona contexto sobre los puntos finales para políticas de acceso as detalladas	Suscripción 1,3,5 años
Apex	Proporciona detalles de cumplimiento sobre los dispositivos finales para políticas de acceso más detalladas	Suscripción 1,3,5 años

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Para un mejor entendimiento de cada una de las licencias y sus funcionalidades se muestra la figura 4-2.

Cisco ISE Feature or Service	License			
	Base	Device Admin	Plus	Apex
Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass	Yes			
Web authentication (local, central, device registration)	Yes			
MACsec (all)	Yes			
SSO, SAML, ODBC – based authentication	Yes			
Guest portal and sponsor services	Yes			
Representational state transfer (monitoring) APIs	Yes			
External RESTful services (CRUD)-capable APIs	Yes			
Security group tagging (Cisco TrustSec® SGT)	Yes			
Device Administration (TACACS+)		Yes		
Profiling			Yes	
Profiler feed service			Yes	
Device registration (My Devices portal) and provisioning for Bring Your Own Device (BYOD) with built-in Certificate Authority (CA)			Yes	
Context sharing (Cisco pxGrid)			Yes	
Endpoint Protection Services (EPS)			Yes	
Suite B			Yes	
TrustSec – ACI Integration			Yes	
Location based integration using CMXMSE			Yes	
Rapid Threat Containment (RTC) using ANC and pxGrid			Yes	
Posture (endpoint compliance and remediation)				Yes

Figura 4-2: Características de Licencias
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Se toma a consideración el costo de las licencias de administración y de base mostrados en la tabla 4-2:

Tabla 4-2: Valores de las licencias

Número de parte	Descripción	Precio
L-ISE-TACACS=	Cisco ISE Device Admin License	4.000,00 $
L-ISE-BSE-100=	Cisco ISE 100 Endpoint Base License	500,00 $
L-ISE-BSE-250=	Cisco ISE 250 Endpoint Base License	1.500,00 $
L-ISE-BSE-500=	Cisco ISE 500 Endpoint Base License	2.500,00 $
L-ISE-BSE-1K=	Cisco ISE 1,000 Endpoint Base License	5.000,00 $

L-ISE-BSE-1500=	Cisco ISE 1,500 Endpoint Base License	6.750,00 $
L-ISE-BSE-2500=	Cisco ISE 2,500 Endpoint Base License	9.900,00 $
L-ISE-BSE-3500=	Cisco ISE 3,500 Endpoint Base License	13.500,00 $
L-ISE-BSE-5K=	Cisco ISE 5,000 Endpoint Base License	15.000,00 $
L-ISE-BSE-10K=	Cisco ISE 10,000 Endpoint Base License	25.000,00 $
L-ISE-BSE-25K=	Cisco ISE 25,000 Endpoint Base License	45.000,00 $
L-ISE-BSE-50K=	Cisco ISE 50,000 Endpoint Base License	80.000,00 $
L-ISE-BSE-100K=	Cisco ISE 100,000 Endpoint Base License	125.000,00 $
L-ISE-BSE-250K=	Cisco ISE 250,000 Endpoint Base License	180.000,00 $

Realizado por: Departamento de Redes, DTIC, 2017

2.5 Densidad de usuarios

El número de conexiones diarias que se registran, varían según el día tomando en cuenta que la extracción de estos datos han sido brindados por parte del DTIC en un horario laborable de 7 am a 7 pm, esto se debe a que la parte administrativa tiene un lugar fijo donde realizar sus labores diarios, a su vez los docentes tienen espacios asignados para realizar sus trabajos específicos y de esta forma su modo de conexión inalámbrico depende de las posibilidades de cada docente, en cambio el alumnado su situación es diferente ya que se encuentran movilizándose constantemente por todo el campus dependiendo de las actividades que vaya a realizar.

En la figura 5-2 se muestra la mayor cantidad de conexiones inalámbricas que se dan por día, teniendo como un máximo 2.653 conexiones inalámbricas dentro del horario establecido, cabe recalcar que esta cantidad es el tope máximo de afluencia de conexiones que se las realiza en un

día, siendo este número de conexiones una combinación entre todo el personal existente de la Espoch quienes son: docentes, estudiantes y administrativos.

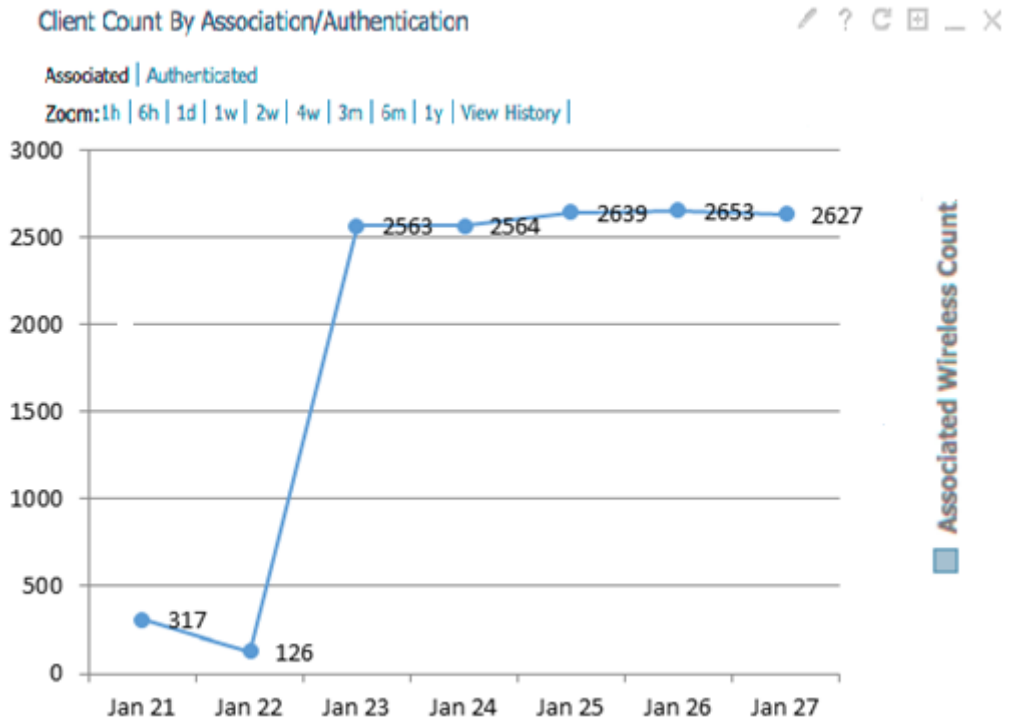


Figura 5-2: Densidad de usuarios
Fuente: Cisco Prime, DTIC, 2017

2.6 Dispositivos por usuarios

Los dispositivos que se usan para acceder a la red wlan de la Espoch son de una gran variedad como: laptops, tablets, smartphones, etc. Mediante el método de observación se define que los dispositivos más usados dentro del campus politécnico son: Android (Samsung, LG, Sony Xperia), iOS (iPhone 4s – 5s- 6), y Windows (7, 8, 10), siendo el grupo de estudiantes el más extenso de ellos, como se observa en la tabla 5-2.

Tabla 5-2: Dispositivos más usados por usuarios

Sistema Operativo	Dispositivo
Android 2.2 en adelante	Samsung, Sony Xperia LG.
iOS 4	Iphone 4,4s
iOS 5,6,7,8,9,10	Iphone 5, 5s, 5c, 6, 6s
Windows XP, Vista, 7, 8, 10	Acer, HP, Dell, Toshiba, Assus

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.7 Postura vigente del acceso a la red inalámbrica

La red inalámbrica de la Espoch se encuentra actualmente manejada por una Wireless Lan Controller (WLC) la cual se encuentra centralizada y operativa en el DTIC, que disponen de la red ESPOCH-OPEN y ESPOCH-PORTAL ambas redes abiertas con la diferencia que la segunda posee un portal cautivo, además el DTIC difunde la red eduroam, la cual cuenta con un nivel de seguridad WAP2-Enterprise dentro del campus politécnico, siendo estas tres redes de libre acceso para todo el personal académico (docentes, estudiantes, administrativos) de la Espoch.

Cada una de las SSID posee su propio segmento de red, al cual tiene libre acceso docentes, estudiantes y administrativos, compartiendo todos los atributos, y no posee un control o regulación específica para cada usuario dependiendo de su función, sea quien sea el usuario que se conecte.

- La red ESPOCH-OPEN no cuenta con ningún tipo de seguridad y la conexión se la realiza de forma única, para lo cual al usuario estudiante y al usuario administrativo al conectarse a esta red se le asigna un único segmento de red como se observa en las figuras 6-2 y 7-2.

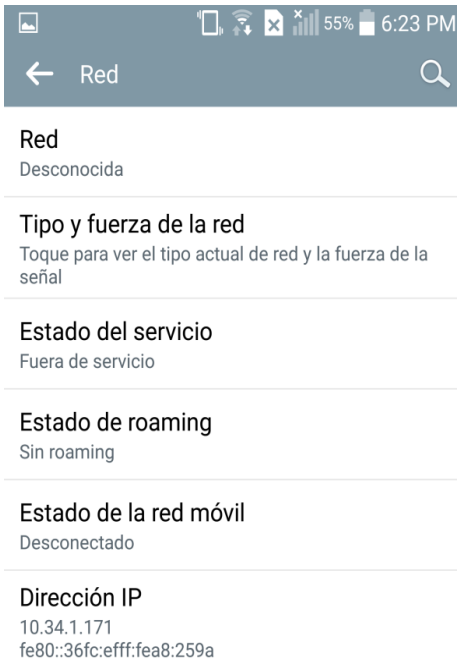


Figura 6-2: ESPOCH-OPEN Estudiante
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

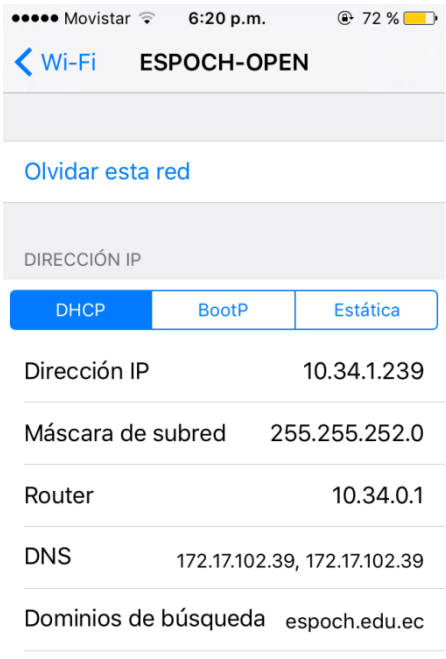


Figura 7-2: ESPOCH-OPEN Administrativo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

- La red ESPOCH-PORTAL su modo de conexión se lo realiza por medio de un portal cautivo ingresando credenciales de usuarios registrados en el sistema de la Espoch,

como se observa en la figura 9-2 muestra un anuncio que la información enviada no es codificada y por ende no es segura. Además se observa el mismo segmento de red independientemente si el usuario es docente, estudiante o administrativo, como se muestra en las figuras 8-2, 10-2, 12-2 respectivamente.

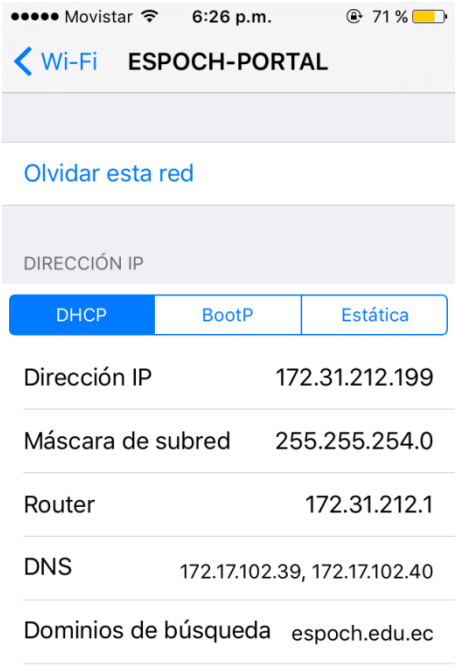


Figura 8-2: ESPOCH-PORTAL Docente
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

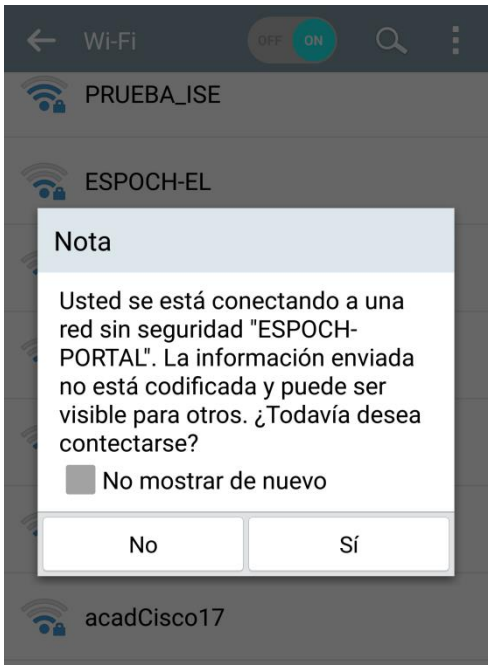


Figura 9-2: Aviso ESPOCH-PORTAL
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

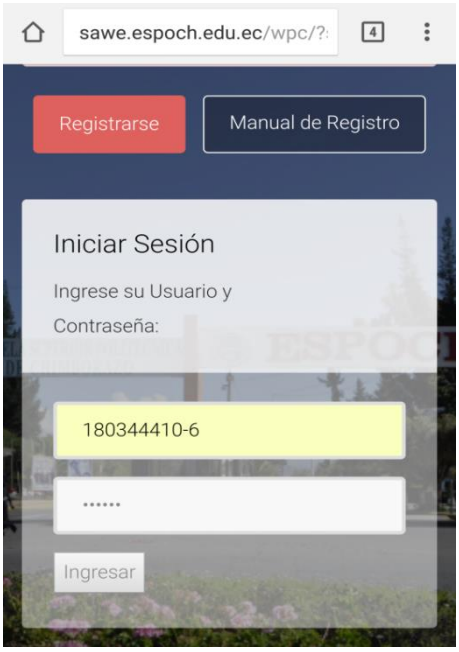


Figura 10-2: ESPOCH-PORTAL Estudiante
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

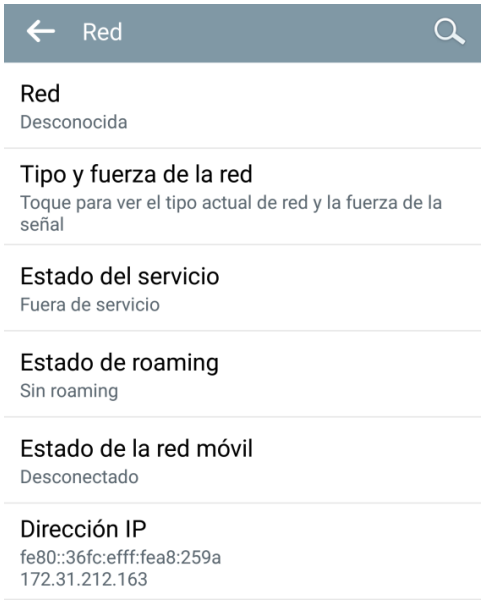


Figura 11-2: Direccionamiento 163
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

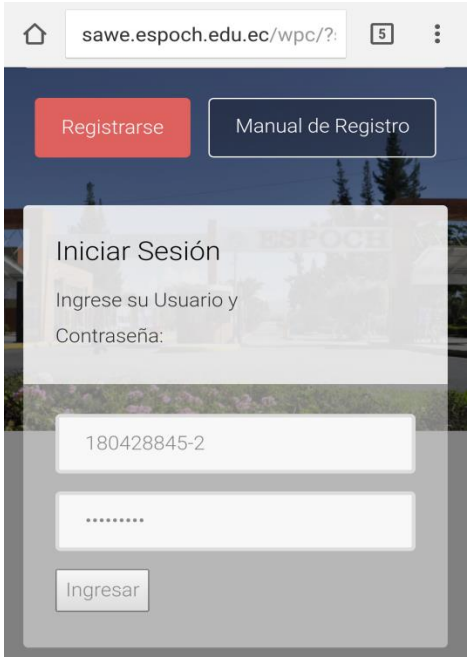


Figura 12-2:ESPOCH-PORTAL Administrativo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

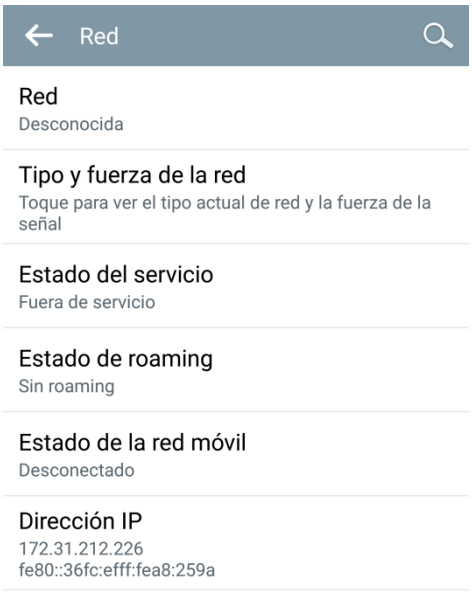


Figura 13-2: Direccionamiento 226
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.8 Cisco ISE y su implicación para la institución

Hoy en día la planificación de la red se debe tomar muy en cuenta, ya que la seguridad del usuario y de la red son indispensables a la hora de transmitir información, por lo tanto se busca una manera de proteger esta información de la mejor manera posible, para lo cual se ve necesario aplicar políticas de acceso según el tipo de usuario y dispositivo. Debido a los factores antes mencionados el diseño de red se inclina a la solución brindada por Cisco permitiendo adaptarse a los nuevos servicios y soluciones, de esta manera Cisco ISE puede ajustarse de forma dinámica y segura a la infraestructura ya existente.

2.9 Instalación y Configuración de ISE (Manual de usuario)

GUÍA DE IMPLEMENTACIÓN Y CONFIGURACIÓN DE CISCO ISE

Proceso 1. Instalación Inicial

Proceso 2. Configurar la lista de confianza de certificados

Proceso 3. Configuraciones Generales de nodo

Proceso 4. Instalar las licencias de Cisco ISE

Proceso 5. Configuración de ISE para usar Active Directory

Proceso 6. Unión y configuración de Wireless Lan Controller (WLC) con Cisco ISE

Proceso 7. Configuración de Cisco ISE para una red inalámbrica y unión con WLC.

Proceso 8. Implementación de certificados digitales

Proceso 9. Creación de políticas de Autenticación y Autorización.

Proceso 1. Instalación Inicial

Para disponer de AD se debe configurar Active Directory Domain Services y Active Directory Certificate Services:

Active Directory Domain Service

Para la instalación y configuración de AD DS se siguen los siguientes pasos:

1. Dentro de la página selección de servidor, se elige el servidor con el cual se va a trabajar y luego clic en el botón siguiente como se muestra en la figura 14-2.

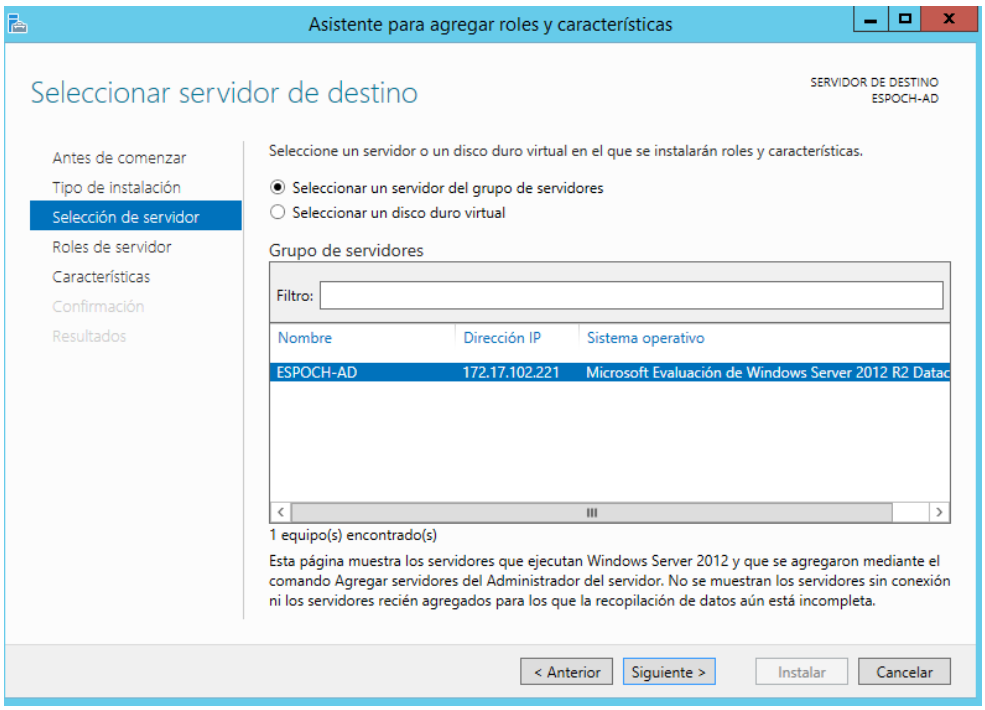


Figura 14-2: Seleccionamos servidor de destino
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2. Para agregar características, se selecciona ciertos parámetros para levantar el servicio de dominio de AD como se muestra en la figura 15-2.

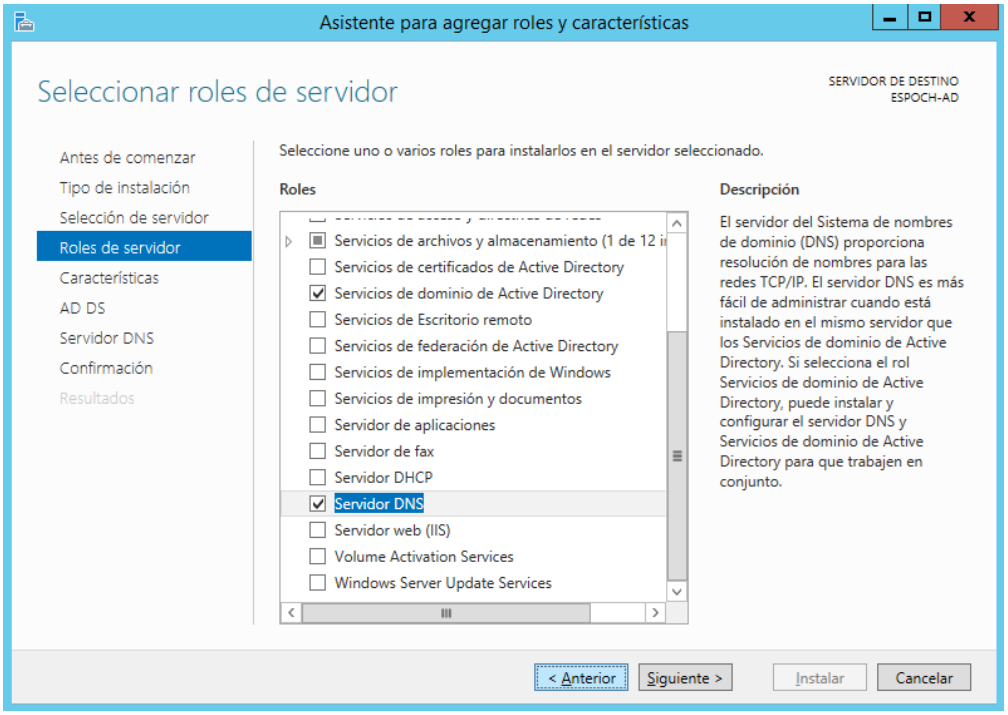


Figura 15-2: Agregación de Roles y Características.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3. En la pantalla Servicios de dominio de Active Directory, se selecciona la pestaña AD DS para comprobar la información y clic en el botón siguiente como se muestra en la figura 16-2.

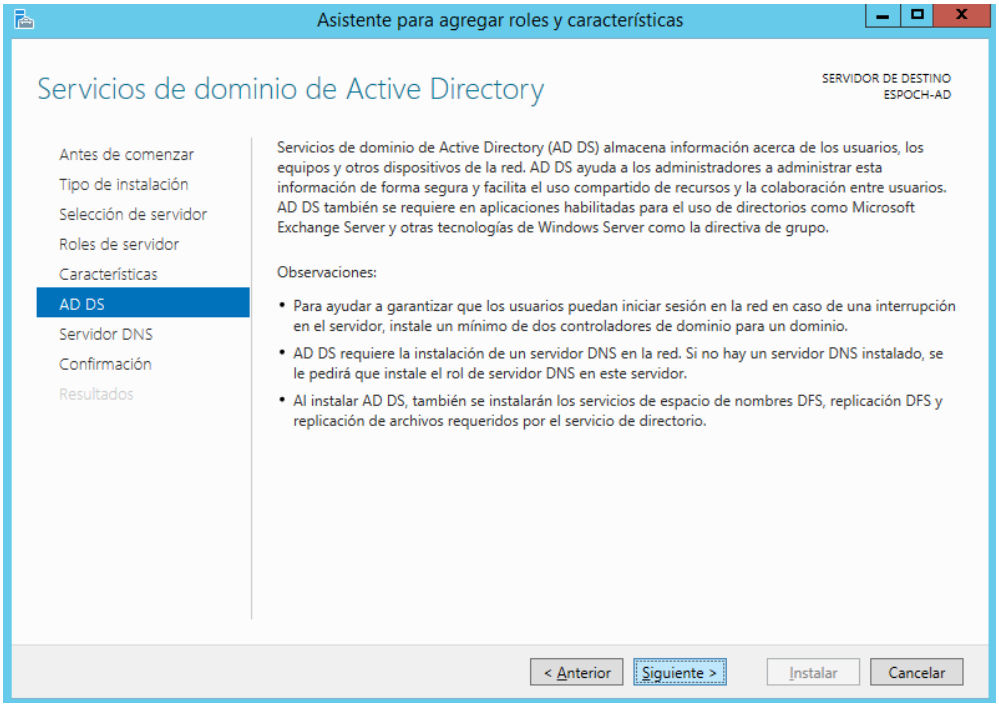


Figura 16-2: Observaciones AD DS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

4. Seleccionar la pestaña Servidor DNS para levantar el servicio DNS necesario en AD DS y luego clic en el botón siguiente como se muestra en la figura 17-2.

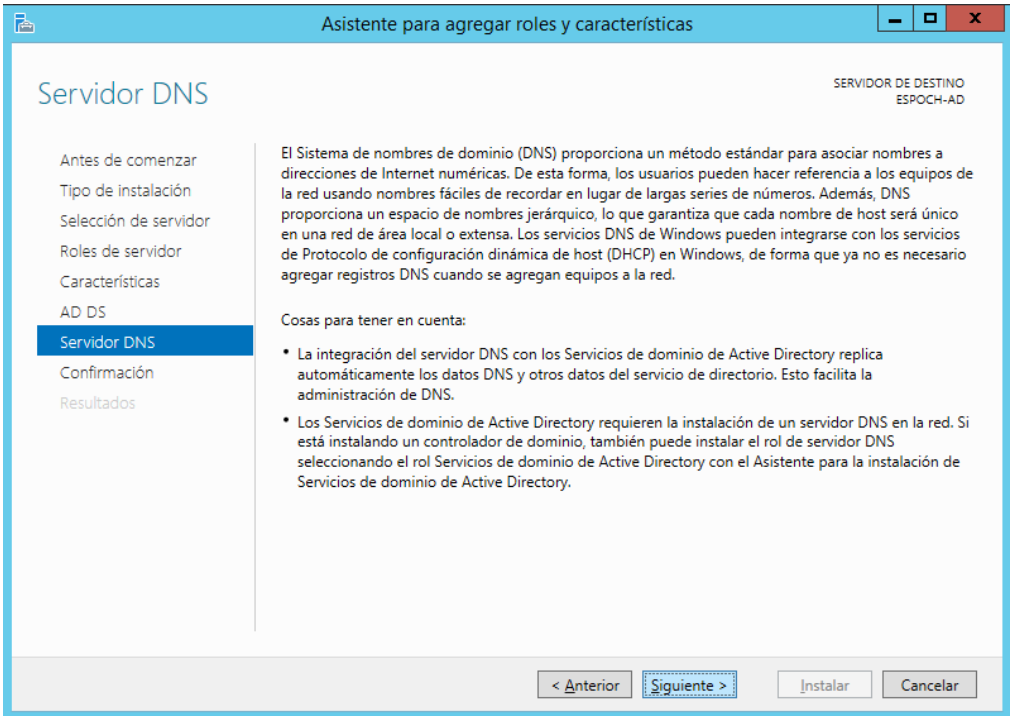


Figura 17-2: Observaciones DNS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

5. La opción de confirmación habilita las opciones antes seleccionadas para un mejor rendimiento del servidor y clic en el botón instalar para continuar, como se

muestra en la figura 18-2.

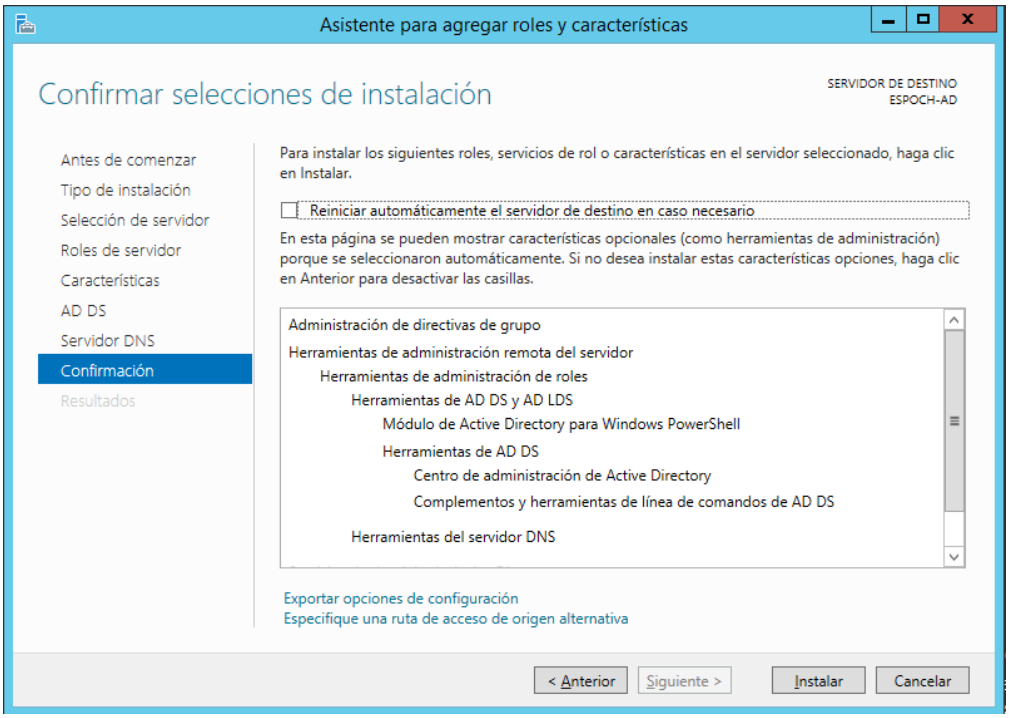


Figura 18-2: Confirmación de instalación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

6. Una vez finalizada la instalación aparece la siguiente pantalla de finalización en donde se presiona la opción cerrar para finalizar la instalación como se muestra en la figura 19-2.

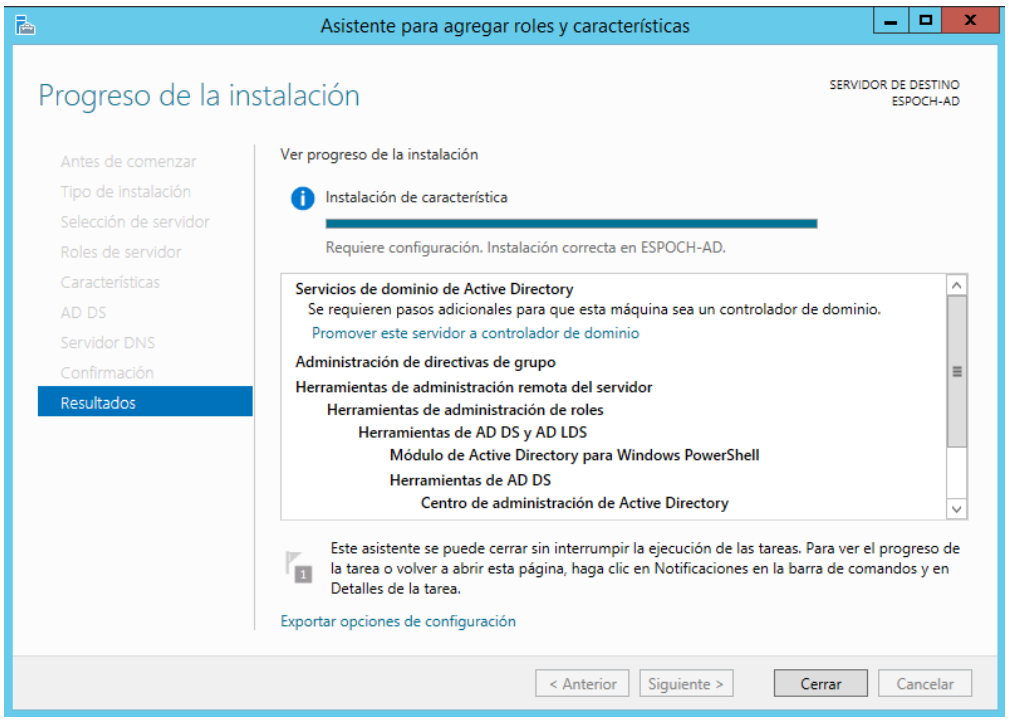


Figura 19-2: Finalización de instalación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

La pantalla de configuración de implementación contiene varias opciones que se debe configurar para agregar los servicios de domino como se muestra continuación:

7. Crear un nuevo bosque con el nombre de dominio raíz **espoch.edu.ec** como se muestra en la figura 20-2.

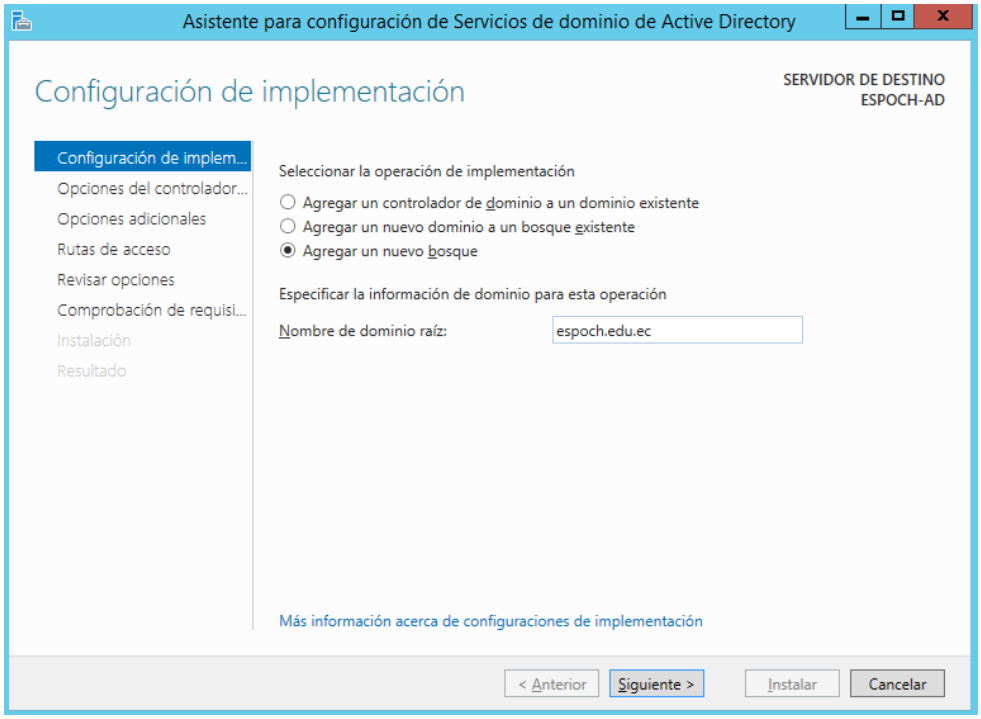


Figura 20-2: Agregación de bosque de AD.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

8. Se asigna una contraseña que tendrá el dominio más la confirmación de la misma como se muestra en la figura 21-2.

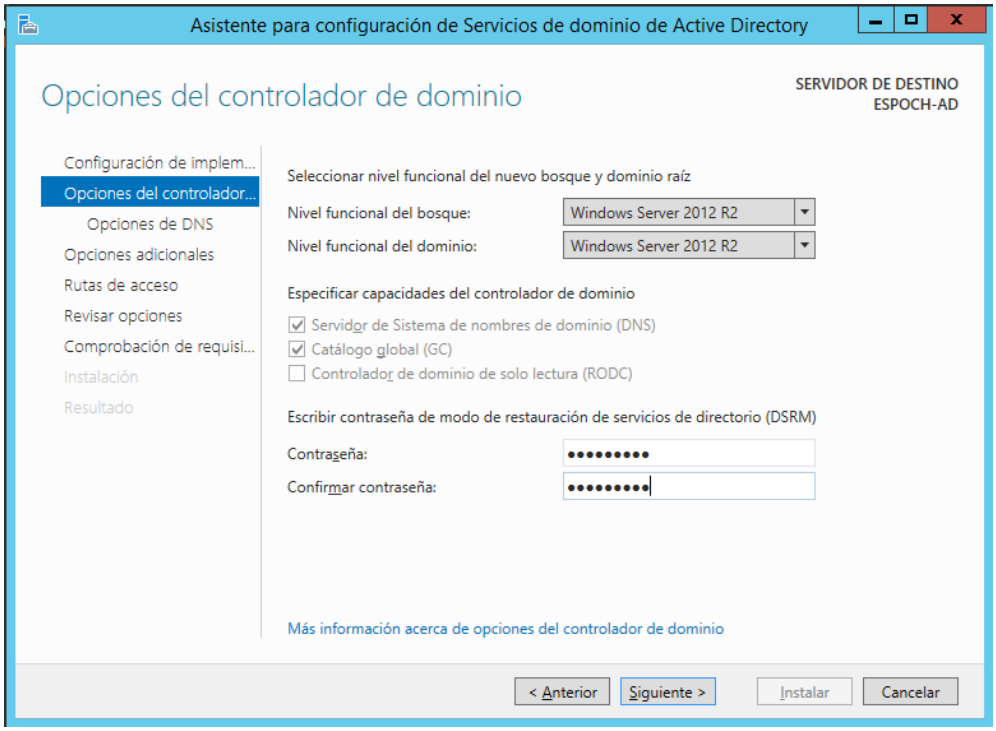


Figura 21-2: Asignación de contraseña del dominio.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

9. Se verifica el nombre asignado al dominio NetBIOS y se pulsa el botón siguiente como se muestra en la figura 22-2.

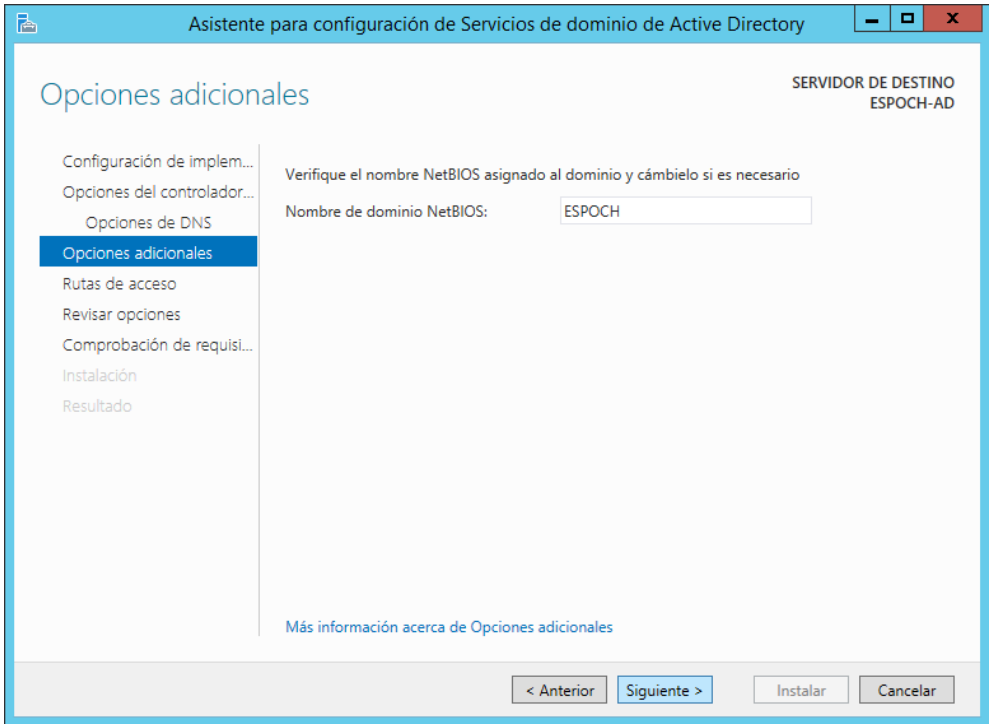


Figura 22-2: Comprobación nombre NetBIOS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

10. Se fija la ubicación de las carpetas en donde se encontrará la base de datos de AD DS, como se muestra en la figura 23-2.

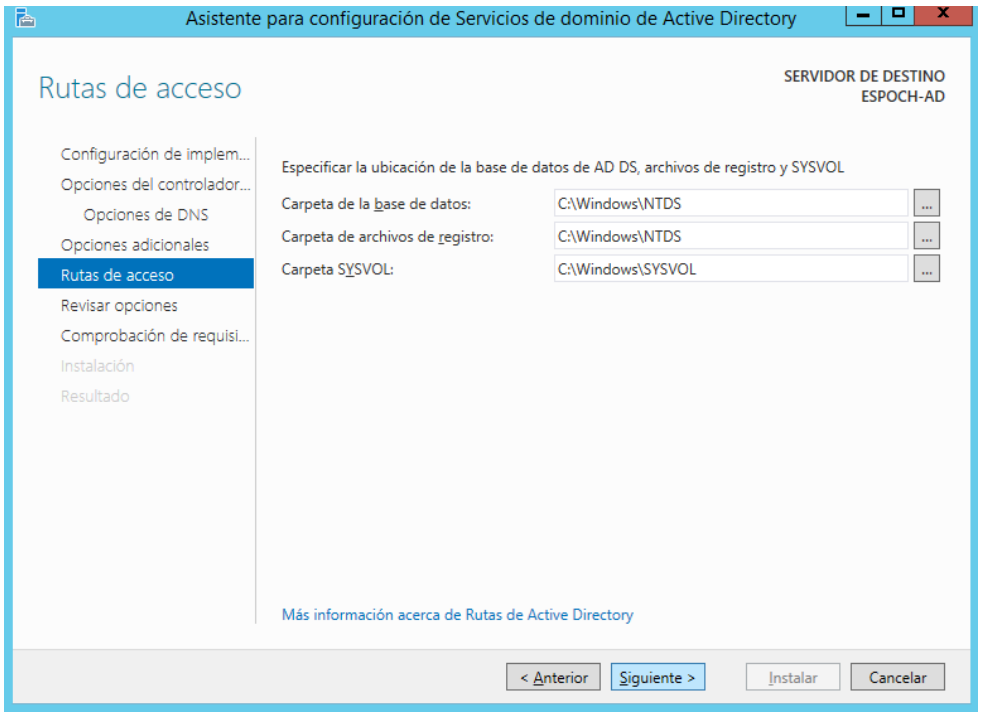


Figura 23-2: Ubicación de carpetas.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

11. Revisar las opciones de instalación y clic en el botón siguiente como se muestra en la figura 24-2.

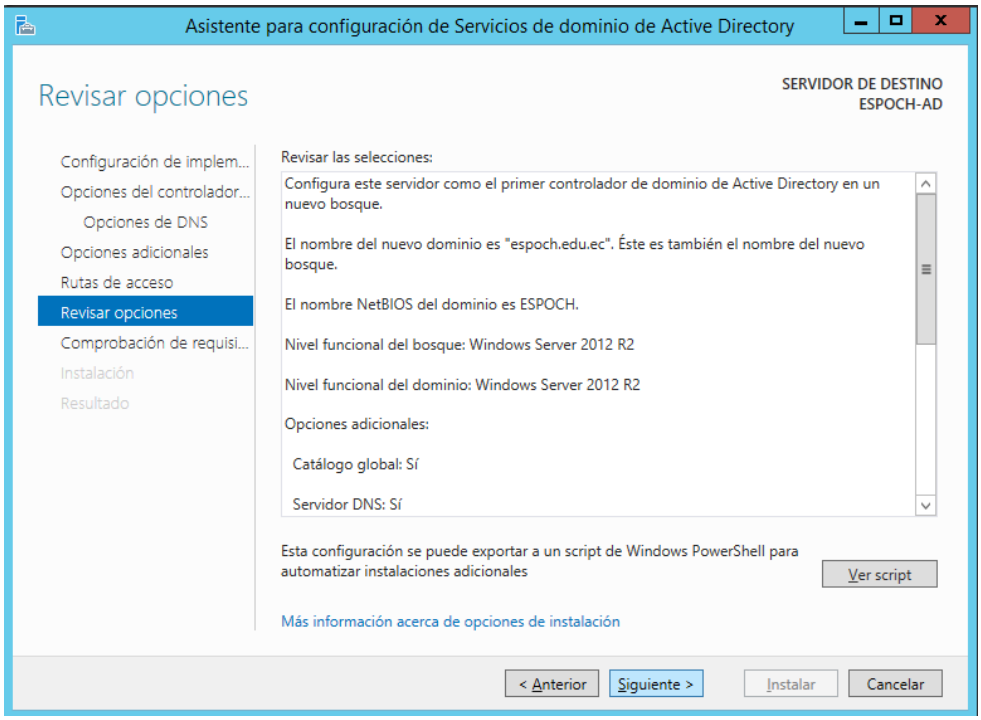


Figura 24-2: Revisión opciones de instalación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

12. Para finalizar se comprueba los prerrequisitos y se presiona el botón instalar

como se muestra en la figura 25-2.

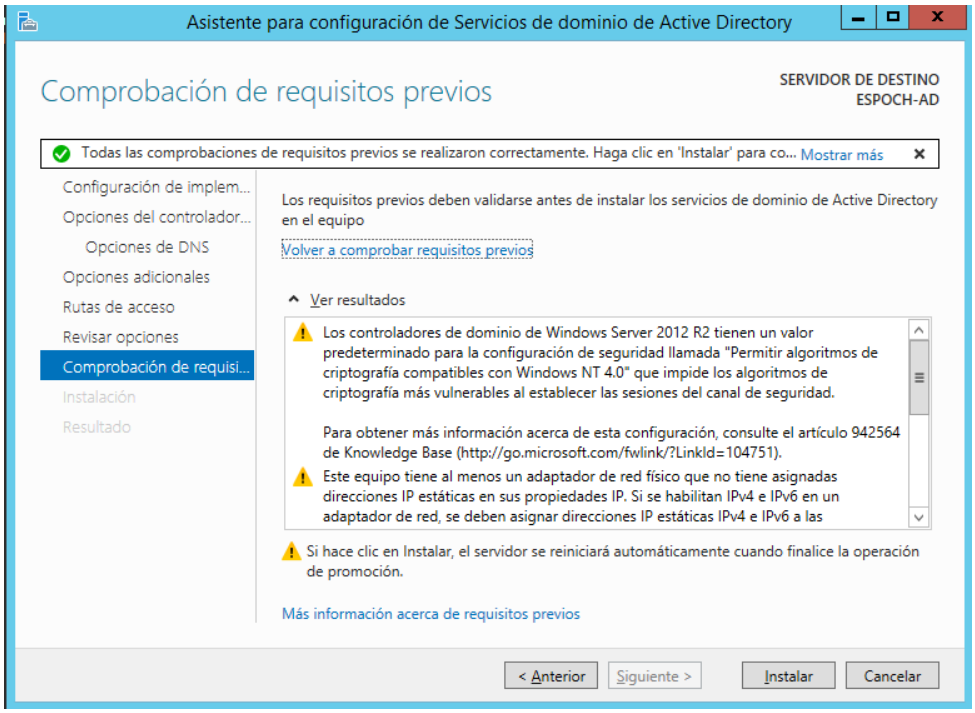


Figura 25-2: Comprobación de requisitos previos para la instalación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Active Directory Certificate Services

Para la instalación y configuración de AD CS se siguen los siguientes pasos:

1. Se ubica en el asistente para agregar roles y características requeridas en la instalación de AD CS como se muestra en la figura 26-2.

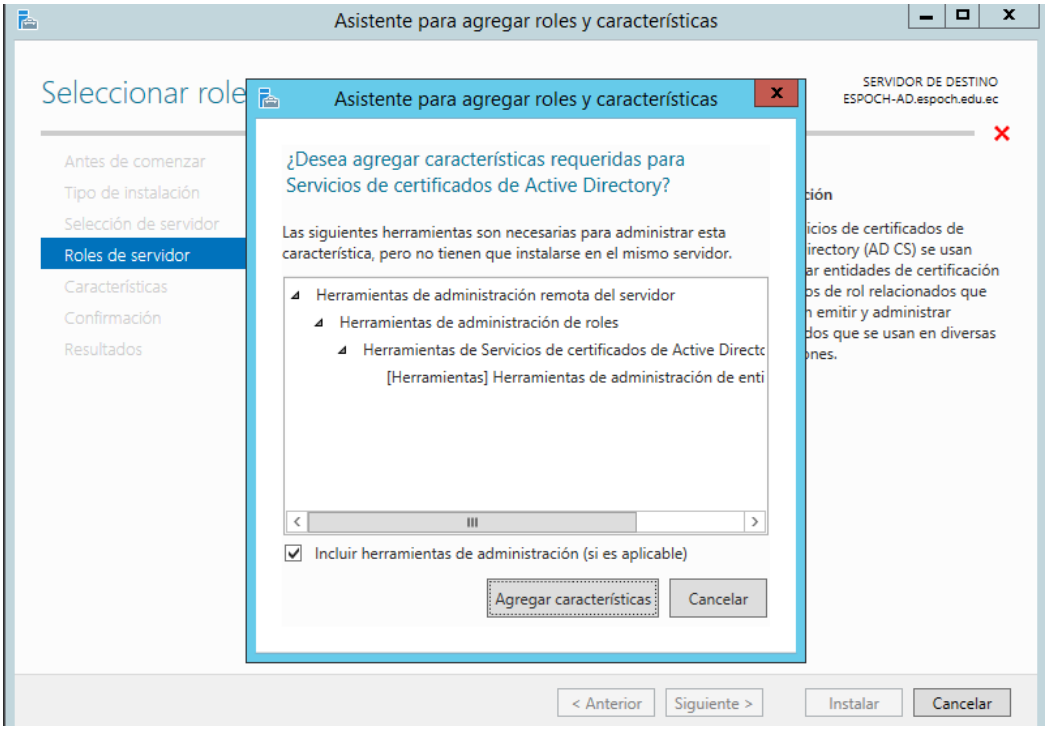


Figura 26-2: Agregación de características en roles de servidor.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2. Seleccionar la pestaña AD CS y pulsar el botón siguiente como se muestra en la figura 27-2.

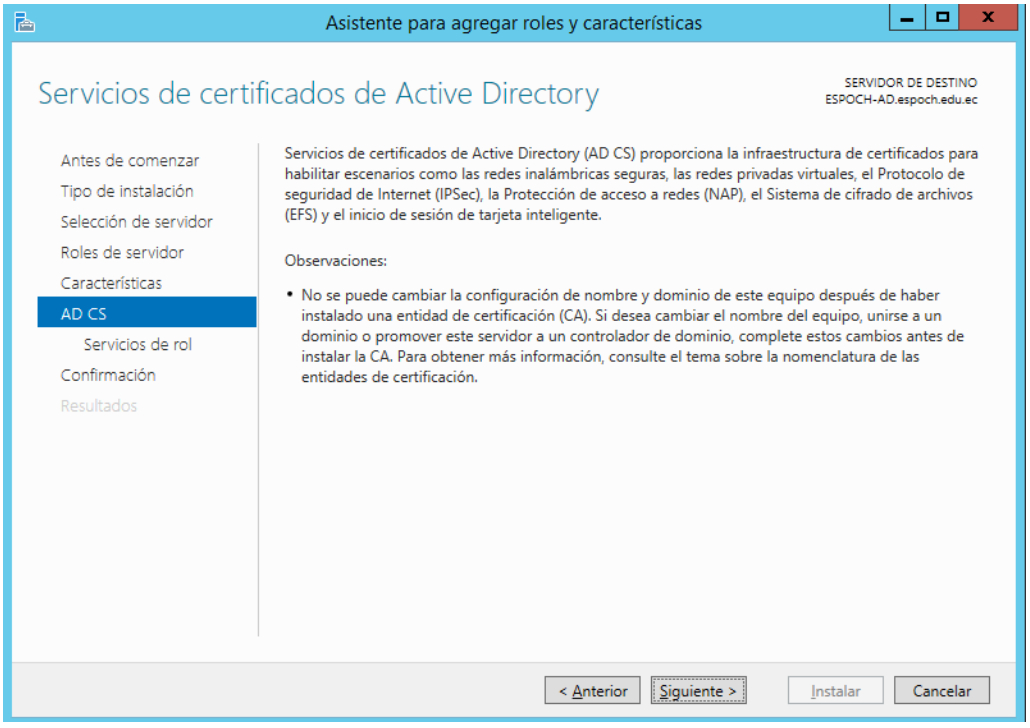


Figura 27-2: Selección de la opción AD CS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3. Seleccionar servicios de rol y marcar las casillas: Entidad de certificación e Inscripción web de entidad de certificación, luego presionar el botón siguiente como se muestra en la figura 28-2.

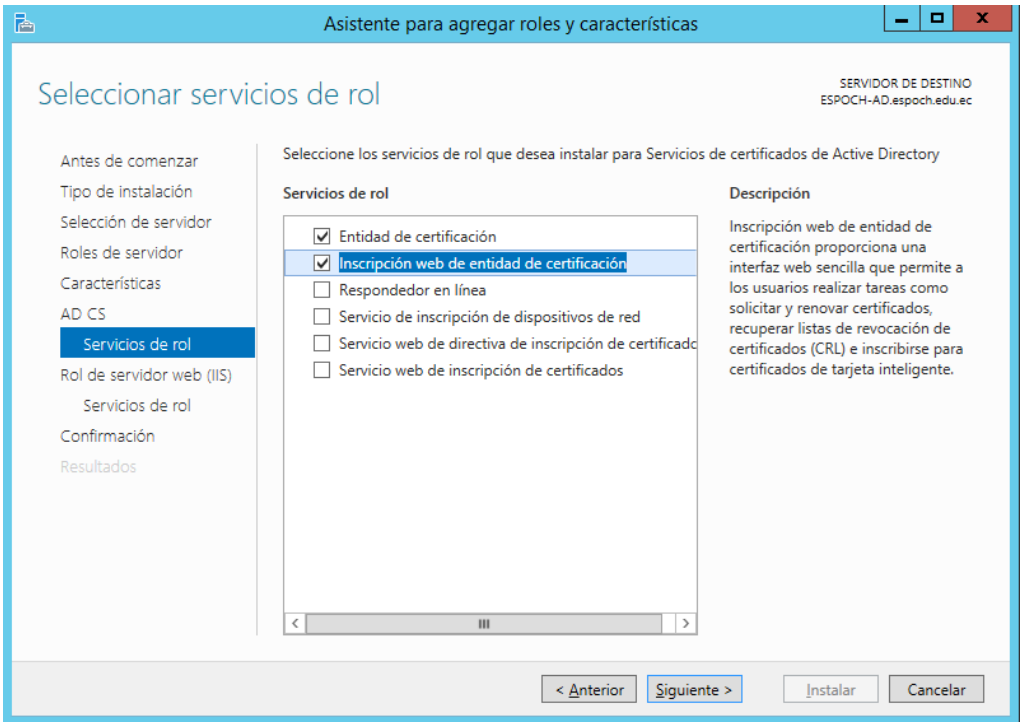


Figura 28-2: Selección de servicios de rol.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

4. Seleccionar la opción Rol de servidor web (IIS) para habilitarlo y luego clic en botón siguiente como se muestra en la figura 29-2.

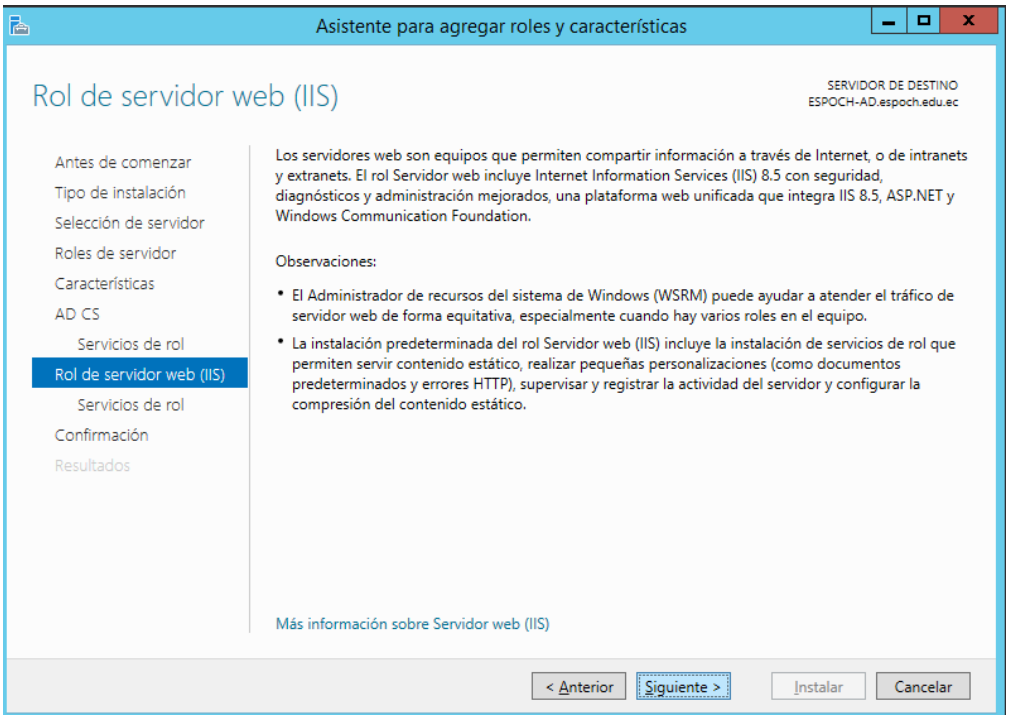


Figura 29-2: Configuración de IIS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

5. En la pestaña Servicios de rol, seleccionar los parámetros que se muestran en la figura 30-2 y luego clic en la opción siguiente.

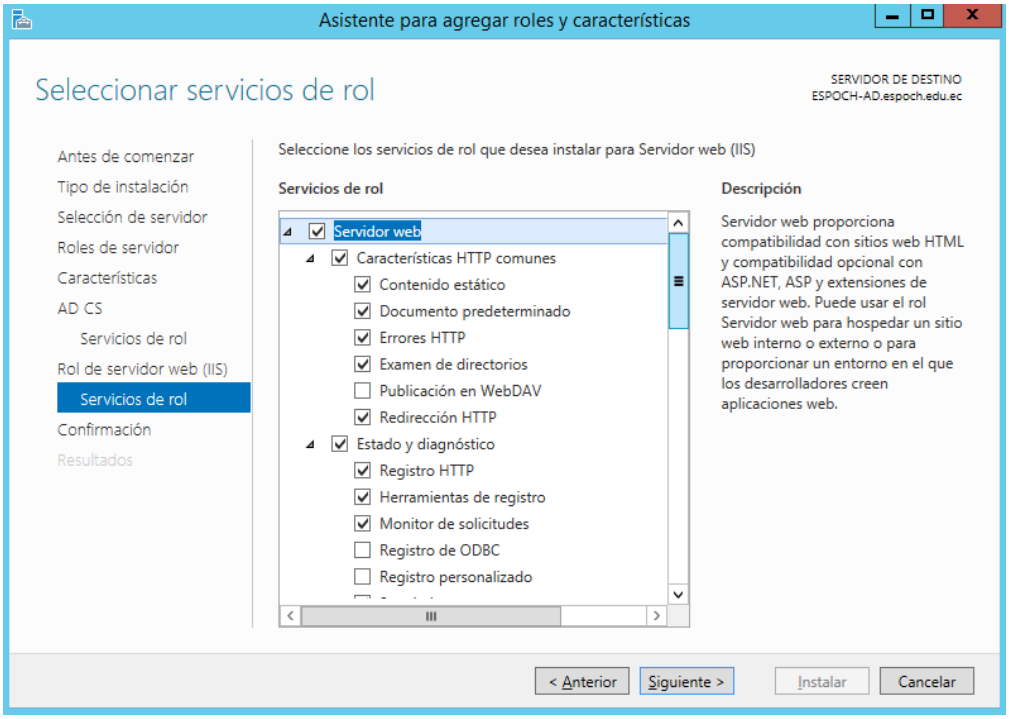


Figura 30-2: Parámetros del servidor web.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

6. En la siguiente pantalla presionar el botón instalar para confirmar los parámetros anteriores como se muestra en la figura 31-2.

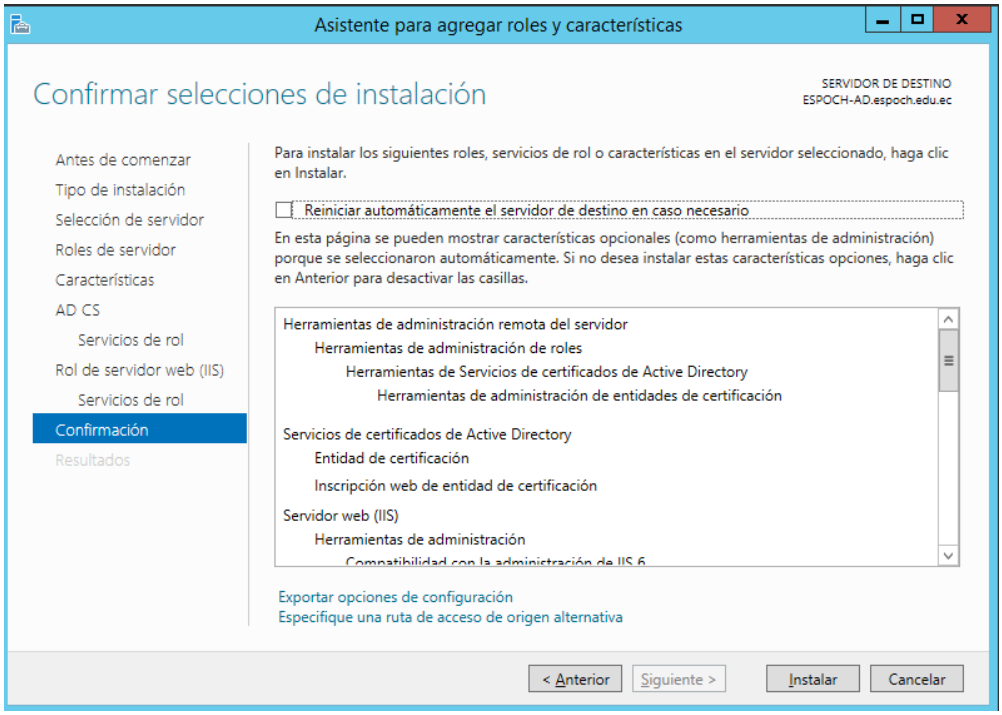


Figura 31-2: Confirmación de instalación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

7. Una vez terminada la instalación se inicia el asistente de configuración desde el administrador del servidor. Se revisa que las credenciales sean las correctas como se muestra en la figura 32-2.

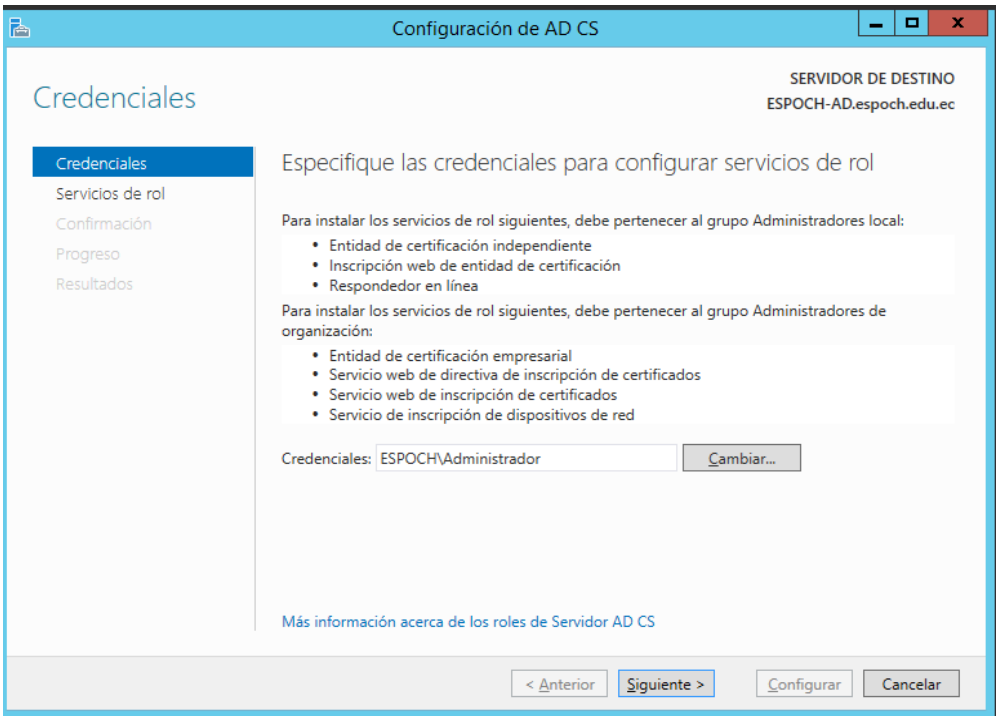


Figura 32-2: Credenciales de AD CS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

8. En la pestaña servicios de rol, se marcan las casillas que se muestran en la figura 33-2.

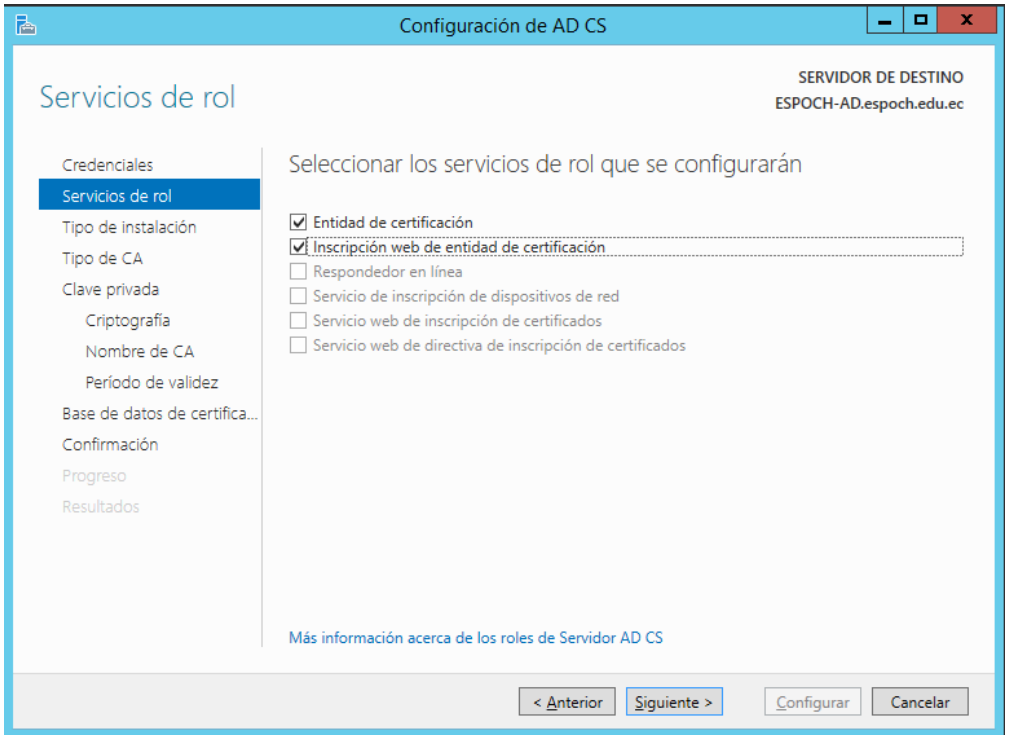


Figura 33-2: Parámetros de configuración en servicios de rol.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

9. En la ventana Tipo de instalación, se selecciona la opción CA empresarial, como se muestra en la figura 34-2.

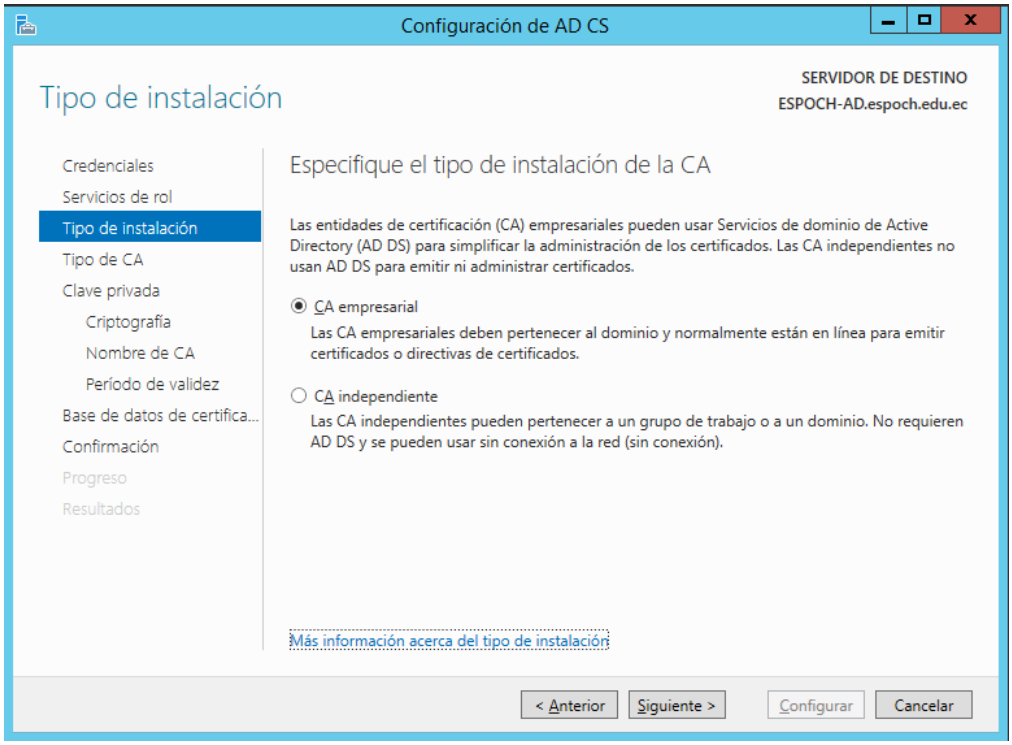


Figura 34-2: Tipo de instalación de CA.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

10. En la pestaña Tipo de CA, se selecciona CA raíz como se muestra en la figura

35-2 y luego se pulsa el botón siguiente.

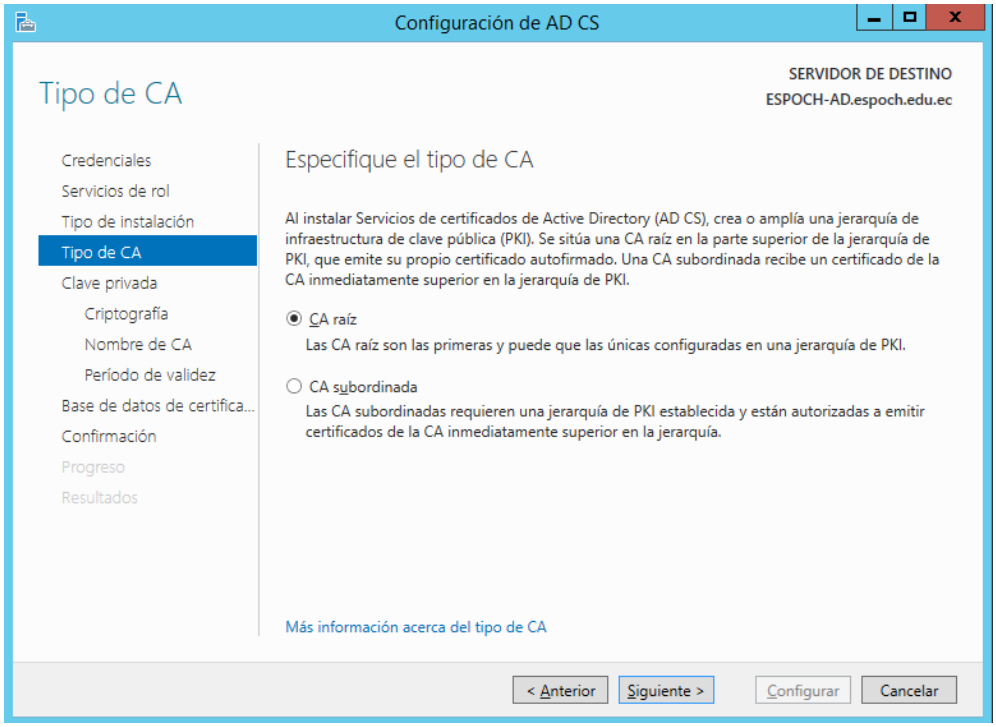


Figura 35-2: Tipo de CA.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

11. En la pantalla criptografía para la CA, se mantiene los parámetros por defecto como se muestra en la figura 36-2 y luego clic en siguiente.

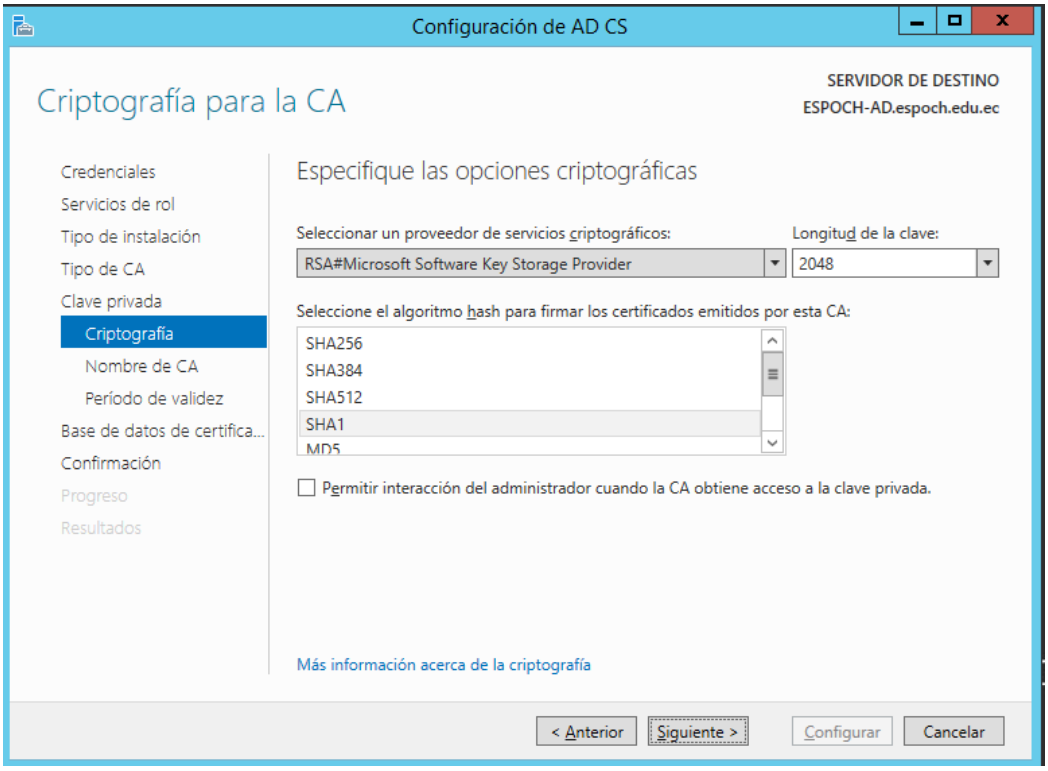


Figura 36-2: Criptografía para la CA.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

En la pantalla Nombre de CA, se escribe el nombre de la CA. Ejemplo: espoch-ESPOCH-AD-CA, cabe indicar que al final del nombre debe estar CA como se muestra en la figura 37-2.

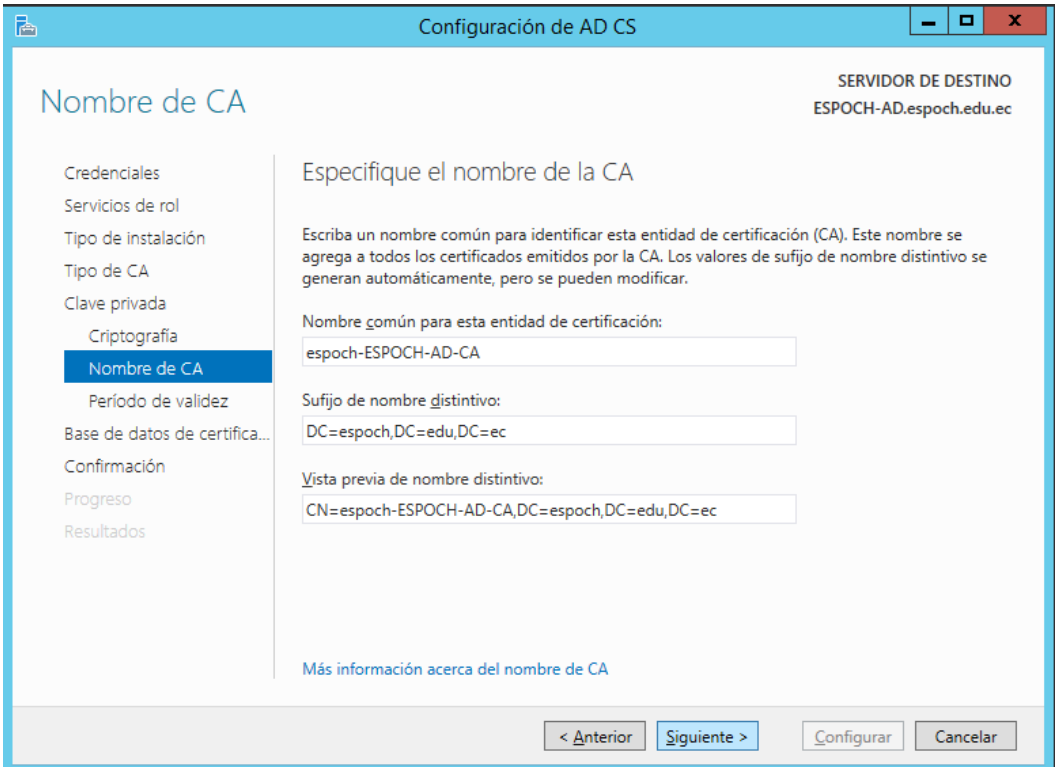


Figura 37-2: Nombre de CA.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

12. En la pantalla período de validez, se selecciona el tiempo de validez de CA como se muestra en la figura 38-2, para el caso 5 años.

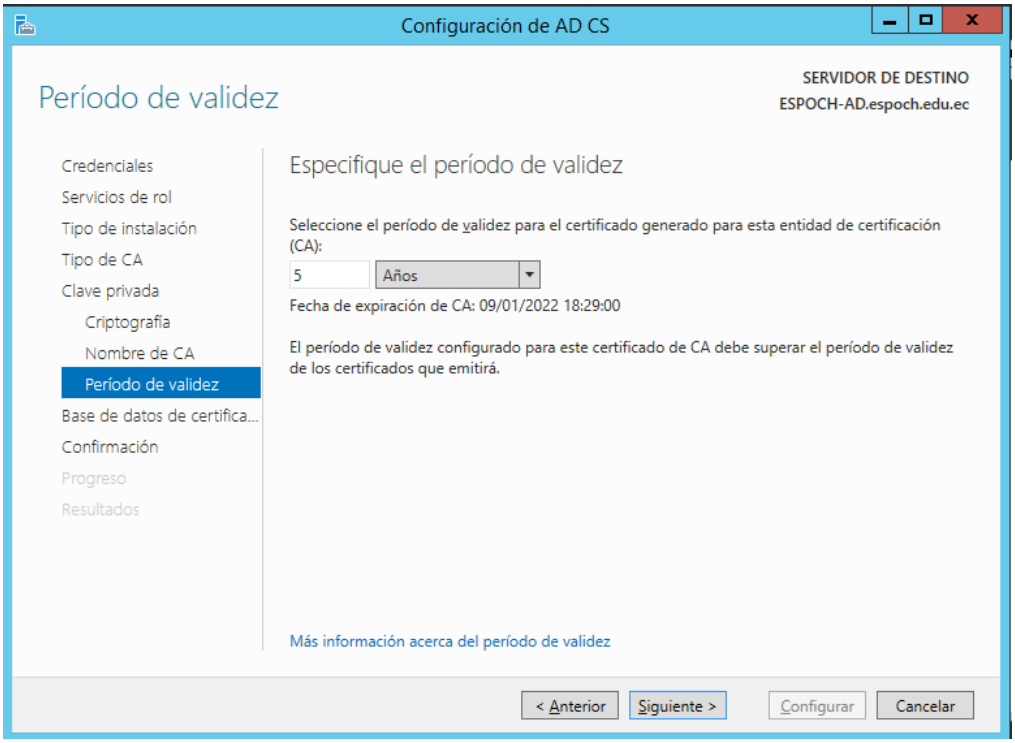


Figura 38-2: Periodo de validez de la CA.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

13. En la ventana confirmación, se presiona el botón configurar para que se apliquen las características como se muestra en la figura 39-2.

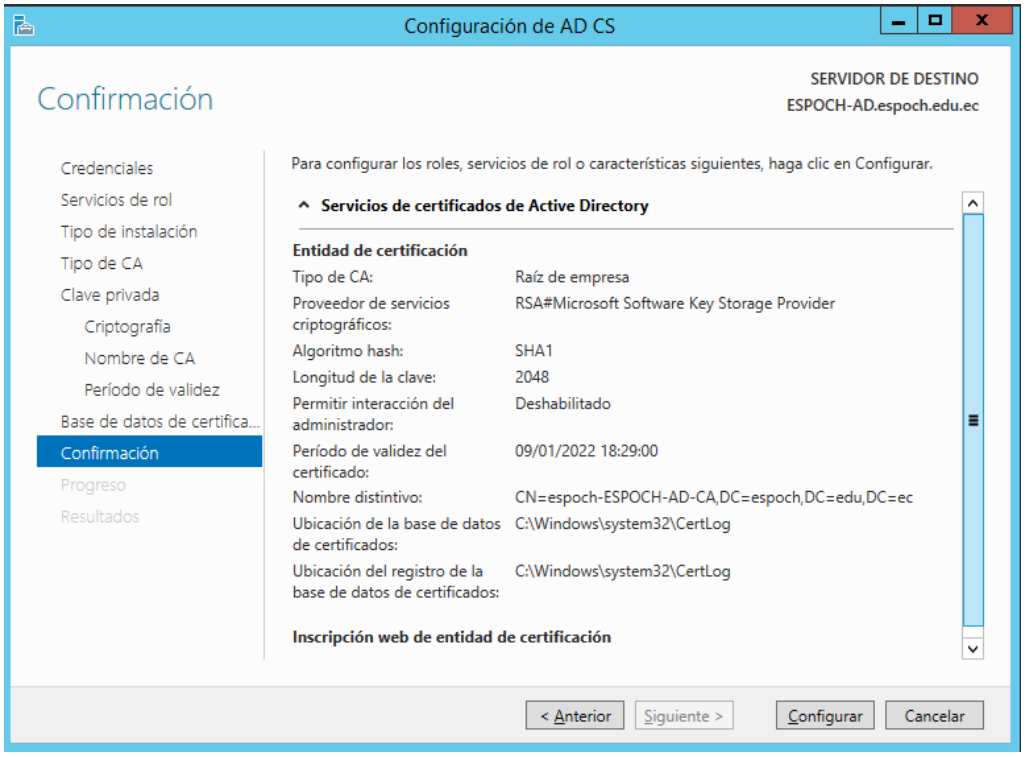


Figura 39-2: Confirmación de certificados.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

14. En la pantalla resultados, se verifica que las configuraciones anteriores sean las correctas y luego se procede a cerrar la ventana como se muestra en la figura 40-2.

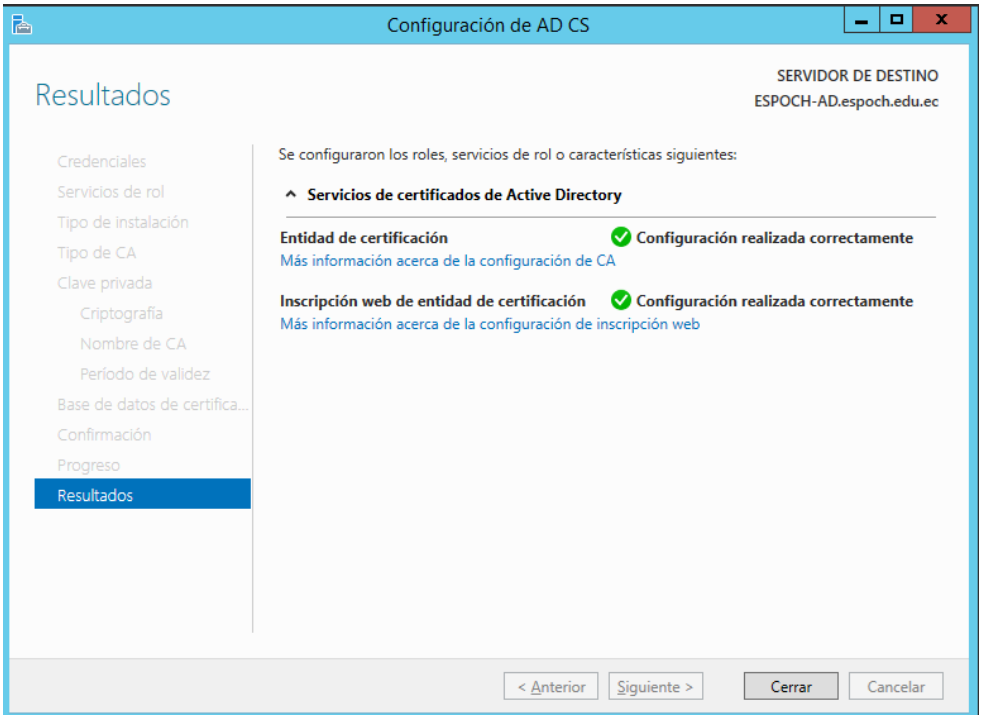


Figura 40-2: Resultados de configuración/instalación de AD CS.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Pasos para la configuración final del AD:

Crear en Active Directory un usuario específico para la unión entre ISE y el AD.

La clave del usuario debe tener los parámetros necesarios como: letras mayúsculas, minúsculas, caracteres especiales y números, mínimo 8 caracteres.

Las opciones para esta cuenta, deben ser que el usuario no pueda cambiar la contraseña y que la misma no expire.

Para iniciar la configuración básica de ISE se deben seguir los siguientes pasos:

a) Cisco ISE puede ser instalado en un dispositivo físico o en modo virtual VMware, para el caso en mención será de forma virtualizada para lo cual se necesita ciertos requerimientos que se los puede encontrar en el enlace siguiente http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html.

b) Instalar la imagen de Cisco ISE, en el menú de opciones de boot presionar la opción 1 o 2 dependiendo de la interfaz a utilizar, como se observa en la imagen 41-2.

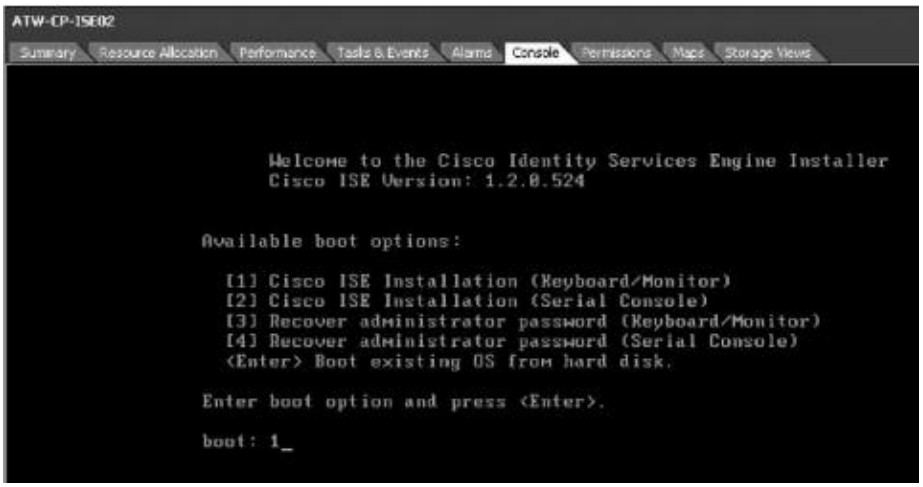


Figura 41-2: Menú de opciones de boot de ISE
Fuente: (Woland, A; Heary, J, 2013, p.96)

c) Cuando el software ha sido instalado en el prompt, se ingresa el comando setup; en donde aparece los parámetros básicos de configuración de ISE como: configuración de IP, default Gateway, servidor DNS y servidor NTP y la activación de un usuario con su clave correspondiente.

d) Finalmente las configuraciones se aplicarán y el servidor iniciara los servicios

necesarios para levantar ISE. Al momento de ingresar por el navegador web se comprueba el correcto funcionamiento.

Se debe tener en cuenta al usar un AD los siguientes requerimientos:

- ISE y AD deben estar sincronizados en tiempo usando NTP.
- El nombre del servidor ISE debe tener una longitud menor a 15 caracteres.
- Si existe un firewall entre ISE y AD debe permitir los siguientes puertos: UDP\389, TCP\445, TCP\88, TCP\3268, TCP\3269, TCP\464, UDP\123, TCP\389, y TCP\636.
- El nombre del dominio del servidor debe estar configurado y trabajando.

Para continuar con la instalación se sigue el siguiente proceso

a) Se ingresa el nombre del host, la dirección IP, máscara de red y el router por defecto la red.

Enter hostname[]: **ISE**
Enter IP address[]: **172.31.204.61**
Enter IP default netmask[]: **255.255.255.0**
Enter IP default gateway[]: **172.32.204.1**

b) Se ingresa la información de DNS

Enter default DNS domain[]: **espoch.edu.ec**
Enter primary nameserver[]: **172.17.102.39**
Add/Edit another nameserver? Y/N : **n**

c) Se configura la cuenta de administrador, para el acceso tanto al CLI como al GUI

Enter username[admin]: **admin**
Enter password: **[password]**
Enter password again: **[password]**

Proceso 2. Configurar la lista de confianza de certificados

ISE usa Infraestructura de clave pública (PKI) para asegurar la comunicación entre ellos, en este desarrollo se usan los certificados locales, pero al tener varios nodos o un AD es necesario crear

una relación de confianza entre ellos, para lo cual se extrae el certificado del nodo o de AD y se lo ingresa como certificado de confianza en la infraestructura.

a) En el buscador se ingresa al segundo nodo.
b) En **Administration > System** se selecciona **Certificates**
c) En la ventana de certificados locales se selecciona con un visto el certificado, y dar clic en **Export.**
d) Cuando guarde el archivo asegúrese de guardar con un nombre familiar al nodo del cual lo extrajo y la ubicación exacta del mismo, porque será importado en el nodo primario
e) En el buscador ingrese a su nodo primario.
f) En **Administration > System** se selecciona **Certificates.**
g) En el panel operaciones de certificado en la izquierda, damos clic en **Certificate Store** y luego clic en **Import.**
h) Siguiente a esto en el campo se selecciona **Certificate File, Browse** y localice el certificado extraído del segundo el cual debe tener un formato .pem, y luego clic en **Submit.**

Proceso 3. Configuraciones Generales de nodo

Se puede configurar ISE de manera centralizada o en varios nodos en los cuales define el rol que lleva en la implementación, ya sea esta como nodo primario o secundario de la misma manera necesaria la configuración de los perfiles y la manera en la que ISE recolecta información para la autenticación.

a) Ingresar al GUI de ISE.
b) Se ubica en **Administration>System>Deployment** en donde se encuentra la información y el rol que este nodo desempeña.
c) En este punto se puede ver que existe la posibilidad de cambiar las condiciones por defecto del nodo las cuales son las **Personas**, **Rol, Grupo de nodo** correspondientes, la cual tener un único nodo principal y se deja las configuraciones por defecto, como se observa en la figura 42-2.

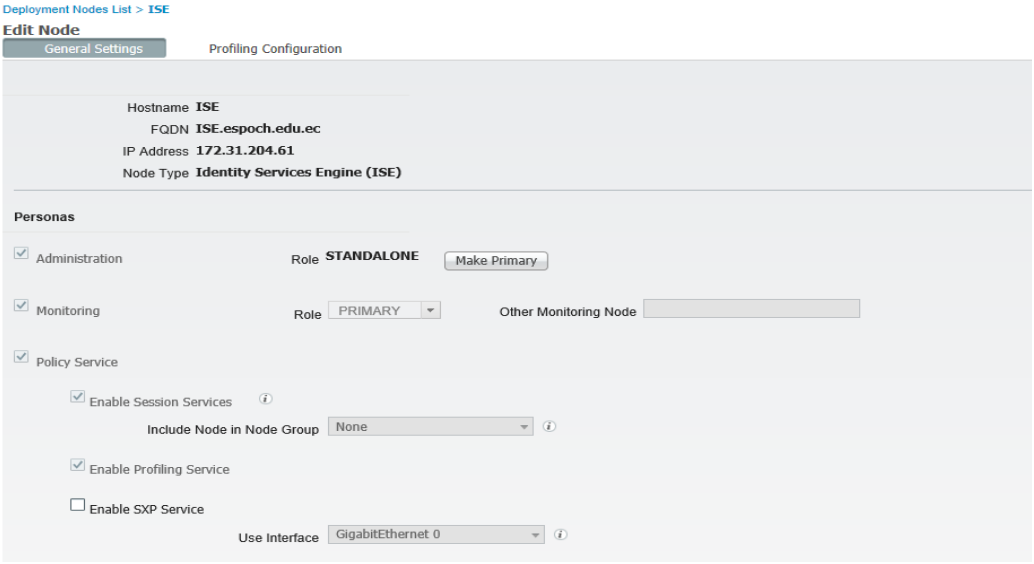


Figura 42-2: Nodo principal
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

d) Finalmente en **Profiling Configuration** se señala los perfiles que se necesitan teniendo en cuenta que necesariamente debe estar señalado el perfil de RADIUS y dar clic en **Save** una vez hecho los cambios, como se observa en la figura 43-2.

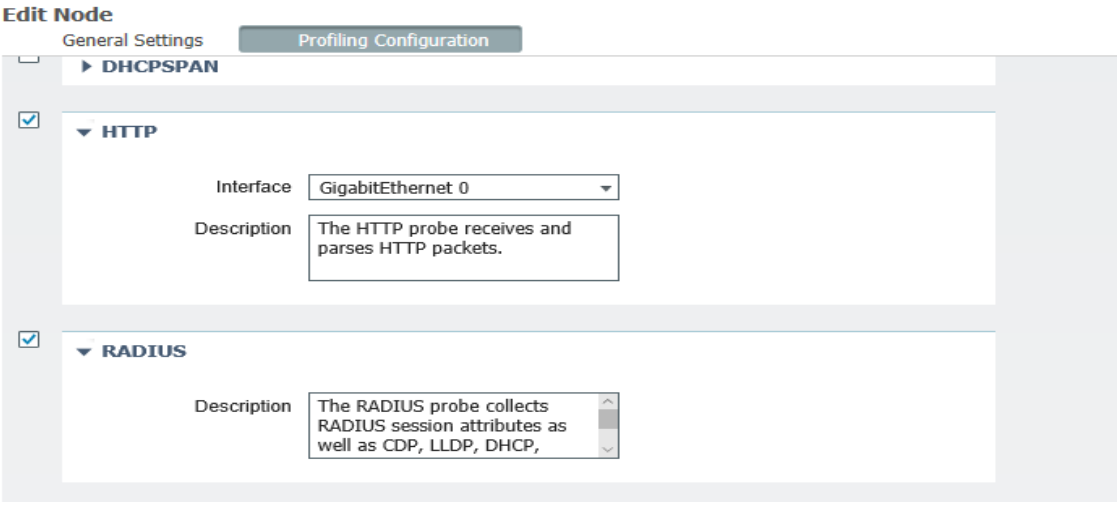


Figura 43-2: Perfiles
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Proceso 4. Instalar las licencias de Cisco ISE

Cisco ISE viene con licencias demo de 90 días de duración las cuales viene con los paquetes base y avanzados, después de los 90 días, se necesita obtener una licencia de Cisco la cual será instalada únicamente en su nodo primario.

a) En **Administration>System>Licensing** en donde se encontrara un solo y único nodo que será el primario, y es cual necesita la licencia.

b) Se da clic en importar licencia y nos dirige a la siguiente pantalla, como se observa en la figura 44-2.

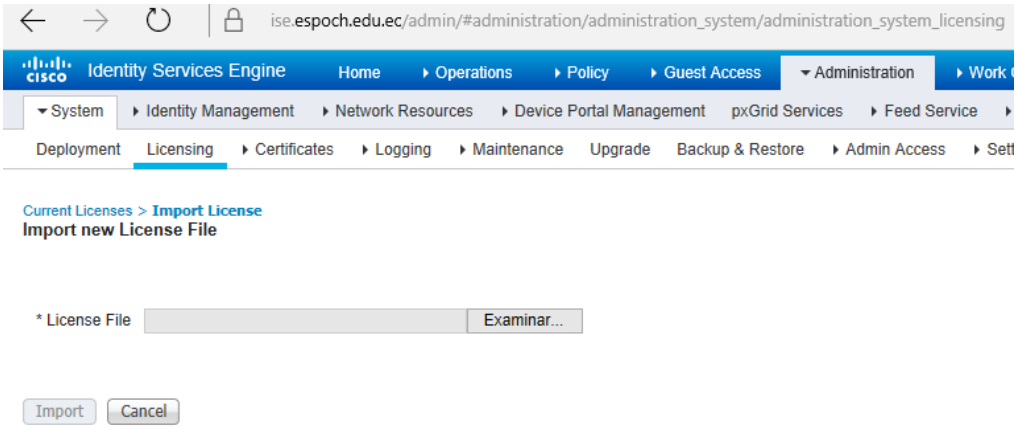


Figura 44-2: Nodo primario
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

c) Se da clic en examinar y se importa el archivo de la licencia y si se tiene varias licencias solo se repite el proceso.

Proceso 5. Configuración de ISE para usar Active Directory

El objetivo de la unión de ISE con AD como se observa en la figura 45-2 consiste en tener un repositorio externo del cual se extraerán los grupos de usuarios, y el encargado de enviar los certificados para la autenticación, a continuación se enumeraran los pasos a seguir para la integración de ISE con AD:

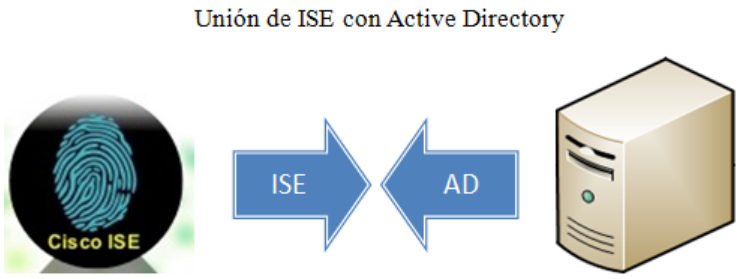


Figura 45-2: Unión ISE con Active Directory
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

a) Se dirige a **Administration** y entonces en el menú de Identity Management se escoge **External Identity Sources.**

b) En el panel izquierdo, clic en Active Directory.

c) En la pestaña de conexión, ingrese el dominio de AD (por ejemplo espoch.edu.ec) y el nombre del servidor (por ejemplo AD1) entonces de clic en **Save** para guardar las configuraciones.

d) Verificar esta conexión seleccionando la casilla que esta junto al nodo y de clic en **Test User**, ingrese las credenciales de usuario de dominio y clic en **close**, como se observa en la figura 46-2.

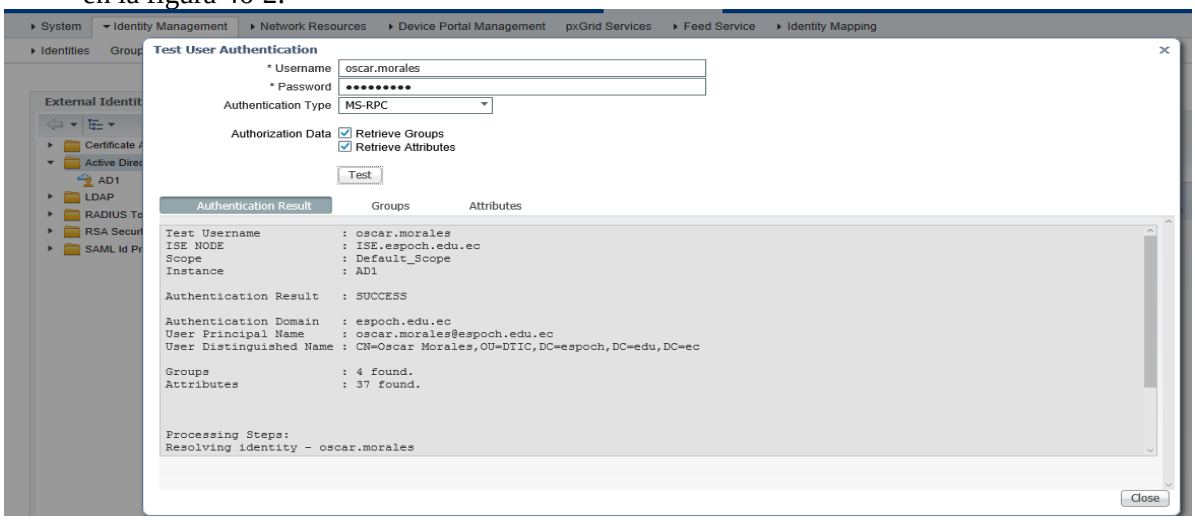


Figura 46-2: Conexión con AD
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

e) Seleccione la pestaña a lado del nodo y de clic en **Join**.

f) Ingrese las credenciales para de una cuenta de administrador de dominio. Ahora Cisco ISE se ha unido al domino. Después de esto selecciona los grupos de usuarios para usarlos en la autenticación

g) Clic en la pestaña de **Groups**, clic en **Add** y entonces clic en **Select Groups from Directory.**

h) Busque los grupos que desea añadir a la lista por defecto y se muestra todos los grupos existentes, clic en **Retrieve Groups** y adquiera la lista de todos los grupos en su dominio.

i) Seleccione los grupos que quiere usar en la autenticación, y entonces de clic en **OK** y guarde las configuraciones, como se observa en la figura 47-2.

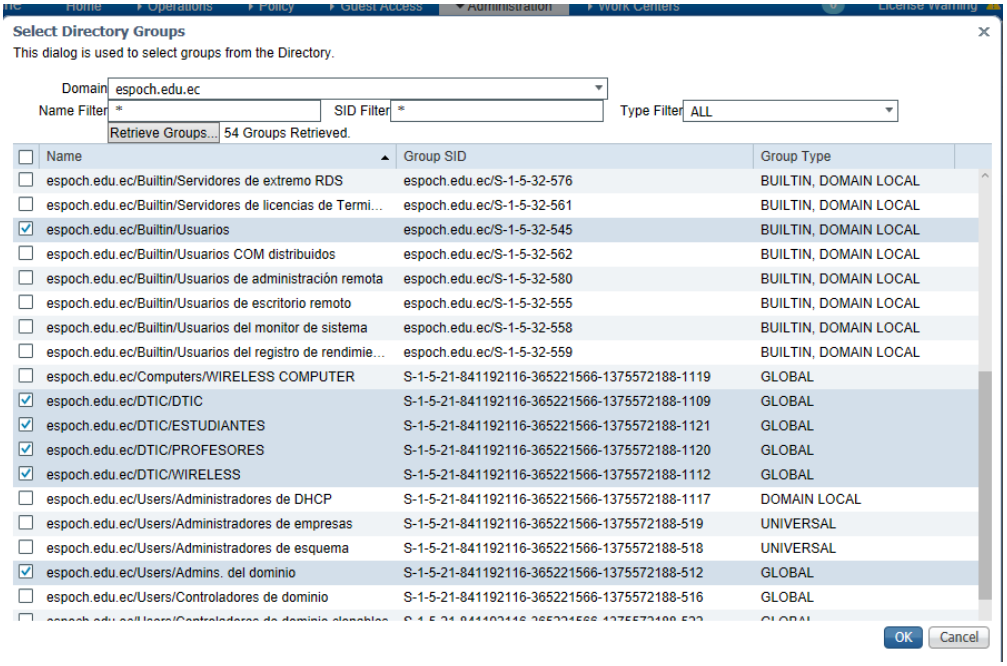


Figura 47-2: Grupos añadidos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Proceso 6. Unión y configuración de Wireless Lan Controller (WLC) con Cisco ISE

El objetivo de la unión de ISE con la WLC como se observa en la figura 48-2 es para que ISE actúe como servidor Radius y que brinde la autenticación y políticas de autorización en el cual la controladora se encarga de difundir el SSID, para que se realice la integración de ISE con WLC se deben seguir los siguientes pasos:

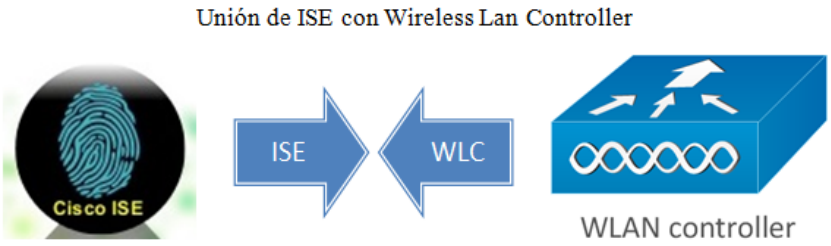


Figura 48-2: Unión ISE con Wireless Lan Controller
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Este proceso es para todas las WLC en la arquitectura con excepción de standalone guest WLC, si se tiene implementada una.

a) Se navega en la consola WLC en el buscador, y en menú principal se dirige a **Security**
b) En el panel izquierdo, debajo de la sección **RADIUS**, clic en **Authentication**.

c) Dar clic en **New** y se añade un nuevo servidor en donde se ingresa la IP de servidor 172.31.204.61, también se ingresa la clave de RADIUS shared secret.

d) Se debe tener en cuenta los parámetros configurados como se observa en la figura 49-2.

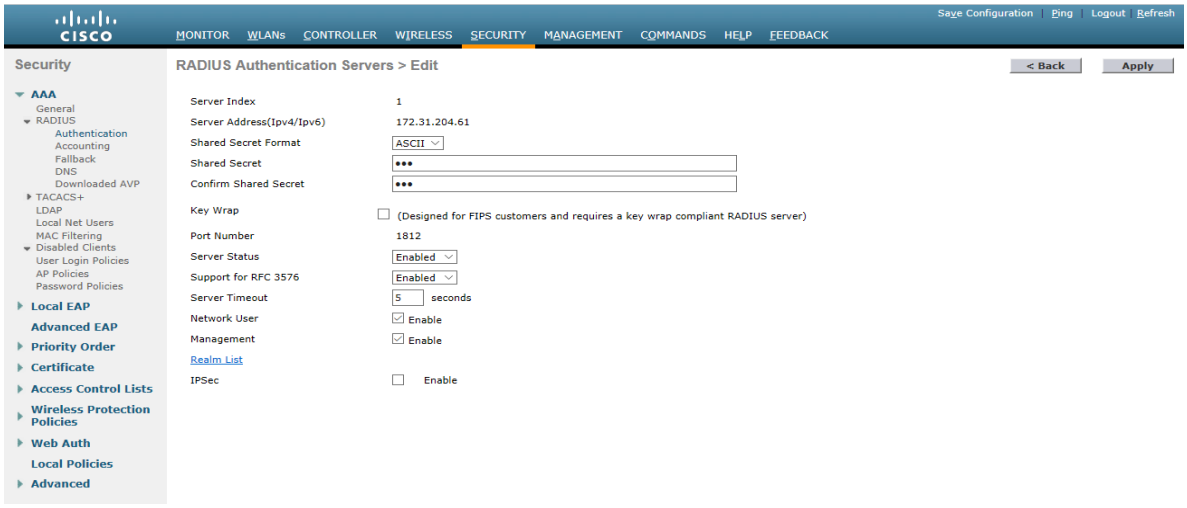


Figura 49-2: Controladora
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

e) Después de añadir Cisco ISE como servidor Radius, se debe desactivar el servidor Radius que se tenga en uso.

f) En el mismo menú de seguridad, en la parte izquierda del menú clic en **Accounting.**

g) Se añade un nuevo servidor y se ingresa la IP del servidor con su respectiva clave de shared secret y clic en **Apply**, como se observa en la figura 50-2.

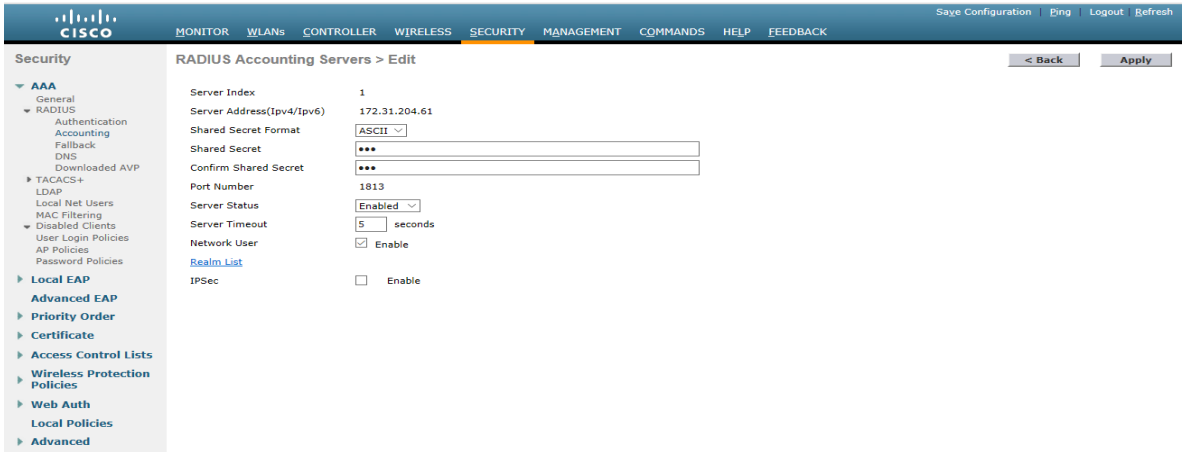


Figura 50-2: Servidor Radius
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

h) En la creación del SSID se debe tener en cuenta parámetros importantes como configurar la seguridad que se vaya a necesitar, como se observa en la figura 51-2

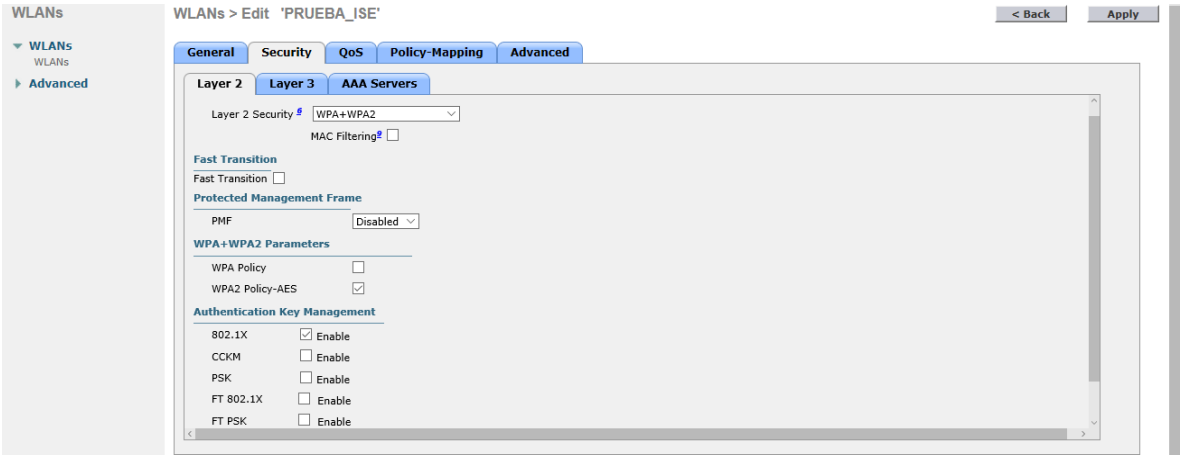


Figura 51-2: Creación de SSID
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

i) Se Configura los servidores AAA en donde se declara la IP de ISE, como se observa en la figura 52-2.

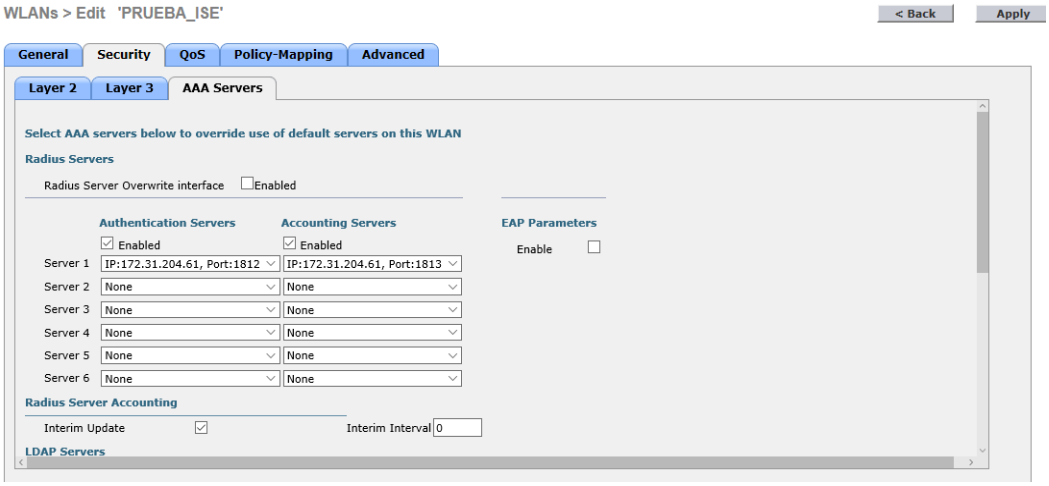


Figura 52-2: Servidores AAA
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

j) En Advanced hay que tener en cuenta que deben estar señaladas las pestañas de los recuadros siguientes, como se observa en la figura 53-2.

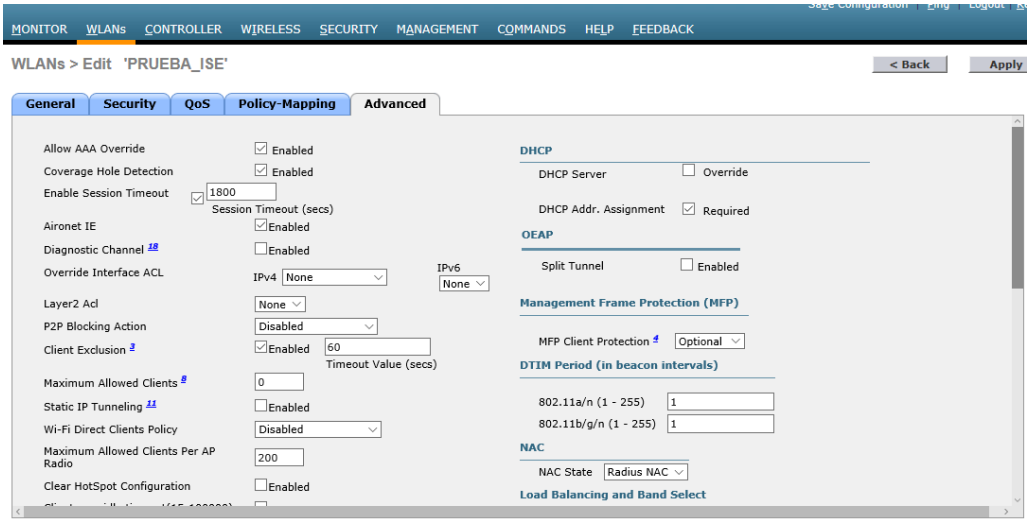


Figura 53-2: Señalamiento
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

k) En **SECURITY** en el panel izquierdo en la pestaña Access Control List se declara las ACLs según la necesidad que se tenga ya sean en modo local o modo Flexconnect.

l) En los Grupos de Flexconnect dirigirse a ACL Mapping en donde se declara la vlan y las ACLs para poder realizar una asignación de las mismas, como se observa en la figura 54-2.

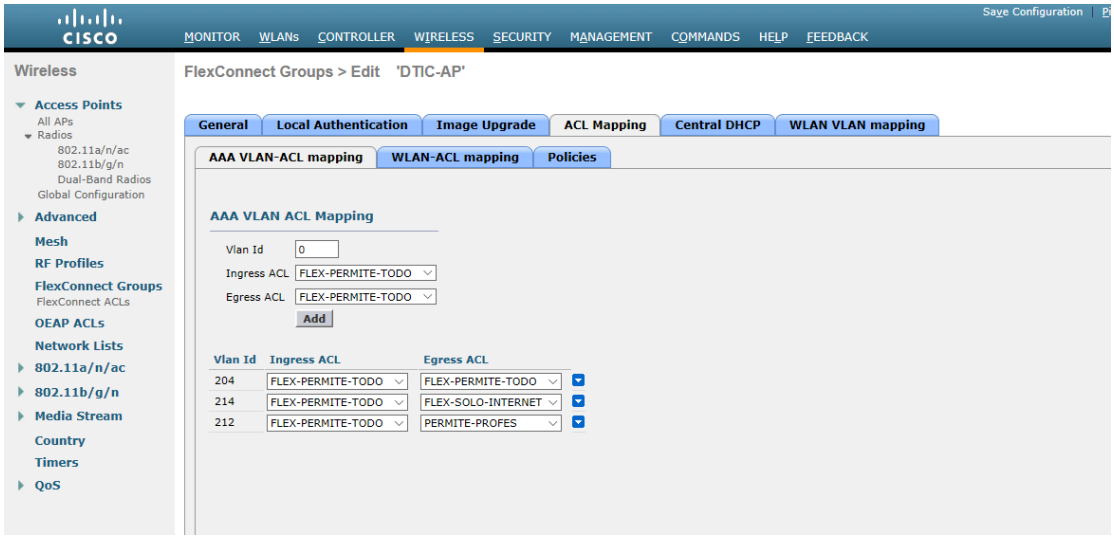


Figura 54-2: Declaración de ACLs
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Proceso 7. Configuración de Cisco ISE para una red inalámbrica y unión con WLC.

Para Autenticar los clientes inalámbricos, se necesita configurar la controladora inalámbrica que use ISE como servidor Radius para autenticación y autorización, el servidor actual de Radius

debe estar desactivado, de modo que en caso de existir algún problema con la unión con Cisco ISE, restaure el servidor que estuvo funcional.

a) En cisco ISE navegue **Policy >Policy Sets** en la regla por defecto en la sección de autenticación en la primera regla por defecto clic en la pestaña derecha y se crea una nueva regla.

b) Se cambia el nombre de la política en este caso INALAMBRICO_DOT1X, se dirige a **Select Existing Condition from library**, como se observa en la figura 55-2.

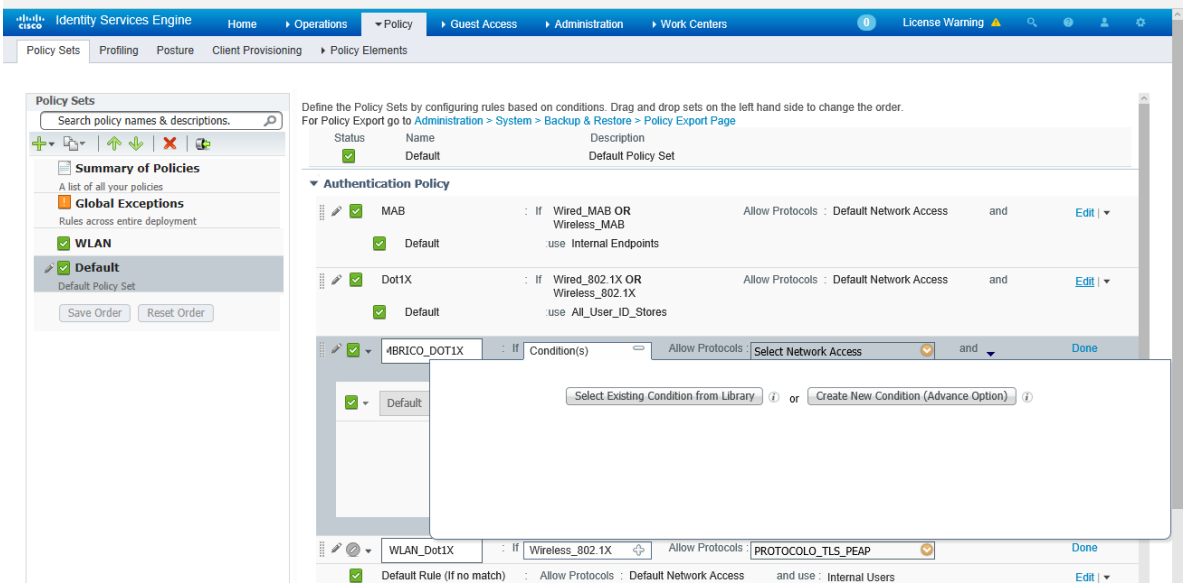


Figura 55-2: Reglas
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

c) Seleccione Wireless_802.1x, como se observa en la figura 56-2.

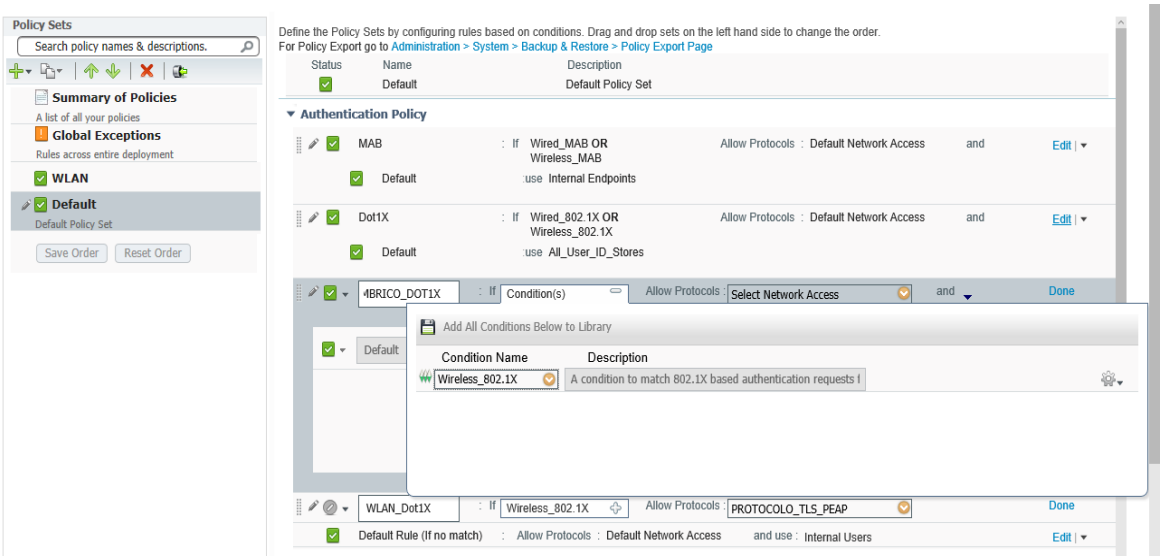


Figura 56-2: Selección Wireless
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

d) A continuación se define los protocolos que se desea permitir, como se observa en la figura 57-2.

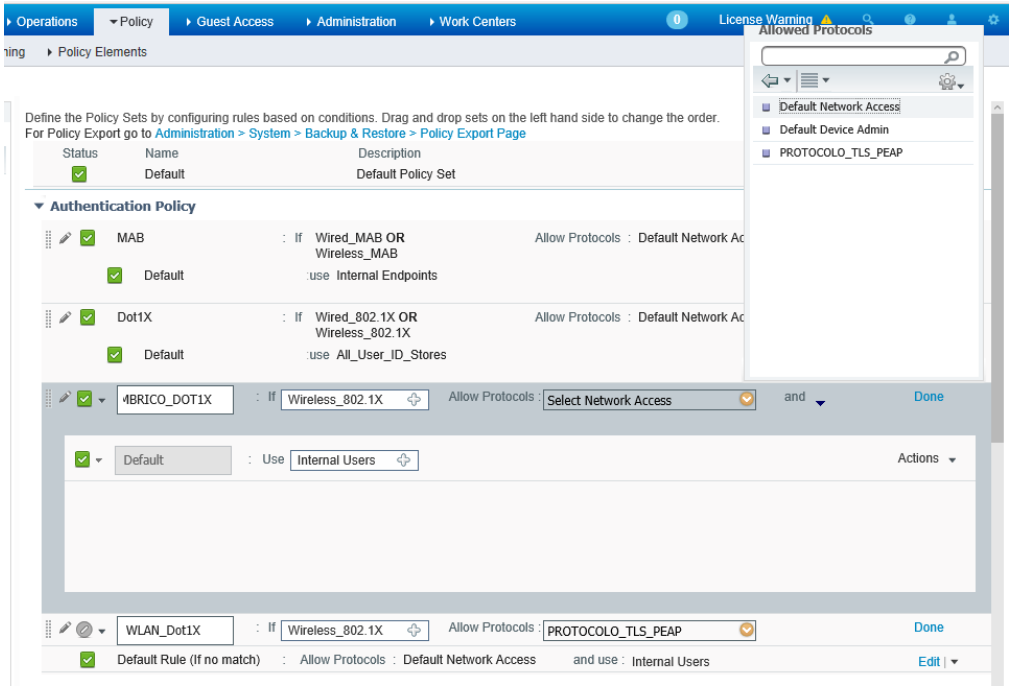


Figura 57-2: Protocolos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

e) Se procede a definir qué tipo de usuarios tendrían el acceso a la red, pueden ser los usuarios internos así como los del servidor de AD, como se observa en la figura 58-2.

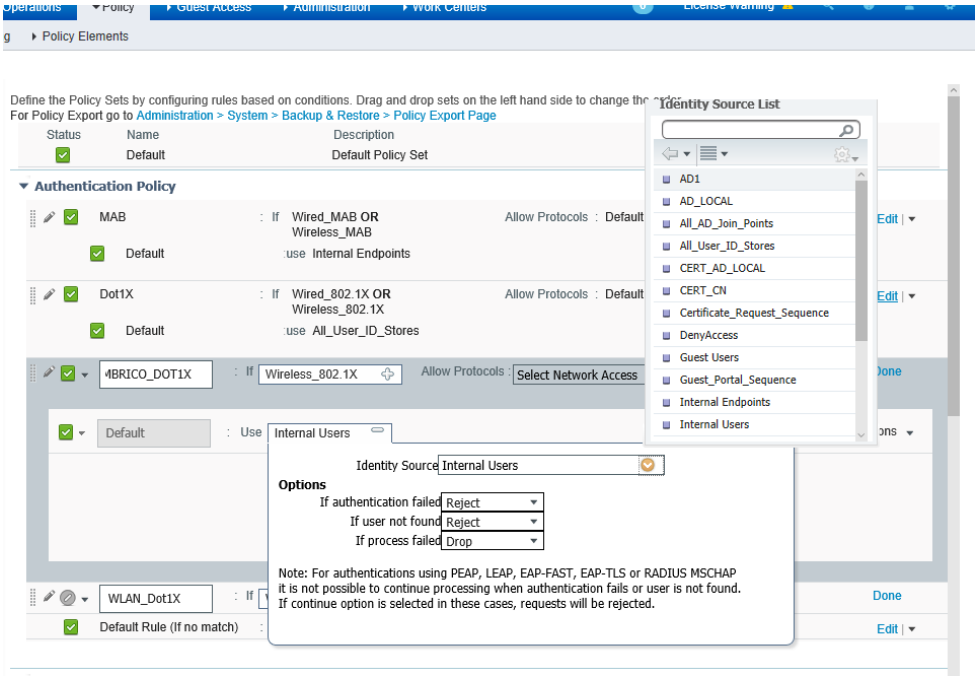


Figura 58-2: Tipos de usuarios
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

f) Se procede a la unión de WLC con ISE para eso se dirige a **Administration>Network Resources>Network devices**, en la pestaña superior clic en **Add.**

g) Se declara los valores requeridos como son la IP y la autenticación del protocolo Radius, como se observa en la figura 59-2.

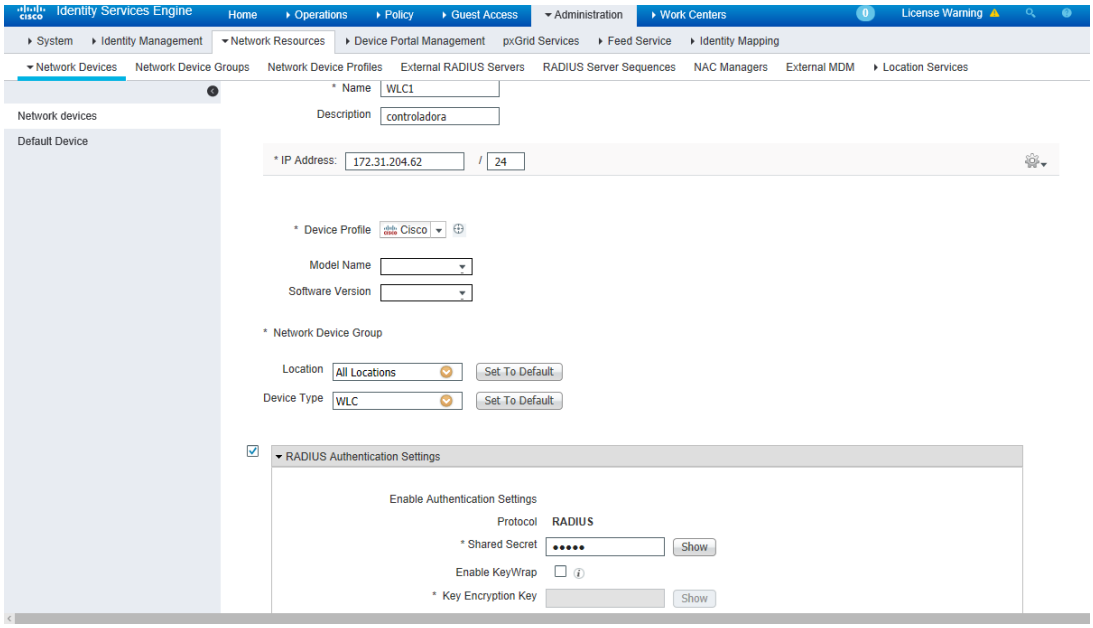


Figura 59-2: Unión WLC con ISE
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Proceso 8. Implementación de certificados digitales

Instalar el certificado de raíz en el AD para distribuirlo a los clientes para que los certificados del servidor del CA sean de confianza:

a) En la consola de CA iniciamos el servidor web y dirigirse a la página del certificado de autoridad. http://172.31.204.63/certsrv/certcarc.asp
b) Dar clic en descargar el certificado CA, cadena de certificados, o CRL.
c) Asegurarse que el certificado actual este señalado y la casilla de método de codificación DER este marcada.
d) Clic en descargar certificado CA, y guardar el archivo de certificado en AD, como se observa en la figura 60-2.

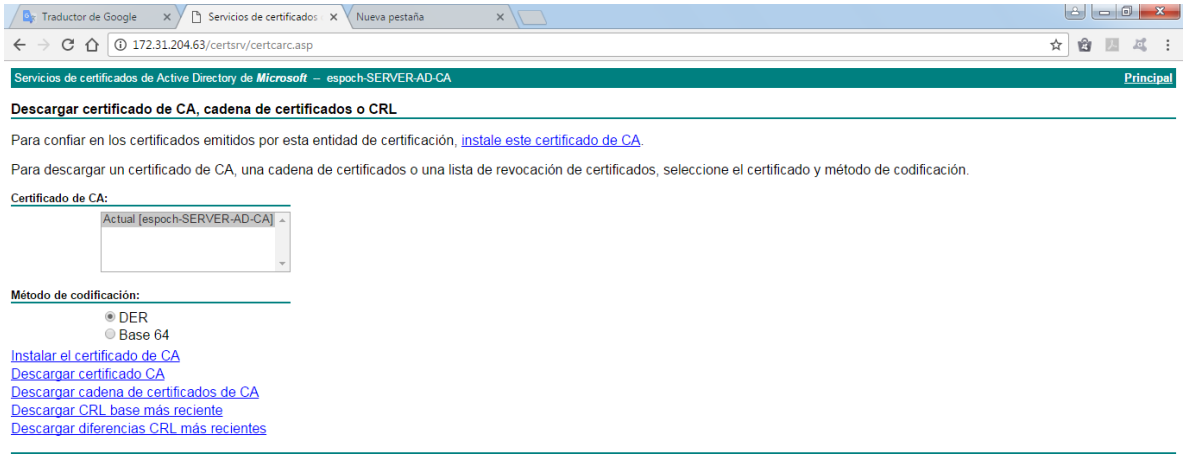


Figura 60-2: Descargar Certificados
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

e) En AD acceder a la consola, ingresamos con windows+R y teclear mmc, luego clic en Archivo> Agregar o quitar complemento, como se observa en la figura 61-2.

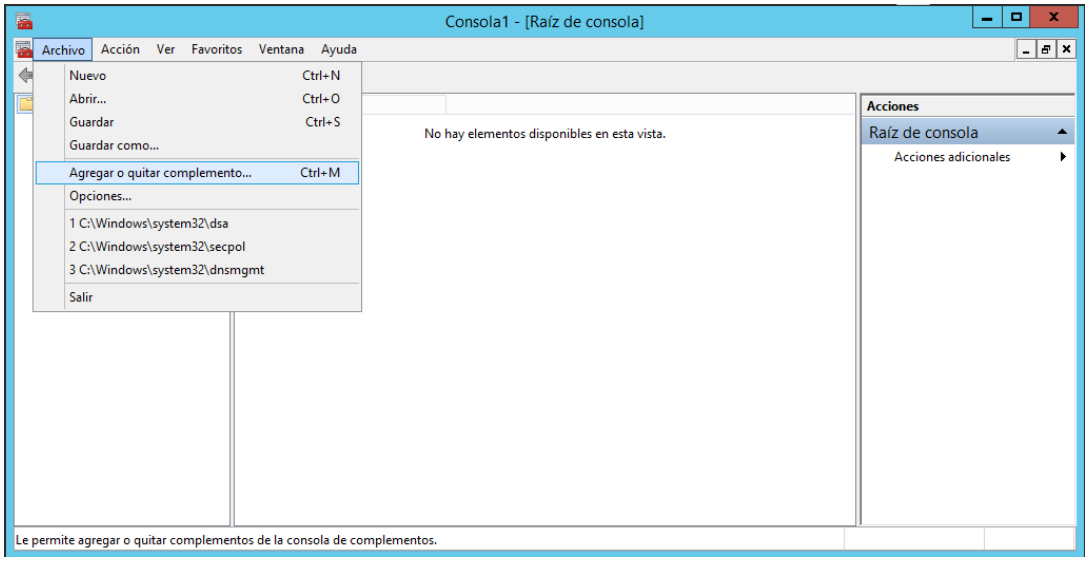


Figura 61-2: Complementos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

f) Seleccionar certificados>agregar > cuenta de equipo> siguiente y finalizar, como se observa en la figura 62-2.

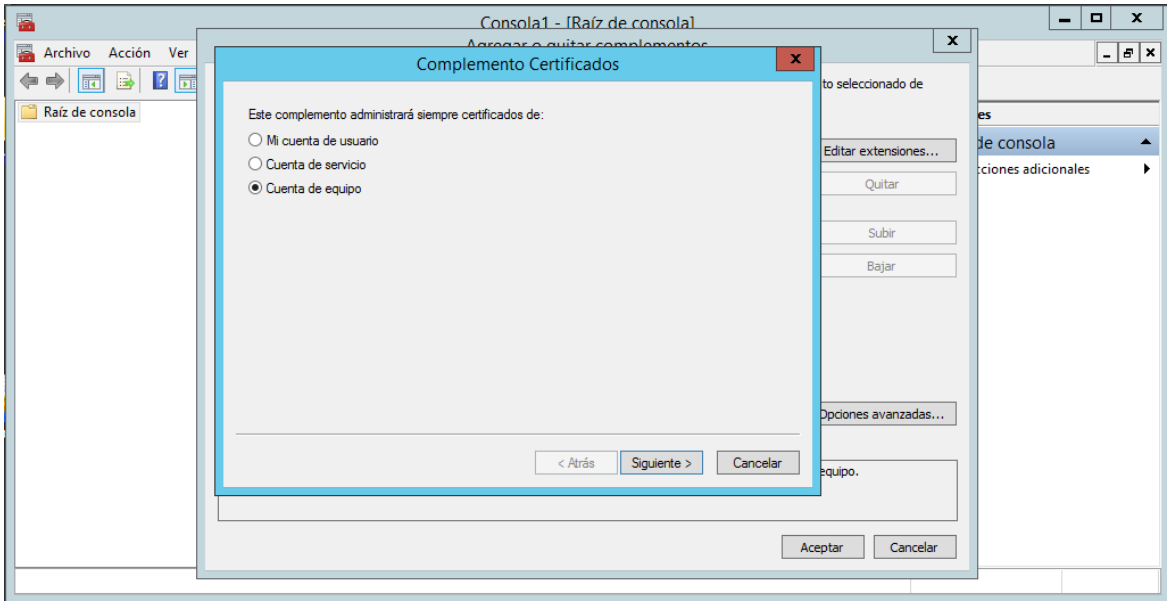


Figura 62-2: Cuenta de equipos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

g) Seleccionar equipo, clic en finalizar y por último aceptar, como se observa en la figura -63-2.

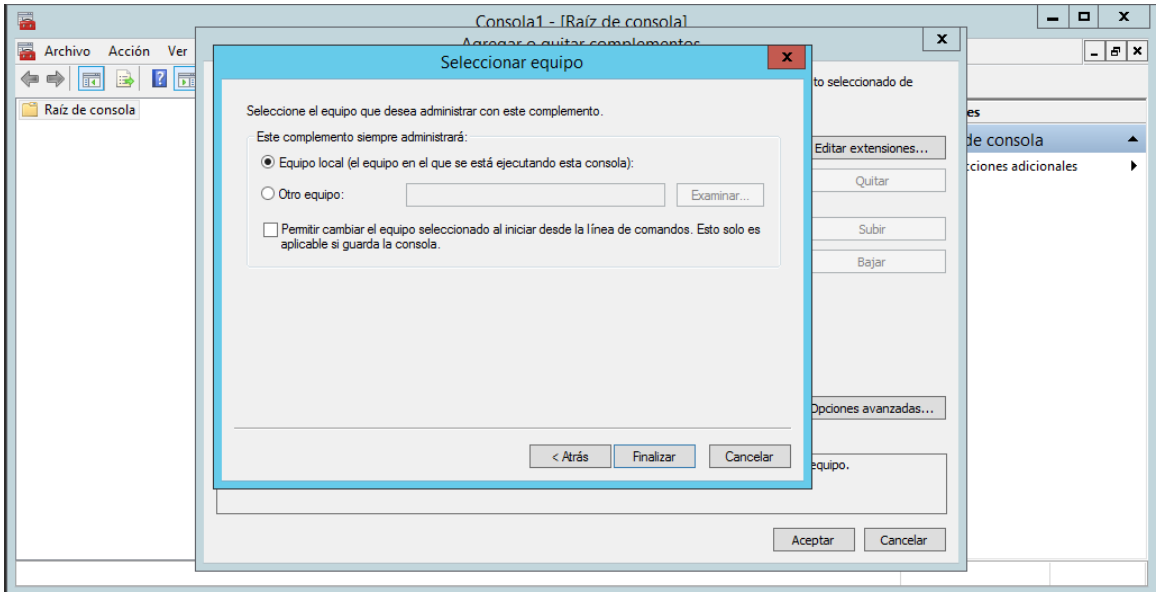


Figura 63-2: Selección de equipos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

h) Entrar a Certificados (equipo local)> Entidades de certificación raíz de confianza> Certificados> y seleccionar nuestro certificado, como se observa en la figura 64-2.

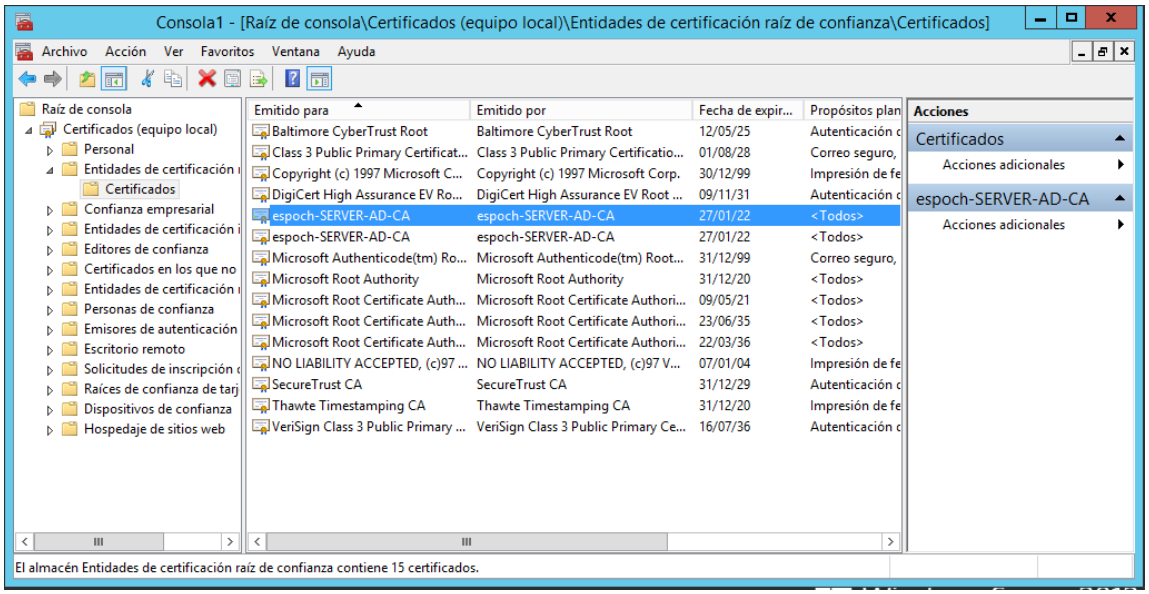


Figura 64-2: Selección de Certificados
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

i) Clic derecho sobre nuestro certificado> Todas las tareas> Exportar, como se observa en la figura 65-2.

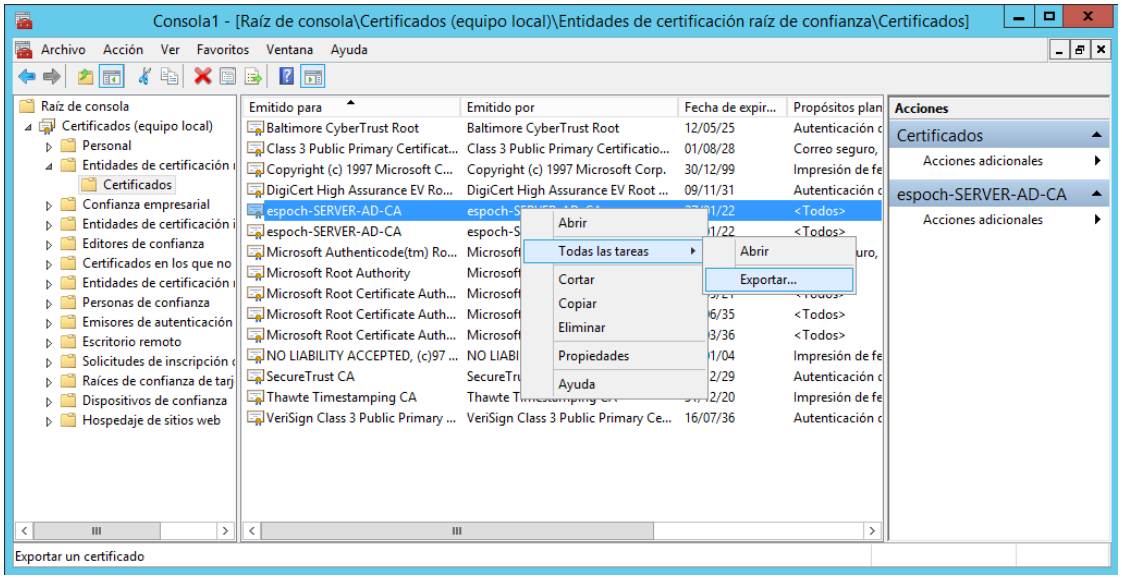


Figura 65-2: Exportar Certificado
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

j) Dar clic en siguiente y seleccionar la segunda opción y otra vez siguiente, como se observa en la figura 66-2.

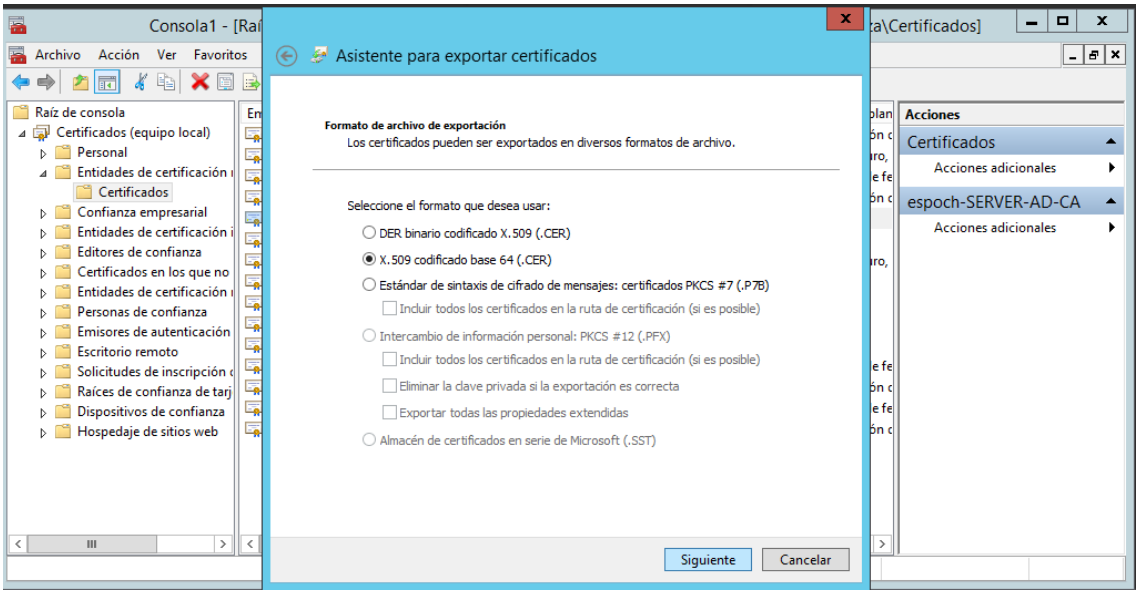


Figura 66-2: Asistente de certificados
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

k) Seleccionar el lugar donde se va a guardar el certificado con su nombre> guardar> siguiente, como se observa en la figura 67-2.

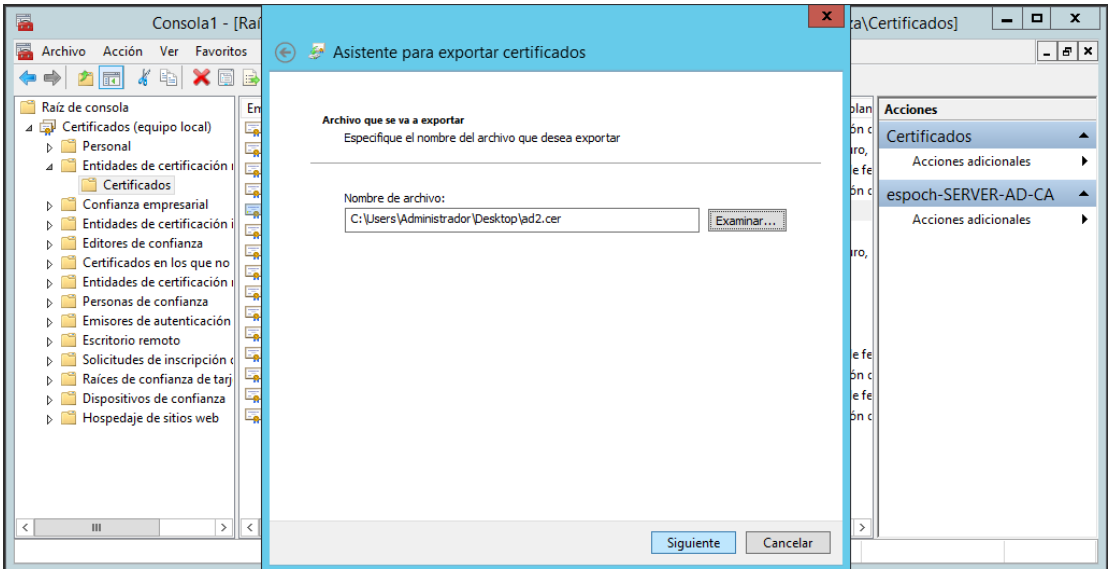


Figura 67-2: Guardar certificado
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

l) Para terminar clic en finalizar, como se observa en la figura 68-2.

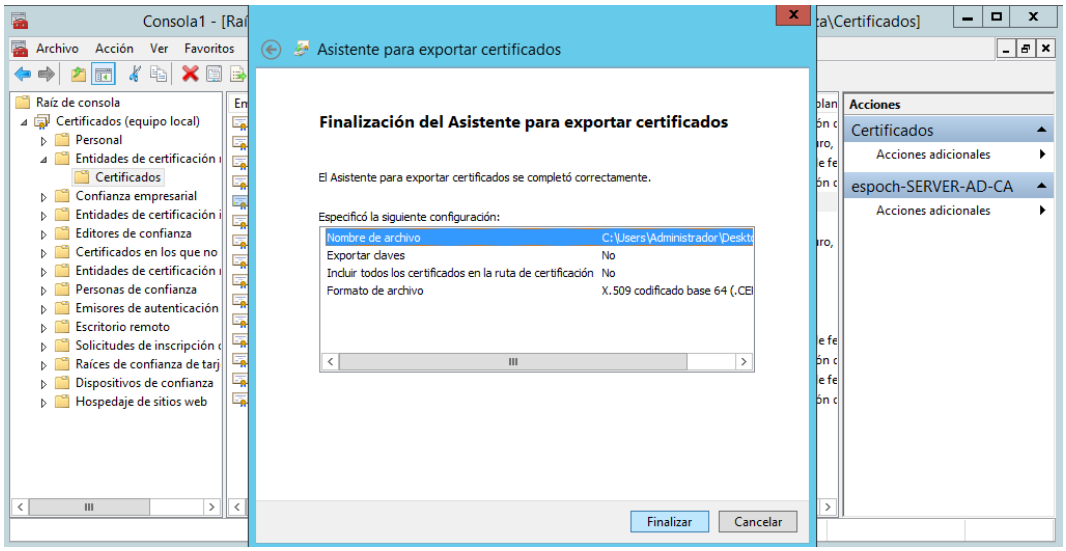


Figura 68-2: Finalización
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

m) Además de configurar el servidor AD para distribuir el certificado raíz de confianza a las estaciones de trabajo, instalar directamente en el servidor de AD.

En la consola de AD, vaya a Inicio> Ejecutar> cmd, y actualizar la directiva de grupo, como se observa en la figura 69-2.

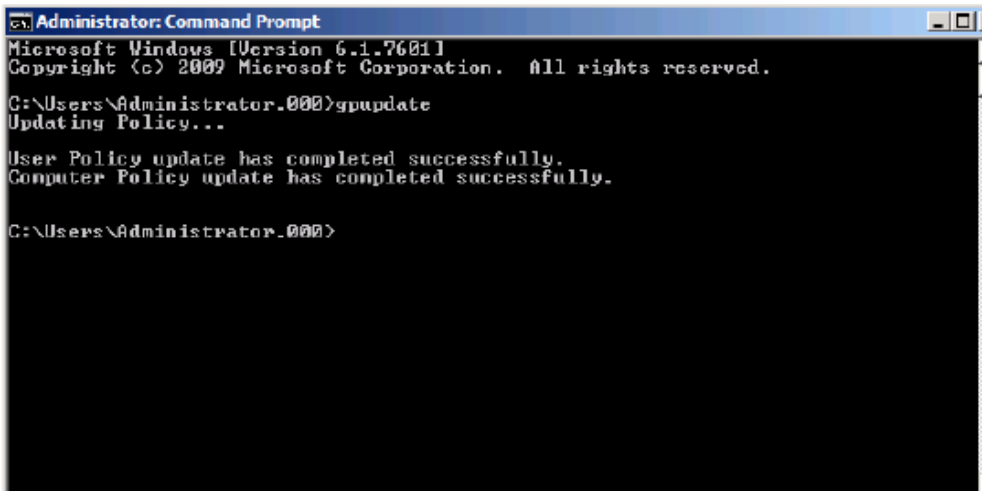


Figura 69-2: Instalación Directa
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

n) Para obtener un certificado de CA para ISE, este debe generar un certificado de petición de firma que utilizara CA para generar un certificado.

Para esto ingresar a la consola de ISE clic en Administration> Certificates> Certificate Management> Certificate Signing Request> y dar clic en Generate Certificate Signing Request, como se observa en la figura 70-2.

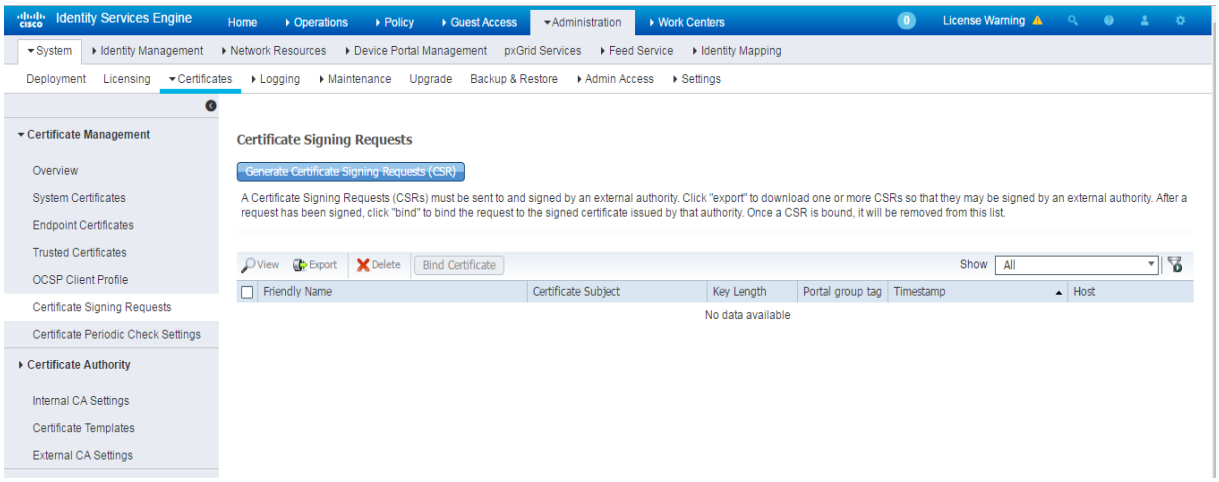


Figura 70-2: Generar Certificado
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

o) Llenar los parámetros solicitados y dar clic en Generate el cual genera el certificado en formato .PEM que servirá para generar un certificado en AD, como se observa en la figura 71-2.

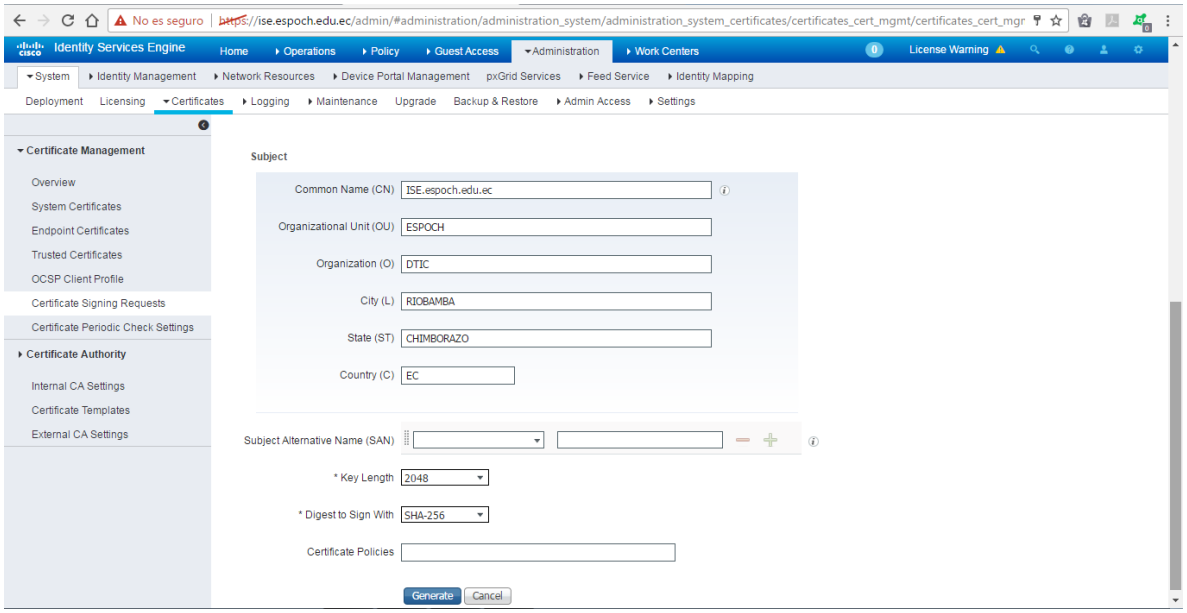


Figura 71-2: Certificado .PEM
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

p) Para descargar el certificado raíz de CA ingresar al buscador a la dirección http://172.31.204.63/certsrv/certrqus.asp, Clic en Solicitar un certificado> Solicitud avanzada de certificado> copiar el código del certificado generado por ISE> En planilla de certificado escoger servidor web> y enviar, como se observa en la figura 72-2.

Figura 72-2: Certificado Raíz
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

q) Para instalar el certificado raíz de confianza en Cisco ISE ingresar a su entorno y clic en Administration> Certification> Certificate Management> System Certificates> clic en import, como se observa en la figura 73-2.

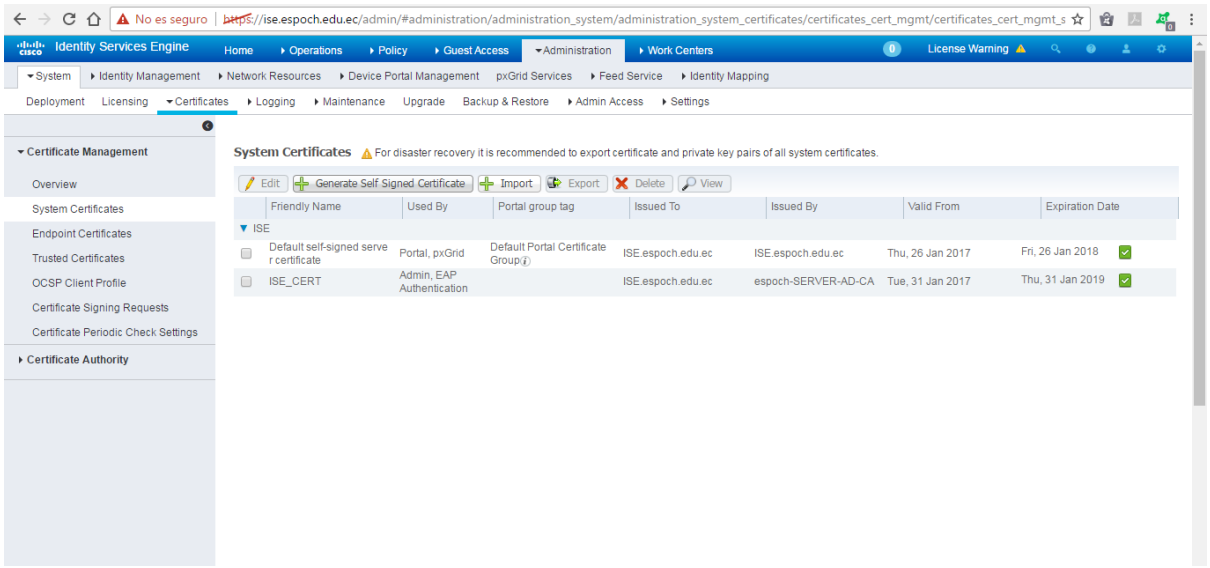


Figura 73-2: Instalación de certificado
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

r) Dar clic en seleccionar archivo y clic en submit, como se observa en la figura 74-2.

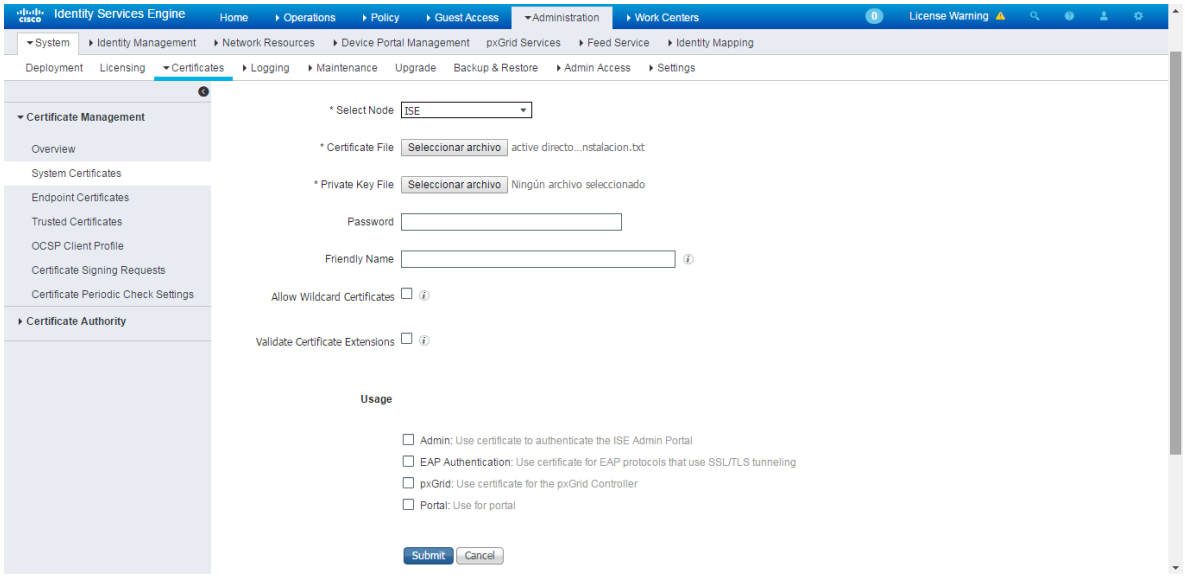


Figura 74-2: Selección de archivo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

s) Para enlazar el certificado ingresar al entorno de ISE, dar clic en Administration> Certification> Certificate Management> Certificate Signing Request> Escoger el certificado existente> clic en Bind Certificate, como se observa en la figura 75-2.

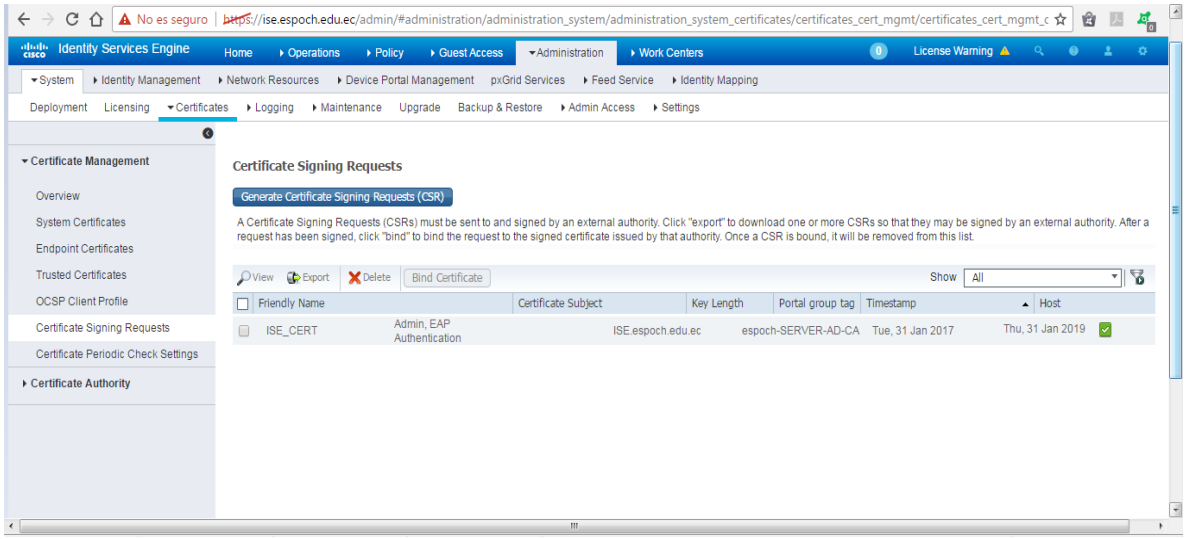


Figura 75-2: Enlace de Certificado
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

t) Una vez enlazado este certificado se recibe un aviso de reiniciar ISE, al cual se da clic en aceptar para finalizar.

u) Una vez que se ha importado el certificado local de ISE es necesario eliminar el antiguo certificado auto firmado, para ello se dirige a la interfaz de ISE y clic en Administration> Certification> Certificate Management> System Certificates> Seleccionamos el Default self-signed server certificate> Clic en Delete, como se observa en la figura 76-2.

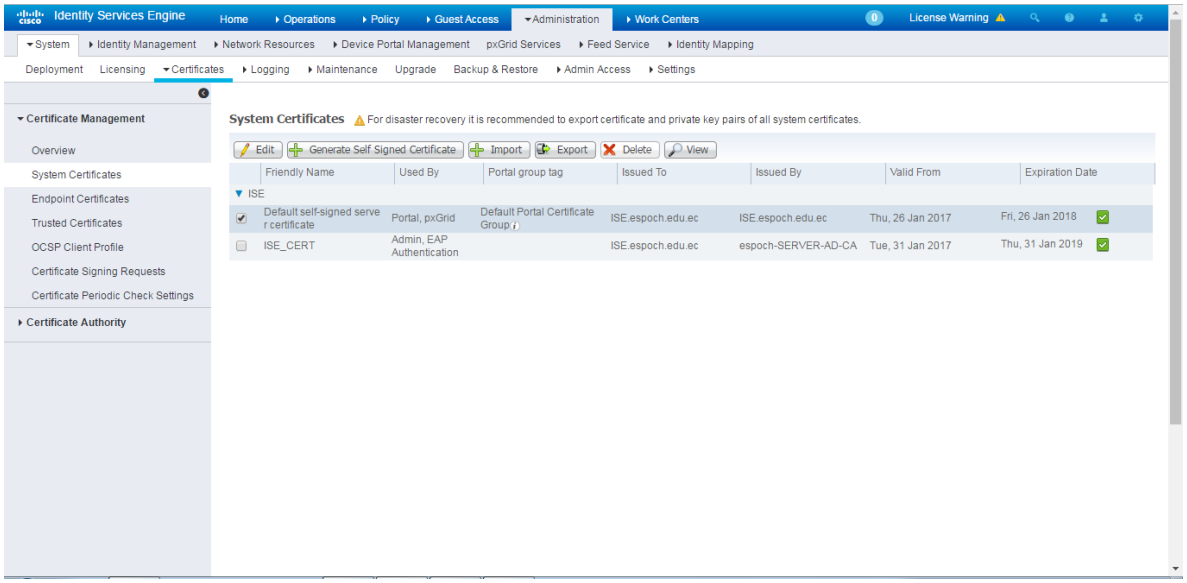


Figura 76-2: Certificado antiguo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

<u>Proceso 9</u>. Creación de políticas de Autenticación y Autorización.

a) Dirigirse a **Administration>Identity Management>Identity Source Sequences** y clic en Add, en donde se crea un perfil con solo usuarios que necesitaremos la autenticación, que serán los usuarios de AD y los usuarios internos de ISE en caso de tenerlos, como se observa en la figura 77-2.

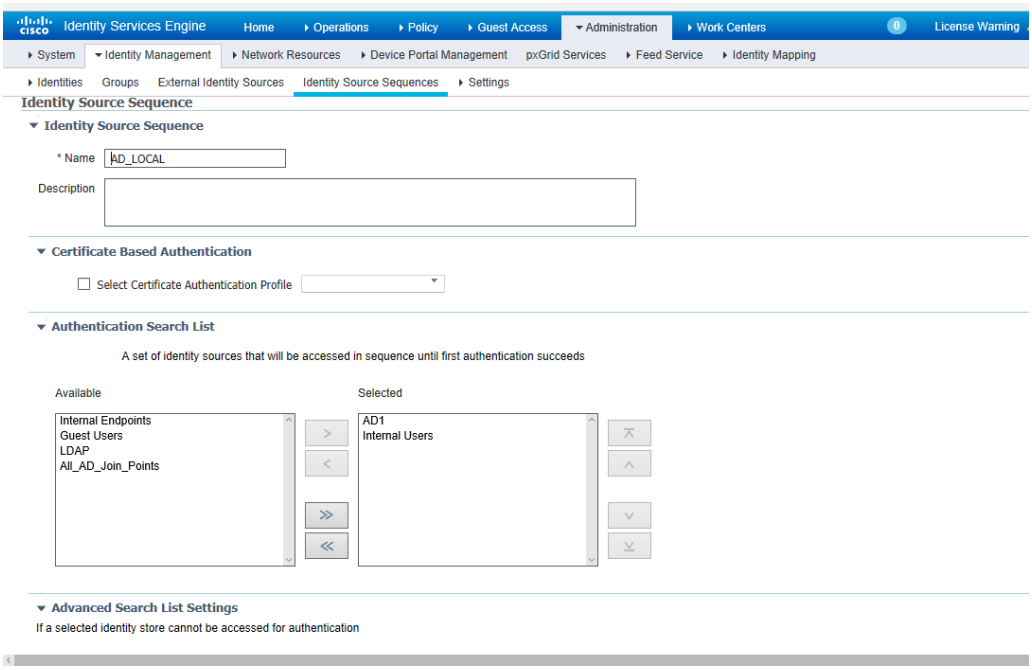


Figura 77-2: Añadir política
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

b) Se creará un perfil de autorización en cual se declara el protocolo de autenticación que se desea usar, para el caso será PEAP, navegar **Policy>Policy Elements>Results** en la sección de autorización añadir una nueva regla y permitir el protocolo que se desee, como se observa en la figura 78-2.

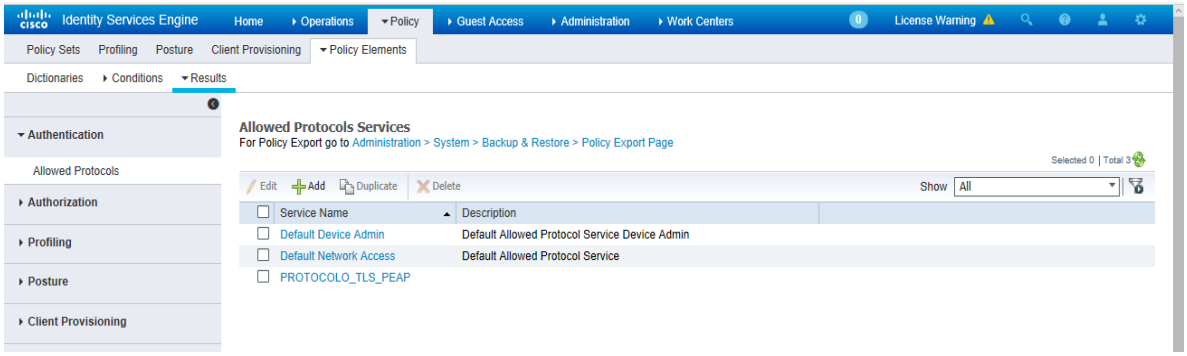


Figura 78-2: Perfil de autorización
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

c) Se crea los perfiles de autorización en donde se añade el resultado para que direccione a una Vlan determinada, como se observa en la figura 79-2.

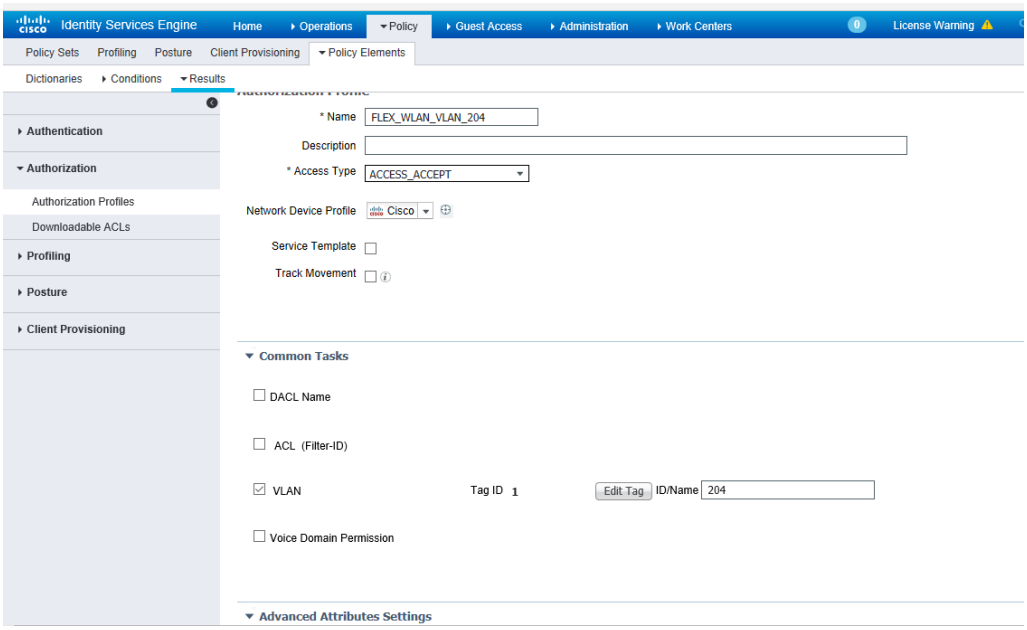


Figura 79-2: Selección de Vlan
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

d) Se repite el mismo paso para los perfiles de Vlans que se desee asignar.

e) Hay que ubicarse en **Policy >Profiling>Profiling Policies** y elegir un perfil de los existentes por ejemplo Android y proceder a configurar como se observa en la figura 80-2 lo cual nos segura un funcionamiento de dicho perfil de dispositivo.

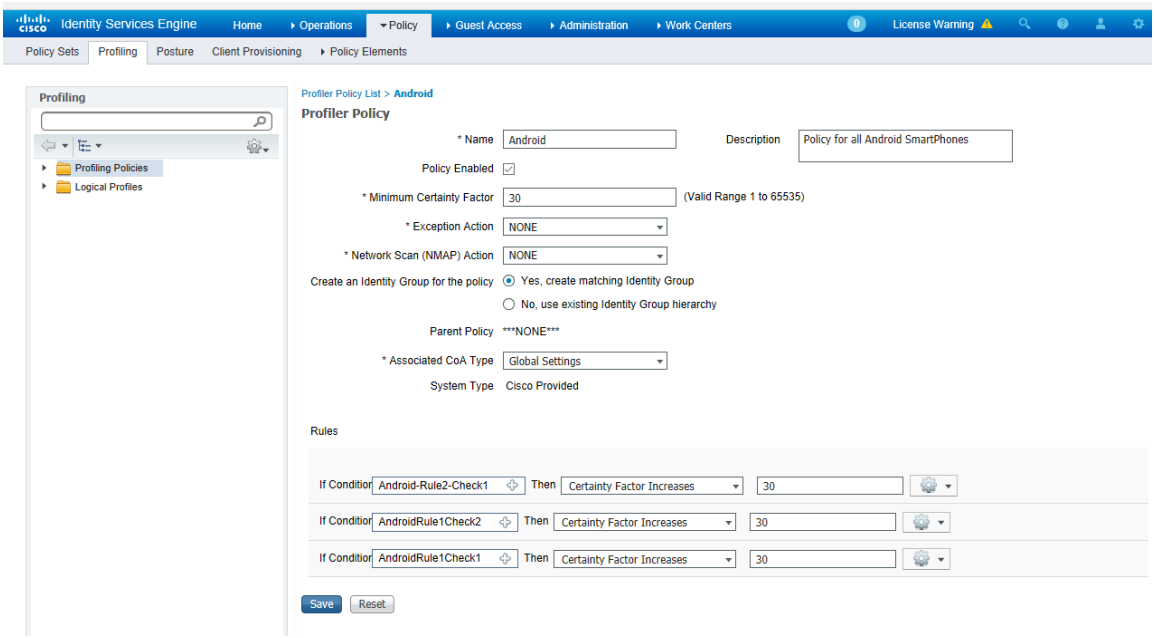


Figura 80-2: Configuración de perfil
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

f) Dar clic en **Policy** y crear una nueva regla, la cual se llamará WLAN y crear la primera regla de seguridad en donde hay que ubicarse en Radius, como se observa en la figura 81-2.

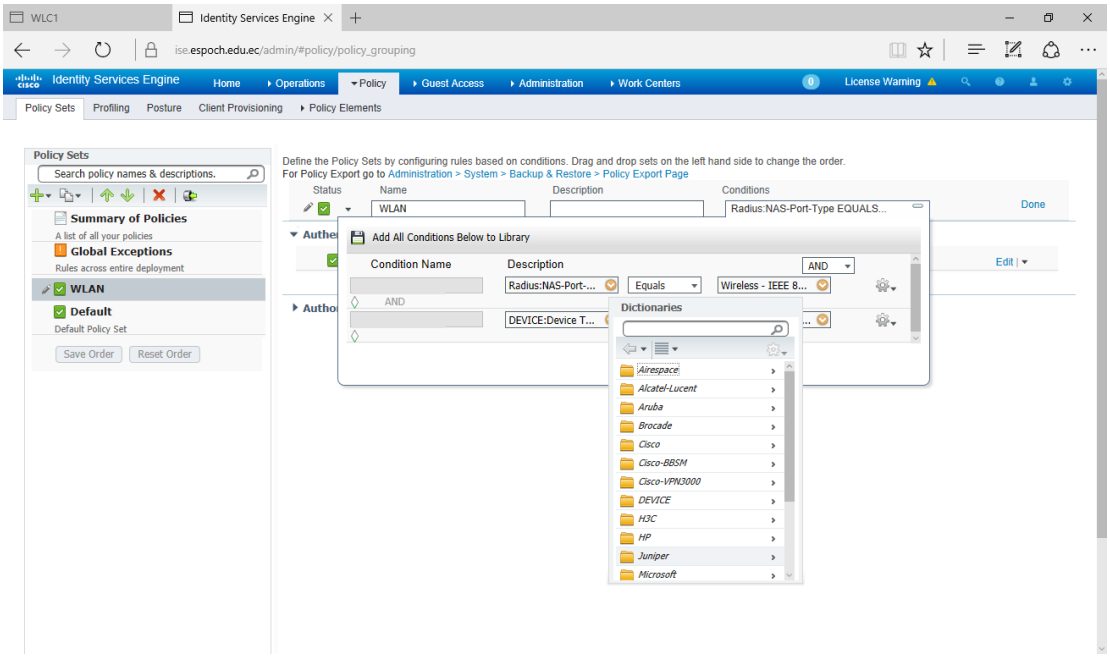


Figura 81-2: Nueva regla
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

g) Se procede a seleccionar el siguiente parámetro Nas-Port-Type y declarar que la condición sea igual al otro parámetro el cual es Wireless-iEEE802.11, como se observa en las figuras 82-2 y 83-2.

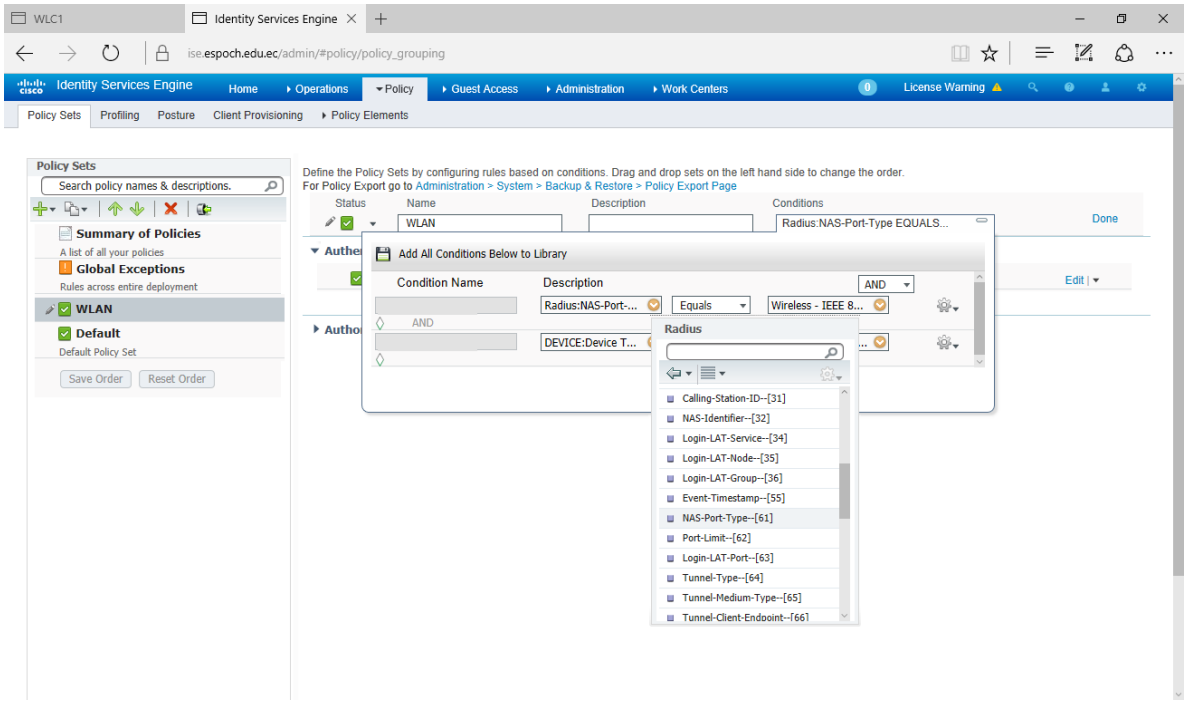


Figura 82-2: Condiciones iguales 1/2
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

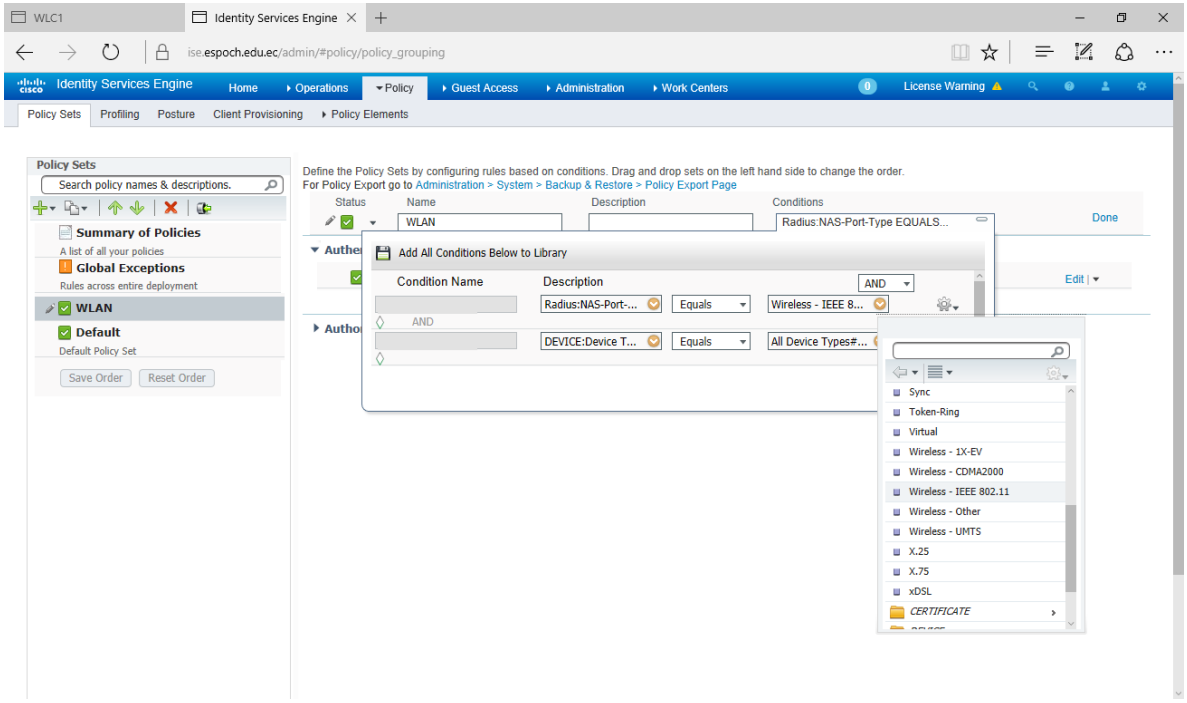


Figura 83-2: Condiciones iguales 2/2
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

h) Se crea otra regla la cual declara el tipo de dispositivo que va a tener acceso para ello dar clic en DIVICE, como se observa en la figura 84-2.

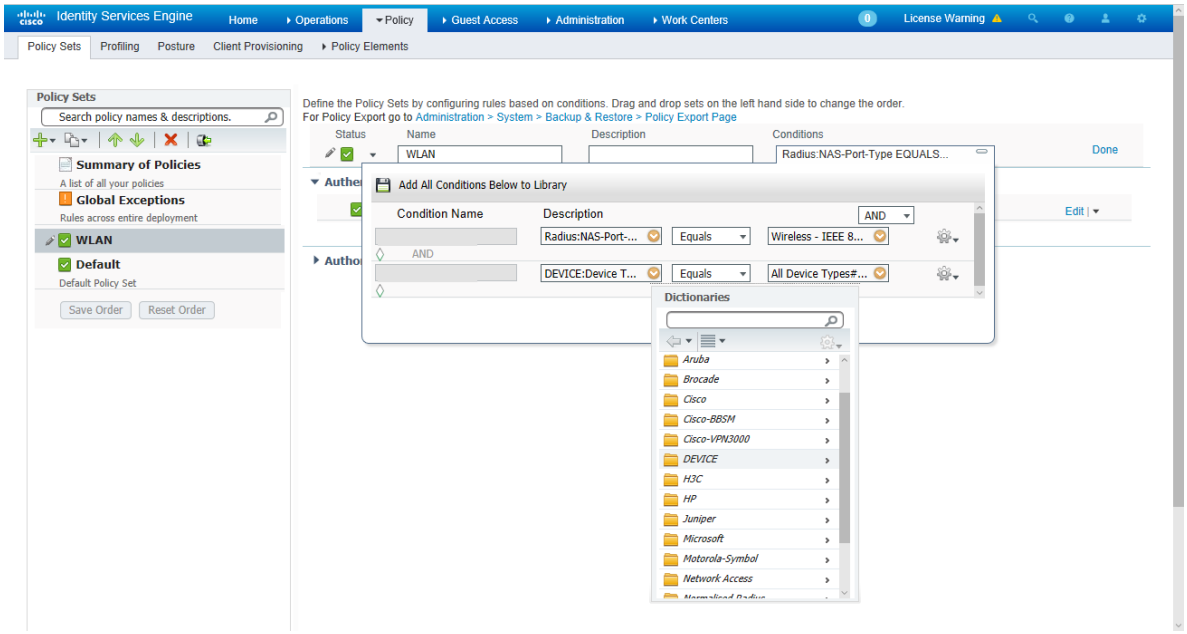


Figura 84-2: Regla según dispositivo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

i) Declarar tipo de dispositivo, como se observa en la figura 85-2.

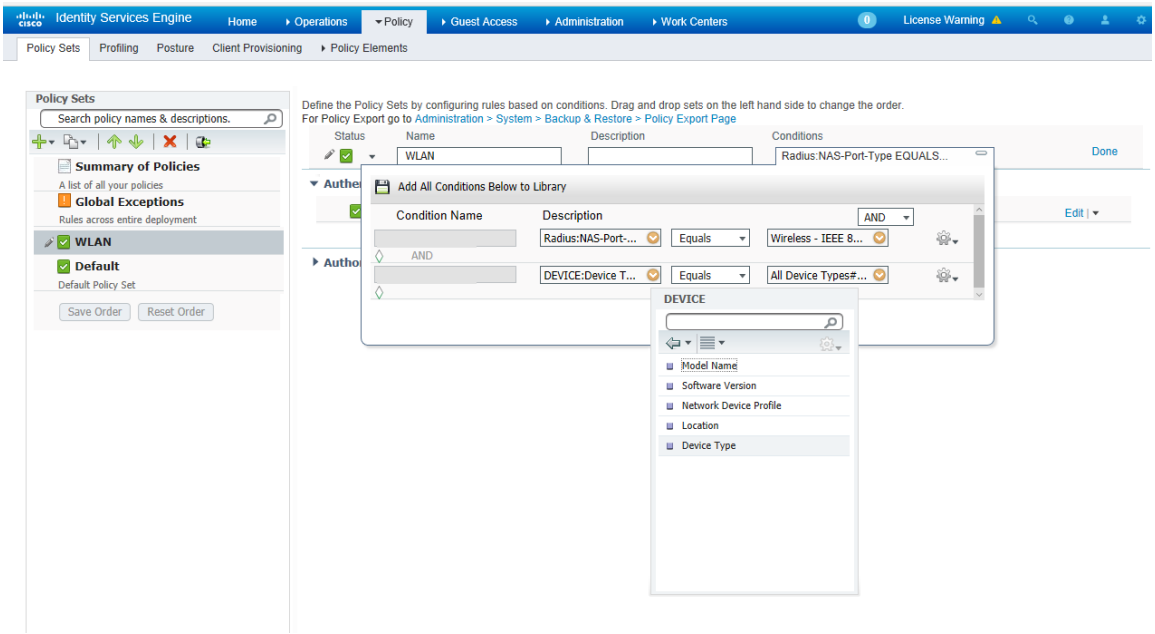


Figura 85-2: Declaración por tipo de dispositivo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Y definir el parámetro siguiente, como se observa en la figura 86-2.

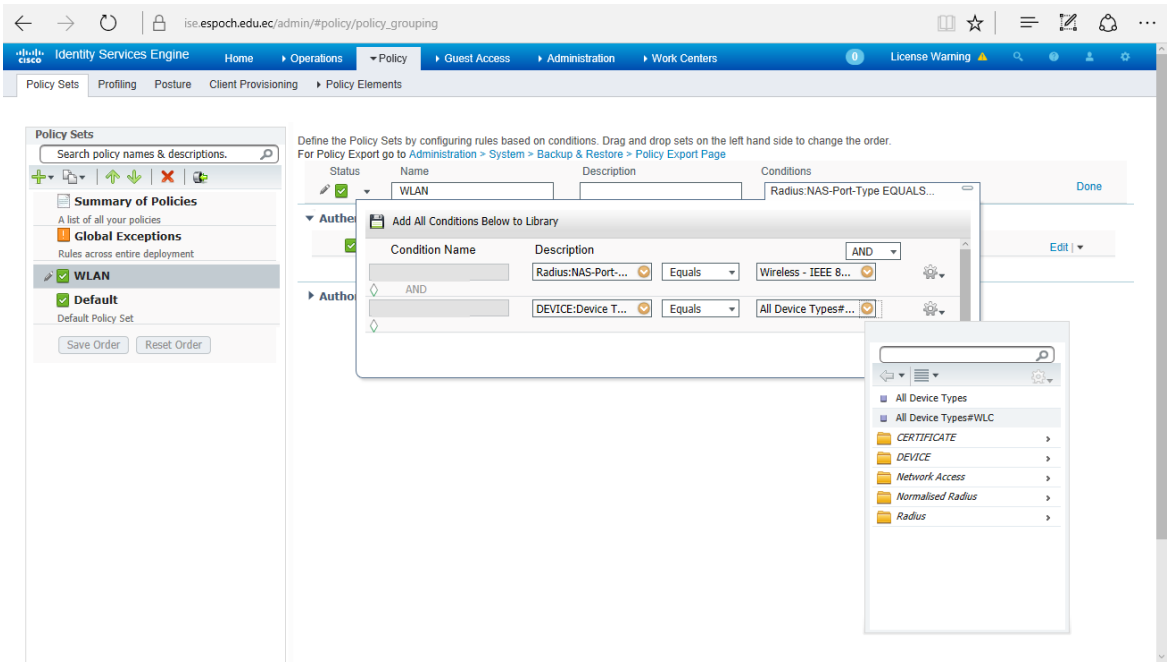


Figura 86-2: Parámetro por dispositivo
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

j) En la sección de autorización declarar los parámetros necesarios, en donde los protocolos permitidos son PEAP para los usuarios de AD, caso contrario será denegado el acceso, como se observa en la figura 87-2.

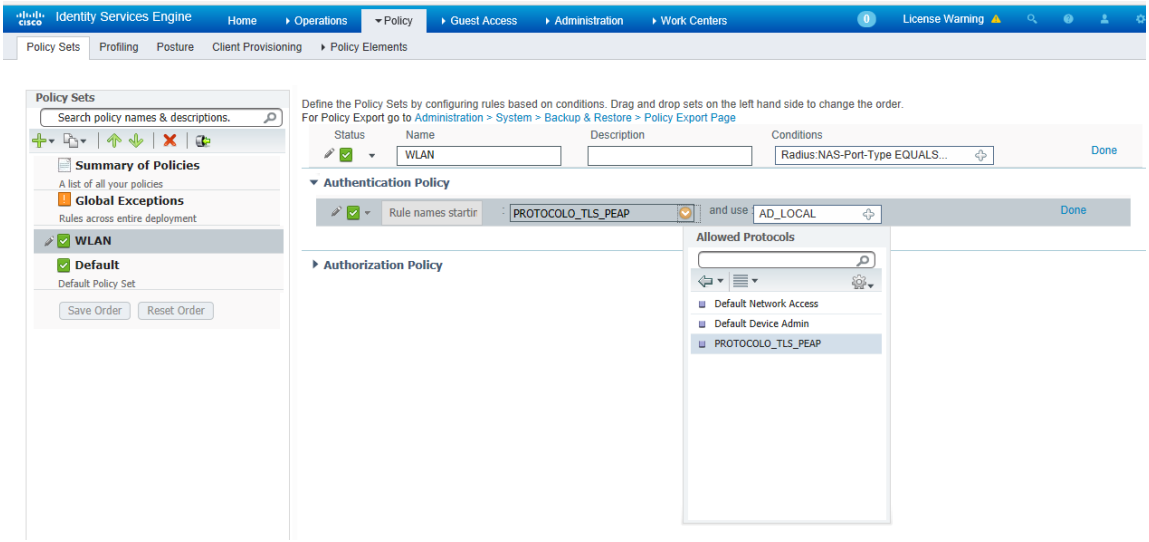


Figura 87-2: Declarar protocolos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

k) Se ubica en la sección de autorización y declarar las reglas, donde se selecciona una condición creada por defecto en ISE, como se observa en la figura 88-2.

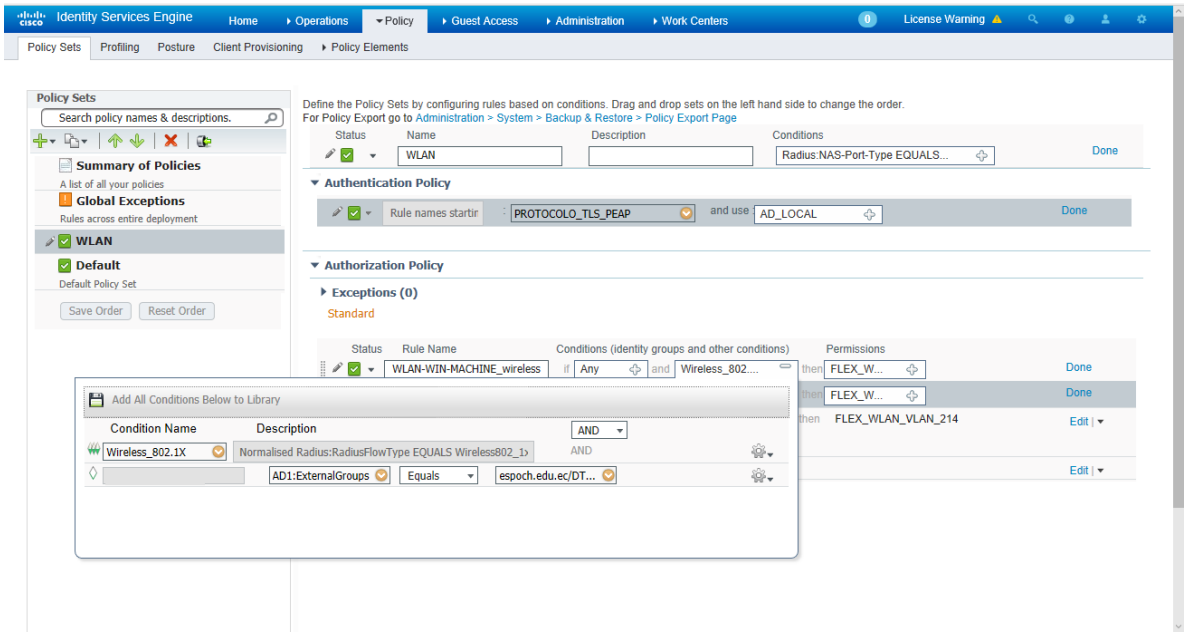


Figura 88-2: Declaración de reglas
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

l) A continuación, se declara el grupo específico al cual va ser aplicado esta regla, para ello seleccionar AD1, como se observa en la figura 89-2.

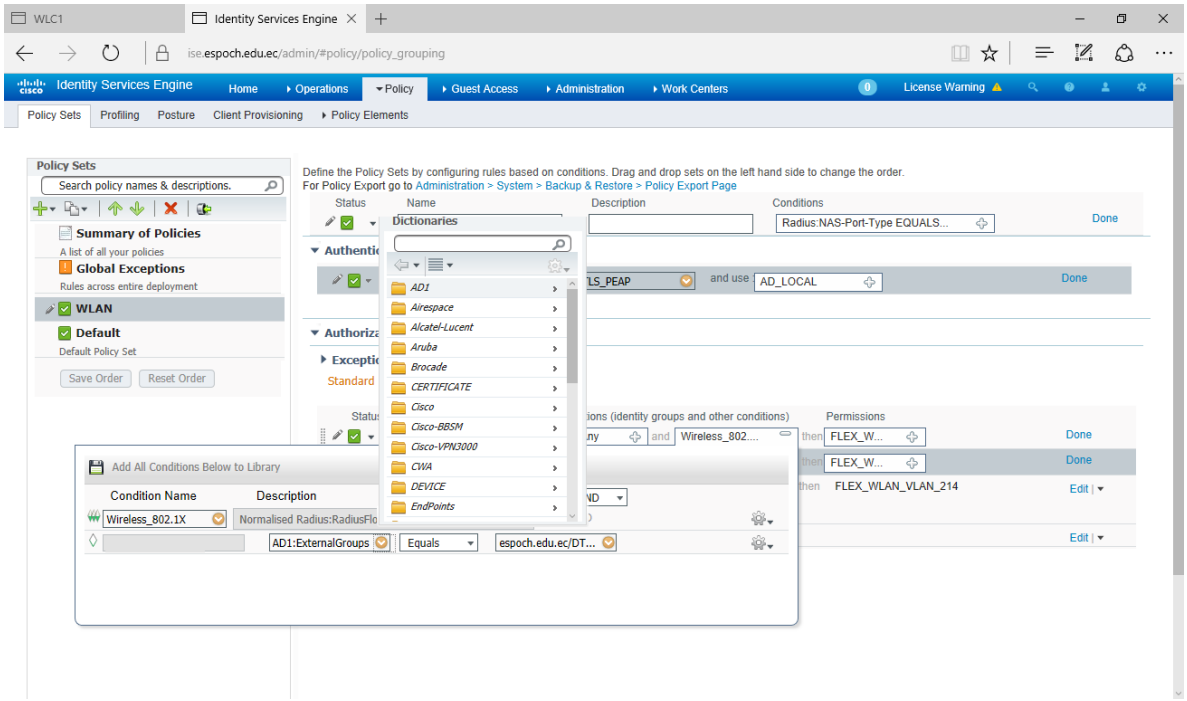


Figura 89-2: Declaración de grupos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

m)Elegir grupos externos, como se observa en la figura 90-2.

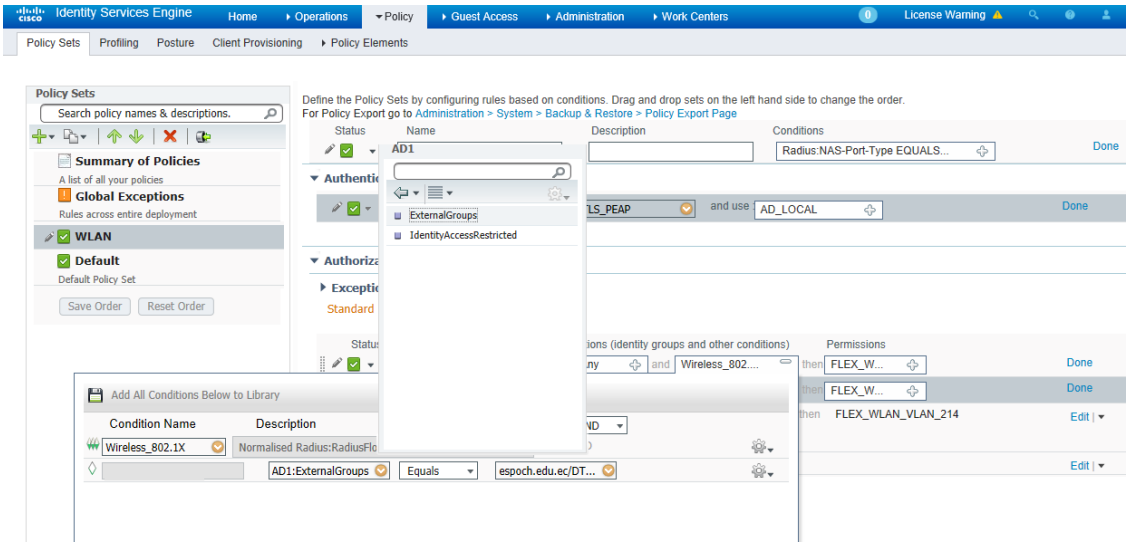


Figura 90-2: Elección de grupos
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

n) Debe ser igual al perfil creado anteriormente, el cual permitirá el acceso a la Vlan específica, como se observa en la figura 91-2.

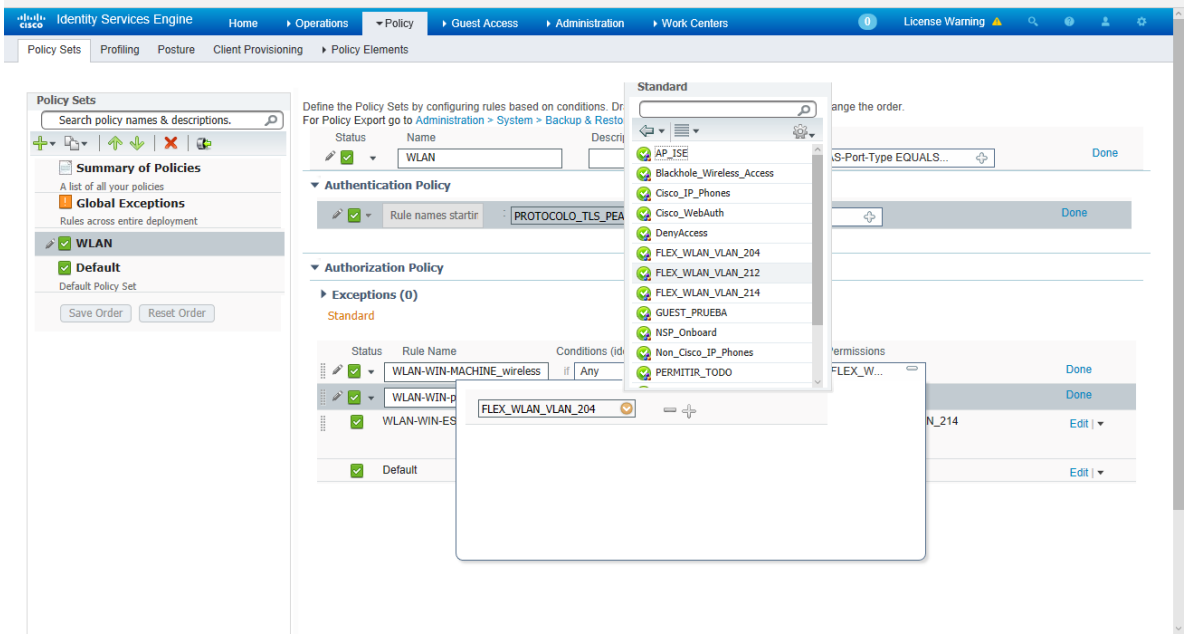


Figura 91-2: Acceso a Vlan
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.10 Configuración de la tarjeta de red de la PC con autenticación

Para obtener los permisos de autenticación requeridos se procede con la configuración de la tarjeta de red de la PC.

1. Como se observa en la figura 92-2 se describe el nombre de la red, el tipo de seguridad y se marcan los ítems subsiguientes.

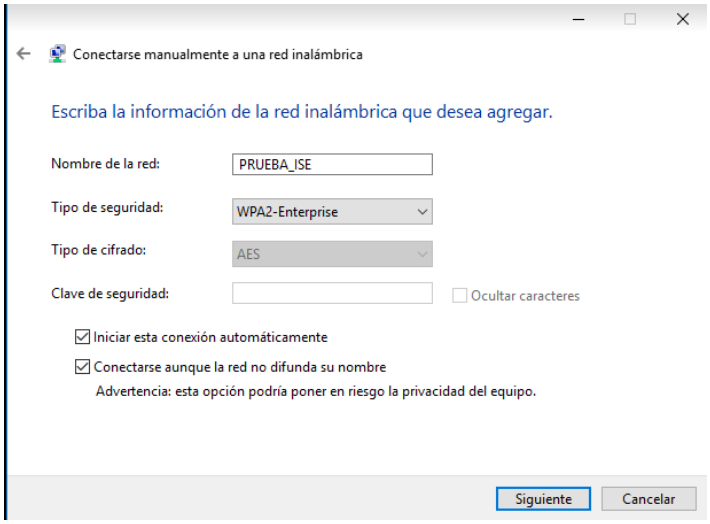


Figura 92-2: Información de la red inalámbrica a agregar
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2. En la pestaña seguridad, se elige el tipo de autenticación EAP protegido y luego se pulsa la opción configuración como se muestra en la figura 93-2.

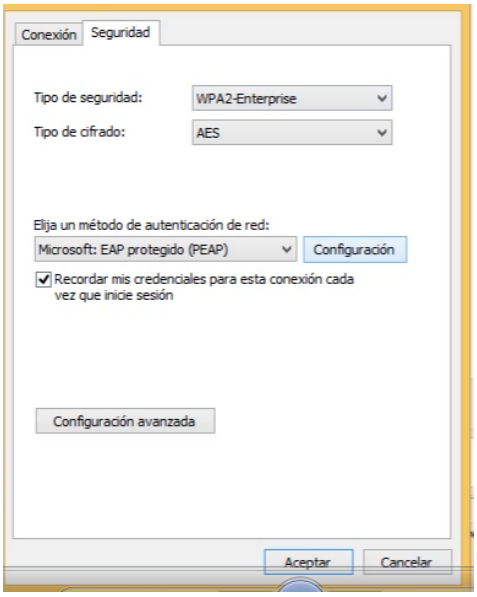


Figura 93-2: Propiedad de la red inalámbrica ISE
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3. Se Selecciona el ítem que se muestra en la figura 94-2.

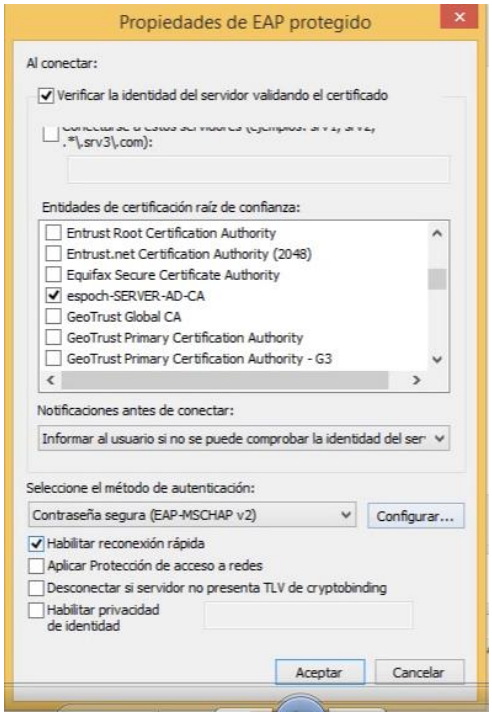


Figura 94-2: Propiedades de EAP protegido
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

4. Luego se pulsa la opción configuración avanzada como se muestra en la figura 95-2.

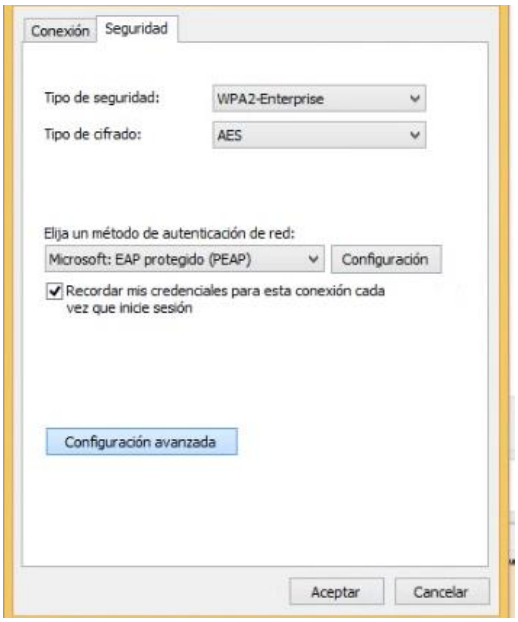


Figura 95-2: Configuración avanzada de la red
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

5. En la opción configuración de 802.1X se marca la casilla de verificación especificar el modo de autenticación como se muestra en la figura 96-2.

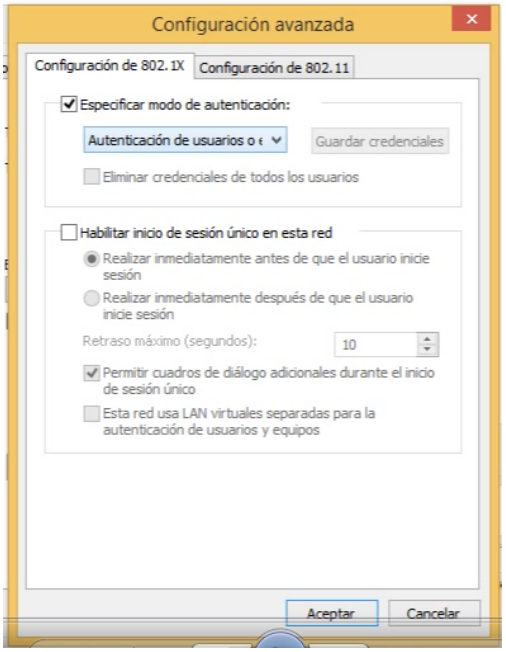


Figura 96-2: Modo de autenticación.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

6. Para poder acceder a la red es necesario tener instalado previamente el certificado que será el validador que permite la conexión del dispositivo final en este caso laptop, caso contrario no se podrá autenticar, como se muestra en la figura 97-2.

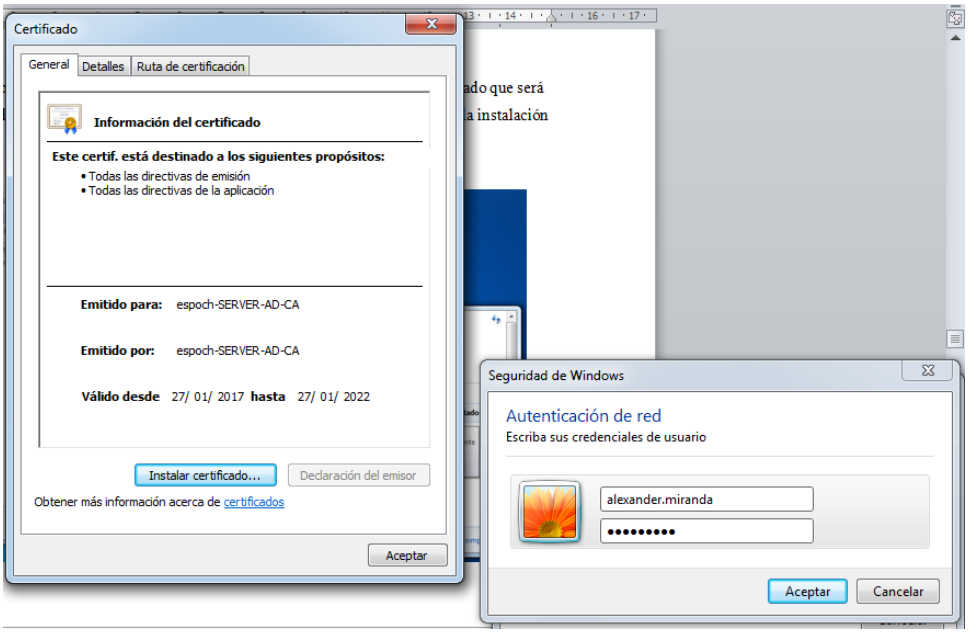


Figura 97-2: Certificado de autenticación
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

7. Una vez que las credenciales fueron ingresadas de forma correcta se realiza la autenticación de forma exitosa como se muestra en la figura 98-2.

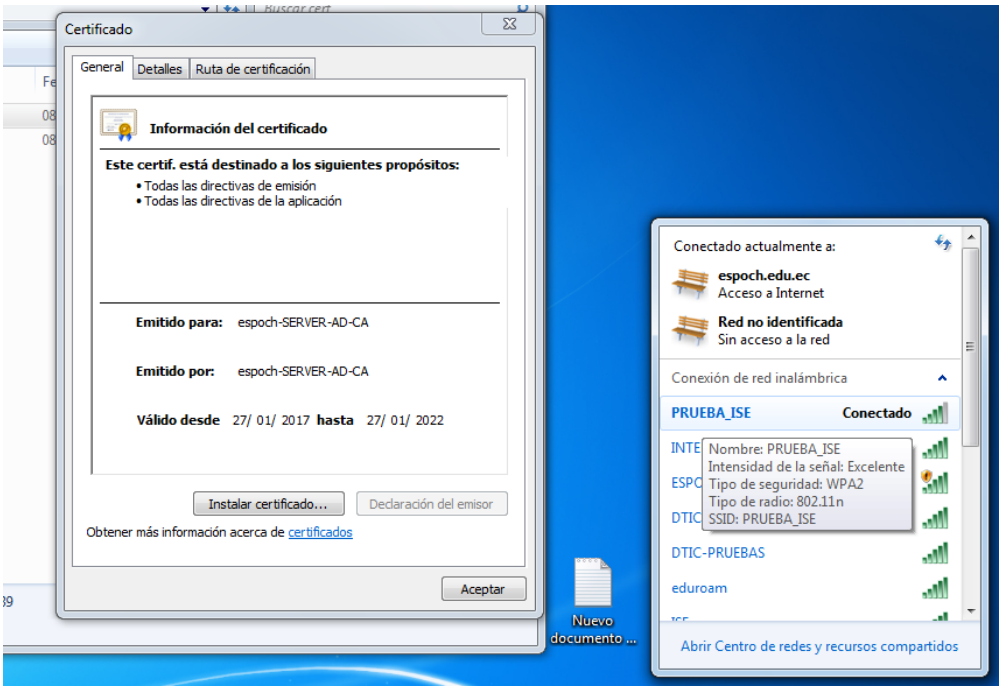


Figura 98-2: Conexión a red de prueba
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.11 Configuración de equipos finales

Configuración de Android

1. Dentro de la plataforma Android, se selecciona la red que se encuentra asociada a ISE como se muestar en la figura 99-2.

Figura 99-2: Selección de la red
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2. Se ingresa las credenciales para la conexión a la red como se muestra en la figura 100-2, teniendo en cuenta que el protocolo para la autenticación sea PEAP.

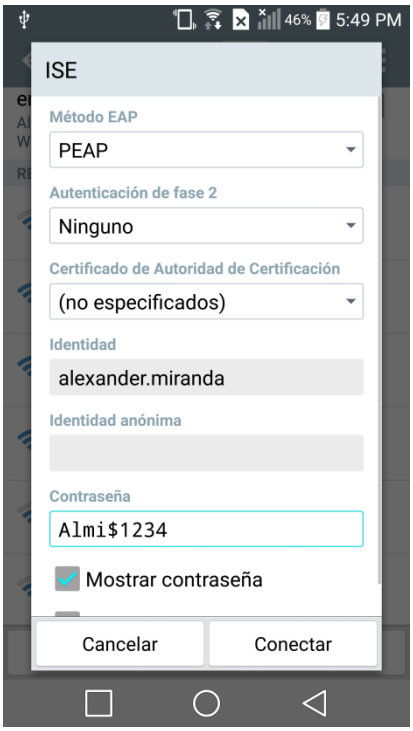


Figura 100-2: Ingreso de credenciales
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3. La figura 101-2 muestra el intento de conexión del dispositivo a la red de prueba.

Figura 101-2: Intento de autenticación
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

4. En la figura 102-2 se puede observar que la autenticación es exitosa, el dispositivo cuenta con los permisos necesarios que fueron ingresados y controlados por ISE, permitiendo una conexión exitosa dentro del ambiente de pruebas en Android.

Figura 102-2: Autenticación exitosa.
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Configuración de iOS

1. Para el sistema operativo iOS, se selecciona la red de prueba ISE como se observa en la figura 103-2.

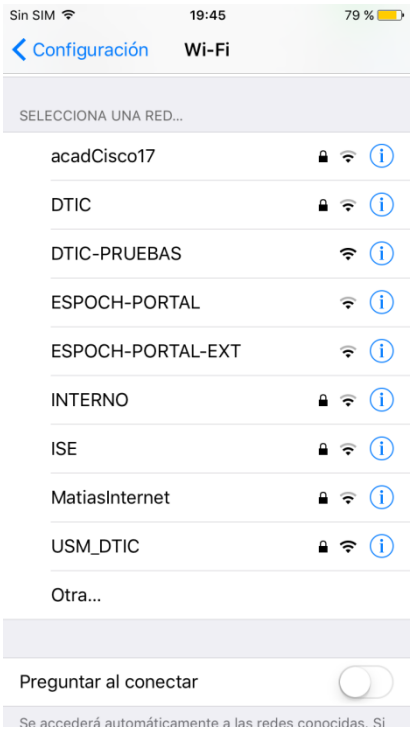


Figura 103-2: Selección de la red
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2. Se ingresa credenciales para comprobar el funcionamiento y la respuesta de ISE con el dispositivo como se observa en la figura 104-2.

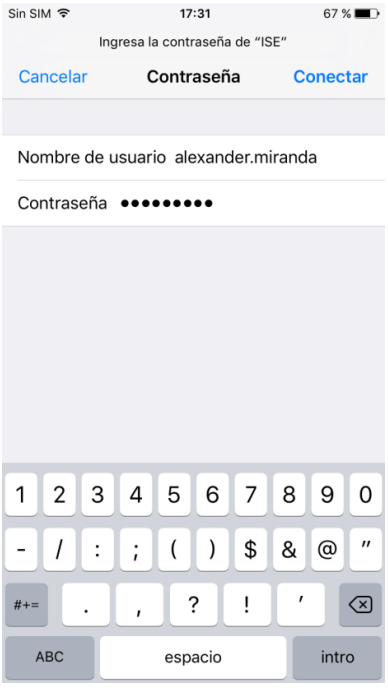


Figura 104-2: Ingreso de credenciales
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3. A diferencia de Android, en iOS se permite confirmar la legitimad del certificado de autenticacion para proceder a la conexión de red, para ello se selecciona la opción confiar que se encuentra en la esquina superior derecha del dispositivo, como se observa en la figura 105-2.

Figura 105-2: Certificado para iOS
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

4. La figura 106-2 muestra la autenticación exitosa y la conexión a la red de prueba.

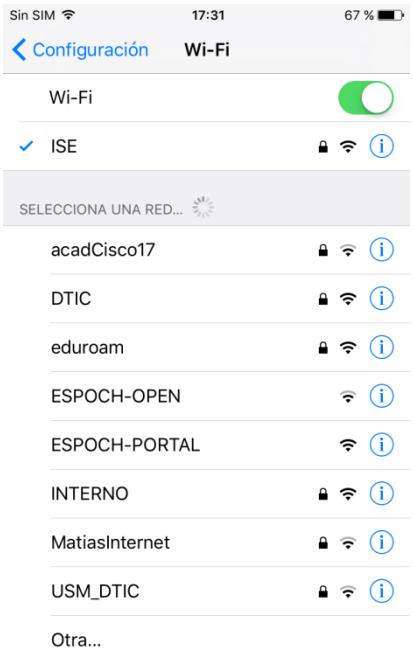


Figura 106-2: Autenticación exitosa
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.12 Planteamiento de grupos de identidad dentro de Active Directory

Los grupos de identidad son los usuarios que se encuentran activos para utilizar los recursos de la red y se los selecciona según sus características y funciones a realizar dentro de la institución, de esta manera se obtiene los perfiles y la asignación a un grupo de trabajo correspondiente.

Se pueden crear varios grupos en el AD, para el caso de estudio se plantea 3 grupos de usuarios, los cuales son miembros activos de la institución, los cuales son: docentes, estudiantes y administrativos, para ello al grupo Wireless se asigna 5 miembros, para el grupo profesores se asigna 5 miembros y para el grupo estudiantes se asigna 20 miembros, con sus respectivos privilegios, los cuales son normados por parte del DTIC, como se muestra en la tabla 6-2:

Tabla 6-2: Grupos de Active Directory

Nombre de Grupo	Descripción	Privilegios
Wireless	Son los usuarios administrativos encargados de gestionar y controlar la red.	Libre acceso a todo los recursos de la red.
Profesores	Pertenecen al grupo los docentes	Acceso a protocolo FTP, TFTP, comunicación intervlan desde vlan profesores hacia vlan estudiantes, restricción a vlan de administración, restricción a los servidores de la Espoch.
Estudiantes	Pertenecen al grupo los estudiantes	Acceso solamente a internet.

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.13 Asignación de Vlans para grupos de usuarios

Para cada grupo de usuarios que existen dentro del Active Directory es necesario asignarlos a una vlan específica, la cual cuenta con sus requerimientos y permisos específicos otorgados por el DTIC. Las vlans correspondientes para que trabajen cada grupo de AD se muestran en la tabla 7-2:

Tabla 7-2 Asignación de Vlans

Grupo de AD	Número de Vlan asignado
Wireless	Vlan 204
Profesores	Vlan 212
Estudiantes	Vlan 214

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

2.14 Políticas aplicadas en ISE

Es necesario definir políticas de seguridad, autenticación y autorización que permitan que el acceso sea confiable a la red inalámbrica de la Espoch. Cabe recordar que las ACLs son creadas y expedidas por el DTIC, dependiendo del rol del usuario que se vaya a conectar a la red, como se muestra en la tabla 8-2.

Tabla 8-2: Políticas de ISE

Usuario	Grupo de Usuario	Política de autenticación	Política de autorización
Administrativo	Wireless	802.1X PEAP	Vlan 204 Acl administrativos
Docente	Profesores	802.1X PEAP	Vlan 212 Acl profesores
Estudiante	Estudiantes	802.1X PEAP	Vlan 214 Acl estudiantes

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

CAPÍTULO III

3. MARCO DE RESULTADOS

3.1 Introducción

Como resultado del estudio de funcionamiento de Cisco Identity Services Engine (ISE) y su uso para aplicación de políticas de seguridad basadas en identidad, se obtiene un mayor y mejorado control en las conexiones y acceso a la red inalámbrica que en las redes inalámbricas existentes no lo poseen.

3.2 Mejoras del acceso inalámbrico

El giro que tomó el acceso a la red inalámbrica fue de gran impacto, puesto que, para la mayoría de usuarios que utilizan conexión inalámbrica mediante dispositivos finales como: laptops, tablets, smartphones se encuentran hoy con una interfaz de conexión diferente a la normalmente usada (usuario y contraseña).

Mediante la autenticación con el protocolo 802.1X PEAP-MSCHAPv2 se notó una mejoría en la seguridad al momento de acceder a la red inalámbrica. Mediante la tecnología Cisco ISE se pudo controlar y administrar los usuarios, los dispositivos y gestionar para que accedan a la SSID de prueba controlada por ISE.

El control en la red inalámbrica limita el acceso a los usuarios y dispositivos, garantizando un mejor uso de la misma, un control de que usuario y tipo de dispositivo es utilizado en la hora determinada en la que se ha conectado en la red además de ser asignados por grupos de seguridad. Con la tecnología (ISE) se garantiza una mejoría en la red inalámbrica aplicando estrictas políticas de seguridad determinando así que tipo de personas, departamentos, privilegios y requerimientos son necesarios en cada regla de autorización.

3.3 Pruebas con Dispositivos Finales a ISE

Se probó los principales tipos de dispositivos como son Android (Samsung, LG, Sony Xperia), iOS (iPhone 4s – 5s), y Windows (7, 8, 10) para autenticarlos a la red de prueba, obteniendo resultados esperados como es la asignación de vlans acorde al registro que maneja el grupo de usuarios de AD, que en las redes inalámbricas difundidas no poseen este tipo de asignación, sino simplemente el direccionamiento en un mismo segmento de red.

1. Como se muestran en las figuras 1-3, 2-3, 3-3 se puede observar que en las direcciones IP de los dispositivos se las asignó a una vlan correspondiente, cabe indicar que el tercer octeto de la dirección IP represente al tag de vlan, independiente al grupo de usuarios al que pertenecen: wireless (204), profesores (212), estudiantes (214) respectivamente.

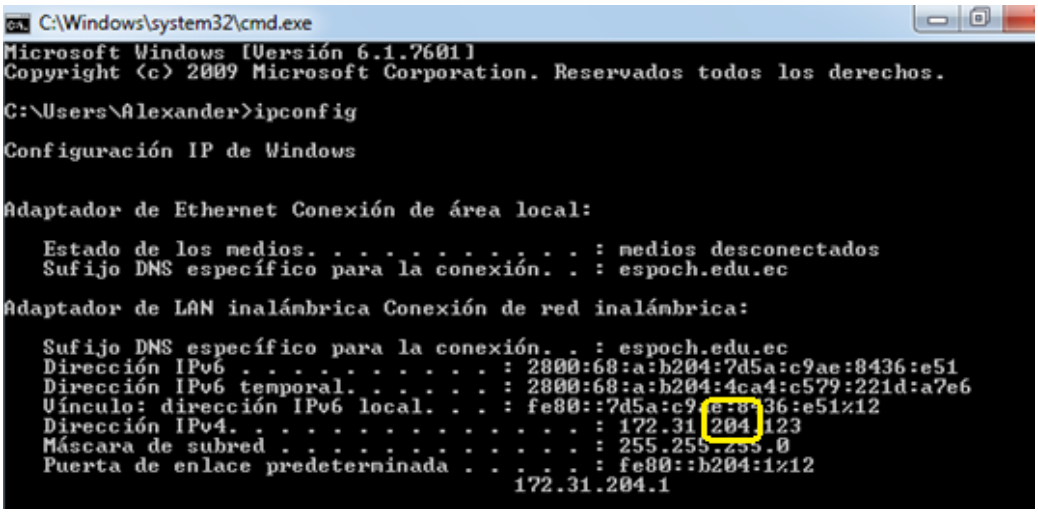


Figura 1-3: Asignación vlan administrativa
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

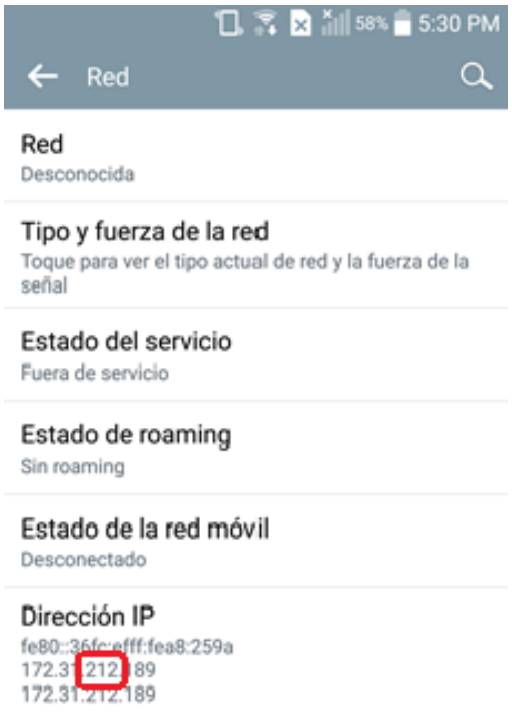


Figura 2-3: Asignación vlan docente
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

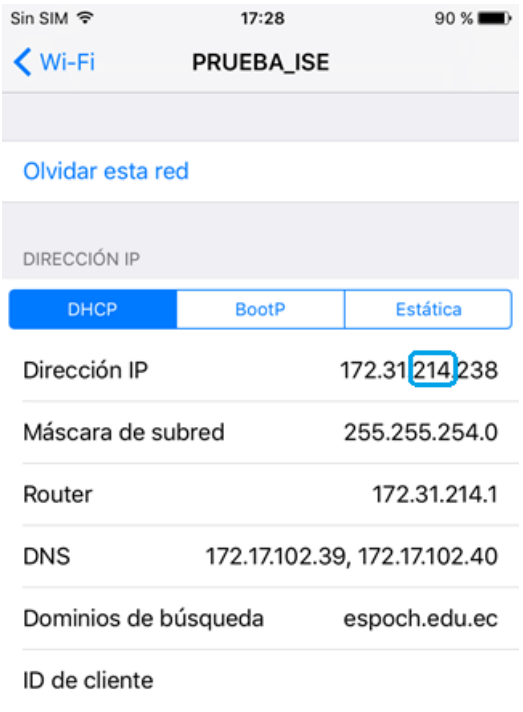


Figura 3-3: Asignación vlan estudiante
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Como se pudo evidenciar en el capítulo 2 ítem 2.7 de éste estudio se observó, que tanto los docentes, estudiantes y administrativos de la institución tienen libre acceso a cualquier red difundida por el DTIC, por lo tanto son asignados a un solo segmento de red dependiendo del SSID a cual se conecten, quedando claro que todas las conexiones, independientemente de qué usuario se trate, se lo direcciona al mismo segmento de red. De esta manera queda demostrado que mediante la tecnología ISE como se observa en las figuras 1-3, 2-3, 3-3, por asignamiento de vlan dinámicas dependiendo el grupo de usuarios con su respectivo privilegio normado por medio de ACLs, se los asignó a una vlan específica para cada grupo, mejorando así notablemente el uso de los recursos de la red inalámbrica.

3.4 Ventajas de utilizar el protocolo 802.1X- PEAP

Las principales bondades que ofrece el protocolo 802.1X en conjunto con la seguridad PEAP implementados en la red de prueba por sobre las otras dos redes existentes es que, esta red tiene requerimientos únicos y un solo camino para que la información sea transmitida entre el cliente y el AP. La cual ofrece la capacidad de permitir o denegar conectividades de capa 2, asignando a una vlan o implementando políticas aplicadas en la red y al usar WPA2-Enterprise fue necesario usar el método PEAP. Este método de seguridad presenta un certificado digital el cual es validado por un tercero para el caso de estudio AD, de la misma manera este método de seguridad negocia un túnel TLS (Transport Layer Security), y así el usuario final puede ser autenticado. En la tabla 1-3 se muestran los beneficios que ofrece el protocolo 802.1X versus la infraestructura de red existente de la Espoch.

Tabla 1-3: Ventajas de 802.1X-PEAP

Nombres De Redes / **Características**	**ESPOCH-OPEN**	**ESPOCH-PORTAL**	**PRUEBA_ISE**
Tipo de seguridad	**Abierta**	**Portal Cautivo**	**802.1X PEAP**
Autenticación Capa 2	Ninguna	Ninguna	WPA2-Enterprise
Autenticación Capa 3	Ninguna	Ninguna	Ninguna
Certificado de cliente requerido	No	No	No
Certificado de servidor requerido	No	No	Sí
Administración de claves WEP	No	No	Si

Dificultad de implementación	Baja	Media	Alta
Seguridad Wi-Fi	Ninguna	Moderada	Alta

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

A continuación se realizó una extracción de los logs que otorga el servidor Radius (ISE), en donde se puede observar el modo de negociación del método de seguridad PEAP y la creación del túnel TLS, como se puede visualizar en las líneas de código extraída del log, se puede ver que la creación del túnel y la negociación ha sido exitosa.

user=oscar.morales,CallingStationID=24-fd-52-a3-8a-74,EAP-TLS: SSL stack trace:139790337627904 routines:SSL3_READ_BYTES:tlsv1 unknown ca:s3_pkt.c:1300:SSL number 48,EapTlsProtocol.cpp:906

Crypto,2017-03-21 17:18:50,717,0x7f23796ad700,NIL-CONTEXT,Crypto::Result=1, Crypto.SSLConnection.pvServerInfoCB - Alert raised: code=0x230=560, direction=read, message=SSL : code=0x230=560 ; source=remote ; message="unknown CA",SSLConnection.cpp:3175

Eap,2017-03-21 17:18:53,716 ,0x7f23796ad700,cntx=0000182432,sesn=ISE/276558790/791,CPMSessionID=3ecc1fac000000decd31bf58,user=oscar.morales,CallingStationID=24-fd-52-a3-8a-74,PEAP report handshake success: openssl ,direction=read, PeapProtocol.cpp:907

En la imagen 4-3 se puede apreciar el log extraído de Radius (ISE).

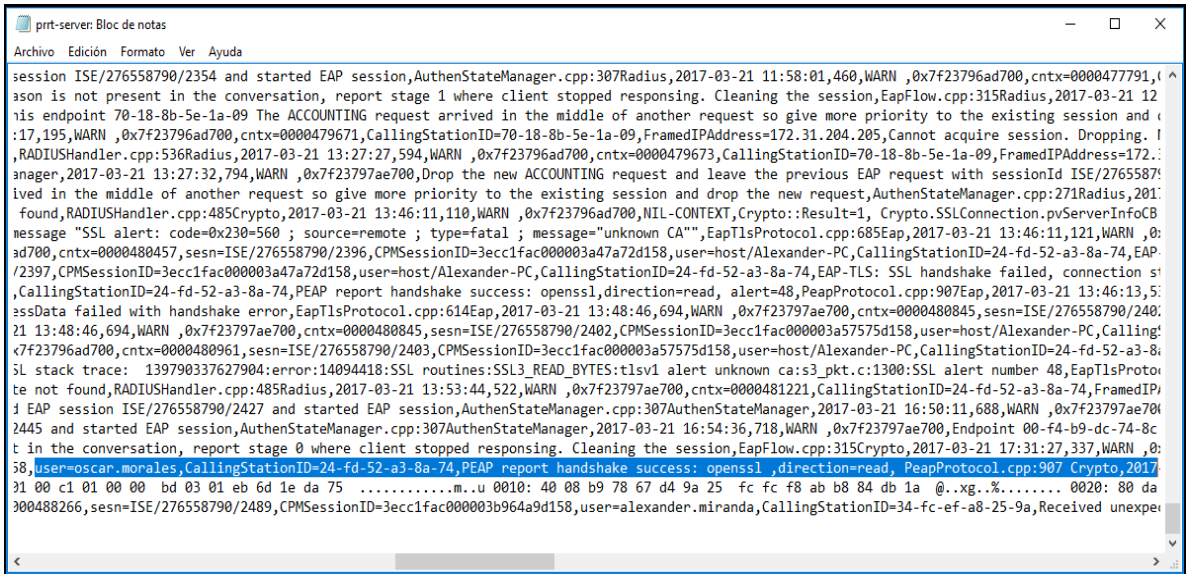


Figura 4-3: Log de Radius (ISE)
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3.5 Atributos que otorga ISE a la infraestructura wlan de la Espoch.

Tomando en cuenta que actualmente la infraestructura wlan de la Espoch carece de algún tipo de plataforma de control, regulación y restricción para normar el acceso a la red se demostró lo beneficioso del estudio de la tecnología ISE y el gran aporte que puede brindar a la infraestructura wlan, dando a conocer las falencias y la gran brecha de inseguridad que posee la red inalámbrica, de esta manera se realizó una tabla comparativa entre la infraestructura sin ISE versus la infraestructura con ISE y se obtuvieron resultados que demuestran que, al poseer un acceso controlado en la infraestructura wlan nos brinda un control sobre el usuario así como ciertas restricciones por lo cual con este estudio, ISE nos presenta los atributos añadidos como se muestra en la tabla 2-3.

Tabla 2-3: Comparación de infraestructuras

	INFRAESTRUCTURA SIN ISE	**INFRAESTRUCTURA CON ISE**
Políticas de autenticación	Sí	Sí
Políticas de autorización	No	Sí
Políticas de dispositivo	No	Sí
Políticas de acceso a grupos de seguridad	No	Sí
Asignación de vlans dinámicas	No	Sí
ACLs descargables	No	Sí

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3.6 Visibilidad por identidad y contexto de ISE

La solución ISE proporciona visibilidad de red comprensiva y consolidada usando identidad y contexto, las cuales incluyen el quién, qué, cuándo y cómo ha sido el acceso a la red, en donde la identidad se enfoca en conocer el usuario o el dispositivo el cual viene dado por el (quién), el contexto en cambio brinda información adicional (qué) (cuándo) (cómo), un ejemplo claro de cómo funciona estos perfiles se muestra en la tabla 3-3.

Tabla 3-3: Identidad y Contexto

Datos de Identidad y Contexto	**Datos del usuario**
¿Quién?	edwin.altamirano
¿Qué?	WLC1
¿Cuándo?	2017-03-16 17:34:03.826
¿Cómo?	Apple-iPhone

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

El ejemplo citado anteriormente se lo puede observar en la figura 5-3.

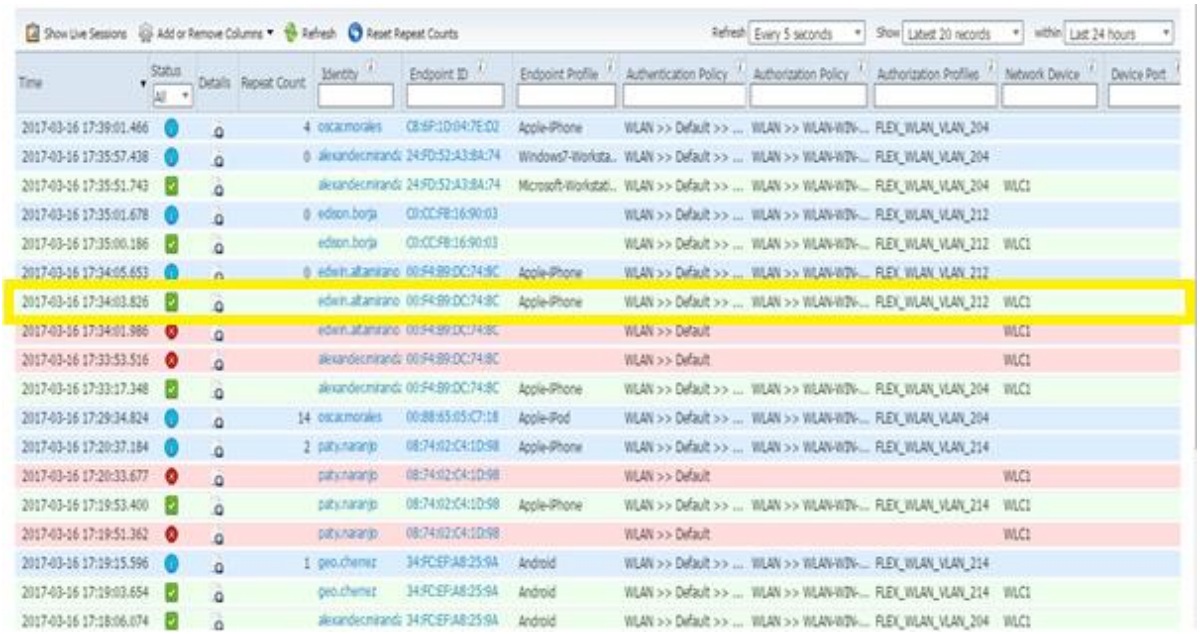


Figura 5-3: Control de Radius
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3.7 Estadísticas de uso de ISE

En esta sección se muestran los resultados que nos ofrece la herramienta Cisco Identity Services Engine (ISE) para el control de acceso de dispositivos finales a la red inalámbrica como se observa en la figura 6-3.

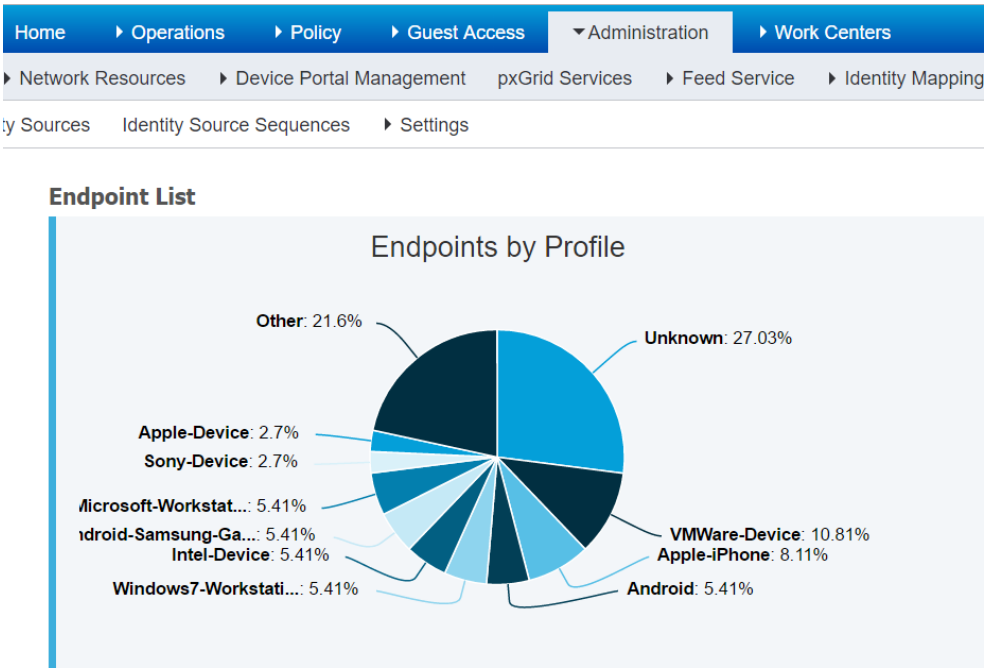


Figura 6-3: Perfiles de puntos finales
Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

Como se observó en la figura 6-3 ISE nos otorga la estadística de conexiones por equipos como desconocidos el 27.03%, los cuales son dispositivos no registrados por perfiles, otros 21,6% los cuales son dispositivos no actualizados o nuevos en el mercado, VMWare-Device 10.81%, Apple-iPhone 8.11%, y con un porcentaje de 5.41% tenemos dispositivos como Android, Windows 7-Workstation, Intel-Device, Android-Samsung-Galaxy, Microsoft-Workstation, de igual manera tenemos con 2.7% los dispositivos Apple-Device y Sony Device.

3.8 Análisis de factibilidad técnica

La factibilidad técnica estuvo destinada a recolectar información sobre los equipos tecnológicos que dispone la Espoch y la posibilidad de hacer uso de los mismos en el desarrollo y una posible implementación de Cisco ISE, para lo cual debe cumplir una serie de requerimientos tanto en equipos, como en versiones de IOS mínimas, las cuales esta detallado en el capítulo dos del documento, en la tabla 4-3 se describe los equipos disponibles en la infraestructura y su compatibilidad con Cisco ISE. Mediante la cual se observa que los dispositivos de la infraestructura actual están dentro de los modelos de equipos, al igual que su versión de IOS recomendados por Cisco para la integración con la tecnología ISE.

Tabla 4-3: Factibilidad Técnica

Componente	Versión de iOS	Observaciones
Switch Cisco Nexus N9K-C9504	v 7.0(3)|1(1)	Satisface el tipo de equipo y su versión IOS
Switch Cisco Catalyst C-4507R	IOS 15.2.2 E5	Satisface el tipo de equipo y su versión IOS
FireWall ASA Cisco 5545	ASA 9.2.1	Satisface el tipo de equipo y su versión IOS
WLC Cisco AIR-CT5508-100-K9	AirOS 8.0.140.0	Satisface el tipo de equipo y su versión IOS
WLC Cisco AIR-WLC4404	AirOS 7.0.252.0	Satisface el tipo de equipo y su versión IOS
Switch Cisco Catalyst 3850	IOS-XE 3.6.5E	Satisface el tipo de equipo y su versión IOS
Switch Cisco Catalyst 2960-S	IOS 15.0.2 SE	Satisface el tipo de equipo y su versión IOS
Switch Cisco Catalyst 2960-SF	IOS 15.0(2)SE7	Satisface el tipo de equipo y su versión IOS
AIR AP Cisco 2700	_____	Satisface el tipo de equipo (IOS otorgado desde la WLC)
AP Cisco 1550 MESH	_____	Satisface el tipo de equipo (IOS otorgado desde la WLC

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

3.9 Análisis de costos

Este análisis de costos se basa en el valor que costará la implementación de ISE a la institución, cabe mencionar que este estudio no tiene fines de lucro, sino el mejoramiento del servicio a toda la comunidad de la Escuela Superior Politécnica de Chimborazo. A continuación, se muestra los costos de la propuesta.

- En la tabla 5-3 se muestra los Costos de equipos.

Tabla 5-3: Costo de ISE

Ítem	Descripción	Cantidad	Valor Unitario	Valor Total
1	Cisco Identity Services Engine VM-5 VM MBunble (eDelivery)	1	19.420,21 $	19.420,21 $

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

- Costos de licencias

Cabe recalcar que el licenciamiento viene por defecto para el uso de redes cableadas, inalámbricas y VPNs, para lo cual se ha tomado en cuenta la proforma original brindada por la empresa proveedora de servicios para el DTIC, en donde se especifica que la licencia es para 10.000 usuarios. La tabla 6-3 muestra el valor de la licencia a implementar las cuales son licencias permanentes que tienen una garantía de dos meses.

Tabla 6-3: Costo de las licencias de ISE

Licencia	**Detalle**	**Cantidad**	**Costo Unitario**	**Costo Total**
L-ISE-TACACS=	Cisco ISE Device Admin License	1	4.000,00 $	4.000,00 $
L-ISE-BSE-10K	Cisco Identity Services Engine 10000 EndPoints Base License	1	25.000,00 $	25.000,00 $
			TOTAL	29.000,00 $

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

- En la tabla 7-3 se muestra el Costo de Instalación.

Tabla 7-3: Costo de instalación

Descripción	**Cantidad**	**Horas**	**Total**
Configuración de equipos existentes para integrar con ISE	1	120	7.040,00 $
Desarrollo ISE	1	160	3.520,00 $
Despliegue ISE	1	320	7.040,00 $
		TOTAL	17.600,00 $

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

- Costo Total

El costo final del proyecto que representaría para la institución implementar Cisco ISE se muestra a continuación, en la tabla 8-3:

Tabla 8-3: Costo total

Descripción	Valor Total
Costos de equipos	19.420,21 $
Costo de licencias	29.000,00 $
Costo de Instalación	17.600,00 $
TOTAL	66.020,21 $

Realizado por: MIRANDA Oscar & MORALES Oscar, 2017

CONCLUSIONES

Cumpliendo con los objetivos propuestos y las respectivas pruebas que se realizaron durante el estudio de la tecnología Cisco ISE se pudo concluir:

- Las redes inalámbricas difundidas en la Espoch cuentan con deficiencias de seguridad, como son la proliferación de dispositivos que no son administrados y menos aún de confianza, así también tenemos que el direccionamiento para todos los usuarios se lo realiza en el mismo segmento de red, sin establecer políticas de seguridad para cada tipo de usuario existente, las mismas brindan muchos riesgos tanto para el usuario como para la institución, por lo que al utilizar el protocolo de Autenticación 802.1X conjuntamente con la tecnología ISE, de la infraestructura wlan de la Espoch, brinda una mejora inminente en seguridad. La cual ayuda a controlar a que usuarios no autorizados tengan acceso, o libre navegación por la red, por tanto fue necesario utilizar el método de seguridad PEAP el cual brinda una mayor seguridad al establecer un túnel TLS y de igual manera maneja validación de certificados de autorización por medio de Active Directory, de esta manera solo personal que conste como usuario de confianza accederá a la red.
- ISE al ser una tecnología estrictamente de seguridad maneja todo tipo de autorización, por lo cual es indispensable el manejo de certificados, los cuales son validados por un repositorio externo o por el mismo ISE. De esta manera es un tema importante a la hora de la configuración, ya que es un requisito para el acceso, de lo contrario puede producir varios inconvenientes en la infraestructura.
- Mediante la configuración de RADIUS la autenticación se la realizó por medio de Active Directoy dados por los grupos de usuarios, la autorización nos permite asignar vlans dinámicas, y la auditoria maneja los parámetros nombrados como quién, qué, cómo y cuándo los cuales son la identidad del usuario, dispositivo y el momento de la conexión.
- Al momento de estudiar la infraestructura actual de la Espoch, se determinó que se cuenta con un 95% de equipos de la marca Cisco, gracias a lo cual se pudo definir que el proyecto es viable para ser aplicado en la red inalámbrica de la Espoch y así aprovechar en su totalidad todas los beneficios que nos otorga la tecnología ISE.
- De los resultados obtenidos en las pruebas de topología se determinó que el protocolo 802.1X con ISE permitió controlar el acceso de una manera eficiente por medio de estrictas políticas de seguridad al no permitir el acceso a la red cuando una autenticación falla o no cumple con los parámetros establecidos en las políticas.

- Con la tecnología ISE se observó en un 100% el status de todos los dispositivos de los usuarios, conociendo así la postura de los dispositivos, credenciales usadas para el acceso, hora de conexión y demás, para poder autenticarlo y autorizarlo a la red.
- La guía de implementación y configuración de ISE para el DTIC de la Espoch posee los pasos y parámetros más importantes a tomar en cuenta en la configuración de ISE, la cual posee información importante sobre el manejo de certificados y detalles a tener muy en cuenta para el manejo de esta tecnología.

RECOMENDACIONES

- Se recomienda que el estudio realizado sea aplicado tanto en redes wlan, cableadas y en VPNs, ya que al utilizar el protocolo 802.1X busca una autenticación por cada puerto existente, la cual puede ser aplicada a políticas de seguridad de acuerdo a las necesidades de la institución.
- Se recomienda que toda la infraestructura pertenezca a un dominio de Active Directory pues de esta manera se evita el problema de instalación de certificados manualmente, ya que estos son enviados a los dispositivos al solo pertenecer al dominio, de la misma forma la configuración del SSID puede ser automática por medio de políticas de grupos que maneja Active Directory.
- Es recomendable que para el uso de ISE hay que tener un conocimiento moderado en tema de Active Directory, especialmente en el uso de certificados digitales de seguridad.
- Es recomendable tener una infraestructura netamente de Cisco, desde la capa de core hasta la capa de acceso, pues de esta manera se puede aprovechar todas las ventajas que brinda la tecnología ISE como son descargar ACLs, asignación de vlans dinámicas, reautenticación, uso de VPNs por medio de ASA, ya que al no poseer la infraestructura de Cisco se limita las bondades que ofrece ISE.

GLOSARIO

802.1X	Norma de IEEE para el control de acceso a la red.
AAA	Autenticación, Autorización, Auditoria
AD	Active Directory
AD DS	Active Directory Domain Service
AD CS	Active Directory Certificate Services
AP	Access Point
ARP	Protocolo de resolución de direcciones
BYOD	Bring Your Own Device
CA	Certificate Authority
CUWN	Red Inalámbrica Unificada de Cisco
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DTIC	Dirección de Tecnologías de la Información y Comunicación
EAP	Extensible Authentication Protocol
EDUROAM	Education Roaming
ETSI	European Telecommunications Standards Institute
HTTP	Hypertext Transfer Protocol
HiperLAN2	High Performance Radio LAN 2.0
IDFW	Firewall de identidad
IP	Protocolo de internet
ISE	Identity Services Engine
LAN	Local Area Network
LAP	Lightweight Access Point
MAC	Media Access Control
MAB	MAC Authentication Bypass
OU	Unidades Organizativas
PDC	Primary domain controller
PSN	Nodo de servicio de políticas
SO	Sistema Operativo
SSID	Service Set Identifier
SGACL	Security Group ACLs
SGT	Security Group Tags
VPN	Virtual Private Network

WAP	Wireless Application Protocol
WEP	Wired Equivalent Protocol
WECA	Wireless Ethernet Compatibility Alliance
WLAN	Wireless Local Area Network
WLC	Wireless Lan Controler
WPA2	Wi-Fi Protected Access 2

BIBLIOGRAFÍA

- **CCM.** *WLAN LAN inalámbrico*. [En línea] 2016. [Citado el: 10 de Julio de 2016.]. Disponible en: http://es.ccm.net/contents/817-wlan-lan-inalambrica

- **CCM.** *Introducción a Wi-Fi (802.11 o Wi-Fi)* [En línea] [Citado el: 10 de Julio de 2016.] Disponible en: http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi

- **CISCO.** *Regulador del Wireless LAN (WLC) FAQ*. [En línea] 2009. [Citado el: 06 de Noviembre de 2016.] Disponible en: http://www.cisco.com/c/es_mx/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html

- **DESITEL-ESPOCH.** *SISTEMA DE AUTENTICACION WIRELESS ESPOCH-SAWE*. [En línea] 2010. pp. 2 [Citado el: 06 de Mayo de 2016.] Disponible en: http://oldwww.espoch.edu.ec/Descargas/sawe.pdf

- **GEIER, J.** **"***Implementing 802.1X Security Solutions for Wired and Wireless Networks."*. Indianapolis – Estados Unidos: Wiley Publising, Inc, 2008, pp. 33-40.

- **LEHEMBRE, G.** **"***Seguridad Wi-Fi – WEP, WPA y WPA2"*. Indianapolis – Estados Unidos, 2006, pp. 17-22. [Citado el: 30 de Abril de 2016.] Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

- **LEXMARK.** *¿Qué es un SSID?* [En línea] 2016. [Citado el: 28 de Abril de 2016.] Disponible en: http://www.cryptoman.com/storage/Pubs/es/ntwk_guide/what-is-ssid-topic.html

- **MARRIAS, Y.** *Introducción al Active Directory* [En línea] 2011. [Citado el: 06 de Mayo de 2016.] Disponible en: http://es.slideshare.net/YulitzaYanetMarrias/active-directory-9953103

- **OLGUÍN GONZÁLEZ, ARTURO.** Wireless Lan Controller (WLC) [En línea] (tesis) (Ingeniería). Universidad Tecnológica de Querétaro, Querétaro, México.2011. pp.11-12. [Consulta: 2016-09-23]. Disponible en: http://www.uteq.edu.mx/tesis/ITIC/079.pdf

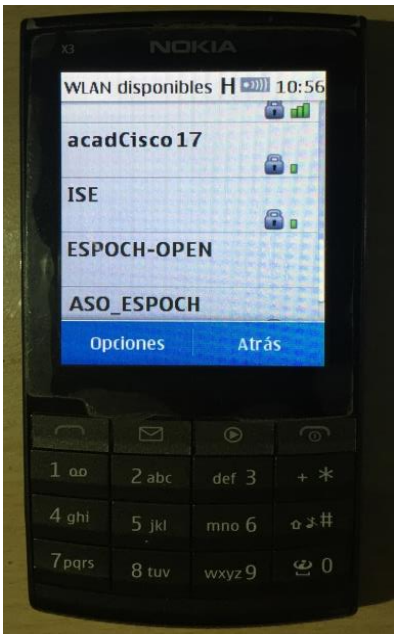
- **ORDENADORES Y PORTÁTILES.** *¿Qué es el directorio activo de Windows?*. [En línea] 2014. [Citado el: 12 de Mayo de 2016.] Disponible en: http://www.ordenadores-y-portatiles.com/directorio-activo.html

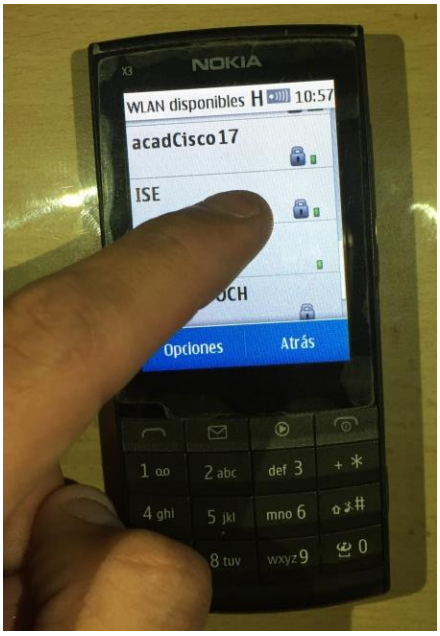
- **PANDA SOFTWARE INTERNATIONAL, S.L.** *Seguridad en redes Inalámbricas* [En línea] 2005 pp. 9 Disponible en: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

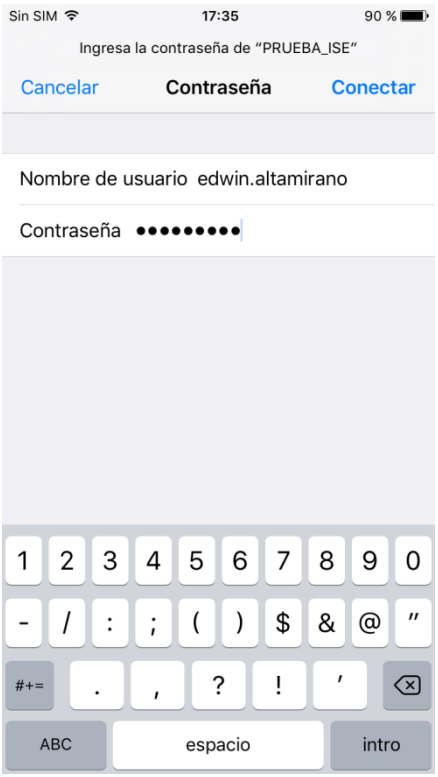
- **STALLINGS, W. "***Wireless Communications and Networks."*.2da Edición. New Jersey – Estados Unidos: Pearson Prentice Hall, 2005, p 453.

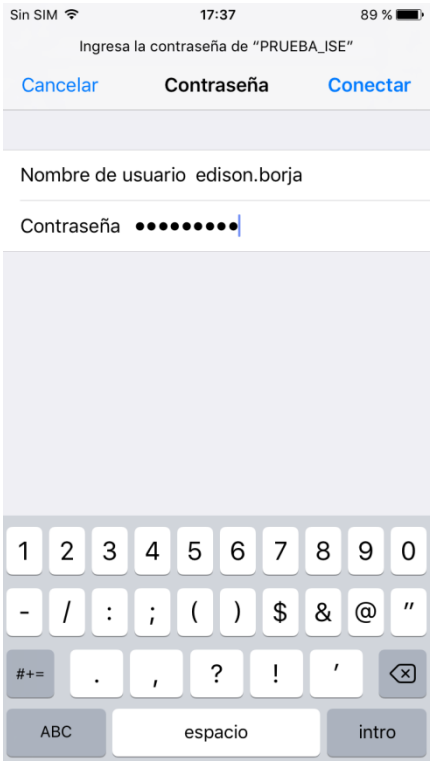
ANEXOS

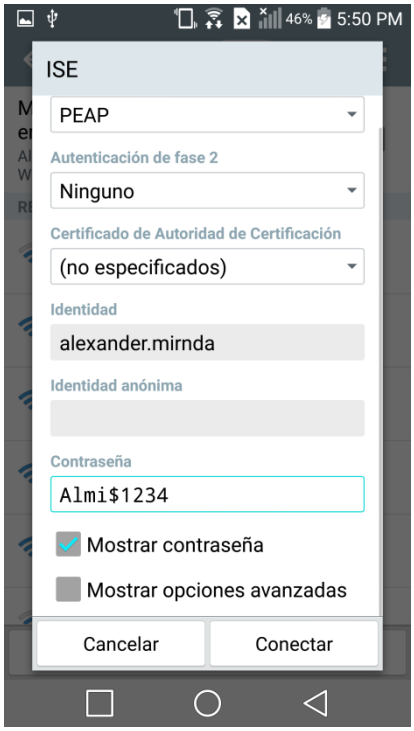
ANEXO A. CAPTURAS EN DISPOSITIVOS FINALES DE PRUEBAS



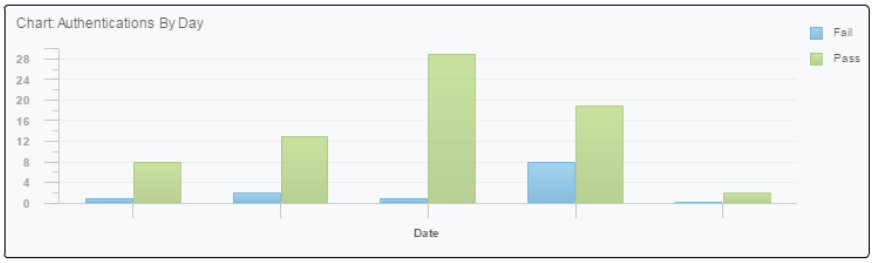



Sin SIM
17:35
90 %
Ingresa la contraseña de “PRUEBA_ISE”
Cancelar
Contraseña
Conectar
Nombre de usuario edwin.altamirano
Contraseña
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ ”
#+= . , ? ! ’
ABC
espacio
intro


Sin SIM
17:37
89 %
Ingresa la contraseña de “PRUEBA_ISE”
Cancelar
Contraseña
Conectar
Nombre de usuario edison.borja
Contraseña
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ ”
#+= . , ? ! ’
ABC
espacio
intro

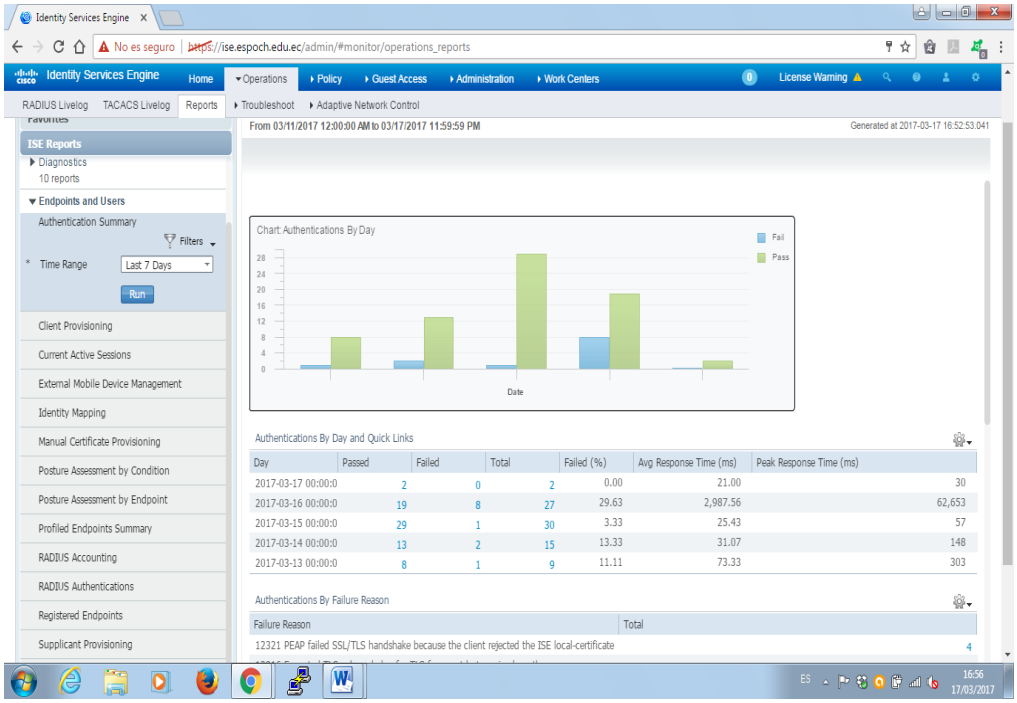

46% 5:50 PM
ISE
PEAP
Autenticación de fase 2
Ninguno
Certificado de Autoridad de Certificación
(no especificados)
Identidad
alexander.mirnda
Identidad anónima
Contraseña
Almi$1234
Mostrar contraseña
Mostrar opciones avanzadas
Cancelar
Conectar

ANEXO B. ESTADÍSTICAS DE CONEXIONES BRINDADAS POR ISE

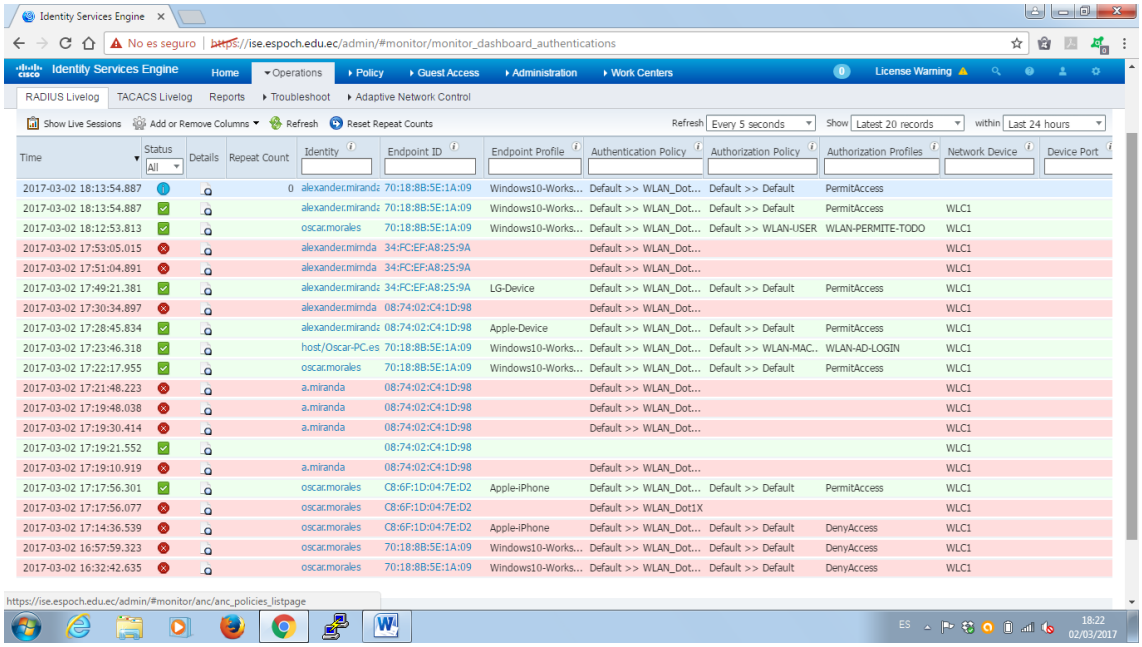


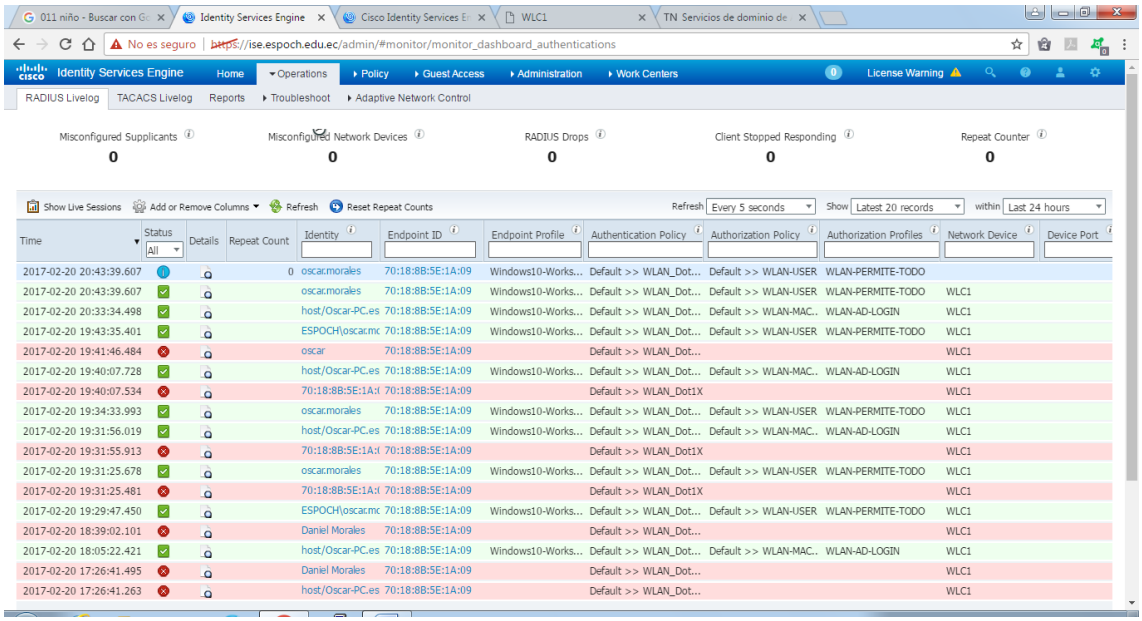
Authentications By Day and Quick Links

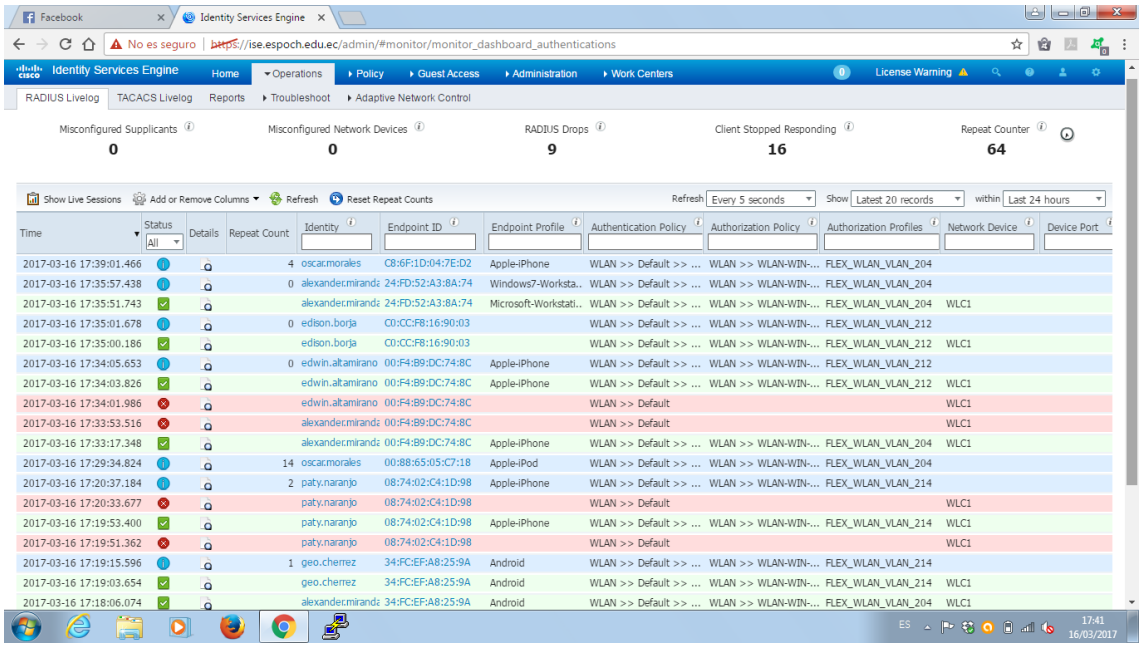
Day	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
2017-03-17 00:00:0	2	0	2	0.00	21.00	30
2017-03-16 00:00:0	19	8	27	29.63	2,987.56	62,653
2017-03-15 00:00:0	29	1	30	3.33	25.43	57
2017-03-14 00:00:0	13	2	15	13.33	31.07	148
2017-03-13 00:00:0	8	1	9	11.11	73.33	303



ANEXO C. CONTROL DE AUTENTICACIÓN POR MEDIO DE RADIUS






Facebook
Identity Services Engine
No es seguro | https://ise.espoch.edu.ec/admin/#monitor/monitor_dashboard_authentications
Identity Services Engine
Home
Operations
Policy
Guest Access
Administration
Work Centers
License Warning
RADIUS Livelog
TACACS Livelog
Reports
Troubleshoot
Adaptive Network Control
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
9
Client Stopped Responding
16
Repeat Counter
64
Show Live Sessions
Add or Remove Columns
Refresh
Reset Repeat Counts
Refresh Every 5 seconds
Show Latest 20 records
within Last 24 hours
Time
Status
Details
Repeat Count
Identity
Endpoint ID
Endpoint Profile
Authentication Policy
Authorization Policy
Authorization Profiles
Network Device
Device Port
2017-03-16 17:39:01.466 4 oscar.morales C8:6F:1D:04:7E:D2 Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204
2017-03-16 17:35:57.438 0 alexander.miranda 24:FD:52:A3:8A:74 Windows7-Worksta.. WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204
2017-03-16 17:35:51.743 alexander.miranda 24:FD:52:A3:8A:74 Microsoft-Workstati.. WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204 WLC1
2017-03-16 17:35:01.678 0 edison.borja C0:CC:F8:16:90:03 WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_212
2017-03-16 17:35:00.186 edison.borja C0:CC:F8:16:90:03 WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_212 WLC1
2017-03-16 17:34:05.653 0 edwin.altamirano 00:F4:B9:DC:74:8C Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_212
2017-03-16 17:34:03.826 edwin.altamirano 00:F4:B9:DC:74:8C Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_212 WLC1
2017-03-16 17:34:01.986 edwin.altamirano 00:F4:B9:DC:74:8C WLAN >> Default WLC1
2017-03-16 17:33:53.516 alexander.miranda 00:F4:B9:DC:74:8C WLAN >> Default WLC1
2017-03-16 17:33:17.348 alexander.miranda 00:F4:B9:DC:74:8C Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204 WLC1
2017-03-16 17:29:34.824 14 oscar.morales 00:88:65:05:C7:18 Apple-iPod WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204
2017-03-16 17:20:37.184 2 paty.naranjo 08:74:02:C4:1D:98 Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_214
2017-03-16 17:20:33.677 paty.naranjo 08:74:02:C4:1D:98 WLAN >> Default WLC1
2017-03-16 17:19:53.400 paty.naranjo 08:74:02:C4:1D:98 Apple-iPhone WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_214 WLC1
2017-03-16 17:19:51.362 paty.naranjo 08:74:02:C4:1D:98 WLAN >> Default WLC1
2017-03-16 17:19:15.596 1 geo.cherrez 34:FC:EF:A8:25:9A Android WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_214
2017-03-16 17:19:03.654 geo.cherrez 34:FC:EF:A8:25:9A Android WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_214 WLC1
2017-03-16 17:18:06.074 alexander.miranda 34:FC:EF:A8:25:9A Android WLAN >> Default >> ... WLAN >> WLAN-WIN-... FLEX_WLAN_VLAN_204 WLC1
ES
17:41
16/03/2017