FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

TRABAJO DE TITULACION PREVIO A LA OBTENCIÓN DEL TÍTULO DE MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN. MENCIÓN REDES DE COMUNICACIONES

“Estudio de la Tecnología NAC para mejorar la seguridad en redes de área local”.

Caso de estudio: Cooperativa de la Policía Nacional Agencia Matriz.

AUTOR: WALTER DAVID CANDELA QUIJIJE

Quito / Octubre - 2020

Tabla de Contenidos

Índice de figuras.

Índice de tablas

Índice de Gráficos

AGRADECIMIENTO

Quiero empezar dando gracias al ser Supremo gestor de mi vida y actitudes, a la Cooperativa Policia Nacional, al Ing. Pedro Victoria y a la Ing. Sabrina Cevallos por brindarme el espacio y apertura para el desarrollo de la investigacion realizada. A la Pontificia Universidad Católica de Quito y a los distintos catedraticos quienes me impartieron sus conocimientos con el fin de conseguir el honroso titulo.

WALTER CANDELA QUIJIJE

DEDICATORIA

A Dios supremo por concederme la dicha de vivir.

A mi papi Jose D.Quijije Ch. quien desde el cielo guia mis pasos. A mi mami Rita, a mi madre, hermano, a mi compañera de vida y a mi hija, motor principal en todo lo relacionado a mi progreso.

WALTER CANDELA QUIJIJE

INTRODUCCIÓN

El siguiente documento está enfocado al estudio de la tecnología NAC para mejorar la seguridad de la redes de área local, mediante el control de acceso aplicando políticas a usuarios y dispositivos.

La Cooperativa de la Policía Nacional se caracteriza por estar a la vanguardia del desarrollo tecnológico, con el fin de controlar el acceso a la red y aportar al crecimiento tecnológico de la institución es necesario conocer la tecnología NAC y el proceso adecuado.

El siguiente documento está dividido en cinco capítulos, la investigación es de tipo descriptiva aplicada, a continuación se describe los aspectos relevantes de cada capítulo:

El Capítulo I, contempla información relacionada a la recolección bibliográfica sobre la institución, Seguridad Informática, norma ISO27001, seguridad en redes, y el Network Access Control (NAC).

El Capítulo II, Se detallan los aspectos encontrados del estudio de campo sobre el estado actual de la red, se realiza el análisis técnico respectivo en base a tres pilares Autorización, Auditabilidad, Autenticación.

El Capítulo III, Se realiza el análisis y selección de la tecnología NAC adecuada para la infraestructura tecnológica de la CPN, también se menciona los integrantes y configuración de la Tecnología.

El Capítulo IV, En base a la tecnología NAC seleccionada, se realiza el despliegue de la tecnología NAC y el proceso de autentificación.

El Capítulo V, Se desarrolla la evaluación del prototipo en base a la metodología de investigación utilizada y los tres pilares referentes a seguridad en redes, los indicadores son Autorización, Auditabilidad, Autenticación.

Por último se realiza las conclusiones y recomendaciones fruto de la investigación realizada.

OBJETIVOS

Objetivos General.

Estudiar la Tecnología ***NAC*** para mejorar la seguridad en redes de área local en una organización. Caso de estudio “CPN Agencia Matriz”

Objetivos Específicos.

- ✓ Determinar la tecnología ***NAC*** y sus diferentes soluciones.
- ✓ Analizar la situación actual de la red ***CPN*** Matriz.
- ✓ Realizar la demostración de Tecnología ***NAC*** seleccionada mediante un prototipo
- ✓ Evaluar los resultados de la tecnología ***NAC*** en la red de área local.

Problemática

Pregunta de investigación Principal.

¿En la ***CPN***[1] se tiene un control de acceso a la red óptimo?

Preguntas de investigación Secundarias.

¿Existen riesgos al no controlar el acceso a la red?
¿Es necesario controlar el acceso a la Red?
¿Se tiene políticas de control de acceso a la red?
¿Cuál es la importancia de contar con tecnología ***[2]NAC*** en la red?

En la ***CPN*** se ha detectado que al momento no se tiene un control de acceso óptimo a la red, es decir no se cuenta con tecnología de control de acceso de manera centralizada, que permita verificar los dispositivos que están conectados a la red, lo que ocasiona que no se tenga una administración adecuada de los dispositivos que se conectan a la red ni su comportamiento dentro de la misma, provocando problemas de inseguridad.

En la actualidad existen riegos en la red a no tener control en el punto de acceso, esto podría dejar expuesta a la red a ***hackeos*** o extracciones de datos. En la CPN se utiliza el control de oficinas remotas y se maneja información de suma relevancia misma que debe estar segura, en la actualidad puede existir riegos de infección de la red, también se puede exponer la información de la institución cuando no se tiene un control de seguridad óptimo, más aun cuando no se logra identificar los dispositivos que se conectan a la red, el comportamiento y el tiempo de conexión en la misma.

[1] CPN Cooperativa de la Policía Nacional
[2] NAC Control de acceso a la red

En el ámbito de comunicaciones se debe tener un control adecuado tanto en dispositivos conectados a la red y los respectivos puntos de acceso, al no haber un control adecuado esto provocarían problemas de inseguridad permitiendo hacer uso de la red de manera irresponsable, de esta manera se estaría exponiendo la información de la institución y también se podría infectar la red lo que afectaría la comunicación adecuada, todos aquellos riesgo se deben a que no están establecidas políticas que regulen los accesos y permisos dentro de la red.

En la ***CPN*** no existen políticas de acceso homogéneos, no se detecta el comportamiento del dispositivo conectado, más aún si está infectando la red. No se tiene perfiles definidos ni se tiene requisitos de conexión a la red.

La institución no cuenta con tecnología que permita controlar la seguridad de la red mediante el acceso de los dispositivos, es decir que adopten políticas de seguridad que permitan regular el comportamiento y acceso a la red, garantizando un uso adecuado de la red y sus recursos.

Antecedentes

El estudio realizado por (Esmoris, 2014). Describe la importancia que tiene la tecnología ***NAC*** en las empresas que cada vez tienen más redes distribuidas en diferentes oficinas y centros de atención.

El informe realizado por (Fortinet, 2018) respecto a la tecnología ***NAC*** señala que se ha convertido en una tecnología referente para el control de acceso a la red, en cuanto a la manera automática de administrar la seguridad, a través del cumplimiento de políticas lo cual aporta con el fin de tener un control de acceso adecuado en la red.

(Jimenez Perez & Joanny, 2017) Mencionan a la tecnología ***NAC*** como la solución para la seguridad de la red, en aspectos técnicos de la funcionalidad es la encargada de controlar a los dispositivos que intentan acceder a la red mediante políticas de seguridad para cualquier tipo de acceso a la red; redes inalámbricas, red de área local, redes de accesos remotos. Debido a que esta tecnología contempla cualquier medio de acceso.

De los estudios anteriores se concluye que la tecnología ***NAC*** mediante la aplicación de políticas de seguridad tiene gran impacto en la administración de redes, debido a su importancia siendo un referente en organizaciones, permitiendo establecer un control integral al acceder a la red por parte de los dispositivos con el fin de garantizar la integridad de la información y los recursos de la red de una organización.

1. CAPÍTULO I

1. Fundamentos teóricos.

1.1 Información de la empresa.

La Cooperativa de Ahorro y Crédito Policía Nacional Ltda. Nace jurídicamente el 29 de Junio de 1976, gracias a un grupo visionario de 35 caballeros de la paz, el propósito común que los unió fue poder ayudar económicamente a sus compañeros policías a través de los beneficios que brinda una entidad cooperativista, por lo cual sustentándose en la filosofía de ayuda mutua y solidaria, encontraron la respuesta adecuada a las necesidades de crecimiento dentro de la Policía Nacional.

***Figura 1**. Institución (Ekos, 2018)*

La Cooperativa de Ahorro y Crédito Policía Nacional, conjuntamente con su equipo de trabajo, camina día a día a la excelencia para alcanzar los objetivos planteados, generando e innovando productos, servicios y beneficios para sus socios y clientes, satisfaciendo las necesidades financieras, mejorando su calidad de vida y crecimiento económico. Dirección de la Matriz Quito, Voz Andes 309 y Av. América.

Nuestra Cooperativa.

La Cooperativa de Ahorro y Crédito Policía Nacional, conjuntamente con su equipo de trabajo, camina día a día a la excelencia para alcanzar los objetivos planteados, generando e innovando productos, servicios y beneficios para sus socios y clientes, satisfaciendo las necesidades financieras, mejorando su calidad de vida y crecimiento económico.

Política de Calidad.

Brindar servicios financieros ágiles, seguros y confiables, comprometidos con mejorar la calidad de vida de socios, clientes y colaboradores, a través, de principios cooperativistas; impulsados por procesos efectivos, mejora continua y cumplimiento con los requisitos aplicables, alineados con la responsabilidad social.

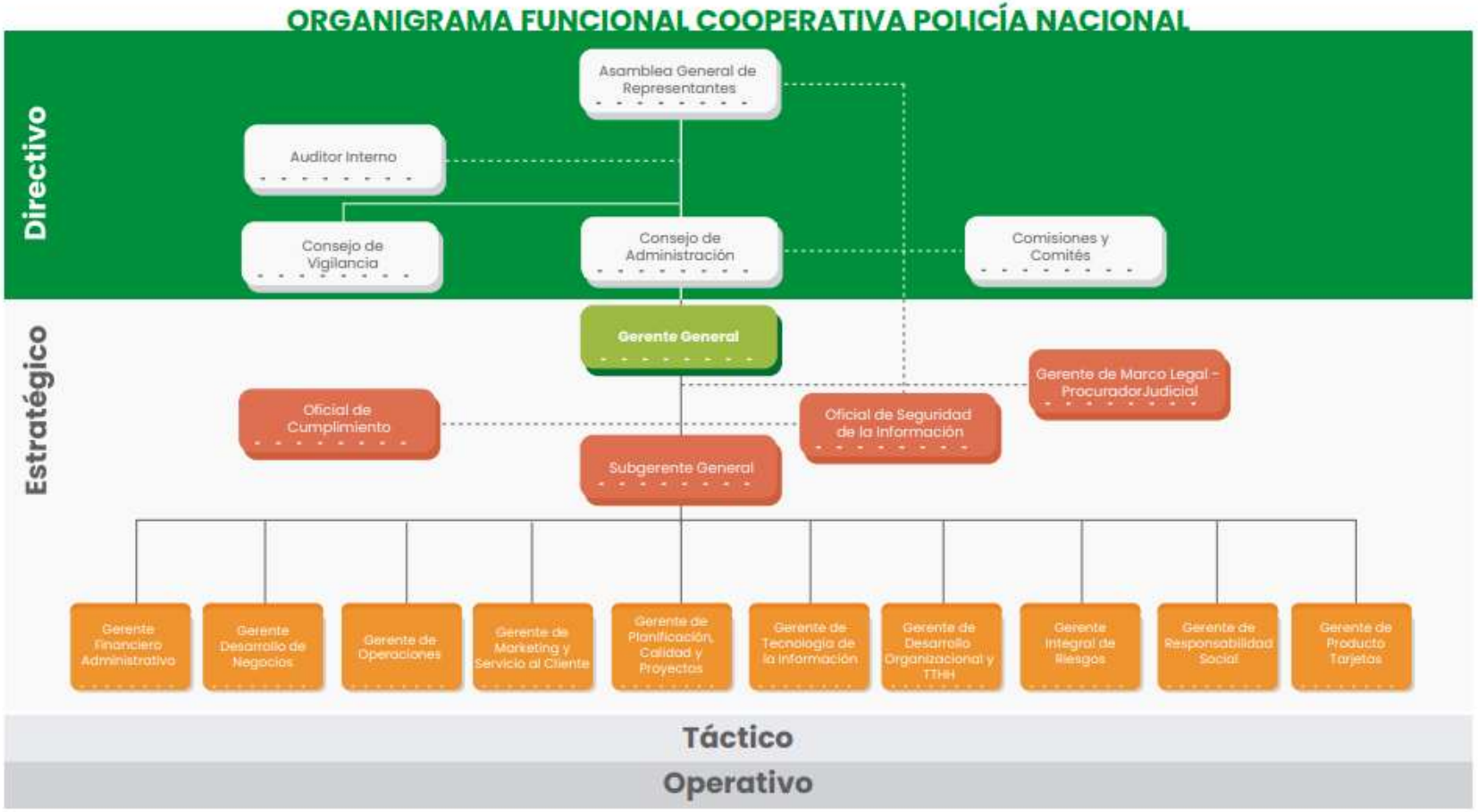

Figura 2. *Organigrama Organizacional (CPN, 2020)*

Misión.

Fomentamos el desarrollo económico y social de nuestros socios, clientes y colaboradores, brindando productos financieros innovadores, ágiles, seguros, oportunos y con servicio de excelencia, para mejorar su calidad de vida.

Visión.

En el 2020 seremos la Cooperativa pionera en la virtualización de productos y servicios financieros, integrando soluciones tecnológicas amigables para nuestros socios, clientes y colaboradores, donde cada contacto con nosotros sea una experiencia que supere sus expectativas.

1.2 ¿Qué es la Seguridad Informática?

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan con-llevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Vieites, 2015)

Figura 3. *Seguridad informática (Vieites, 2015)*

1.2.1 Concepto de autenticación.

La autentificación es un proceso de seguridad utilizado comúnmente en el ámbito de la informática, este proceso es utilizado para solicitar accesos ya sea a un aplicativo o portal web entre otros, permite validar la identidad de un usuario y confirmar la veracidad de la información ingresada, al ser validada la información como verdadera se permite el acceso caso contrario se niega la solicitud de acceso.

Existen varios tipos de autentificación, comúnmente se utiliza la autentificación mediante usuarios y contraseñas para ingresar a ciertos aplicativos informáticos, el inconveniente de esto es que de ser conocidos por otra persona puede obtener acceso sin ser el dueño de la cuenta por ejemplo de un correo electrónico. También existe la autentificación por medio de ***Tokens***, este tipo de autentificación se utiliza comúnmente para tarjeta de créditos, al ser utilizadas se generan números aleatorios o palabra claves que son enviada a un dispositivo móvil o correo para confirmar el proceso de autentificación. También se puede mencionar a la tarjetas inteligentes mismas que contiene cierta cantidad de información para realizar el proceso de autentificación, estas por ejemplo son usadas al momento de ingresar a una oficina son expuestas a un lector que valida la información y habilita el acceso.

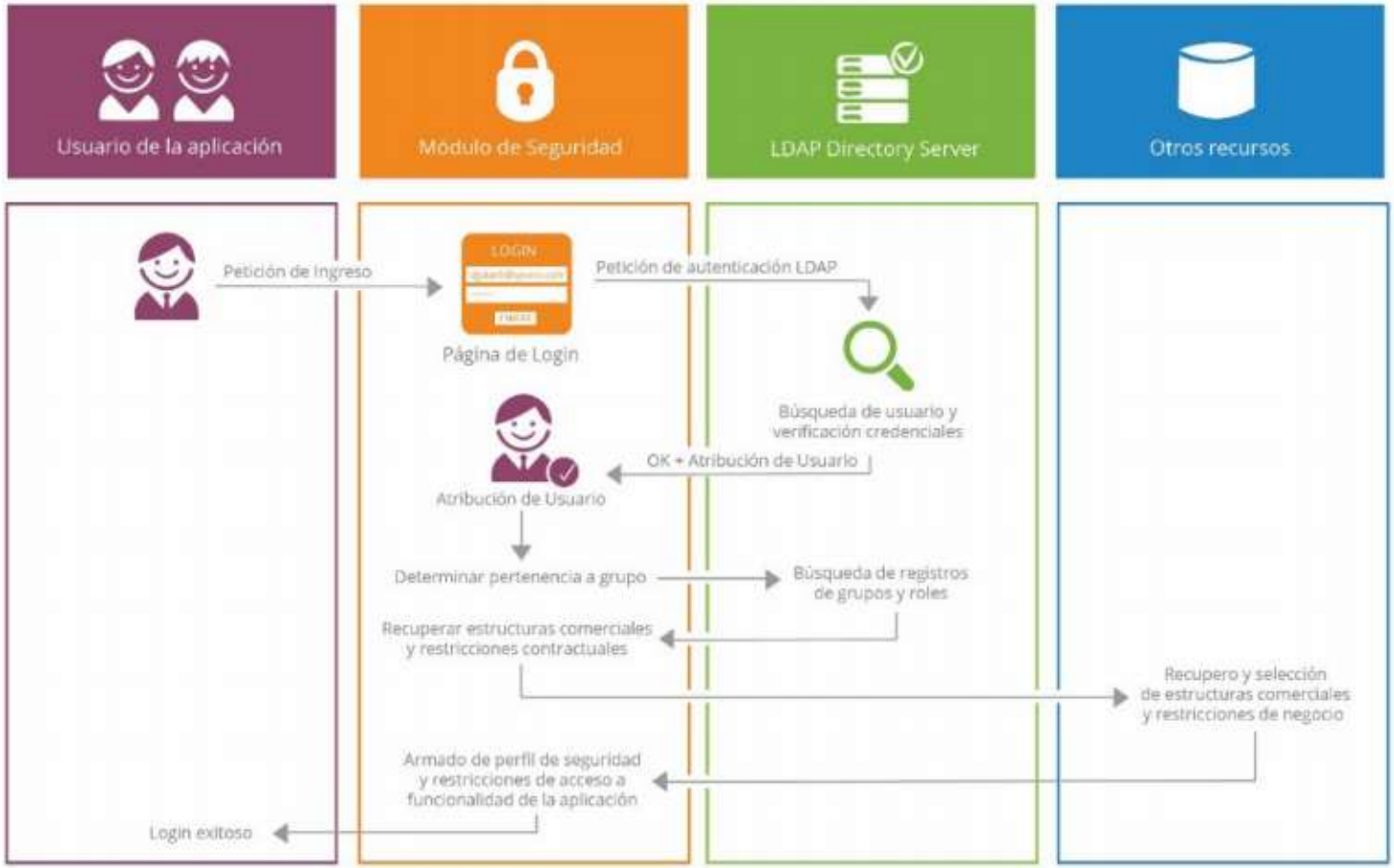

Figura 4. *Autenticación (Romero Castro, 2018)*

Los procesos de autentificación contemplan tres pilares: Los usuarios, la información y la infraestructura.

Los usuarios comúnmente son considerados como la parte más débil debido a que se puede olvidar de las credenciales de autentificación o dejarlas expuesta, puede sufrir un accidente o puede cometer un error echando a perder un trabajo o la información de mucho tiempo. Es por aquello que el sistema y la información deben ser protegidos del usuario mismo.

La información, en toda institución la información es considerara como oro y principal activo, es por aquello que debe ser protegida y tenerla a salvo.

La infraestructura es una parte importante para controlar y evitar riesgos que afecten a la información, aquí se deben manejar procesos complejos para evitar por ejemplo alteraciones o robo de equipos, desastres naturales etc.

1.2.2 Los tres pilares de la seguridad.

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía. Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo. La Figura 4 muestra los principales pilares de la seguridad de la información (Romero Castro, 2018).

Figura 5. *Pilares de la seguridad (Romero Castro, 2018)*

Confidencialidad: Este pilar consiste en restringir la información o recursos para que solo la persona que tenga previa autorización pueda acceder, este modelo es utilizado para que cada usuario solo realice las tareas encomendadas y acceda a cierta cantidad de información permitida. Para obtener un grado de confidencialidad efectivo se necesitan tres recursos:

Autentificación de usuarios: Esto es quien accede a la información y bajo que recurso.

Gestión de privilegios: En este aspecto la persona que obtiene un acceso a la información debe cumplir con ciertas restricciones de autorización, por ejemplo los permisos de una carpeta compartida pueden ser de lectura, escritura o ambos.

Confidencialidad. Significa asegurar que la información no se revele a personas no autorizadas y que se proteja los datos transmitidos contra ataques pasivos, como la intercepción. Garantiza que los datos no hayan sido alterados interna o externamente en el sistema. Hay varios niveles de protección del mensaje: En el servicio más amplio se protege todo los datos del usuario, transmitidos durante un periodo de tiempo. Formas más restringidas. Por ejemplo: la protección de determinado mensaje o parte de éste (García, 2020).

La integridad: Es otro pilar de seguridad, este se basa en garantizar que la información no sea alterada ni se pierda, debido que trabajar con información errónea afectaría considerablemente a cualquier institución derivando decisiones y procesos equivocados. Con el fin de proteger la integridad de la información se debe considerar aspectos como: realizar monitoreo de tráfico de red con el fin de verificar si no existe posibles irrupciones y también auditar los sistemas para identificar por quién, cuándo y que información fue utilizada.

Integridad. El objeto de la integridad de la información es proteger los datos evitando que sean modificados, alterados o borrados por personas sin autorización. Este servicio asegura que la información transmitida sólo podrá ser modificada por las partes autorizadas (García, 2020).

Disponibilidad: Para que la información sea útil se debe establecer procesos de accesos que no sean tediosos pero sin dejar de lado los aspectos de seguridad mínimos, todo aquello permite que se pueda acceder a la información requerida para que sea útil y valiosa en el momento oportuno, es decir la información debe estar accesible para personas autorizadas cuando sea necesaria.

1.2.3 Gestión de seguridad Activa.

La seguridad activa se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema. Ejemplo de seguridad activa los problemas encontrar en el empleo de contraseñas o claves de acceso, uso de antivirus, cortafuegos o firewall (Ramos, 2011).

La seguridad activa se basa en el uso de contraseñas, existen aspectos que se deben considerar en el uso de contraseñas para que sean más seguras y complejas tales como la longitud y el uso de caracteres especiales como símbolos, mayúsculas y números. Se debe evitar de usar en contraseñas nombres propios o palabras reales que se pueden encontrar en diccionarios, todo aquello con el fin de evitar que sea desencriptada fácilmente.

Figura 6.Entrada al sistema (Ramos, 2011)

1.3 Gestión de seguridad de la información con la norma ISO27001.

La ISO 27001 es una norma internacional de Seguridad de la Información que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan. Este estándar ha sido desarrollado por la Organización Internacional de Normalización ISO y por la Comisión Electrotécnica Internacional IEC (Universidad Internacional de la Rioja, 2019).

La norma ISO se basa en las políticas, procedimientos y procesos que se deben considerar en una organización con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

¿Qué es la gestión de seguridad de la red según la ISO 27001?

Normalmente las empresas pueden contar con red interna y externa. La gestión de la seguridad de la red se basa en los aspectos que se deben considerar para proteger la red y los datos ante riesgos tales como accesos no autorizados, mal utilización de los recursos de la red, divulgación de información y acceso a los ordenadores.

La gestión de seguridad de la red también puede hacer uso de otros controles para mejorar su eficacia, como puede ser la política de control de acceso, la gestión del cambio, la protección contra el malware y la gestión de vulnerabilidades técnicas. La verificación de los controles de red se puede realizar mediante auditorías periódicas y revisiones por parte de la dirección, lo que puede conducir a distintos controles y ajustes mediante las acciones correctivas o planes de mejora (ISO Tools Excellence, 2016).

La información es un activo que como otros es esencial para la operación y negocio de una organización, por tanto debe ser protegido adecuadamente. El riesgo es la medida de la probabilidad de que una amenaza aproveche una vulnerabilidad y consiga afectar a un activo de información (Guerra Mantilla, 2018).

1.4 Seguridad en Redes.

La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos (Waldo de la Ossa, pág. 13)**.**

- ✓ Autorización. Persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático.
- ✓ Auditabilidad. Permite registrar monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios.
- ✓ Autenticación. Es el proceso de verificar la identidad de los usuarios antes de dejarlos ingresar al sistema el cual se realiza confrontando la información recibida aquella almacenada en una base de datos. Provee la seguridad de la identidad de una entidad, entendiéndose como entidad a todo aquello capaz de producir o recibir información.

Control de acceso. La función principal del NAC es básicamente controlar el acceso a la red para evitar accesos no autorizados, el acceso no autorizado se refiere a la falta de permisos para hacer uso de la red y por ende acceder a recursos. Todo aquello con el fin de controlar accesos a computadoras y aplicaciones mediante la red y los enlaces de comunicaciones, para obtener acceso primero el usuario debe autentificarse para obtener los permisos respectivos.

RADIUS. Permite a los administradores de red administrar centralizadamente a los usuarios de acceso remoto, a los métodos de acceso y dar las restricciones de acceso. Esto permite una capacidad de auditoría centralizada, tal como el mantener un registro del volumen del tráfico enviado y la cantidad de tiempo en línea de cada usuario. RADIUS también fortalece las limitaciones de acceso remoto, como restricciones de acceso servidor o limitaciones en línea en cantidad de tiempo (García, 2020).

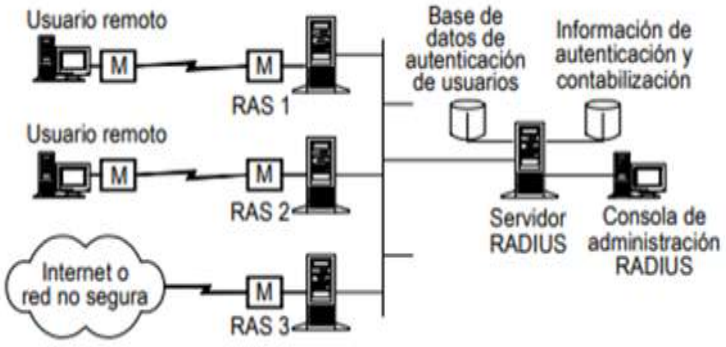

Figura 7. *Servicio de autentificación de usuarios remotos por Radius (García, 2020)*

RADIUS soporta una variedad de protocolos de autentificación entre ellos esta password (Password Authentication Procotol–PAB), de la misma manera el protocolo de autenticación de intercambio de retos (Challenge Handshake Authentication Protocol–CHAP) y también se puede realizar la autenticación de Token SecureID.

Autenticación por password – PAP.

El Protocolo de Autenticación por Password (Password Authentication Protocol–PAP), definido en la RFC 1334, provee un modo sencillo para que un par establezca su identidad recurriendo a un intercambio de información de dos pasos. Una vez que se ha completado la etapa de establecimiento del enlace, el par envía el Identificativo del usuario –Id– y el Password al autenticador hasta que el reconocimiento o que la conexión concluyan. El PAP no es un método de autenticación fuerte, pues los password son enviados por el enlace y no existe protección contra intentos de acceso mediante grabaciones de accesos anteriores (replay). Además, el par controla la frecuencia y la duración de los intentos (García, 2020).

Figura 8. *Mecanismo del PAP (García, 2020)*

Autenticación por confirmación de reto (chap).

El Protocolo de Autenticación por Confirmación de Reto (Challenge Handshake Authentication Protocol –CHAP), definido por la RFC 1334, provee un modo sencillo para que un par establezca su identidad mediante un intercambio de información de tres pasos. El CHAP, a diferencia del PAP, protege contra intentos de accesos mediante grabaciones de accesos anteriores a través del cambio frecuente de identificadores y de retos. Además, el autenticador tiene el control, la frecuencia y la duración de los retos. Este método de autenticación se basa en una clave secreta conocida únicamente por el autenticador y el par, lo cual evita la necesidad de enviarla por el enlace (García, 2020).

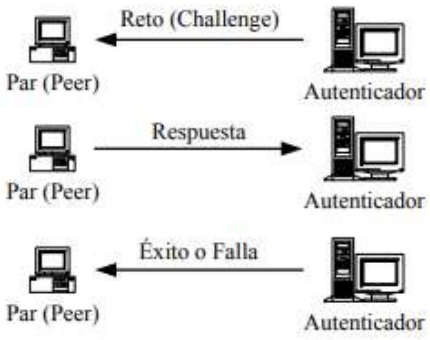

Figura 9. *Autentificación CHAP (García, 2020)*

1.5 Network Access Control (NAC).

El control de acceso a la red permite a los administradores automatizar la validación de las políticas previamente establecidas, con el fin de controlar el acceso y gestionar la seguridad de la red de una manera centralizada y automática.

Control de acceso a red (del inglés Network Access Control, NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificarla tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso (Murillo, 2020).

NAC le permite definir una política de seguridad integral para su red, implementar esa política en un servidor centralizado y hacer que la red haga cumplir automáticamente esa política en todos los usuarios de la red. ***NAC*** es mucho más que la autenticación de usuarios: también está diseñado para proteger la red de usuarios y dispositivos que pueden estar autorizados, pero que aún representan amenazas (Allied Telesis, 2016).

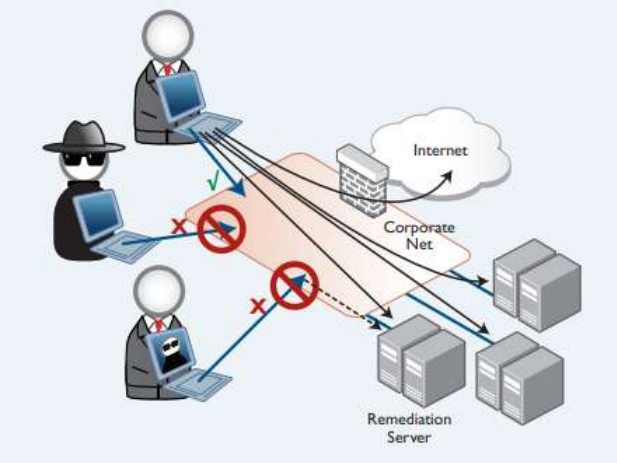

Figura 10. *Network Access Control (Allied Telesis, 2016)*

Los ***NAC*** de soluciones 802.1x funcionan primordialmente para autenticar al usuario en el acceso a la red. El objetivo de ***NAC*** es prevenir que los dispositivos que hayan sido contaminados, estén mal configurados o que presenten riesgos potenciales accedan a la red corporativa. ***NAC*** permite comprobar si una máquina o dispositivo cumple con los requisitos corporativos de configuración y seguridad antes de que acceda a la red, y que necesite un mecanismo para restringir el acceso si tal dispositivo viola las políticas de seguridad una vez admitido (Loredo, 2010).

NAC está diseñado como una solución global de control de acceso a la red que ofrece lo siguiente:

- ✓ Control de quién accede a la red y restricción del número de recursos con los que puede operar.
- ✓ Protección de red IP.

- ✓ Control del acceso de los usuarios no conocidos o con menos garantías de seguridad, como proveedores, clientes o usuarios remotos.
- ✓ Restricción del acceso a información.
- ✓ Control de los accesos en función del rol del usuario, hora del día, localización y aplicación.
- ✓ Segmentación de usuarios en función del cumplimiento normativo.
- ✓ Protección contra malware y virus, conocidos y desconocidos.
- ✓ Notificaciones sobre la vigencia y falta de parches sistemas operativos de las máquinas de los usuarios de la red.

Política de control de admisión de acceso.

El control de acceso a la red se define como una tecnología o arquitectura que permite controlar el acceso de los usuarios a la red en un punto de acceso verificando además de su identidad el cumplimiento de todas las políticas de seguridad establecidas por la organización (Esmoris, 2014).

1.5.1 Actores de un escenario NAC.

El acceso a la red se garantiza en base a la aplicación de políticas de seguridad, aquello gestiona los niveles de calidad y servicios remotos alcanzables por cada usuario autentificado en la red.

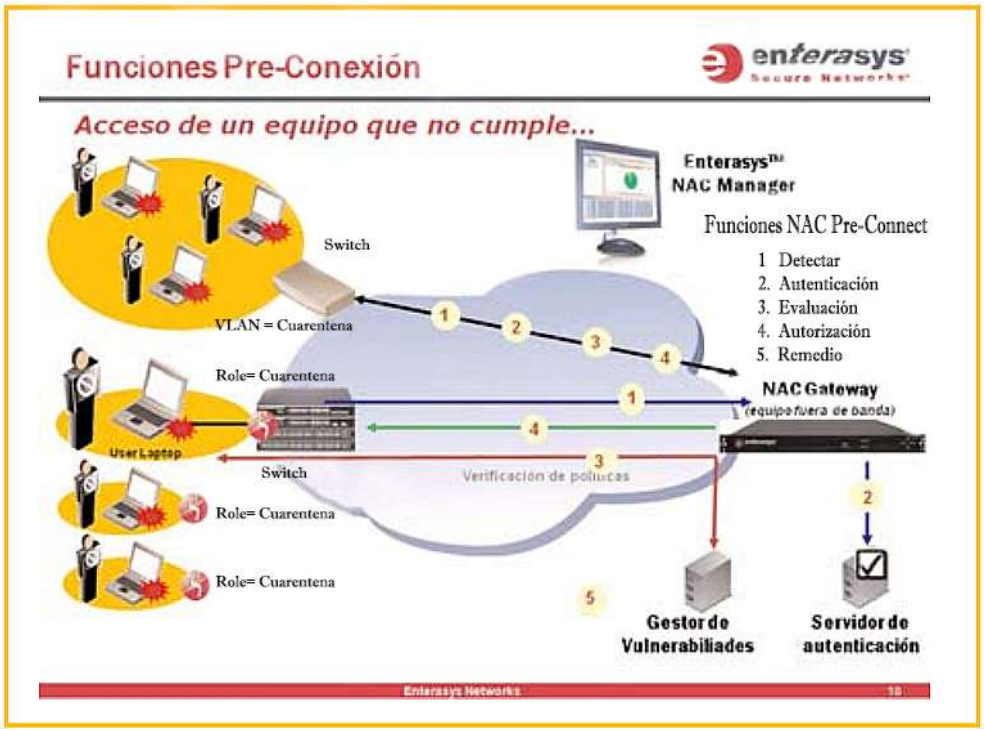

Figura 11. *Actores de un NAC (Bonete, 2008)*

La electrónica de red (1) detecta que existe un nuevo usuario intentando acceder a la red y realiza las funciones de (2) autenticación, actuando como intermediario en la validación de la identidad del usuario o del sistema que se conecta, ya estamos en disposición de conocer qué tipo de (3) evaluación debemos aplicar al dispositivo que pretende acceder a la red, la solución de ***NAC*** deberá contar con herramientas flexibles de (4) remediación. El remedio pasa por informar al usuario sobre cuál ha sido el motivo que le ha llevado a ser aislado con mediante una política de cuarentena. Por último, una vez se han subsanado los motivos que llevaron al usuario a una política de cuarentena, se procede a (5) autorizar el acceso a la red con el perfil correspondiente al usuario (Bonete, 2008).

1.5.2 Ámbito de aplicación de *NAC*.

La implementación de soluciones ***NAC*** permiten el despliegue aplicado al control de acceso por bloques o diferentes áreas, la implementación de NAC aborda el control de acceso tanto de los equipos externos que se conectan a la red y los equipos conectados en red LAN interna, los ámbitos de aplicación de NAC podría ser acometida de varias formas (Bonete, 2008).

Usuarios VPN: El ***NAC*** permite controlar a los usuarios que acceden de manera remota a la red, debido a que están en otras ubicaciones geográficas ya sea por temas de teletrabajo, estos usuarios generalmente realizan la conexión mediante (1) ***VPN***[3] LAN a LAN.

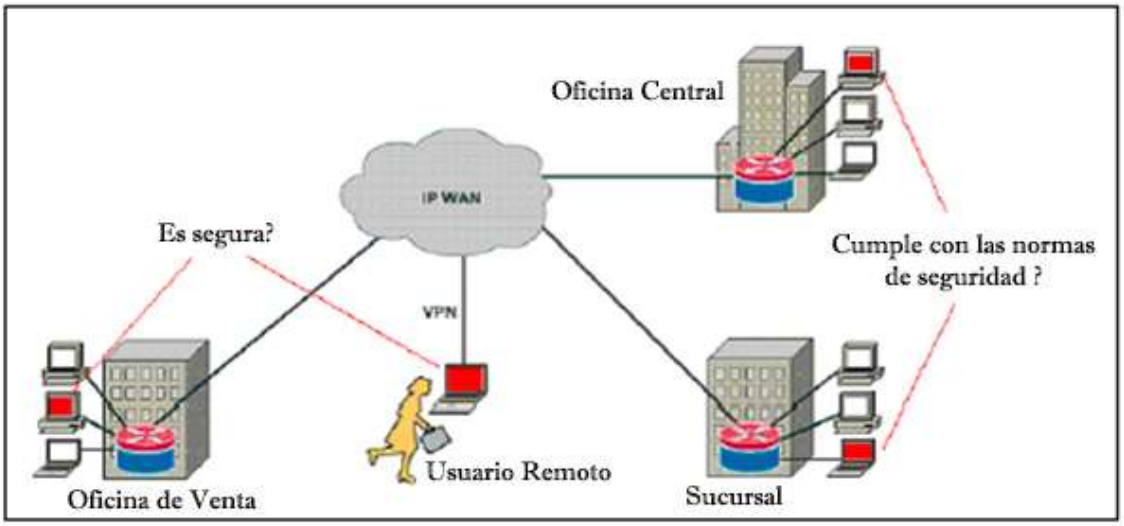

Figura 12. *Conexión usuarios VPN (Esmoris, 2014)*

Otro ámbito de uso del ***NAC*** es mediante el acceso de usuarios que utiliza el Wifi de la red (2). El despliegue de redes de Seguridad física dedicada para dispositivos de control de seguridad, aplicando autentificación y políticas para evitar que una persona no autorizada se conecte a esta red (3).

[3] VPN Red privada virtual

La solución de control de acceso ***NAC*** también se aplica en los centros de procesamiento de datos (4), en base a la aplicación de políticas basadas en ***MAC***[4], y aplicando políticas de acceso en los puertos, o en una agregación de puertos, de esta manera se controla el acceso a la red. Por ultimo también se aplica el control de acceso dentro de la misma red de la organización de los usuarios ***LAN***[5] (5).

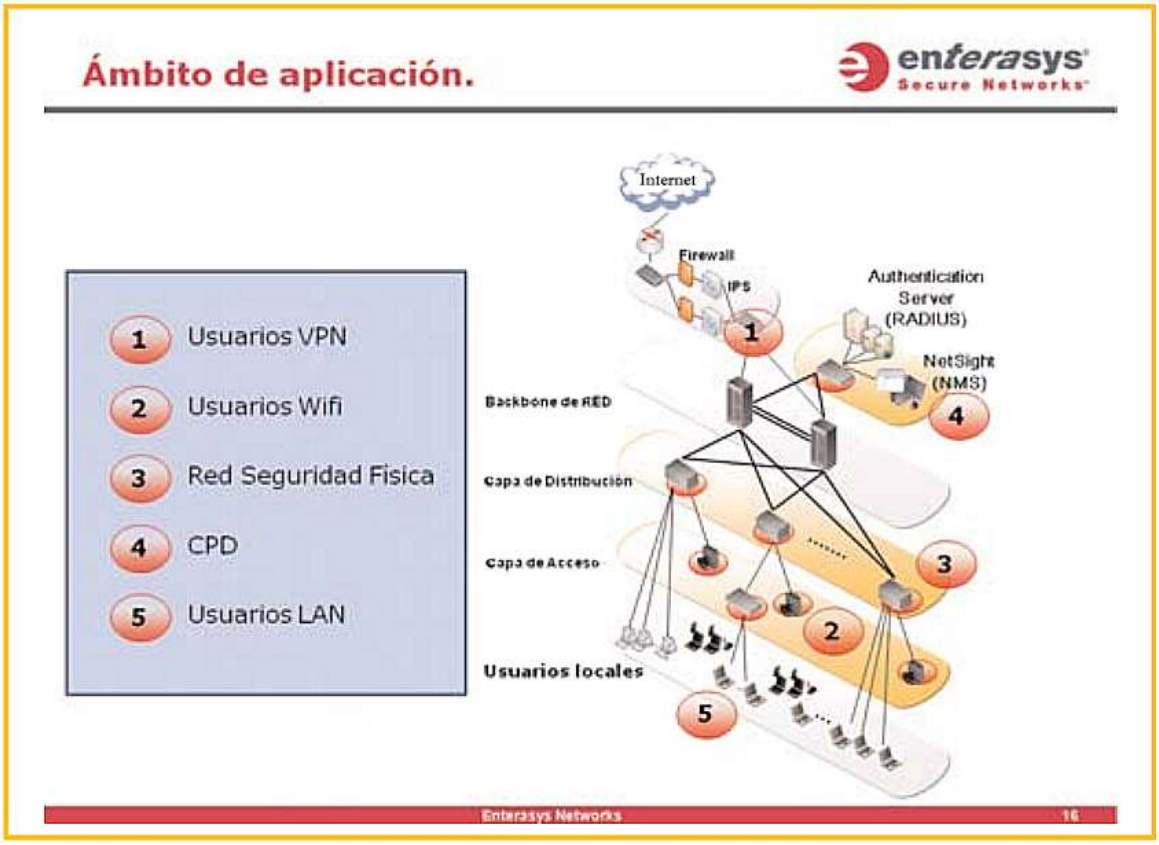

Figura 13. *Ámbitos de aplicación (Bonete, 2008)*

1.5.3 ¿Cómo trabajan las soluciones NAC actuales?

La soluciones ***NAC*** actuales consisten en controlar el acceso a la red de manera automática y centralizada mediante un servidor que gestione y administre las políticas previamente establecidas, también permite identificar los dispositivos y las actividades de los usuarios en la red con el fin de hacer cumplir restricciones del uso de la red. De esta manera se aumenta la productividad y se reduce un posible impacto de algún intruso. Las principales características de funcionamiento son:

- ✓ Descubre cada dispositivo conectado a la red y controla su comportamiento
- ✓ Adapta y configura la red dinámicamente y sin intervención humana
- ✓ Detecta un dispositivo infectado en la red.

[4] MAC Control de acceso a medios
[5] LAN Red área local

El ***NAC*** establece a qué tipo de entornos de red puede acceder cada usuario. Un ejemplo claro: consultores externos que necesitan conectarse a máquinas de nuestros servidores pero que no tengan por qué acceder a ninguna parte adicional de nuestra red. Las aplicaciones ***NAC*** permiten establecer una serie de parámetros: perfiles definidos, requisitos de conexión (que tengan instalados antivirus, reconocimientos personale) llegando incluso a la virtualización de los entornos de networking, permitiendo sustanciales ahorros en los servicios básicos de infraestructura de red (Pello, 2017).

Las soluciones de control de acceso a la red (NAC) permiten a las organizaciones implementar políticas para el control de dispositivos y acceso de usuarios a redes corporativas. Las políticas pueden estar basadas en la autenticación de dispositivos y/o la configuración de función/identidad del usuario. NAC también incluye directivas (políticas) de post-conexión para supervisar el estado de seguridad de end point y para la implementación de la remediación si esta se requiere (Alternativas en Computación S.A, 2019).

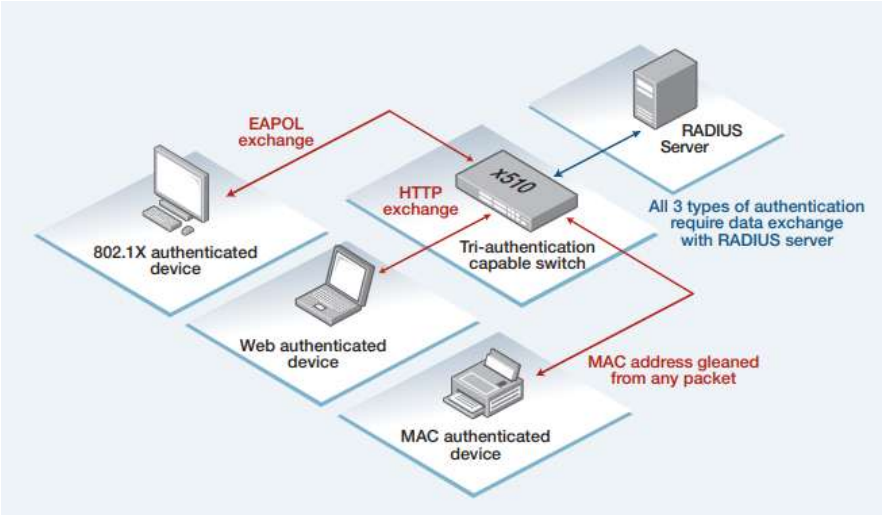

Figura 14.*Autentificación NAC (Allied Telesis, 2016)*

En el corazón del uso de ***NAC*** para la seguridad de su red hay tres elementos claves (Allied Telesis, 2016).

- ✓ Sin acceso (o muy limitado) sin identificación
- ✓ La cuarentena y la remediación de dispositivos no conformes
- ✓ Establecer el nivel de acceso a los recursos de la red en función de la autenticación de un dispositivo identidad.

NAC de Cisco.

El sistema de control de admisión de red de Cisco, compuesto por el administrador y servidor Cisco NAC, es un componente de política de la solución Cisco TrustSec. Puede implementar este sistema como una solución de superposición para cuentas que requieren autenticación de red, control de acceso basado en roles y evaluación de postura.

El dispositivo Cisco NAC extiende el NAC a todos los métodos de acceso a la red, incluido el acceso a través de LAN, puertas de enlace de acceso remoto y puntos de acceso inalámbrico. También es compatible con la evaluación de la postura para los usuarios invitados. Puede combinar Cisco NAC con Cisco NAC Guest Server y Cisco NAC Profiler para obtener funciones adicionales (Cisco, 2020).

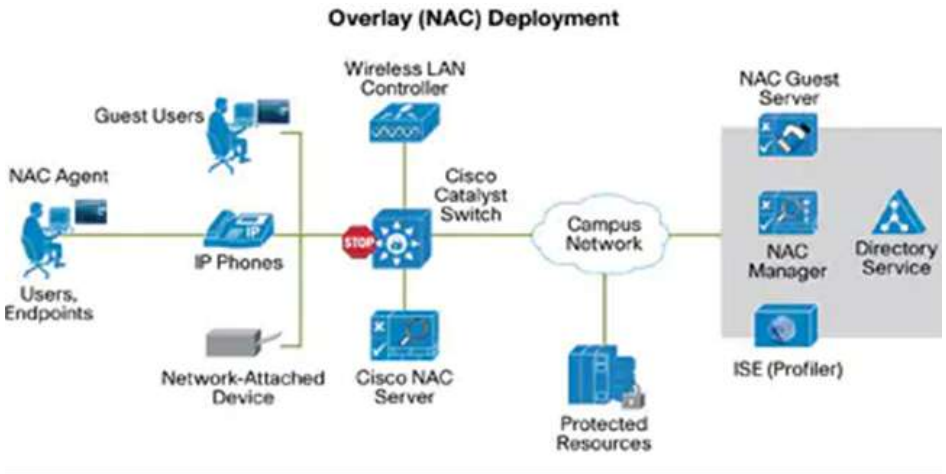

Figura 15. *NAC de Cisco (Cisco, 2020)*

El NAC de Microsoft.

Microsoft dispone de una variedad de tecnologías que permiten realizar control de acceso a la red.

- ✓ Microsoft Network Protection (NAP)
- ✓ 802.1X vía Microsoft
- ✓ Microsoft Network Access Quarantine Control (NAQC)

Microsoft NAP. Está definida como la plataforma que permite gestionar la protección del acceso a la red (Network Access Protection NAP), esta plataforma permite administrar los componentes para aplicar políticas que permitan controlar el acceso a la red, tanto para las computadoras conectadas o las que se conectan a la red cumplan con las políticas y requisitos previos establecidos en el sistema.

Microsoft 802.1X es una protección de control de acceso basada en port, esta tecnología de control de acceso se puede aplicar tanto para redes alámbricas como inalámbricas, el proceso de autentificación inicia en el port de acceso y utiliza dos elementos primarios:

- ✓ Suplicante – requiere el acceso a la red
- ✓ Autenticador- autentica suplicantes y decide o no darle acceso a red

NAQC proporciona solamente protección agregada para las conexiones de acceso remoto. NAP proporciona la protección agregada para las conexiones virtuales (VPN), Configuración del protocolo de configuración de anfitrión dinámico (DHCP), y comunicaciones basadas en IPsec (Esmoris, 2014, pág. 16).

El mecanismo 802.1x se basa en una serie de protocolos:

EAPOL el protocolo de autentificación extensible sobre LAN (EAPOL, Extensible Authentication ProtocolOver LAN) intercambio entre el solicitante y el autentificado, el protocolo de autentificación extensible EAP (Extensible de authenticatión Protocol) intercambiado entre el solicitante y el autentificador o servidor de autentificación; el EAP es compatible con el EAPOL sobre la interfaz entre el solicitante y el auntentificador, EAP-Method intercabiado entre el solicitante y el servidor de la solicitud, el EAP-Method esta soportado por el EAP (Pérez, 2020).

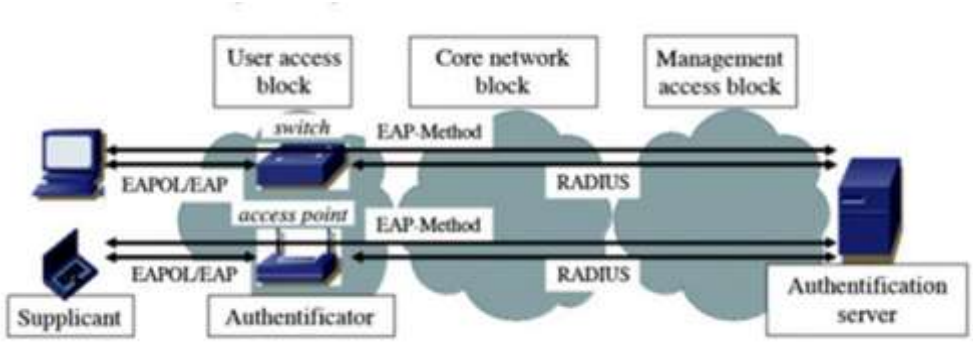

Figura 16. *El mecanismo 802.1x (Pérez, 2020)*

1.5.4 Casos de uso soluciones NAC.

De a acuerdo al estudio de la tecnología NAC se mencionan los siguientes casos en los que se utiliza la soluciones NAC y los beneficios de gestión y control de seguridad de la redes.

Detección de cada dispositivo conectado a la red y control de su comportamiento.

Algo fundamental del control de acceso es poder realizar un inventario en tiempo real de los dispositivos que están conectados a la red, se puede monitorear el comportamiento de los dispositivos tanto el uso de la red y las acciones realizadas, consiguiendo una visibilidad de tanto usuario internos e invitados, detectando acciones inadecuadas.

Adaptación y configuración de la red dinámicamente y sin intervención humana.

Mediante el NAC se definen políticas de acceso en función de cada usuario y se asignan los permisos de manera dinámica, previamente establecidas las políticas del acceso y uso de la red, automatizando la gestión de la red se minimiza la carga del personal de TIC.

Productividad sin riesgos.

La solución NAC se encarga de organizar y clasificar los usuarios que acceden a la red, acorde a los permisos de cada usuario, de esta manera se evita que usuarios externos accedan a la red sin previa autenticación.

Políticas de acceso homogéneas para tu red.

Somos conscientes de que la gestión de VPNs es complicada. Pero por su seguridad es imprescindible establecer la misma seguridad para conexiones locales y conexiones remotas. Las NAC lo hacen a través de VPN y añade un nivel extra de seguridad en los accesos remotos mediante la combinación de doble factor de autenticación con One-Time-Password

Realiza una gestión de acceso centralizada y homogénea a través de una política global de acceso para conexiones wifi, wired y VPN, además de definir las condiciones de seguridad que debe cumplir un dispositivo para acceder a la red (Gámez, 2017).

2 CAPÍTULO II

2. Situación Actual de la red CPN.

2.1 Aplicación de técnicas de recolección de información.

En la CPN al momento no existe una administración centralizada que permita controlar de manera automática y valide las credenciales del usuario que intenta acceder a la red, solo se mantiene la red segmentada por ***VLANs*** de acuerdo a cada área y gestión, actualmente es posible que un usuario conociendo la ***VLANs*** puede acceder a la red sin autorización, por ejemplo en la red cableada de la sala de Juntas.

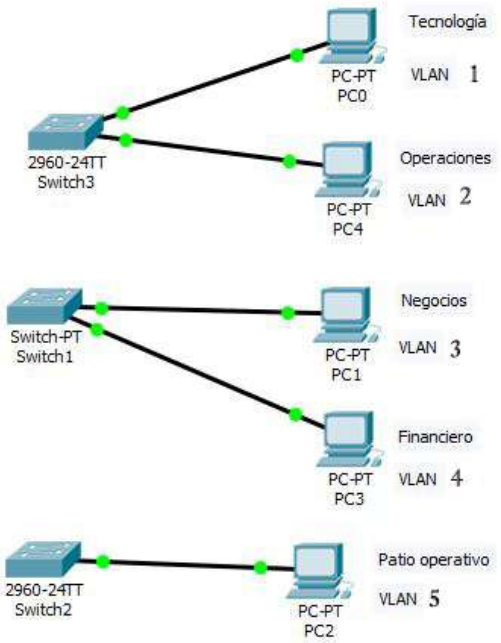

Figura 17. *Red segmentada por VLANS en la CPN*

En la administración de la red al momento no existe ningún tipo de proceso de autentificación de usuario mediante el puerto de red cableada, por lo tanto no se tiene establecidas políticas de acceso a la red. El escenario de conexión de los usuarios a la red al momento es el siguiente:

En las instalaciones de la ***CPN*** se utiliza un direccionamiento de IP estático para cada equipo de acuerdo a la ***VLAN*** asignada, se gestiona para validar la conexión del puerto al switch para asignarle la ***VLAN*** correspondiente, por medio de la IP se le asigna permisos de navegación, accesos a los aplicativos que están protegidos por firewall de perímetro y datacenter.

Se utiliza herramientas para ciertos segmentos de red tal como servidores de producción, mismos que se mantienen protegidos por firewall de perímetro, sin embargo, la red no se encuentra protegida por ninguna tecnología de control de acceso solo se mantiene segmentada por ***VLANS***.

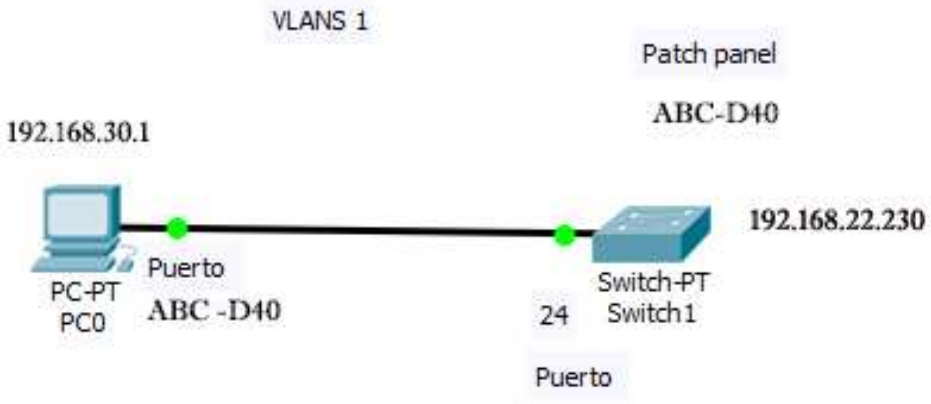

Figura 18. *Conexión mediante VLANS*

En la ***CPN*** el medio de acceso a la red es de manera cableada, por wifi y por VPN mediante acceso al escritorio remoto. Se investigó si la institución está en la posibilidad de adquirir y destinar un servidor para la administración de políticas que permitan controlar el acceso a la red, lo cual se manifestó que si y se cuenta con los recursos ya que se pretende mejorar y garantizar un acceso a la red de manera segura, debido a que al momento se tiene conocimiento y buenas referencias sobre la Tecnología ***NAC***. Con el fin de administrar la red de manera automática con funciones tales como:

- ✓ Controlar el acceso a la red
- ✓ Identificación de los dispositivos conectados
- ✓ Especificar Perfiles y asignar automáticamente un entorno
- ✓ Cumplimiento de políticas de seguridad
- ✓ Monitoreo de tráfico en la red.

En la red de la ***CPN*** no se cuenta con una tecnología como la ***NAC*** que controle el acceso a la red de manera centralizada y automática, a su vez aporte seguridad, permitiendo la autentificación de las conexiones, luego de autentificar validar las políticas, asignar permisos, realizar el monitoreo y administración de los equipos conectados.

2.1.1 Análisis sobre seguridad de la red.

En cuanto a Confidencialidad y Autentificación depende del análisis y de los controles que por metodología se implementen, por ejemplo:

- ✓ Confidencialidad: Fuga de Información.
- ✓ Autenticación: Doble Factor, contraseñas robustas (ambientes, BDD / D.A.).

Que se trasladan en controles o proyectos dependiendo del análisis, como ***CPN*** se tienen atados controles por los 3 pilares del C.I.D., y eso trasladados a controles y proyectos.

- ✓ Integridad: Control de Acceso: roles y perfiles / accesos a BDD, aplicaciones y monolíticos.
- ✓ Disponibilidad: Enlaces de comunicaciones, sistemas, performance de equipos, disponibilidad de sistemas o aplicaciones.

En la CPN se pone énfasis tanto en los ámbitos de seguridad activa y seguridad pasiva.

En realidad, se gestionan los dos ámbitos debido a que las activas probablemente son seguridades tecnológicas a través de infraestructura ***resiliente*** o ***autogestionada***, y también puede ser pasiva es decir post mortem, donde analizas eventos o validas eventos una vez generados.

Pero también hay seguridad pasiva como roles, segregación de funciones, roles, políticas u otras.

2.1.2 Norma ISO 27001.

En la CPN se aplica la norma ISO 27001 establecida como marco de referencia para un SGSI, dentro de este marco existen dominios como buenas prácticas donde se definen desde compromisos de dirección hasta auditoria y ejecución de controles, planes de tratamiento de riesgos, seguimiento y un nivel de madurez del SGSI (ver anexo 1).

En la ***CPN*** existe falencia en la aplicación de la norma ISO 27001, no se controla el acceso a la red por lo tanto no se está cumpliendo con el código 10, mismo que menciona. Rastree y supervise todos los accesos a los recursos de red. Tampoco el 1.1.6 literal b y c mencionan que se deben realizar configuraciones para que los puertos sean seguros.

Esto también tiene definición de roles, responsabilidad y compromiso de la dirección, así como los recursos necesarios para su ejecución, financieros y personas. Todos estos cúmulos de experiencia y de dominio hacen la ejecución de un SGSI dentro de este marco de referencia.

Posterior existen ***métricas*** y controles que se aplican para elevar el SGSI a un sistema certificable, por lo cual la recomendación inicial es determinar un alcance medible en tiempo, recurso y personal, ya que un marco muy grande del SGSI resultaría muy complejo de manejarlo.

2.2 Estudio Técnico de seguridad de la red.

En la institución se maneja exclusivamente servicios bancarios, una persona puede asignar una ***IP*** a otro computador y puede acceder a la red sin inconveniente, es decir, que no existe una administración centralizada que valide la petición de acceso y autorice o deniegue el acceso a la red con el propósito de precautelar la seguridad de la misma.

2.2.1 Autorización.

Este pilar de seguridad permite evaluar los parámetros relacionados al control de acceso a la red de la ***CPN***, a continuación se detalla aspectos de la red en base a la Autorización.

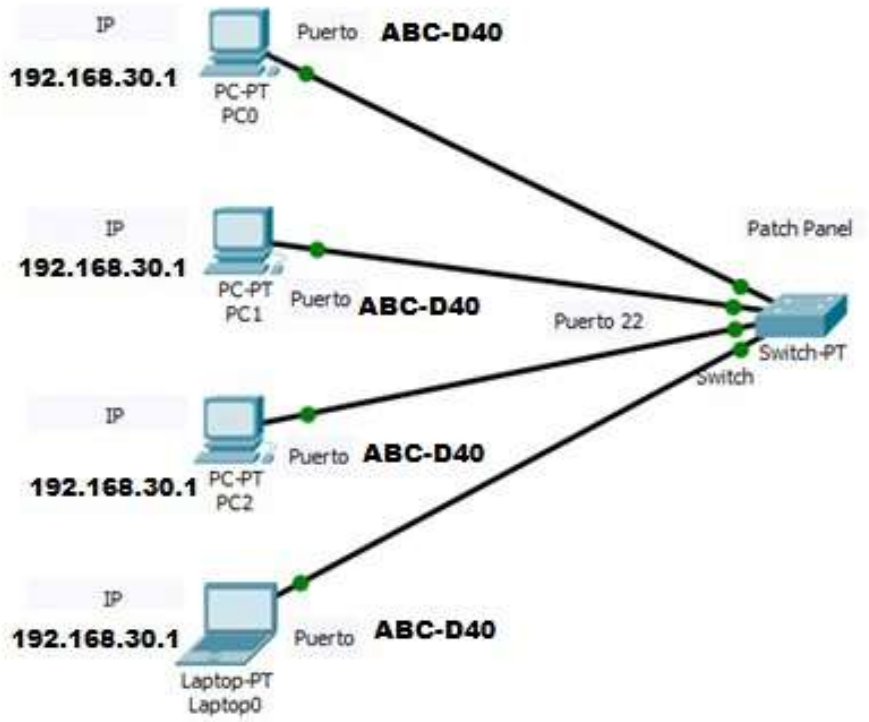

Figura 19. *Red CPN Matriz*

En la red de la CPN se obtiene acceso mediante la ***IP***[6] independientemente del equipo que esté conectado, si un usuario conoce la ***IP*** y ***VLANs*** [7]puede hacer uso de la red sin previa autentificación. Por lo tanto, si es posible que un usuario tenga acceso a la red cableada sin autorización, por supuesto para aquello, el usuario debe tener conocimiento de la red y ***VLANs*** a la cual desea conectarse usando el punto de red al que haya tenido acceso, por ejemplo el de la Sala de Juntas.

Al momento no existe un control automático y centralizado que autentifique al usuario que intenta acceder a la red. En la ***CPN*** no se cuenta con tecnología que permita controlar el acceso a la red mediante la autentificación de usuario por tal motivo no se realizan las siguientes actividades.

- ✓ Controlar el acceso a la red en función del rol del usuario, hora del día, localización y aplicación.

No existe ningún proceso de autenticación.

[6] IP Protocolo de internet
[7] Vlans Red de área local virtual

- ✓ Identificación de los dispositivos conectados y controlar el acceso de los usuarios no conocidos o con menos garantías de seguridad, como proveedores, y Especificar Perfiles y asignar automáticamente un entorno

No se cuenta con una herramienta de ese tipo para la red ***LAN*** de la ***CPN***.

- ✓ Cumplir con políticas de seguridad.

  En la red de la ***CPN*** no se cuenta con una herramienta tecnología que permita establecer políticas de acceso a la red ***LAN***.

2.2.2 Auditabilidad.

En la siguiente imagen se presenta aspectos referentes a la Auditabilidad del registro y acceso a la red de la CPN.

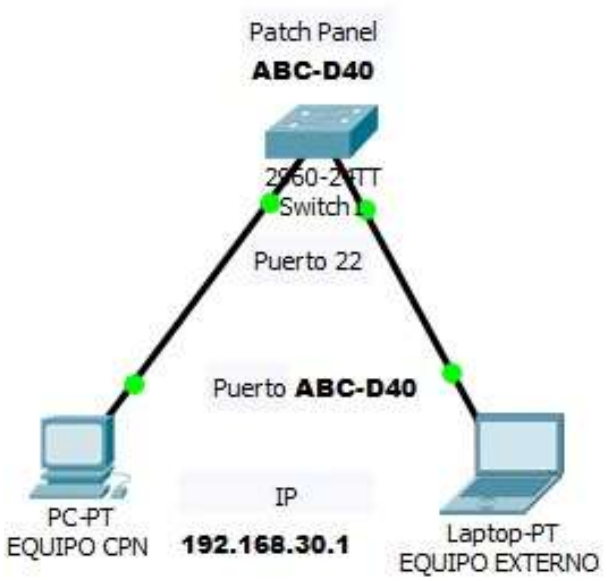

Figura 20. *Red de CPN Matriz*

.

Si un usuario conoce la ***VLANs,*** las credenciales de red y los equipos están configurados en el dominio, puede acceder a los recursos de la red y tener acceso incluso a la información de otro computador. Aquí la necesidad de implementar tecnología ***NAC*** para ofrecer un mayor control y seguridad de la red, mismo que permita autenticar las conexiones, asignar permisos en base políticas previamente establecidas, monitoreo y administración de manera automática y centralizada. Mejorando la seguridad de la red mediante un control sobre las conexiones realizadas tanto de equipos y usuarios. En la CPN no se cuenta con tecnología que permita controlar el acceso a la red, para la Auditabilidad de usuario se consideran los siguientes aspectos.

- ✓ Restricción del acceso a información.

Si es posible que pueda encontrar un punto de red por ejemplo sala de juntas, sin embargo, necesitaría tener más datos como la red y ***VLANs*** a la cual pueda conectarse a través del puerto de red que haya podido tener acceso.

- ✓ Control de quién accede a la red y restricción del número de recursos con los que puede operar.

Por medio de la ***IP*** los usuarios cuentan con accesos a navegación y accesos algunos servicios y aplicaciones que están protegidos por firewall de perímetro y datacenter respectivamente, sin embargo no hay un control de acceso a la red automático o centralizado.

- ✓ Detección de cada dispositivo conectado a la red y control de su comportamiento. - Productividad sin riesgos.

No existe un control automático, se mantiene una división de ***VLANs*** por Gestiones.

2.2.3 Autenticación.

En la autentificación para comprobar la identidad de usuarios, antes de otorgar el acceso a la red en la CPN se asignan las VLANs de manera manual y se tiene un direccionamiento IP estático, un usuario local o proveedor no puede acceder a la red hasta que no se le asigne manualmente una VLANs. Esto se debe a que no se dispone de un control automático que asigne perfiles tanto para usuario locales como invitados.

- ✓ Segmentación de usuarios en función del cumplimiento normativo.

En la red de la ***CPN*** se mantiene una segmentación de usuario manualmente, por ejemplo se tiene segmentadas la ***VLANs*** y se asignan ***IP*** al usuario acorde al área, también se tienen destinadas ***IP*** para asignar a un proveedor que hace las veces de invitado en la red.

- ✓ Protección de red IP - Adaptación y configuración de la red manual.

Actualmente se mantiene direccionamiento ***IP*** estático, acorde al área en la cual está conectado el host se realiza la configuración del puerto en el switch y se asigna la ***VLANs*** respectiva.

Tabla 1. *Aspectos de seguridad.*

Criterios a los que está expuesta la red	Descripción
Ataque a la red.	Interrumpir procesos y actividades de transferencia bancaria.
Fuga de información	Información sensible, alteración o perdida de información

En base a los aspectos de seguridad, es necesarios que se cumpla con un control de acceso en la red con administración centralizada mismos que fortalezcan los criterios de seguridad.

Tabla 2. *Riesgos en la red.*

Criterios que no se cumplen actualmente en la red	**Descripción.**
Autentificación	No existe proceso para autentificar usuarios, ni tecnología que controle el proceso de acceso a la red de forma automática y centraliza, solo esta segmentada la red por ***VLANS***.
Controlar equipos conectados a la red	En la red de la ***CPN*** no se existe restricciones para conexiones de equipos, por ejemplo un empleado puede conectar un equipo personal en la red y sabiendo la ***VLAN*** puede acceder huso de la red y propagar virus dentro de la misma.
Políticas de seguridad.	No existen políticas basadas en protocolos que validen y gestionen las credenciales de los usuarios internos y remotos que intentan acceder a la red a través de sus cuentas de usuarios y permitan o nieguen el acceso a la red y los servicios.
VLANS	La red esta segmentada por ***VLANS*** lo cual no brinda un servicio de autentificación seguro debido a que no se cuenta con un control de acceso, es decir los equipos se conectan a la ***VLAN*** sin tener un proceso de autentificación previo. Dentro de la red existe un control mediante firewall y antivirus como el macafe para equipos de la ***CPN***.

De acuerdo a lo revisado en la red es importante la implementación de tecnología que controle y restrinja la conexión de los equipos a la red, esto se realiza mediante autentificación de direcciones MAC para dispositivos como impresora y teléfonos, para equipos de cómputo el protocolo de autentificación 802.1x.

3 CAPÍTULO III

3. Análisis y Selección de tecnología NAC en la CPN.

La institución cuenta con infraestructura AVAYA, la misma que cuenta con una solución de ***NAC*** a través de 802.1x. De acuerdo al análisis y la entrevista realiza al personal de infraestructura se considera que la tecnología NAC adecuada es la siguiente.

3.1 Tecnologías con funcionalidad NAC/NAP: 802.1X y SSL VPN.

Esta tecnología está conformada por la autentificación en la red mediante puertos, y está compuesta por varias tecnologías que integran la solución ***NAC.***

3.1.1 802.1X.

Es un protocolo de autenticación altamente seguro que permite el intercambio de contraseña encriptado y el certificado validación. Se le solicita a un usuario su nombre y contraseña, y esto luego se verifica contra una base de datos de usuario antes de que puedan acceder a la red (Telesis Allied, 2016).

IEEE 802.1. Estándar del IEEE de 2001 para promocionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un puerto del punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto bloqueado hasta que el usuario se autentique. Con el fin se utiliza el Protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso como priorizar cierto tráfico o descartar otros (De la Cruz, 2013).

EAP es un protocolo de autentificación extensible, permite realizar tareas de autentificación, autorización y contabilidad. El protocolo EAP es encapsulado en la solicitud de autentificación realizada entre la estación y el servidor Radius aquello está definido en el estándar 802.1x bajo el nombre EAPOL, el protocolo EAP es definido en la RFC 2284.

Radius. El protocolo RADIUS (Remote Authentication Dial-In user service) intercambio entre el autentificador de identificación y el servidor de autentificación, el protocolo RADIUS soporta el EAP en la interfaz entre el autenficador y el servidor de autentificación (Pérez, 2020, pág. 6).

3.1.2 Mac.

La autenticación MAC es una alternativa para dispositivos que no admitan 802.1x, esta autentificación se puede usar para dispositivos no interactivos como teléfonos Avaya, impresoras o cámaras web.

La dirección MAC del dispositivo proporciona una identidad única que puede ser utilizada para autenticar el dispositivo. Para realizar el proceso de autentificación del dispositivo se utiliza la dirección MAC de origen de la trama recibida.

Para el proceso de autentificación por medio de MAC el autentificador envía la MAC de origen del dispositivo como credencial de autentificación, estos datos se envían al servidor RADIUS para su autentificación, si las credenciales son válidas se permite el acceso a la red del dispositivo.

3.1.3 Exos.

La autenticación web se proporciona para atender a las computadoras en el que 802.1X no está presente o configurado. El interruptor detecta la actividad de navegación web desde la computadora del cliente, y presenta una pantalla de inicio de sesión para el navegador web. El usuario no puede avanzar más hasta que hayan enviado una identidad válida utilizando la pantalla de inicio de sesión. Esta autenticación puede realizarse en texto claro, utilizando el protocolo HTTP, o realizado en forma encriptada usando el protocolo HTTPS.

3.1.4 Atributos de Direccionamiento IP.

En la ***CPN*** se utiliza ***IPs*** estáticas de acuerdo al grupo o departamento al que está asignado el host, es decir el usuario no puede ser móvil debido a que la ***VLAN*** esta quemada como IP estática en el host y no se le asigna la subred de manera automática, esto impide que el usuario sea móvil y al trasladarse a otro departamento con el host no se le asigna la subred de manera dinámica.

Con la implementación del ***NAC*** se permite la posibilidad de que los usuarios sean móviles y se conecten a la ***VLAN*** que les corresponde, aquello se debe a que más de un usuario puede hacer uso de un equipo y se le asigna la ***VLAN*** mediante el directorio activo y las políticas de acceso establecidas en el ***NAC***, es aquí donde se aplica el direccionamiento por ***DHCP*** esto permite que una vez autentificado el usuario y asignada la ***VLAN*** a la que corresponde se le asigne una IP de manera dinámica.

3.1.5 Configuración 802.1x en equipo cliente.

Los aspectos a considerar para la configuración de 802.1x en los host son los siguientes:

- ✓ Tarjeta de red Eternet. y conexión a un puerto de red.
- ✓ El equipo debe pertenecer al dominio de la institución
- ✓ Configuración de políticas para la tarjetas de red con parámetros 802.1x
- ✓ Tener el servicio de configuración de redes cableadas en inicio automático
- ✓ Configuración de tarjetas de red respecto al tipo de EAP

El equipo debe tener un nombre de host que pertenezca a un grupo.

3.1.6 Perfiles.

De acuerdo al análisis que se ha hecho en la CPN, la solución NAC para el control de acceso a la red debe permitir los siguientes perfiles de usuarios.

Tabla 3. *Perfiles de usuarios.*

Rol	Acceso
Personal de la institución	Acceso a la red corporativa acorde a la VLANS.
Invitados	Acceso restringido a la red y sitios concretos, VLAN 3000 de invitados, no tiene acceso sitios aplicativos CPN, solo segmentos de internet.
Acceso Remoto	El acceso a la red mediante la autentificación e identificación de conexión remota llamado capa segura mediante SLL VPN.

3.2 Integrantes de la Autentificación NAC.

La solución NAC de Microsoft mediante el control de acceso 802.1x se basa en una serie de protocolos utilizados en las LAN y herramientas tecnológicas para controlar el acceso a la red, para lo cual se utiliza las siguientes tecnologías:

- ✓ Active Directory
- ✓ El switch
- ✓ Servidor AAA.
- ✓ Administrador de control

3.2.1 Active Directory.

El Active Directory es una herramienta de Microsoft que presta los servicios de directorio centralizado en la red para administrar usuario y equipos de la CPN. Para la solución NAC es necesario asociar un usuario a una directiva de grupo con sus respetivas credenciales, mismas que se utilizan para el proceso de autentificación mediante 802.1x.

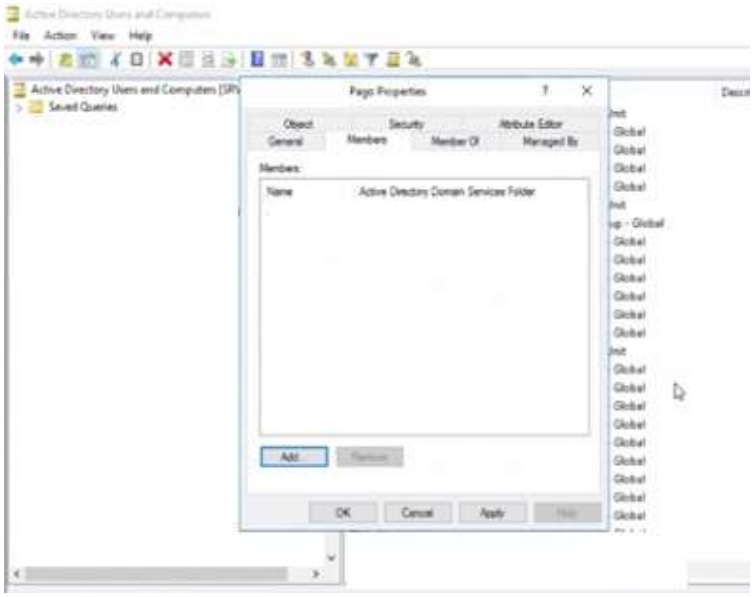

***Figura 21**. Active Directory.*

Se crea un grupo de AD, se establece un nombre al grupo de usuarios, luego se configura alcance (modo global) y tipo de grupo (seguridad).

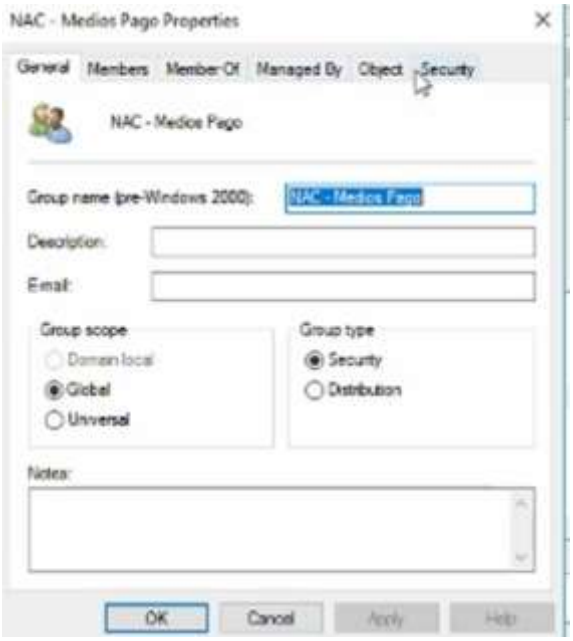

***Figura 22.** Grupo en AD para NAC*

Este grupo sirve concentrar los usuarios y asociarlos a la política de redes cableadas.

3.2.2 El Switch.

Figura 23. *Switch (Extreme, 2019)*

La serie ExtremeSwitching X440-G2, son switches con escalabilidad y rentabilidad, pertenece a extreme Networks posee un SO que permiten continuidad, seguridad integral y eficiencia operativa. Entre otros aspectos relevantes que se destacan es la flexibilidad permitiendo enrutamiento y conmutación de alto rendimiento, son PoE-Plus y tienen seguridad integral.

Los servicios de administración de la serie X440-G2, fáciles de usar y potentes, incluyen políticas basadas en roles para el acceso controlado a aplicaciones de red específicas. Los conmutadores de la serie X440-G2 también se pueden gestionar en la nube a través de ExtremeCloud, una solución innovadora de gestión basada en suscripción de un solo panel de Extreme Networks (Extreme, 2019).

Avaya Ethernet ERS4850GTS-PWR+- 48 ports.

Figura 24. *Switch Avaya (Avaya In, 2015)*

Ethernet Routing Switch 4800 Series permiten obtener un ancho de banda alto, capacidades de convergencia, seguridad, QoS y alta capacidad de gestión. En cuanto a la capa 2 permite conmutación de alto rendimiento y en la capa 3 enrutamiento.

El ERS 4800 Series es una solución preparada para el futuro y adecuada para el armario de cableado de alta tecnología. Junto con otros productos de Avaya, el Ethernet Routing Switch 4800 Series puede aumentar la rentabilidad y productividad, simplificar las operaciones comerciales, disminuir los costos y ayudar a su empresa a obtener una ventaja competitiva (Avaya In, 2015).

Generales y de rendimiento.

- ✓ 802.1X Clients: up to 768
- ✓ Compatibilidad con los estándares ERS 4800
- ✓ EEE 802.1X Ethernet Authentication Protocol

- ✓ Authentication Method

Extensible Authentication Protocol (EAP), RADIUS, Secure Shell (SSH), Secure Shell v.2 (SSH2)

- ✓ Authentication Method

Secure Shell (SSH), RADIUS, Secure Shell v.2 (SSH2), Extensible Authentication Protocol (EAP).

Estándares que cumplen.

IEEE 802.1AX, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ab (LLDP), IEEE 802.1ag, IEEE 802.1aq, IEEE 802.1p, IEEE 802.1s, IEEE 802.1t, IEEE 802.1w, **IEEE 802.1x**, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad (LACP), IEEE 802.3ae, IEEE 802.3af, IEEE 802.3ak, IEEE 802.3at, IEEE 802.3i, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z.

Conexión remota mediante VPN y NAC.

Se utiliza VPN mediante el aplicativo Foticlient, el usuario debe contar con permisos de acceso remoto con las credenciales de usuario VPN y acceso mediante escritorio remoto configurado en el equipo, la versión es 6.2.6 y se utiliza la configuración mediante SSL-VPN.

El acceso remoto a un host de la CPN es posible, a pesar de que ningún usuario físicamente haya hecho el inicio de sesión, para autentificar al usuario que accede a la red se crea una política que autentifique la MAC del equipo y verifique las credenciales del usuario. El acceso remoto y autentificación se realiza mediante la MAC del equipo y las credenciales del usuario enviadas en la conexión de SSL de la VPN.

3.2.3 Configuración de switches.

Es necesario integrar los swicthes en la plataforma de Exos extreme en la pestaña de Access control se escoge la opción Engines.

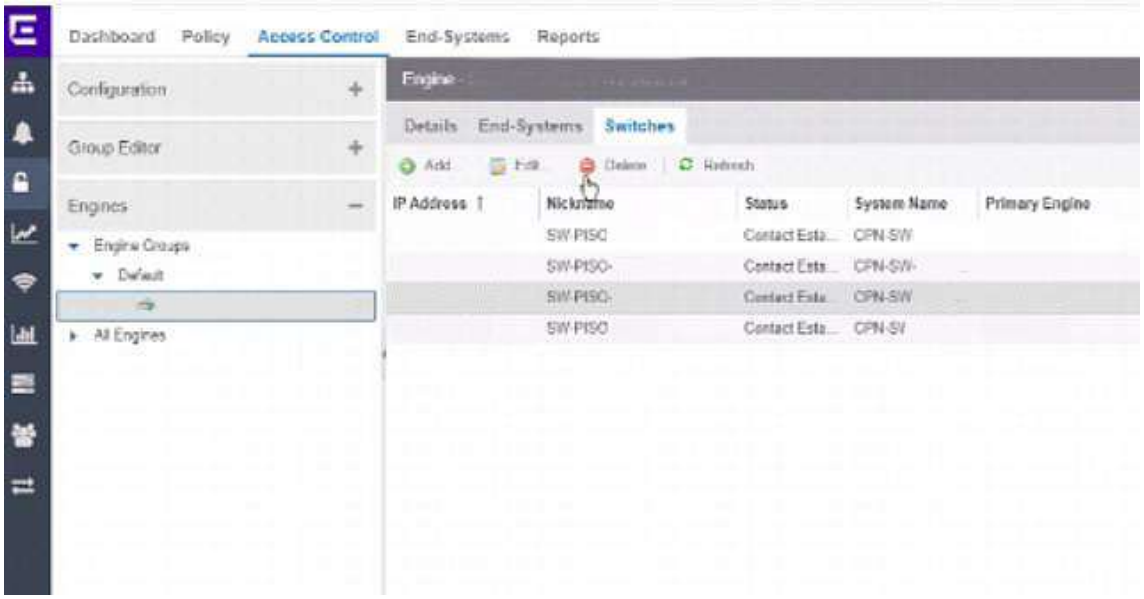

Figura 25. *Switch de acceso*

Se ingresa a la plataforma NAC y se verifica los switch de acceso registrado.

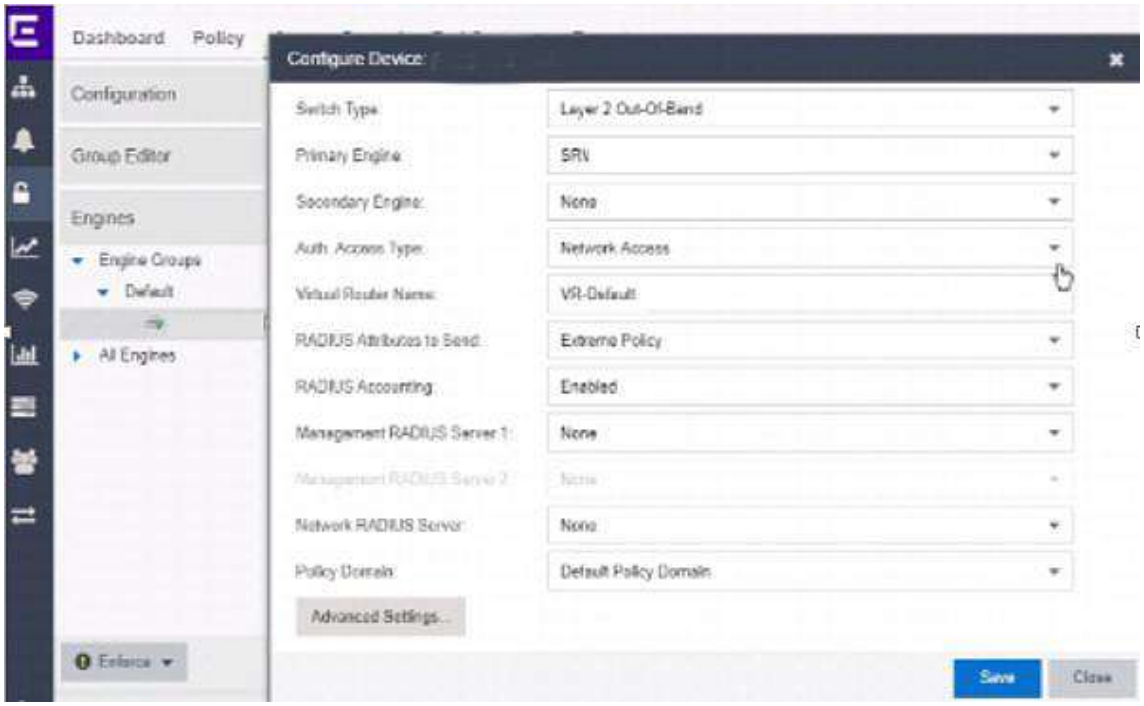

Figura 26 *Configuración Switch de acceso.*

Se configura el switch acorde a los parámetros que debe cumplir, se especifica el switch de tipo control de acceso y lo añadimos al groups, tales como acceso a la red y los atributos RADIUS y las políticas de extreme.

3.2.4 Servidor AAA.

La solución del NAC funcionará en un entorno del active Directory con Windows Server, el servidor RADIUS permiten la validación y ejecución del proceso de autentificación y autorización de los equipos que acceden a la red, así mismo permite tener un control y realizar un análisis de los equipos que fueron habilitados para acceder a la red mediante el NAC.

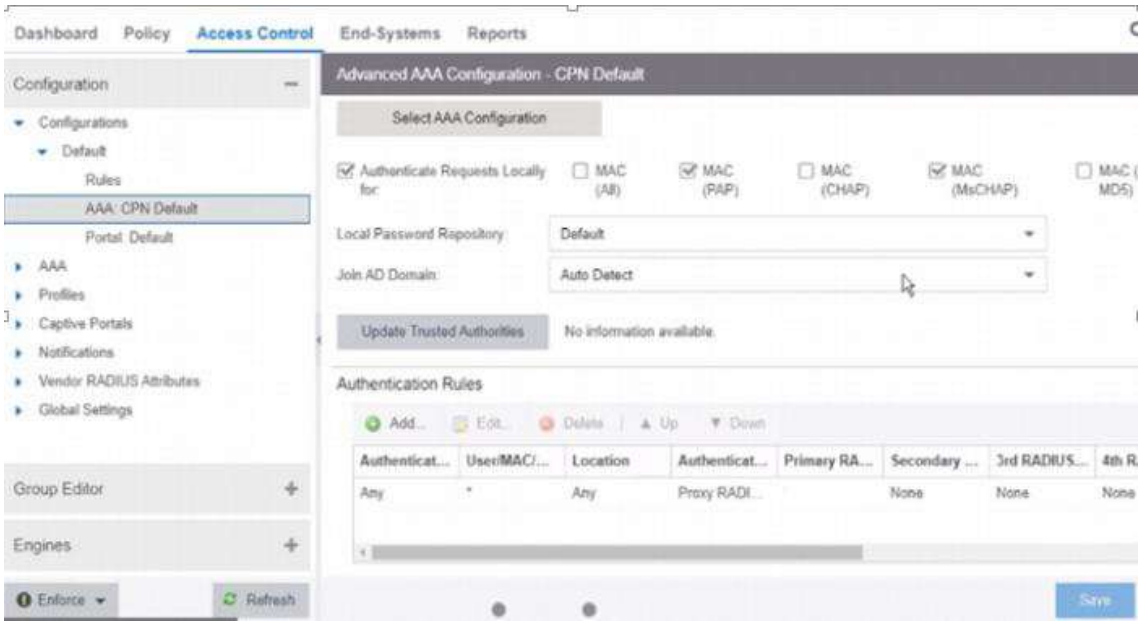

Figura 27. *Servidor AAA*

El servidor AAA (Authentication Authorization Accounting) consiste en la autentificación, autorización y auditoria, es decir registrar los usuarios que acceden a la red, así también permite realizar el proceso de validar si la autentificación es correcta, de ser este el caso el puerto de red es abierto, el servidor RADIUS permite gestionar las diferentes políticas para cada usuario concreto. Se utiliza el servidor de LDAP para levantar NPS en servidor para la autentificación NAC mediante RAIDUS.

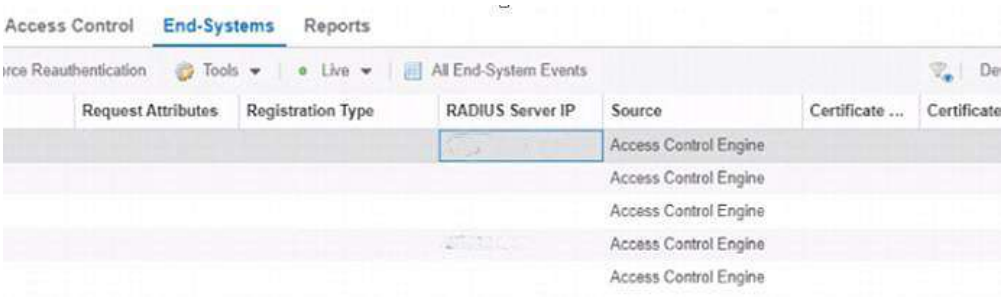

Figura 28*. Servidor RADIUS*

3.2.5 Políticas para autentificación.

Para el proceso de autentificación mediante NAC se configura políticas de redes cableadas, a continuación se muestra el proceso de configuración de las políticas para equipo de cómputo.

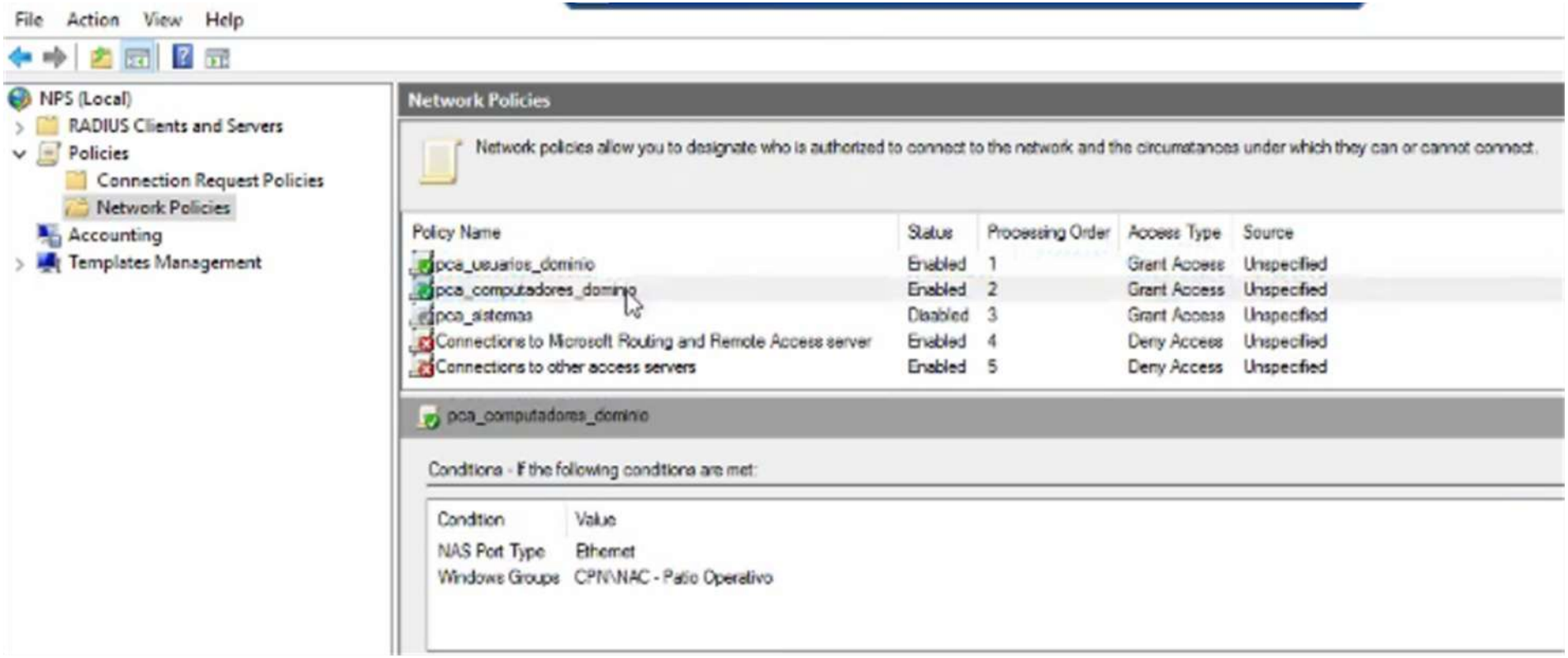

Figura 29. *Políticas de redes*

En primer lugar se configura en el servidor RADIUS las políticas de redes y servicio para autentificación cableada.

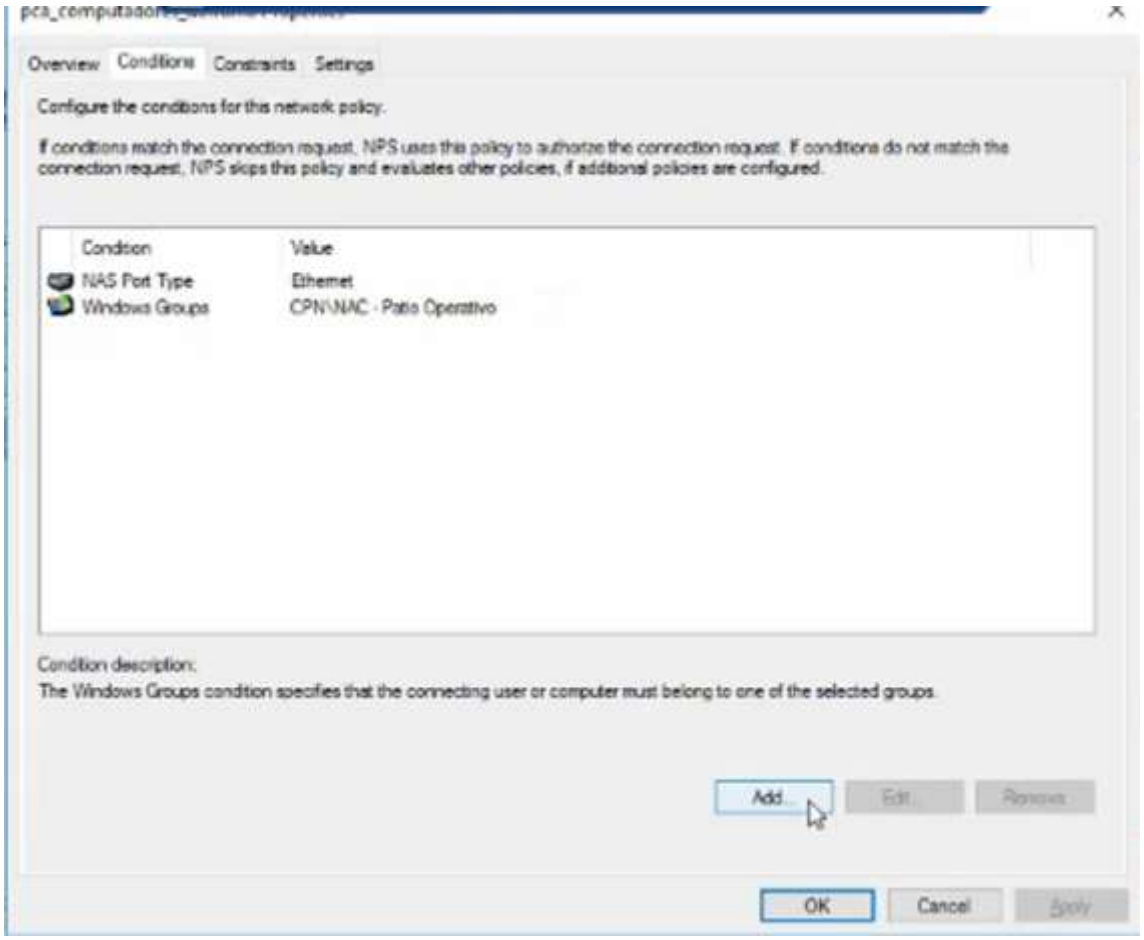

Figura 30. *Configuración de políticas.*

En la política creada como computadores dominio, se da clic en add y se agrega una condición

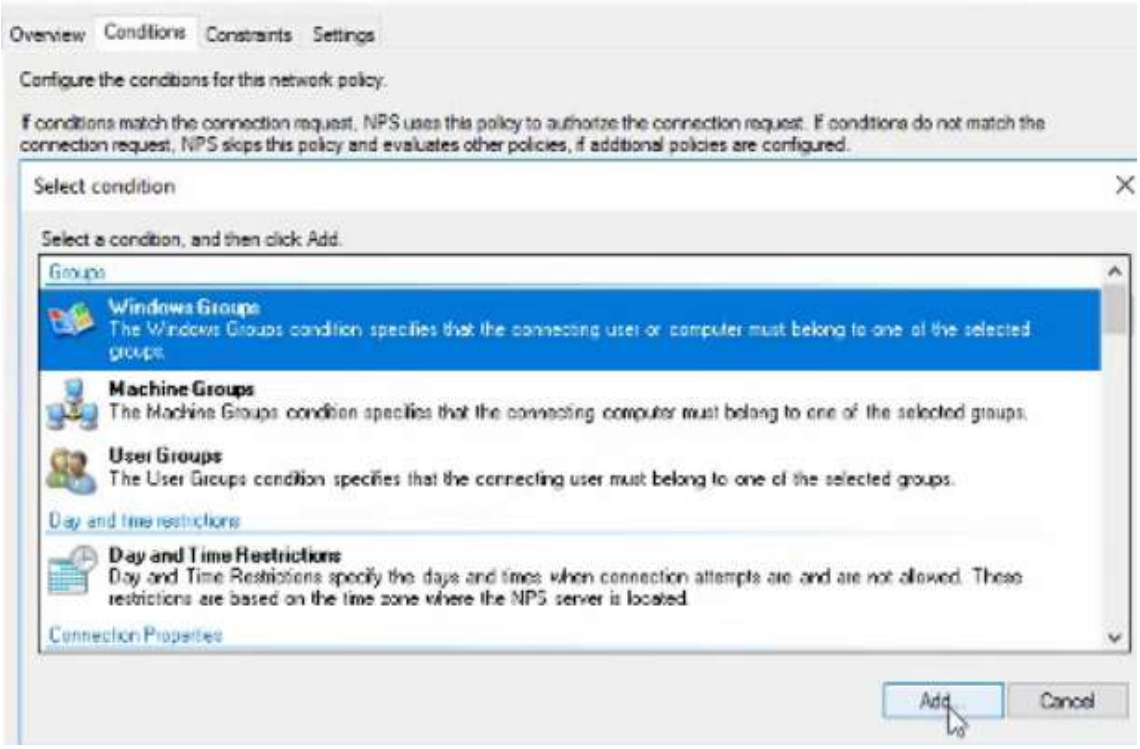

Figura 31. *Listado de condiciones*

Del listado que se despliega se escoge Windows Groups y se da clic en add.

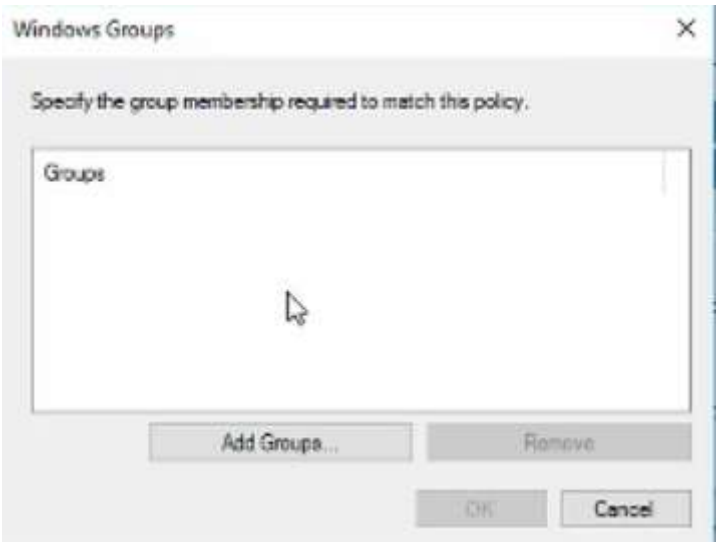

Figura 32.*Grupos de windows*

Se añade el grupo del AD al cual se le aplica la política.

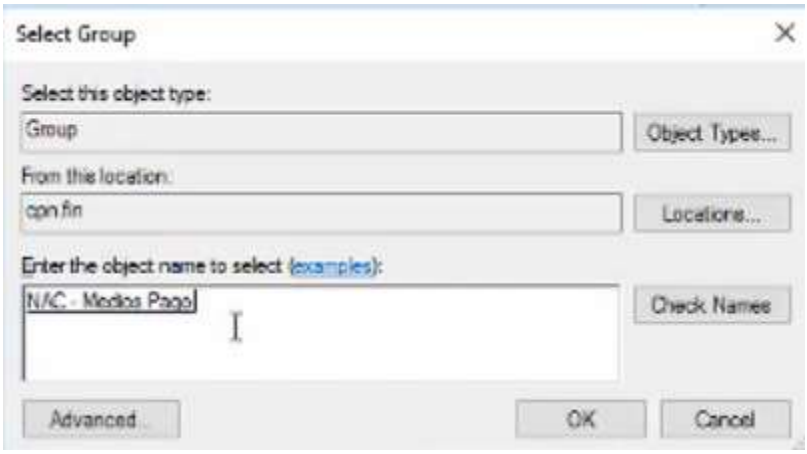

Figura 33. *Selección de grupo*

Se registra el nombre del grupo de AD para NAC.

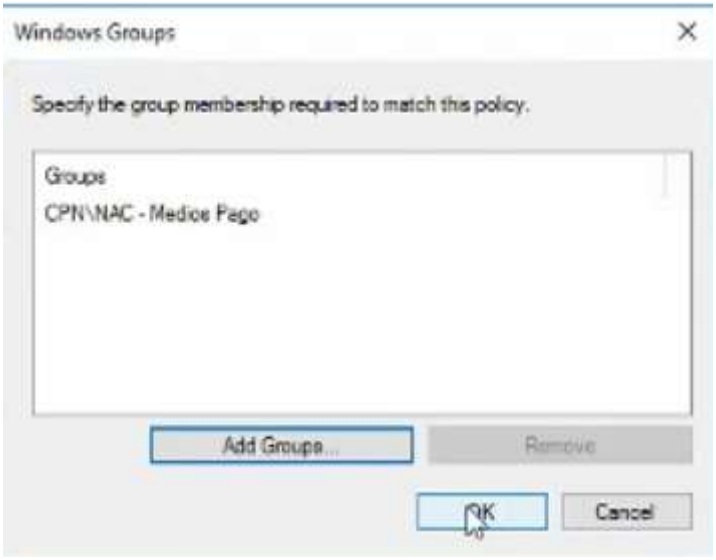

Figura 34.*Grupo de Windows*

Una vez añadido el grupo se guarda la configuración realizada.

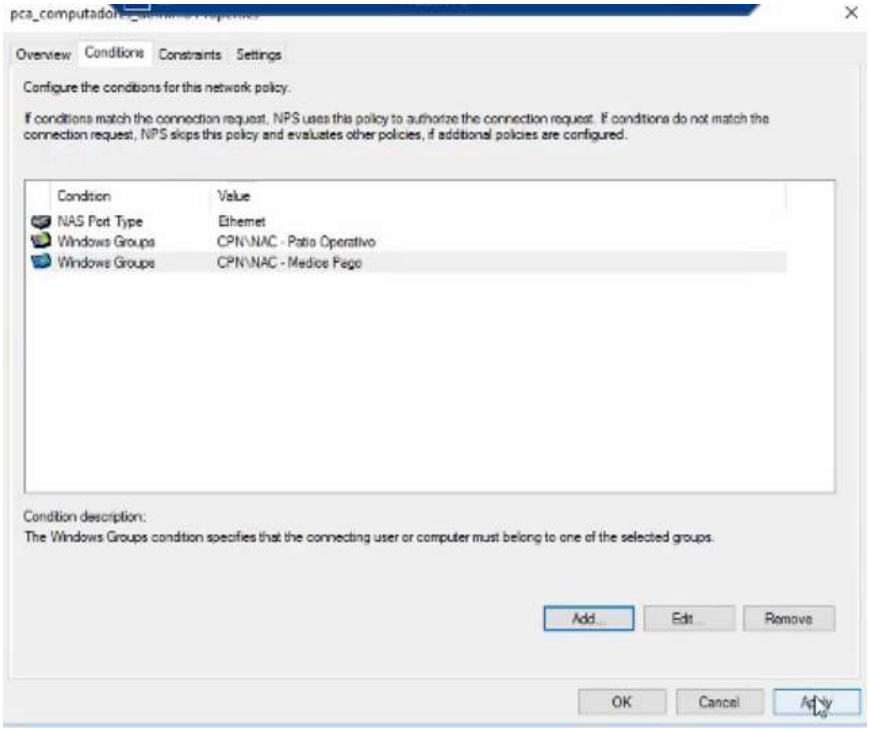

Figura 35. *Grupos y políticas*

Se observa que el grupo esta añadido a la política creada y se da clic en aplicar.

Políticas para usuario de Dominio.

Figura 36. *Políticas de red para usuarios*

En la política creada para usuarios dominio, se habilita y al dar doble clic se ingresa al panel para realizar la configuración respectiva.

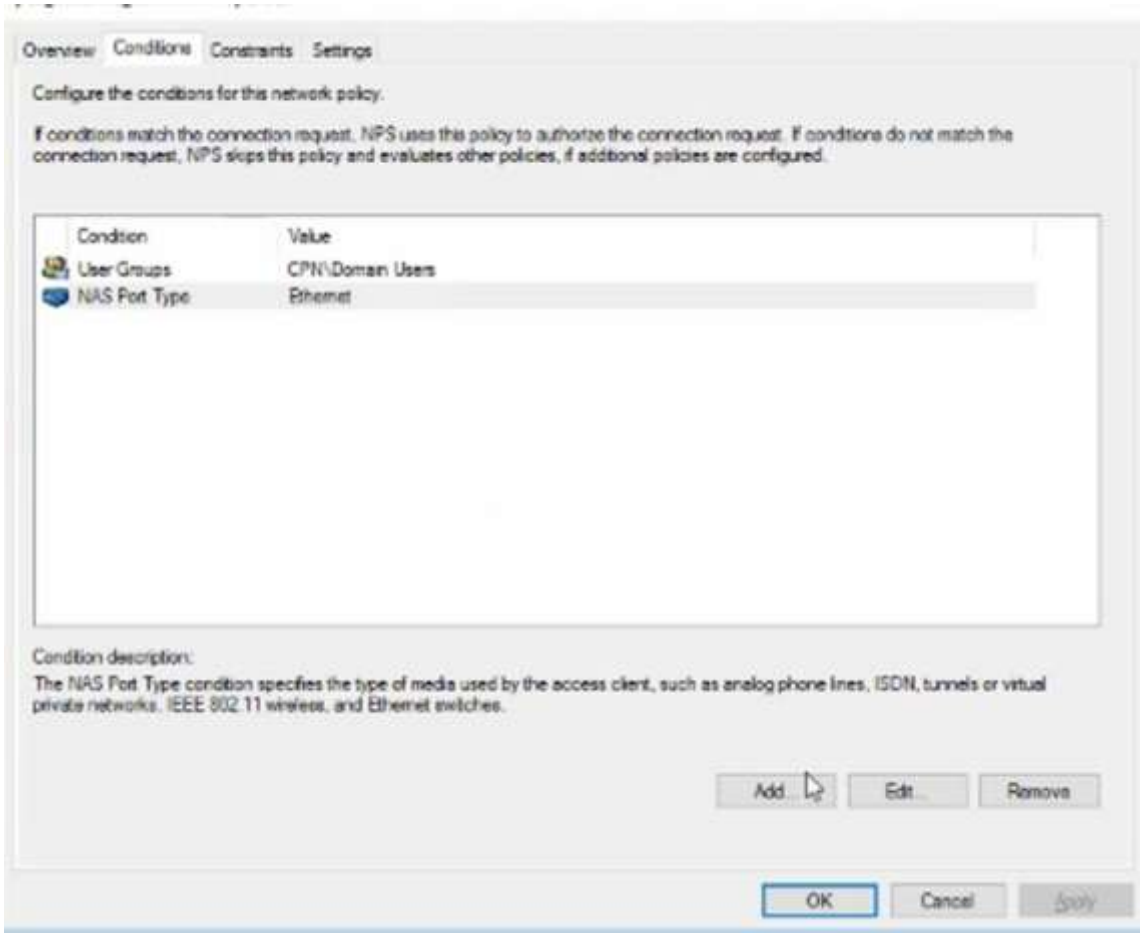

Figura 37. *Configuración para condiciones*

Una vez ingresado en la política se escoge la pestaña condición y se da clic en add, se agrega una condición NAS port Type.

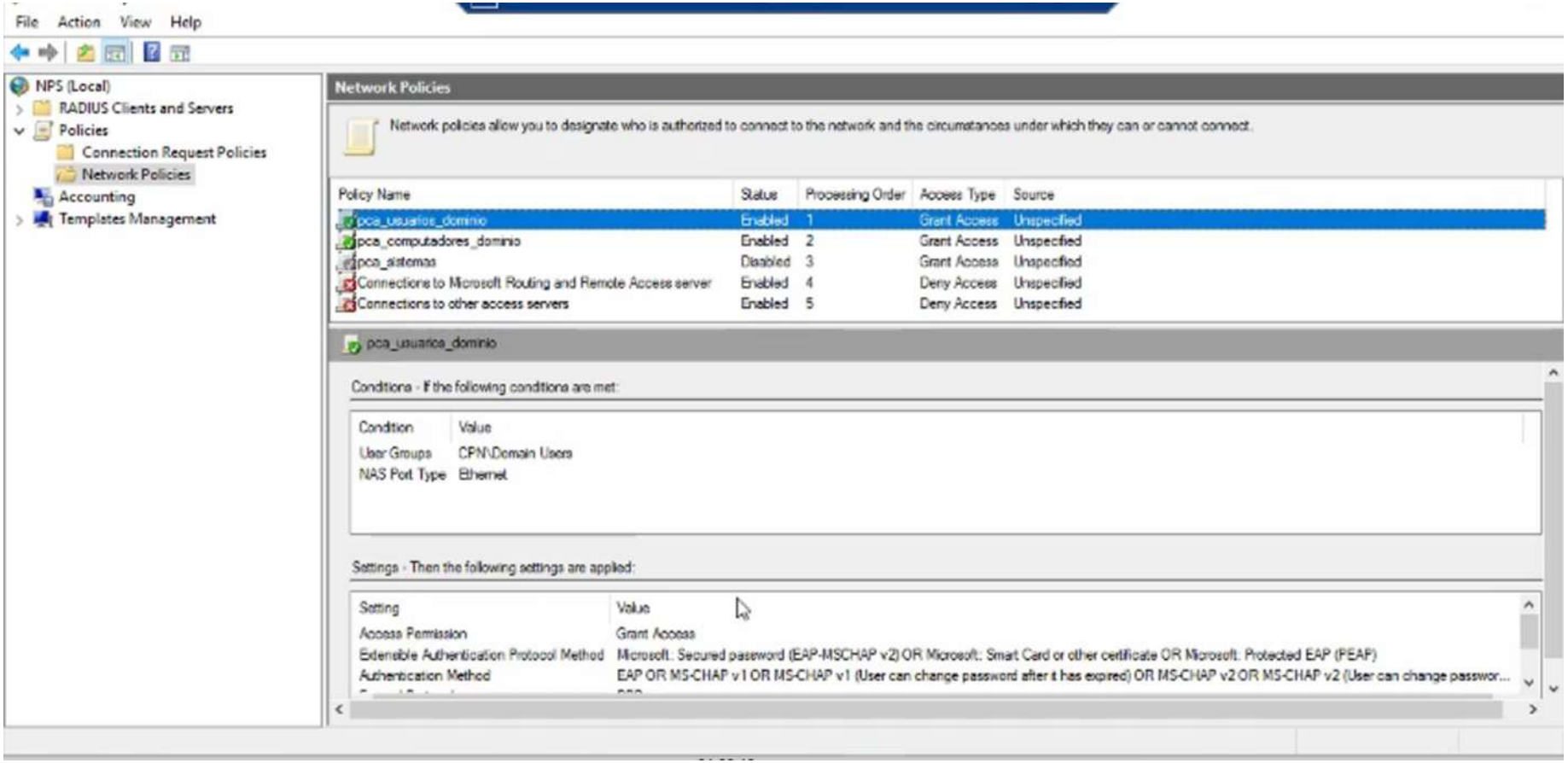

Figura 38. *Configuración de política de usuario*

La política de usuario para dominio se configura tipo de autentificación NAS port con el valor Ethernet, el método de autentificación EAP-MSCHAPv2 proteccion PEAP.

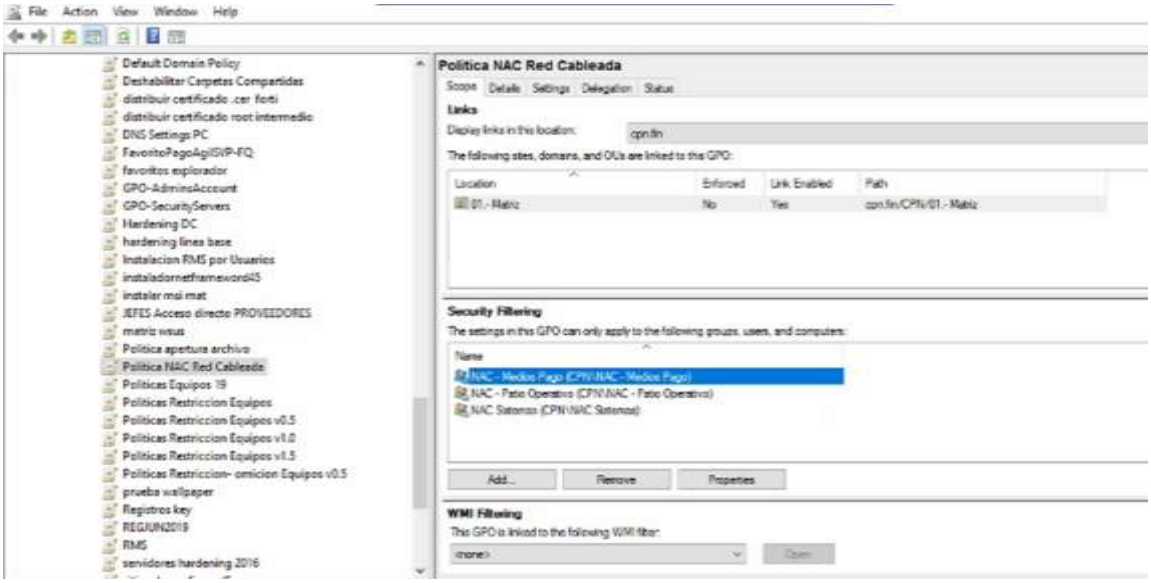

Figura 39. *Vista de asociación de grupo a política*

En la imagen anterior se observa la configuración y asociación del grupo NAC Medio de Pago a la Política de redes cableadas.

GPO.

802.1x este tipo de autentificación Windows utiliza protocolo EAP, se basa en autentificar clientes mediante contraseñas con EAP-MSCHAPV2. El EAP dentro del PEAP (Protocolo extensible autentificación protegido) permite la autentificación de usuario basada en credenciales con PEAP Y MSCHAPV2 constituye como una solución para validar las credenciales enviadas por el usuario.

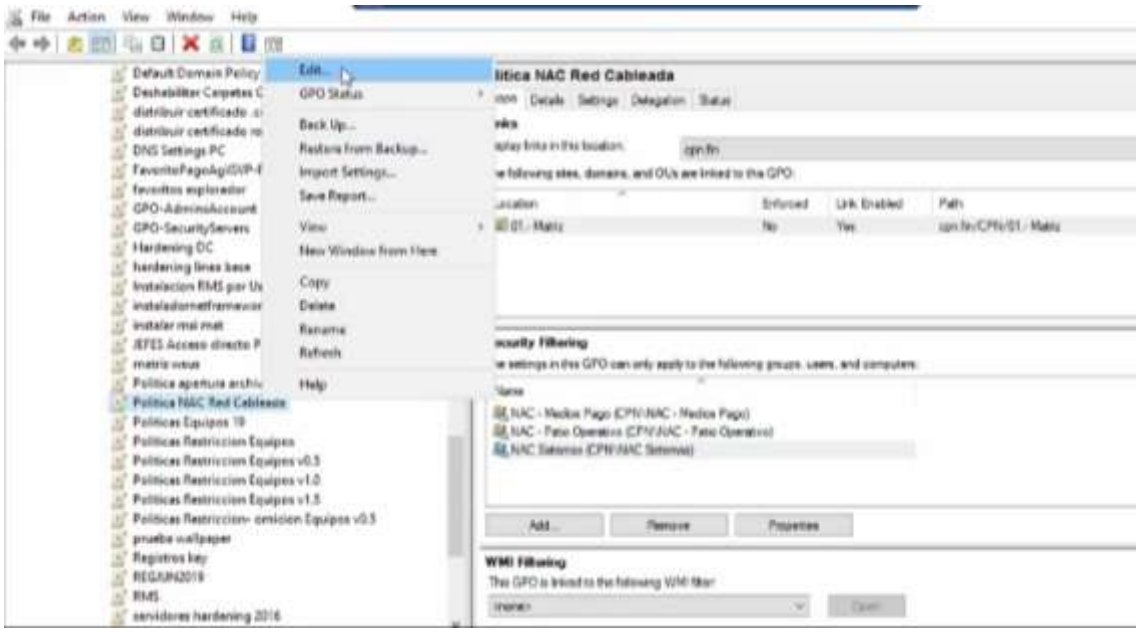

Figura 40. *Configuración de GPO*

Se configura los protocolos de la política creada para redes cableadas, para aquello en GPO seleccionamos la política y se da clic en editar.

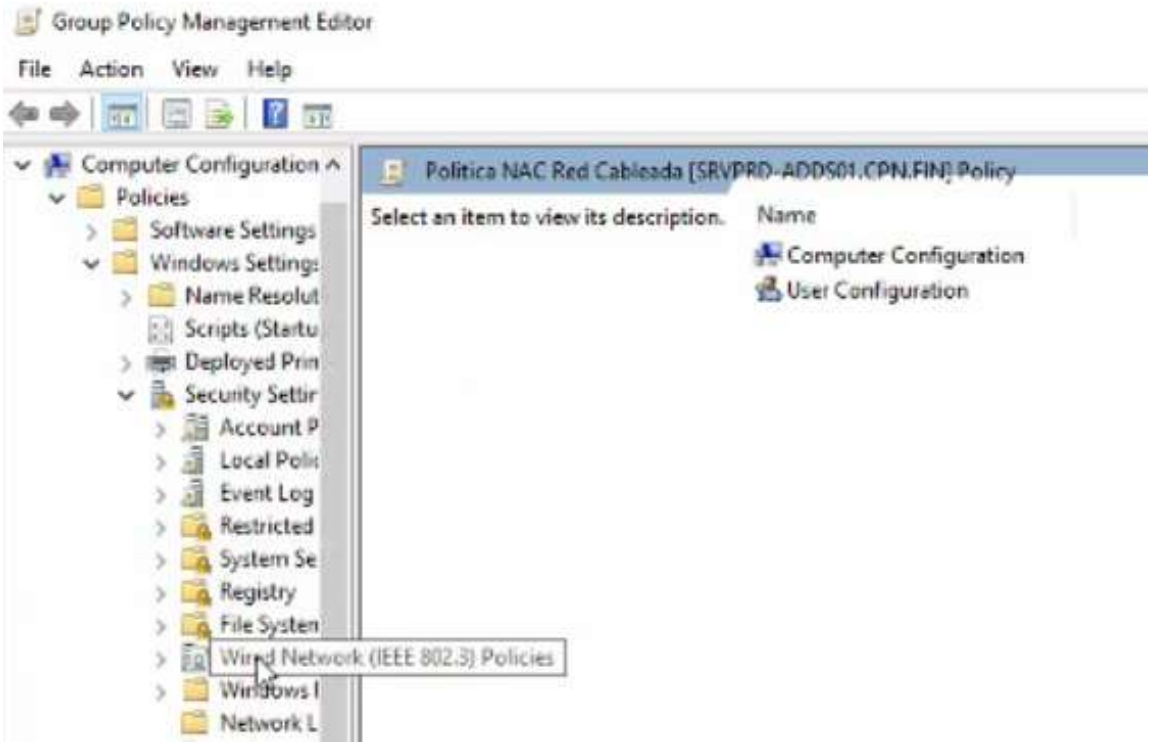

Figura 41. *Editor de grupo de políticas*

Se despliega la opciones policies, Windows setlings, Security y se escoge winred.

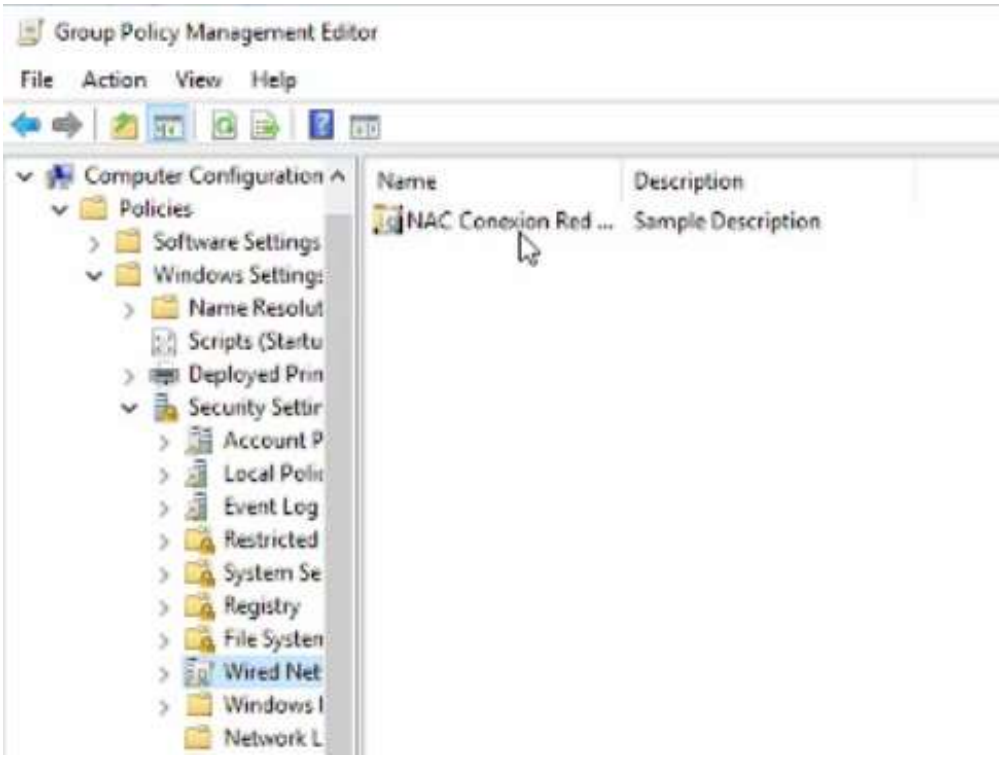

Figura 42. *Winred*

Al dar doble clic en Winred despliega NAC Conexión red cableada.

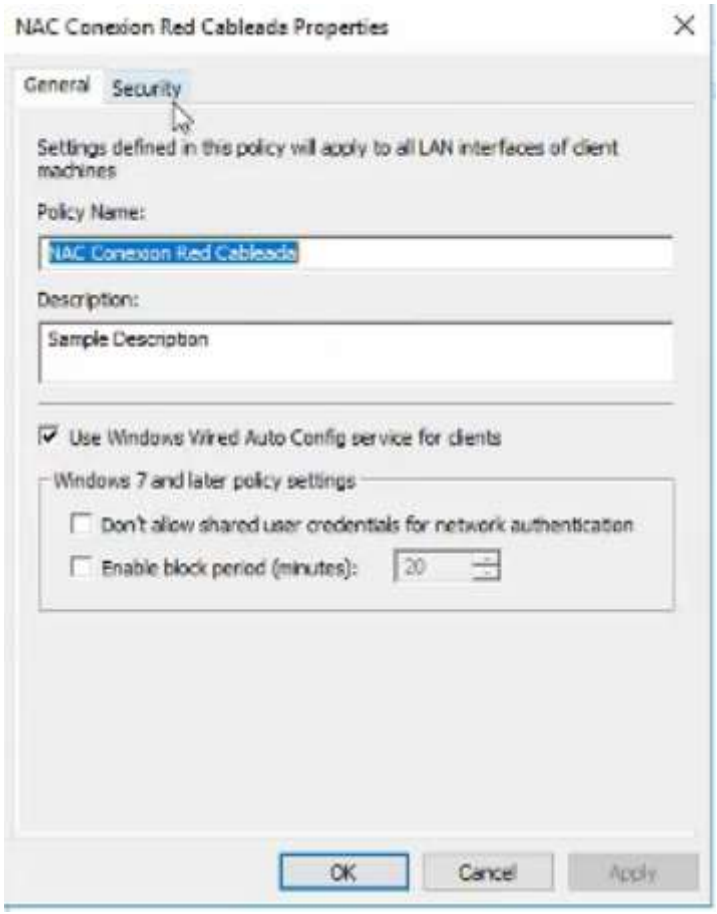

Figura 43. *Configuración general NAC*

Para la conexión cableada se ingresa el nombre de la política, la descripción y se da clic en use Windows winred.

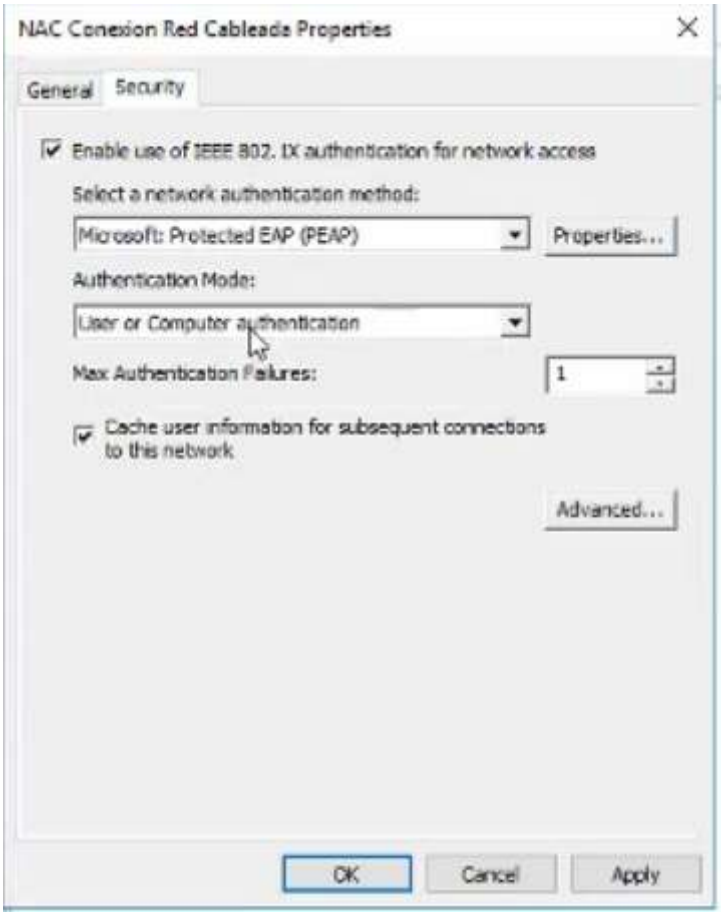

Figura 44. *Configuración NAC seguridad para red cableada*

Luego en la pestaña seguridad, se habilita la IEEE 802.1x, se escoge la autentificación PEAP, el modo de autentificación usuarios y computadoras. Por último se ingresa en la opción propiedades.

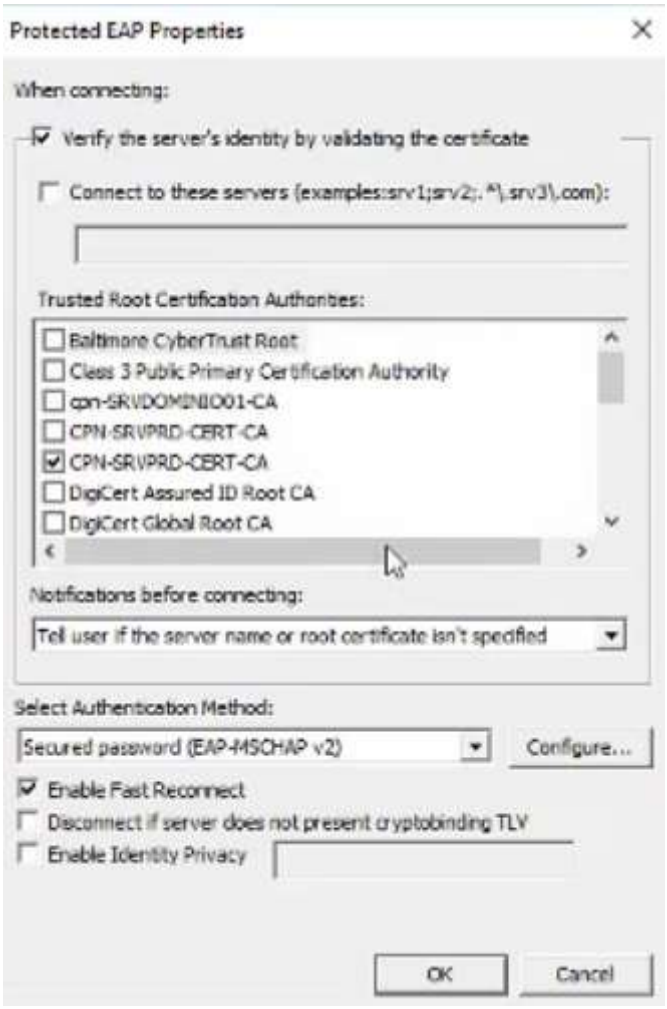

Figura 45. *Configuración EAP*

Se activa la verificación y validación mediante servidor, luego se escoge el certificado CPN-SRVPRD-CERT-CA para que los clientes se autentifiquen al servidor. Se selecciona el modo de autentificación extensible mediante el protocolo EAP para implementar el túnel de seguridad de acceso a la red y crear la capa de autentificado, el protocolo EAP utilizado es MSCHAPV2, mismo que proporciona una comunicación mutua entre el cliente y el servidor realizando el proceso de autentificación interna en Microsoft Windows.

3.2.6 El administrador de control (Extreme Management Center XMC).

Se utilizará la plataforma de NAC EXTREME debido a que la institución tiene como proveedor a Extreme, y ellos ofertan la solución requerida por la institución mediante entorno web con las características para la solución de administración centralizada.

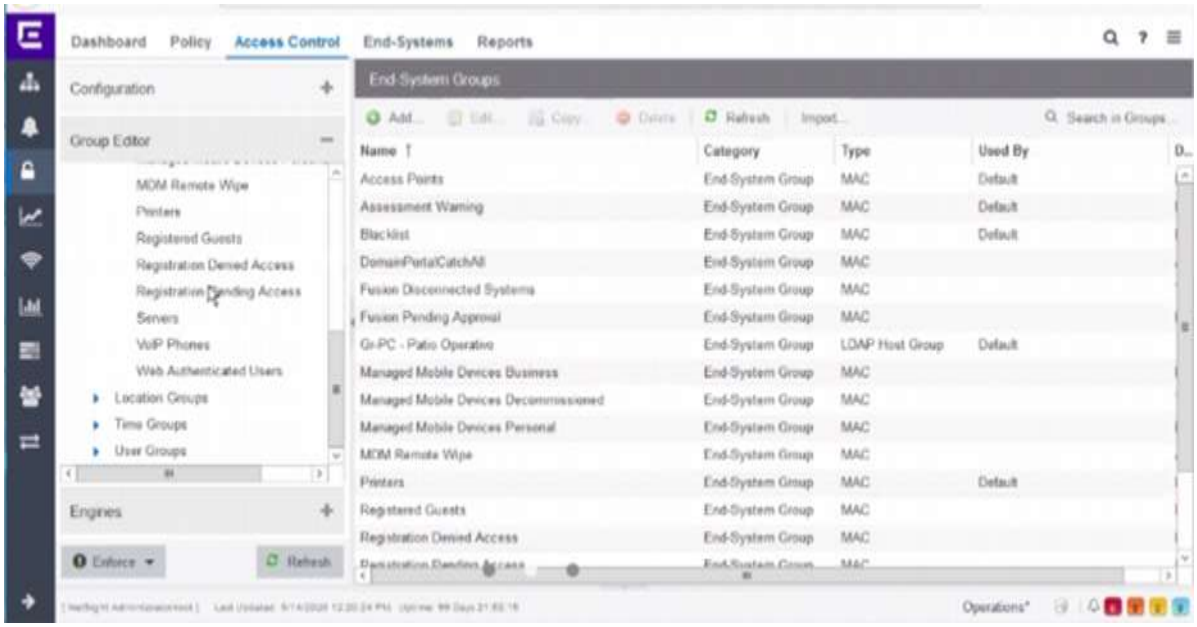

Figura 46. *Entorno XMC.*

Configuración de grupo.

En la ***CPN*** se crean los diferentes grupos de usuarios acorde a los departamentos del edificio Matriz, para el user groups los usuarios son extraídos desde el servidor LDAP.

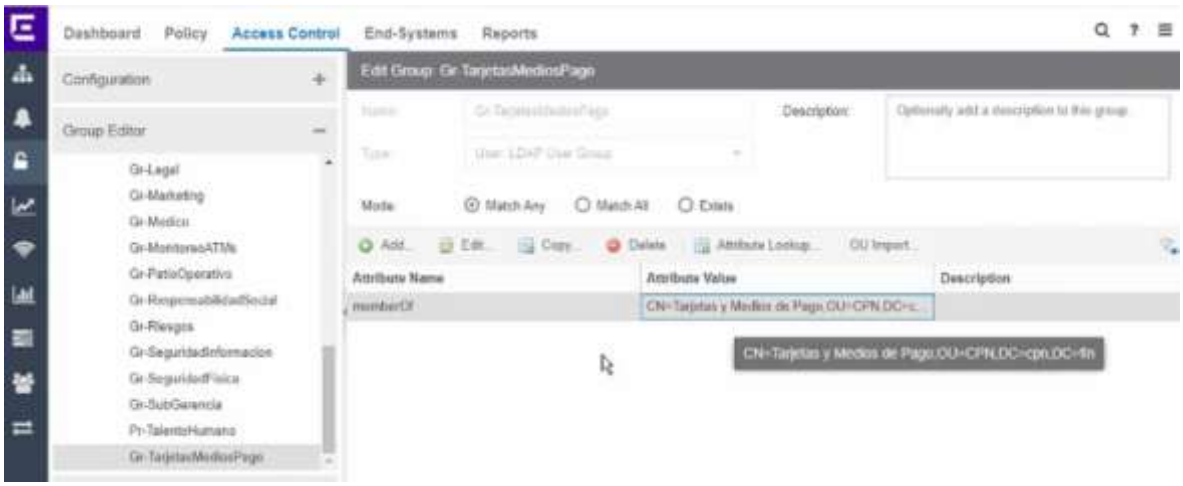

Figura 47. *User Groups*

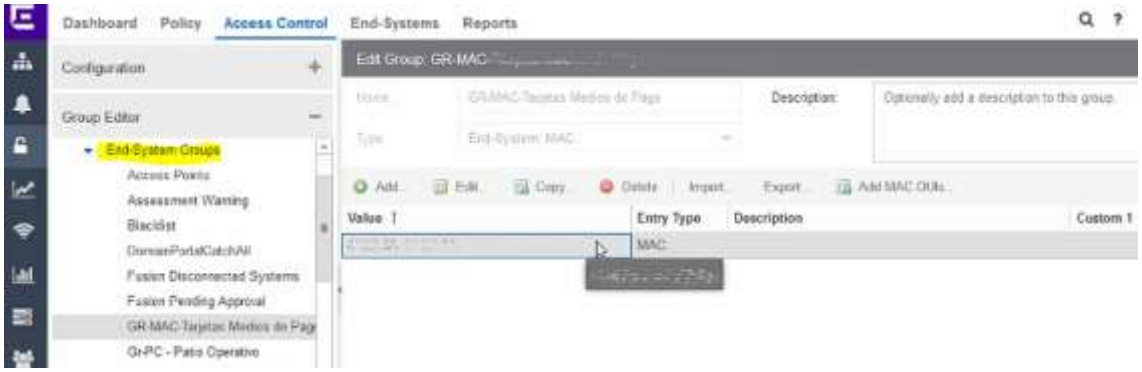

Figura 48. *End System Groups*

Vista de grupo End Systems para dispositivos que no soportan 802.1x y realizan la autentificación tipo MAC. Grupo para dispositivos finales (End System Groups) cuya función es agrupar dispositivos físicos con direcciones **MAC** y que no admitan 802.1x, por ejemplo teléfonos Avaya y de Host.

3.2.7 Reglas.

Las reglas son utilizadas para establecer la manera en que los usuarios van a ser autentificados, según el grupo al que pertenezcan se establece el tipo de autentificación y ***VLANs*****.**

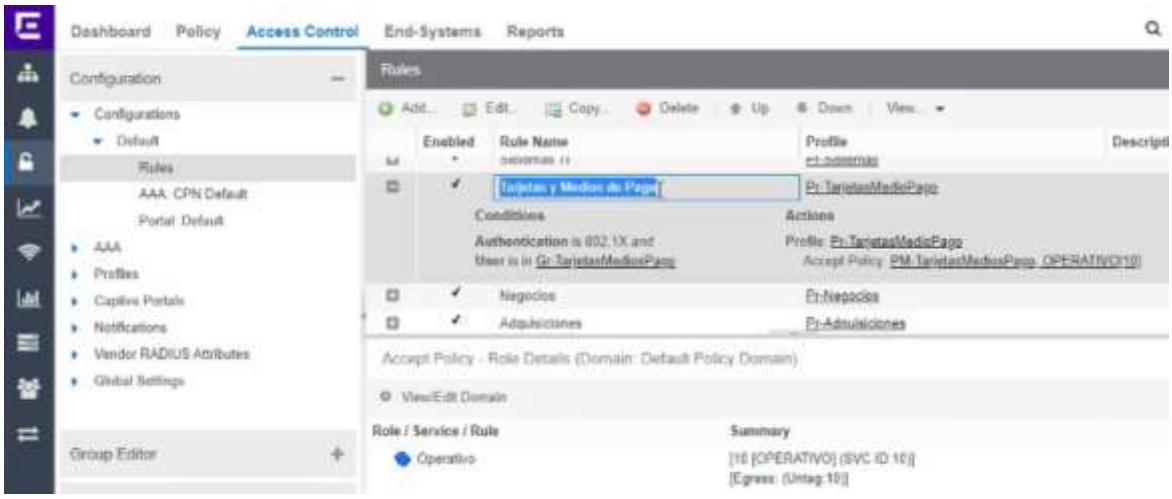

Figura 49. *Reglas*

El policy maping.

Cabe mencionar que el Policy Mappings se asocia a la regla, y permite realizar la asociación de un perfil a un id correspondiente a cada ***VLANs,***

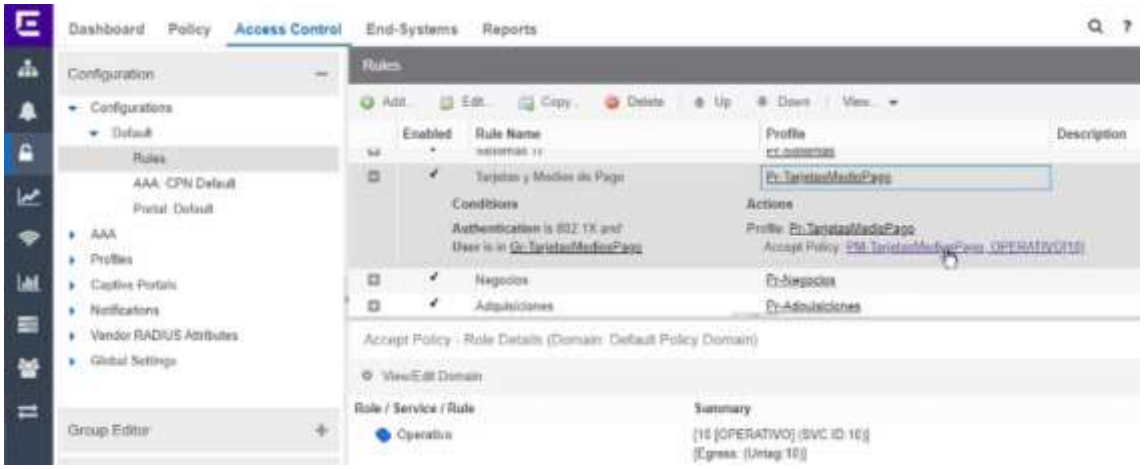

Figura 50. *Policy Rol*

Por ejemplo esta autentificación se asocia al policy rol operativo ***Vlan*** 10.

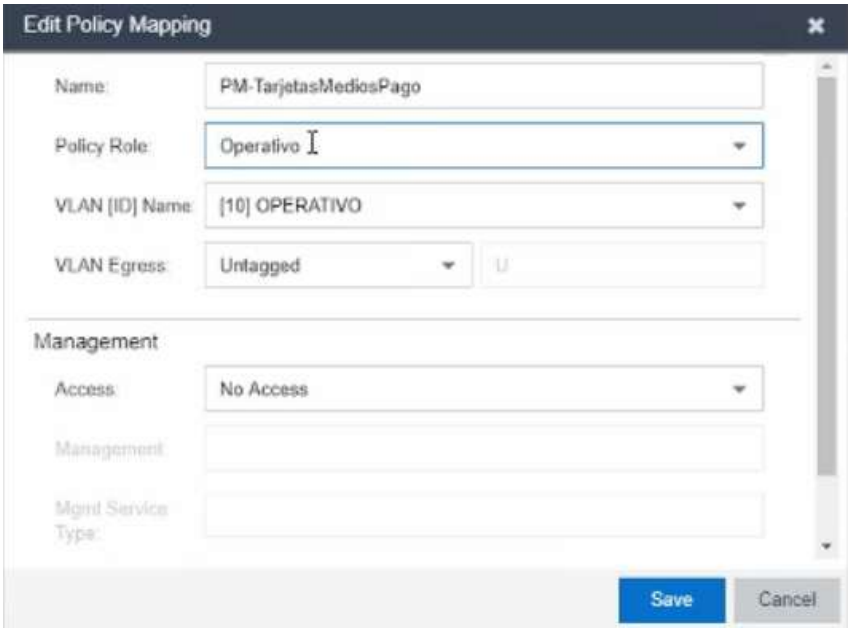

Figura 51.*Policy Mapping*

Configuración de directivas (Policies).

En esta parte se puede configurar y controlar el tráfico de la red, aquí se puede establecer parámetros de acceso a la red, tales como transformación de VLANs y parámetros de calidad de servicio.

Roles.

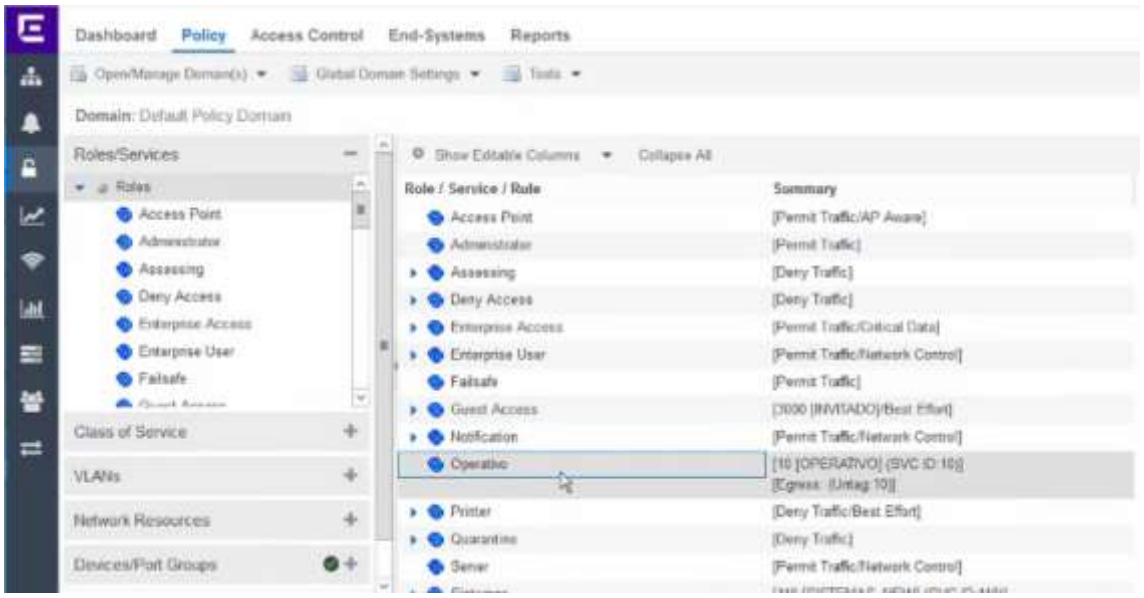

Figura 52. *Roles*

Todo el que se autentifique con medio de pagos se asocia al policy maping que asigna el rol operativo, operativo lo que hace es contener todo el tráfico en la ***Vlan*** 10.

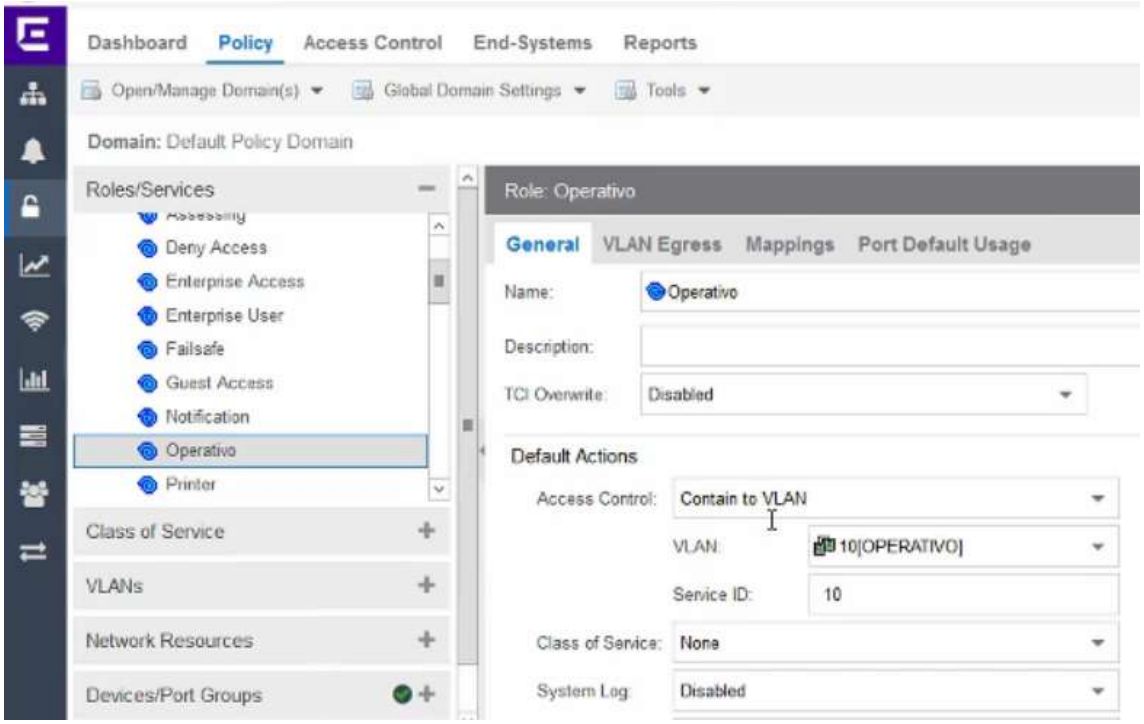

Figura 53. *Rol operativo*

Se observa la configuración general del rol operativo y la ***Vlan*** a la cual está asociado el rol.

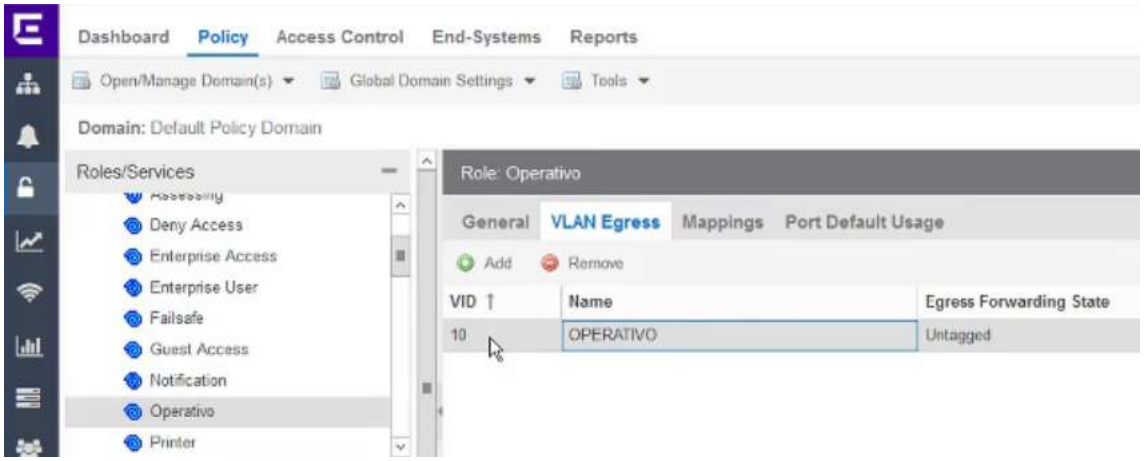

Figura 54. *Tráfico Vlan 10*

En el egreso sale como no tallado el tráfico en la ***Vlan*** 10.

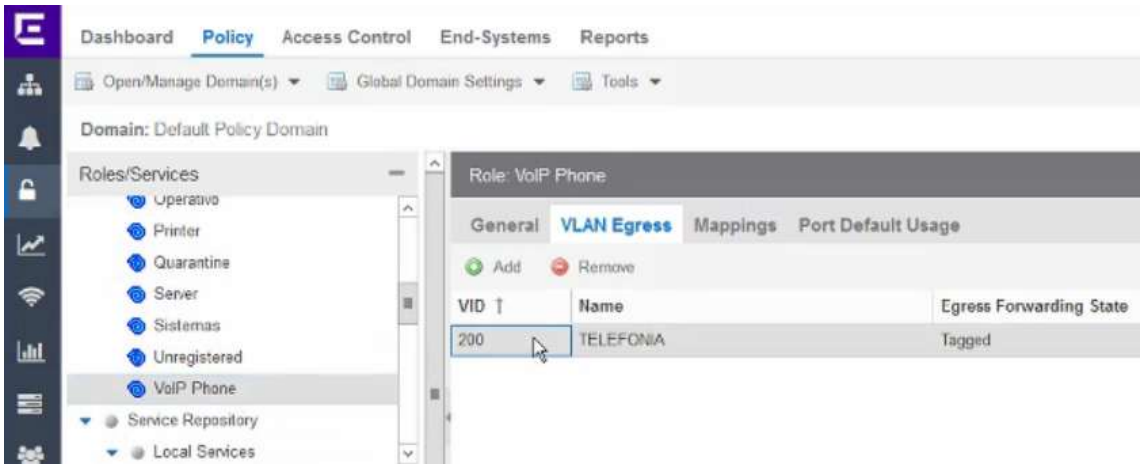

Figura 55*. Tráfico Vlan 200*

En la gráfica anterior se muestra la Regla para teléfono en la ***Vlan*** 200 pero tageado.

3.2.8 Diseño y estructura del escenario NAC.

A continuación se muestran los diferentes diseños del escenario para el proceso de solicitud de acceso a la red, NAP (802.1X) y el funcionamiento del RADIUS.

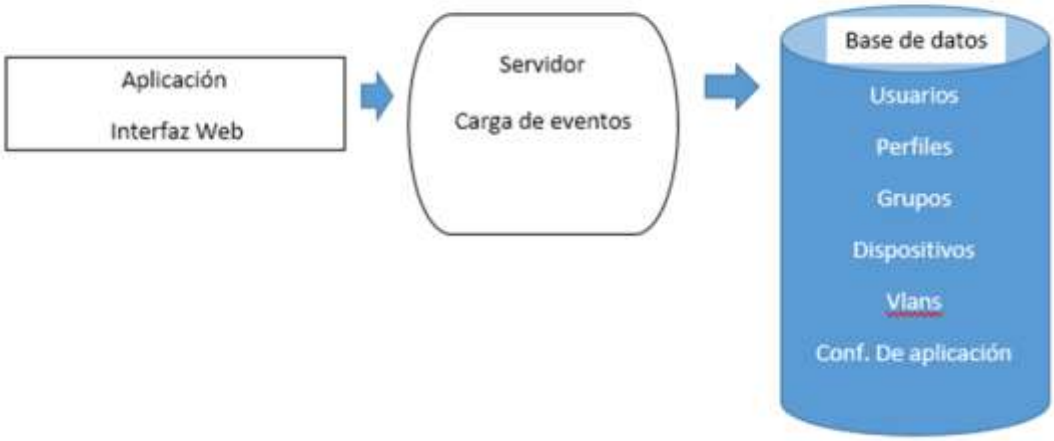

Figura 56. Arquitectura Lógica NAC en la CPN

La arquitectura de NAC Extreme Management Center es de tipo cliente servidor basadas en tres capas.

Dispositivos que integran el NAC.

En la siguiente gráfica se muestran los dispositivos y nodos que intervienen en la solución de control de acceso.

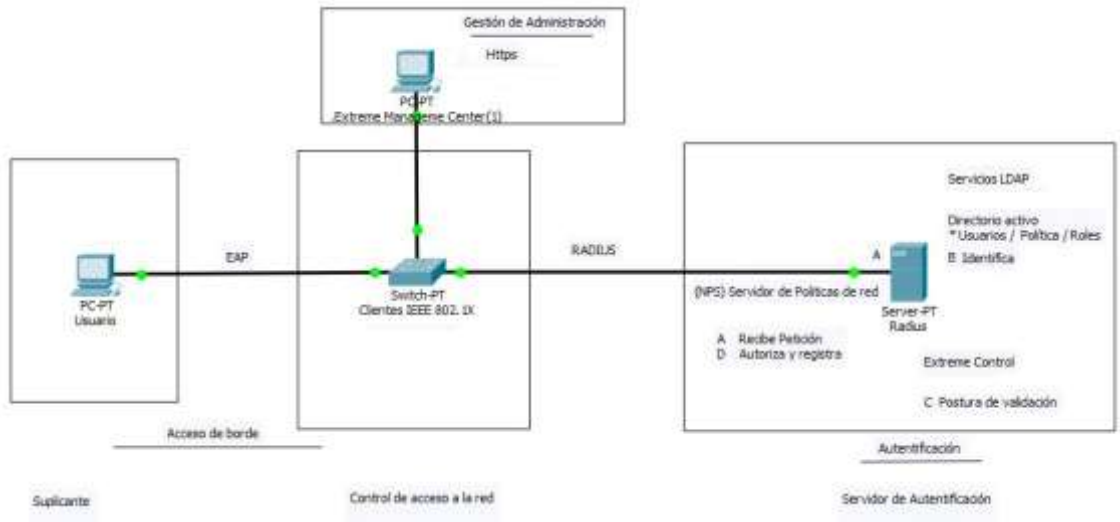

Figura 57. *Arquitectura Física NAC en la CPN*

La tecnología 802.1x para el control de acceso mediante puertos en un Switch, los componentes de autentificación son los el siguiente:

- ✓ Se menciona como solicitante al computador que intenta obtener recursos de la red Ethernet.
- ✓ El componente que hace de medio de acceso es el Switch que permite o desniega el acceso a la red por parte del solicitante.
- ✓ El servidor que autentifica y valida las credenciales recibidas del solicitante y deniega o autoriza el acceso en base a las políticas establecidas.
- ✓ La plataforma XMC es un entorno web con las características para la administración centralizada del NAC.

Tabla 4. *Elementos del NAC.*

Acceso de borde	**Autentificación**	**Gestión de Administración**
Switch Solicitante	Server Radius	Administrador de Control (XMC)

Proceso de autentificación.

En la siguiente grafica se muestra el escenario de autentificación y control de acceso.

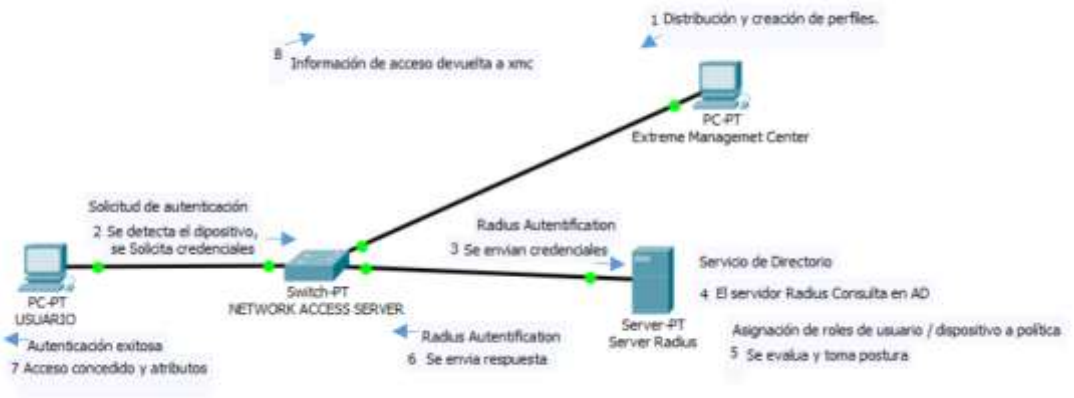

Figura 58. *Arquitectura despliegue NAC en la CPN*

1. En primer lugar se crean las políticas de autentificación para grupo de usuario según el perfil.

2. Al momento que un usuario se conecta al puerto de red e intenta conectarse a la red, la tarjeta de red detecta que hay un usuario que intenta acceder al usuario y por ende a la red, se procede a realizar la autentificación mediante el ingreso de las credenciales de usuario de dominio.

3. Se envían las credenciales del usuario al servidor Radius de autentificación.

4. El servidor Radius procede a evaluar las políticas de seguridad de acuerdo a las credenciales enviadas.

5. Una vez realizado el proceso de autentificación se asigna el entorno al usuario de acuerdo a los roles y las políticas que se establecen los permisos obtenidos para el usuario autentificado y hacer uso del dispositivo conectado a la red

6. Se procede autorizar el acceso a la red al usuario con su perfil correspondiente.

7. Se procede a permitir el acceso a la red con los privilegios correspondientes, el usuario ya está dentro del entorno de la red.

8. Se envían los resultados de la autentificación y la información del acceso a la red.

Propuestas del diseño.

Con el propósito de mitigar las vulnerabilidades detectadas de los indicadores Autorización, Auditabilidad, Autenticación del CAP II, se realiza la siguiente propuesta.

- ✓ Implementar una administración de red centralizada.
- ✓ Controlar de manera automática y validar las credenciales del usuario que intenta acceder a la red.
- ✓ Configurar políticas y reglas que permitan autentificar el acceso a la red mediante 802.1 x.

Con los aspectos mencionados mitigan los problemas de vulnerabilidades y las falencias de la aplicación de la norma ISO 27001, tanto para controlar el acceso a la red y configurar los puertos para que sean seguros.

4 CAPÍTULO IV

4. Implementación del prototipo.

En el siguiente Capítulo se implementa la configuración realizadas en el CAP III mediante la utilización de Extreme Management Center, el servidor RADIUS y el AD.

4.1 Configuración de Prototipo.

De acuerdo con las políticas configuradas en el capítulo III, subtitulo 3.2.5 se procede a verificar que se apliquen las políticas en el host.

Figura 59. *Configuración NAC para adaptador de red cableada*

Se observa que está habilitado en el host la autentificación de IEEE 802.x y el protocolo PEAP de acuerdo las políticas diseñadas en el capítulo III.

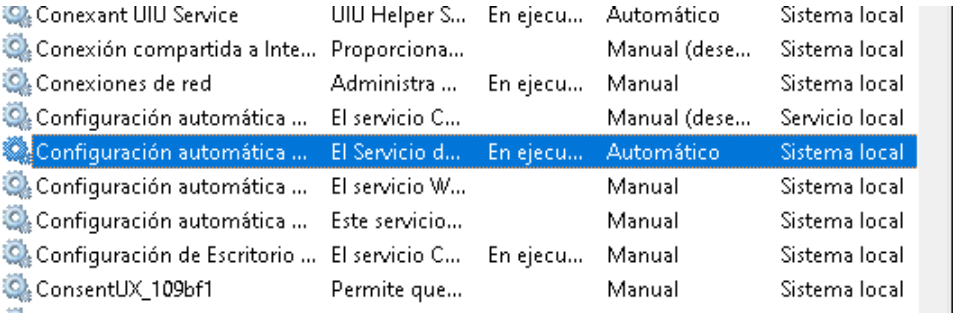

Figura 60. *Servicio de Red Cableada*

Se aplica en el host el servicio de configuración automática de redes cableadas de acuerdo a la política configurada en el CAP III.

Figura 61. *Gestor de Administración*

Se realiza el inicio de sesión en el portal de administración centralizada.

```
10.1.10
48:0F:C
```

Figura 62. *Datos del host*

Se identifica la ***IP*** y ***MAC*** del equipo.

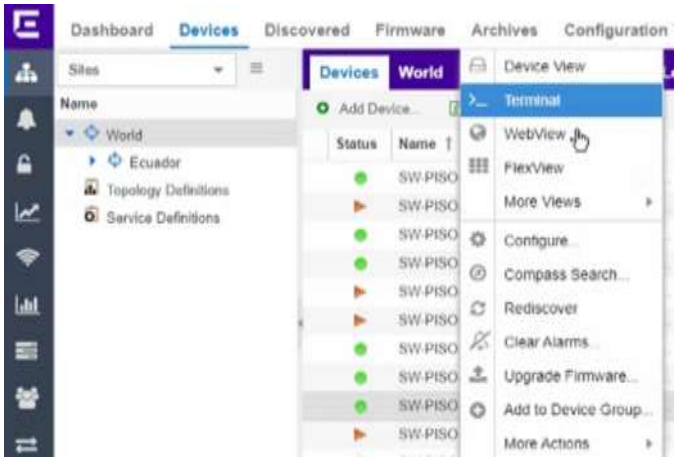

Figura 63. *Switch*

Se identifica el switch en el cual está conectado el host, posteriormente se da clic en el switch y se abre el terminal.

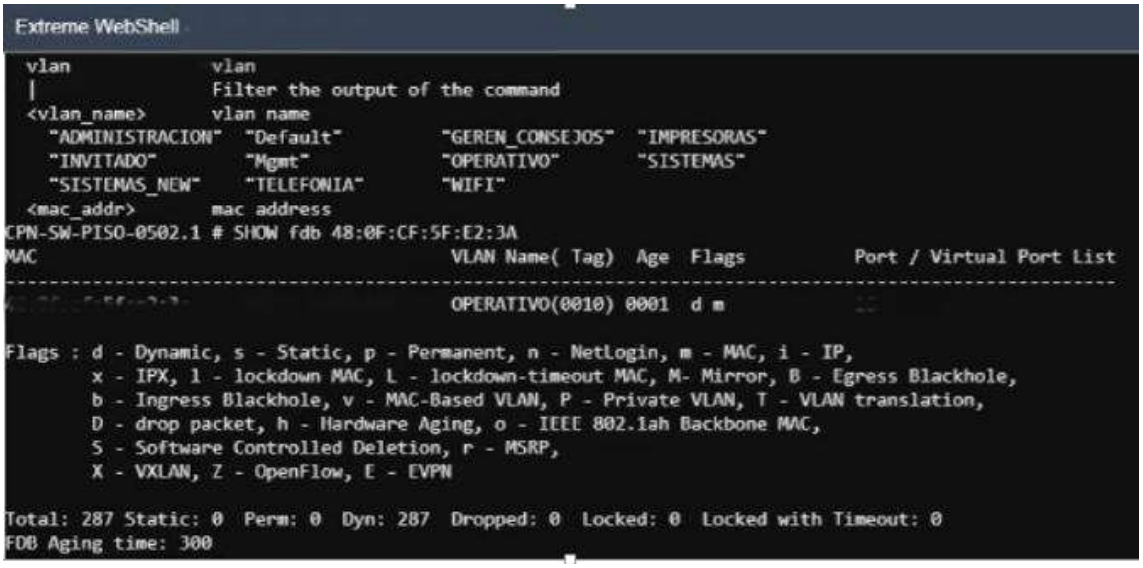

Figura 64. *Verificación de conexiones*

Se verifica el puerto en cual está conectado el host mediante la ***MAC.***

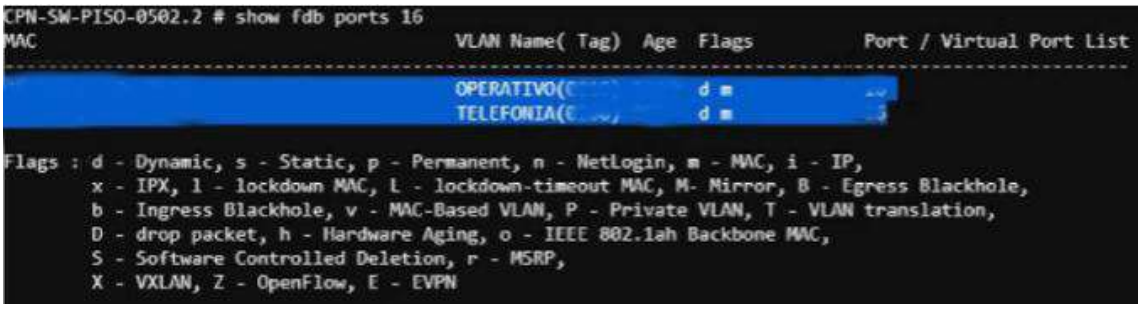

Figura 65. *Validación de conexiones*

Se puede comprobar que dos equipos están intentando establecer conexión en el puerto 16.

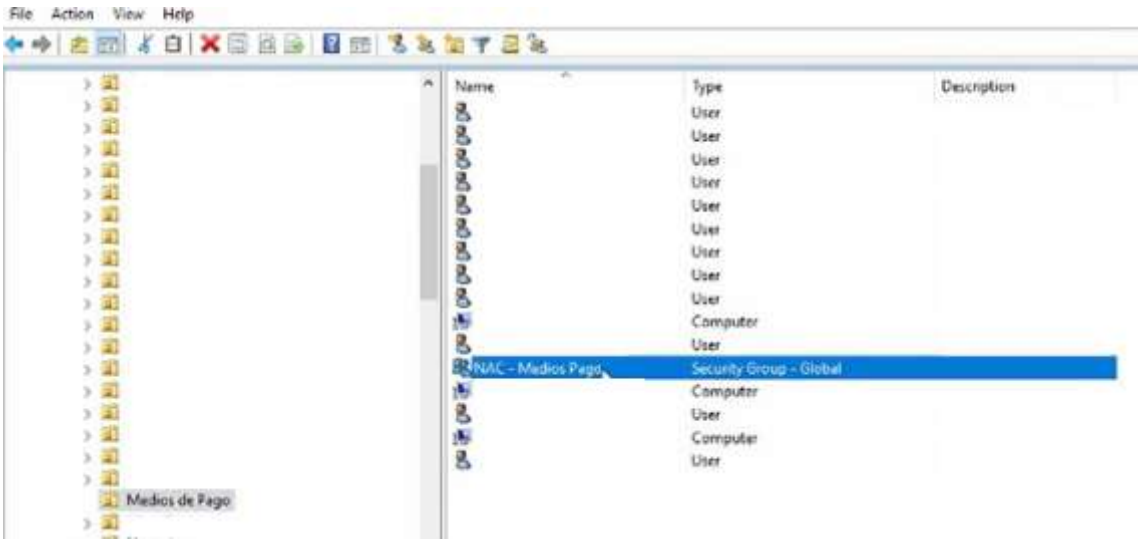

Figura 66. *AD – usuarios y grupos*

Se Ingresa al grupo medio de pago, mismo que tiene mapeado equipos y se identifica el grupo NAC – medios de pagos, el cual está asociado a la políticas de redes cableadas establecido en el capítulo III, subtitulo 3.2.5, figura 39. Una vez identificado el grupo ***NAC*** lo abrimos con doble clic.

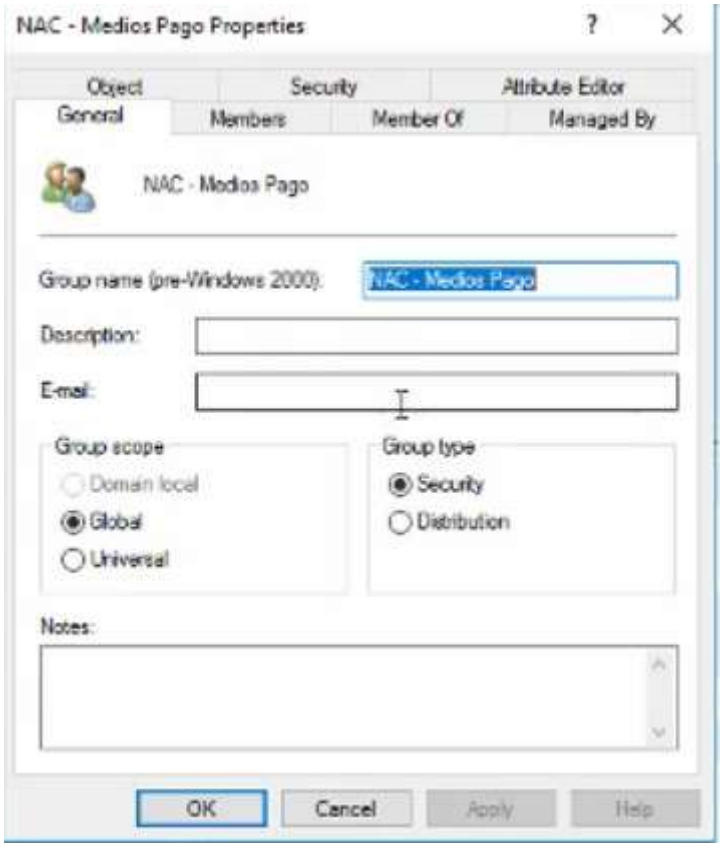

Figura 67*. Grupo NAC*

Se escoge la pestaña miembros y se da clic.

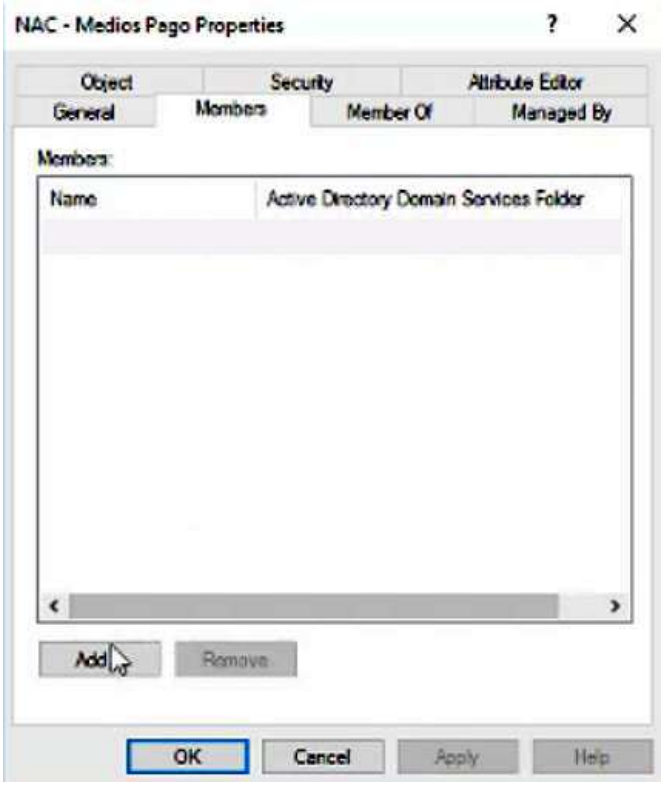

Figura 68. *Propiedades de grupo NAC*

Luego se escoge la opción añadir.

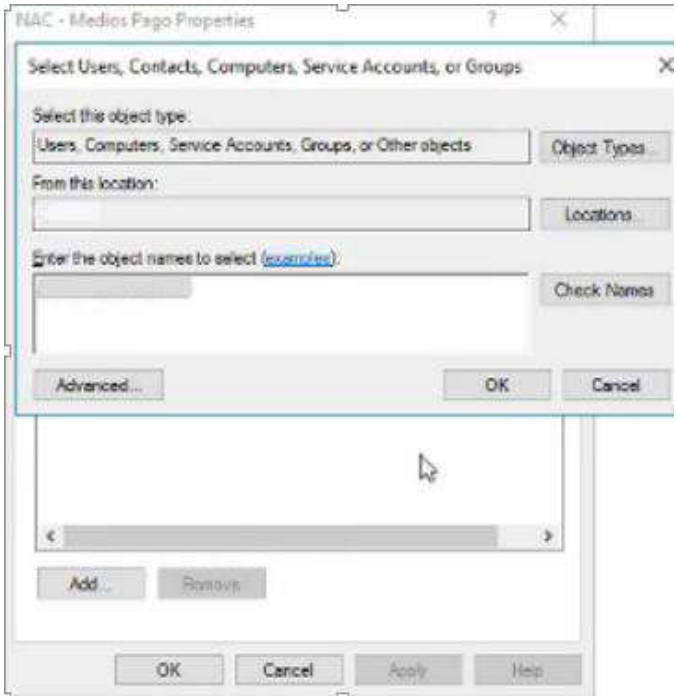

Figura 69. *Selección de host*

Se ingresa el nombre del host al grupo.

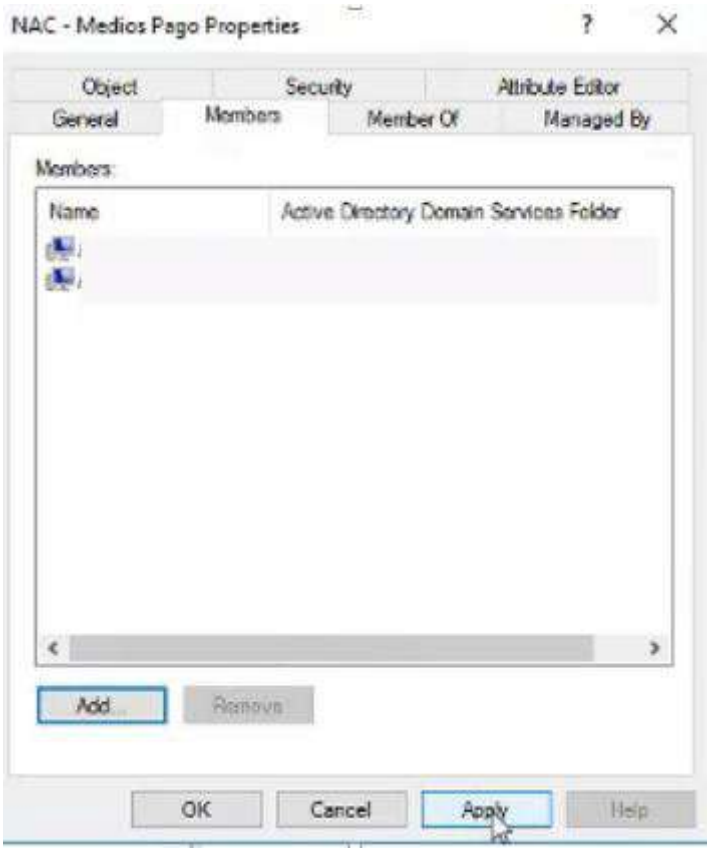

Figura 70. *Vista de Miembros de grupo*

Una vez añadimos el host se guarda y luego se aplica.

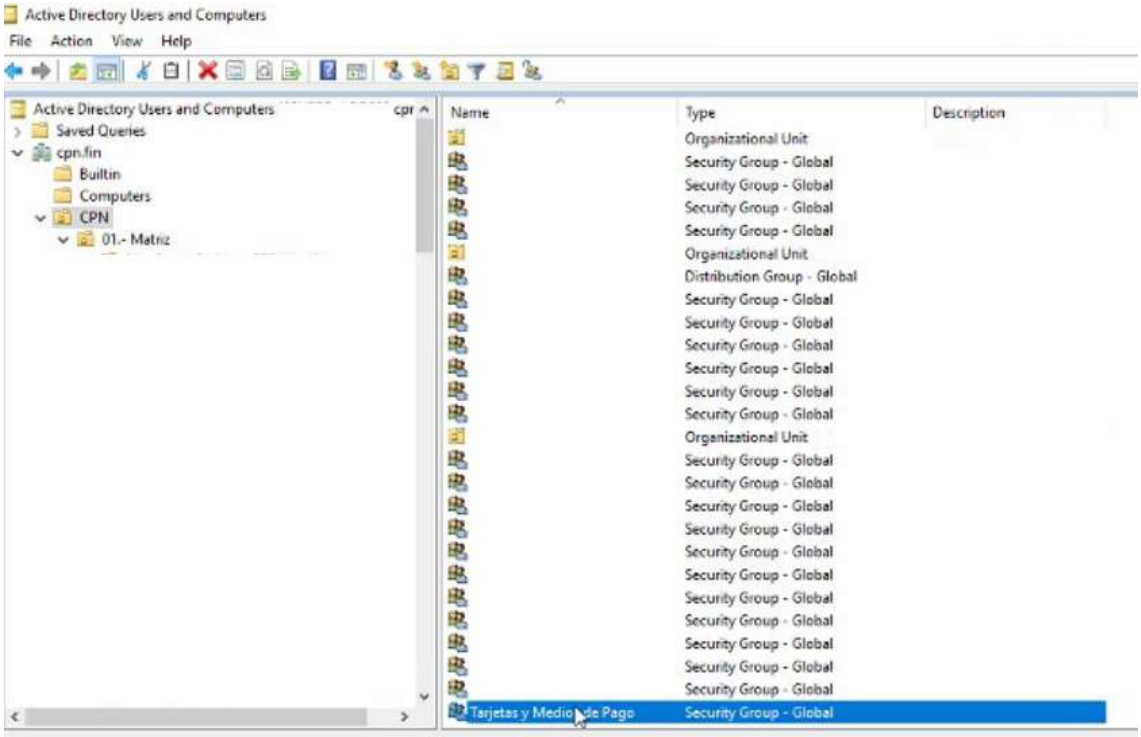

Figura 71. *Grupos de AD*

Una vez añadido el equipo al grupo NAC, se procede añadir al usuario al grupo.

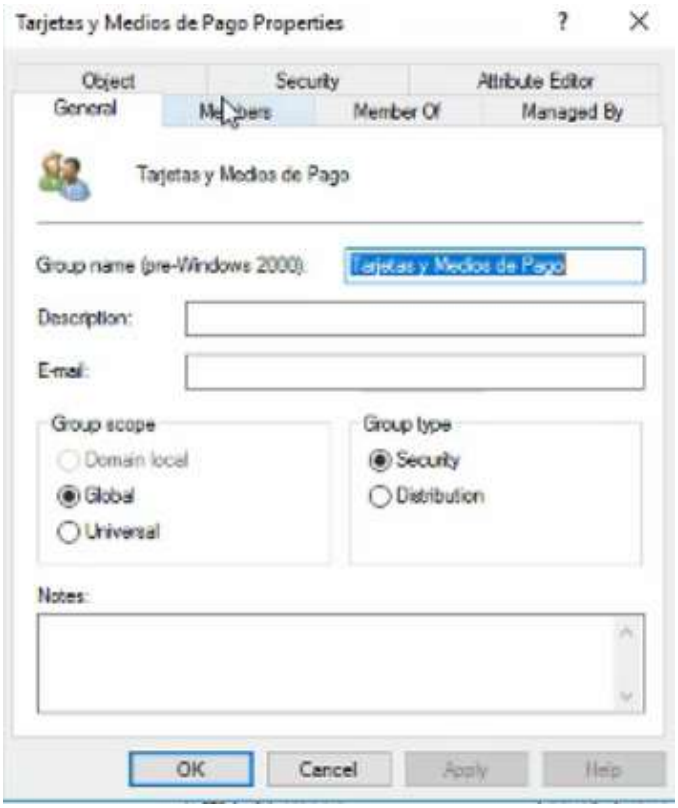

Figura 72. *Miembros de grupo*

Se abre el grupo y se escoge la pestaña miembros.

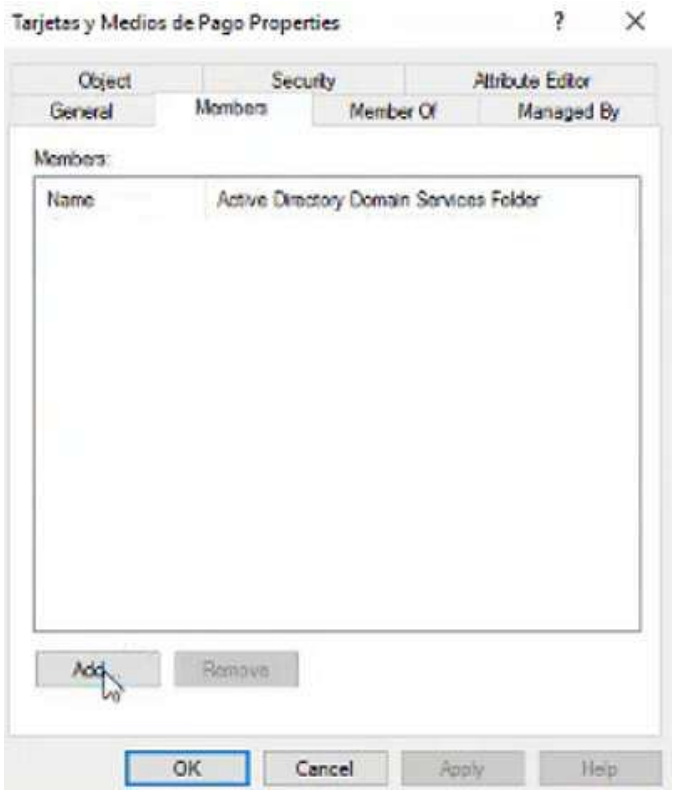

Figura 73. *Vista de miembros grupo tarjetas y medios de pagos*

Se escoge la opción añadir.

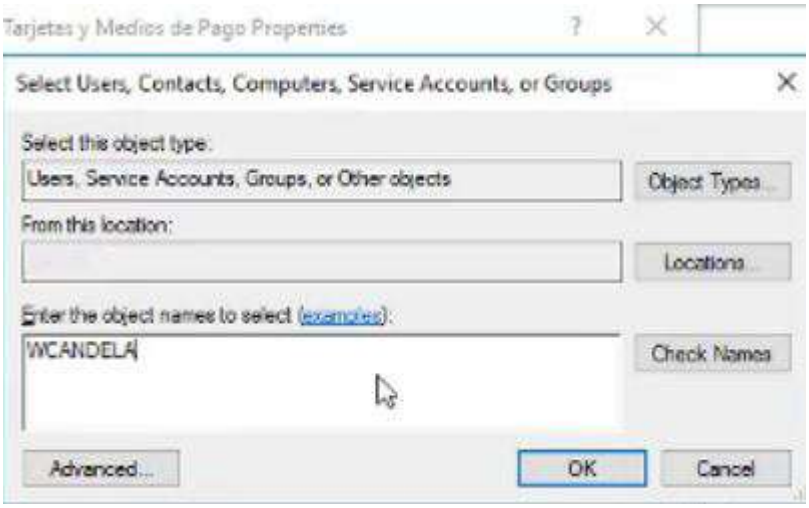

Figura 74. *Selección de usuario*

Acorde ha como esta creado en el AD el usuario, se añade al grupo.

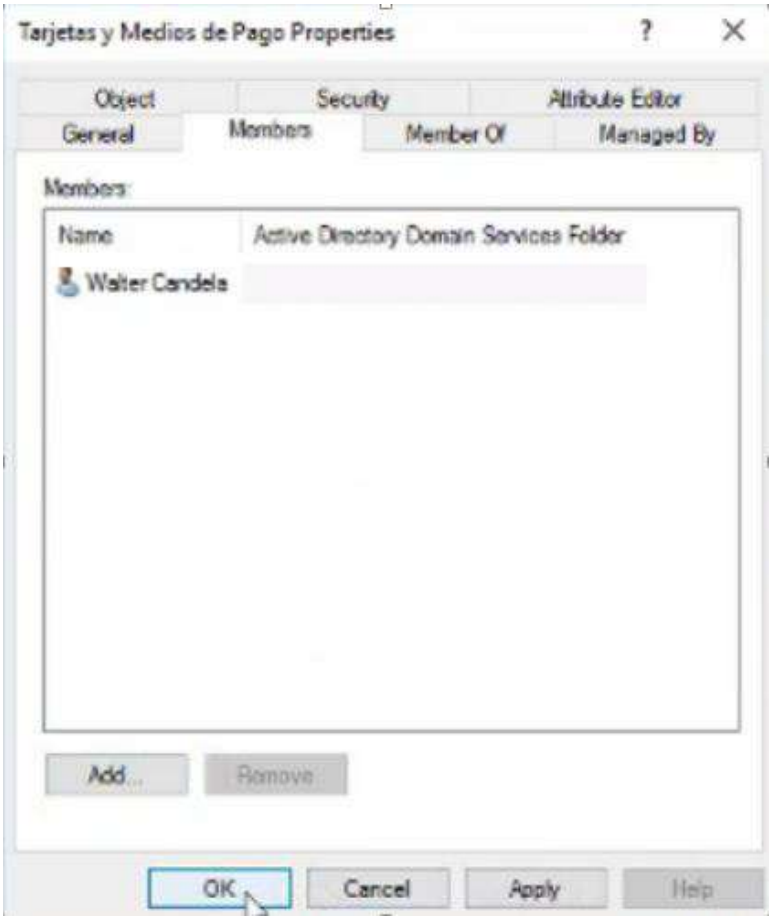

Figura 75.*Vista de miembros de grupo*

Se aplica y guarda los cambios realizados.

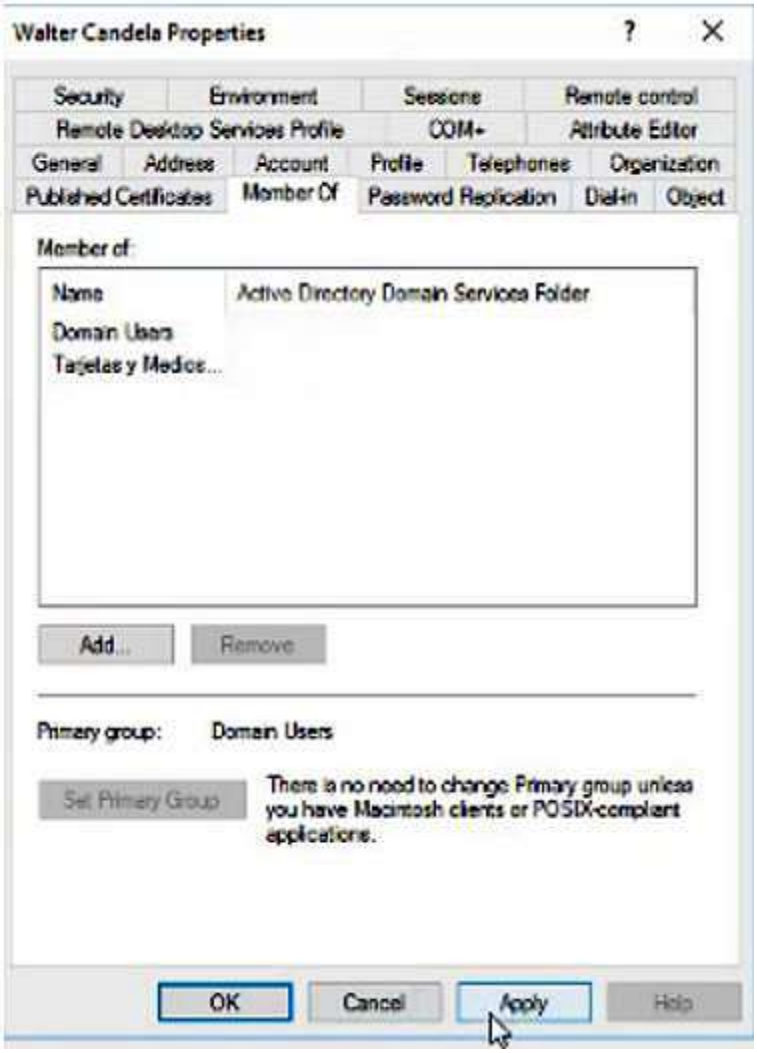

Figura 76. *Registro de grupos para usuario*

Se observa que el registro fue satisfactorio. Una vez añadido el usuario al grupo medio de pagos se le aplican las Reglas y policy Mapping configurados en el capítulo III, subtitulo 3.3.5.

A continuación se configura el puerto del Switch.

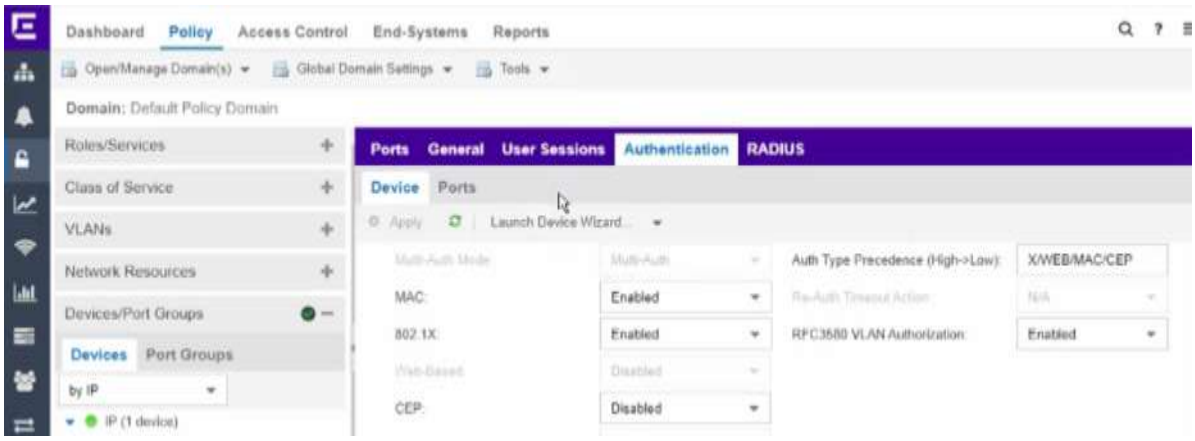

Figura 77. *Configuración de puertos*

De acuerdo a la configuración realizada del Switch en el capítulo III, subtitulo 3.4, se habilita autentificación MAC y 802.1x en nivel autentificación por puerto entre el switch y el dispositivo.

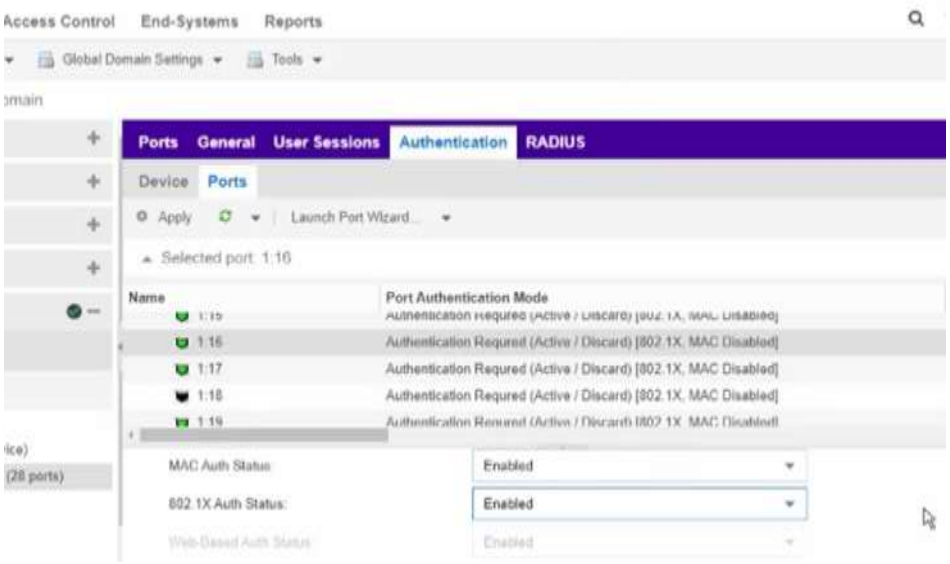

Figura 78 *Autentificación de puertos*

En la pestaña ports aparecen los diferentes puertos del Switch, se habilita autentificación MAC y 802.1x en nivel autentificación por puerto, en este caso puerto 16.

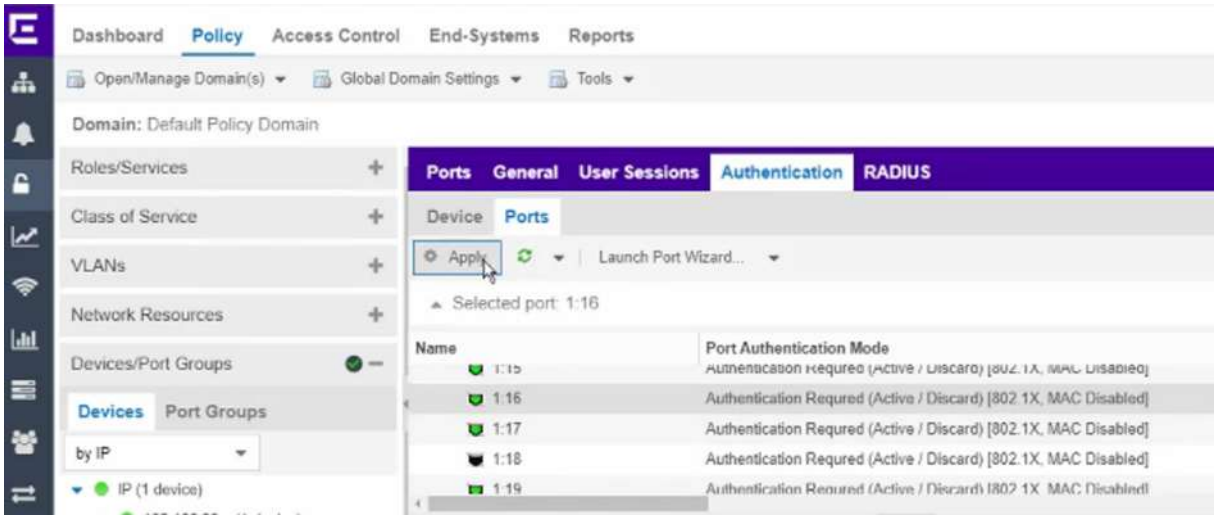

Figura 79. *Vista de autentificación de puertos*

Se procede a dar clic en aplicar para guardar los cambios.

4.2 Proceso de autentificación.

La configuración de autentificación fue realizada mediante LDAP, aquello permite que los usuarios mediante sus credenciales de Activite Directory puedan ser autentificados y accedan a la red.

4.2.1 Detección.

En este proceso la electrónica de red detecta que existe un dispositivo conectado al puerto e intentando acceder a la red.

La detección está compuesta por la identificación del dispositivo, esto se logra mediante la propia dirección ***MAC*** del equipo, aquí se determina en que ***VLANS*** se encuentra conectado el equipo, los clientes que están conectados a la red pueden estar con el perfil arrendatario ***DHCP*** o ***IP*** fija, estos aspectos que sirven para detectar el equipo son considerados las huellas dactilares del host. Es decir aquí se detecta el host que intenta acceder a la red.

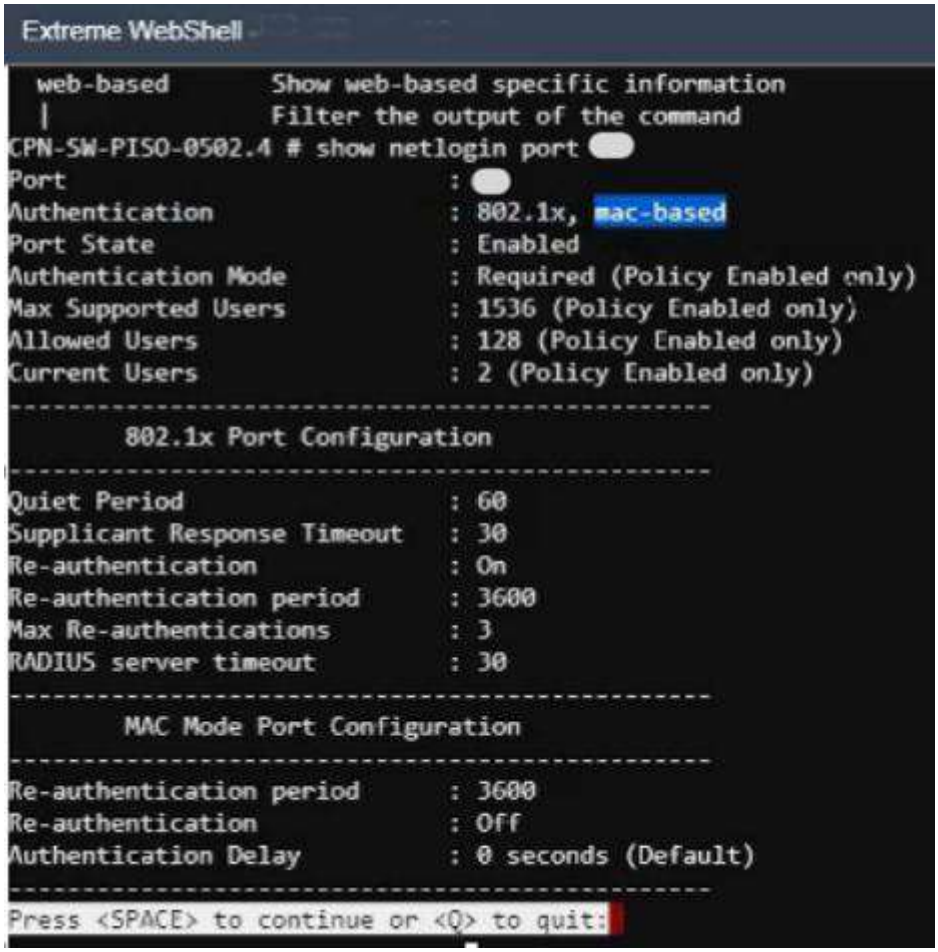

Figura 80. *Detección del host*

De acuerdo a la configuración realizada del switch en el subtítulo 3.2.3, en la figura 80 se observar que efectivamente se habilita la autentificación en puertos por 802.1x y MAC, los clientes se intentan autentificar mediante 802.1x y por MAC. Se valida la dirección MAC del computador y la VLAN en la que se encuentra conectado.

4.2.2 Autentifica.

El proceso de autentificar consiste en la verificación del usuario mediante él envió de las credenciales y por ende la validación del dispositivo mediante la MAC dispositivo, el host envía las credenciales al servidor AAA.

Figura 81. *Ingreso de credenciales.*

El servidor AAA requiere las credenciales del usuario, se ingresan y envían credenciales de autentificación de Windows. La autenticación es el proceso intermediario en la validación de la identidad del usuario, el host responde a la petición con las credenciales.

4.2.3 Acceso.

Para el proceso de acceso a la red se valida mediante el servidor AAA las credenciales del usuario y las políticas establecidas, en base al cumplimiento se toma la postura de autorización acorde al perfil correspondiente.

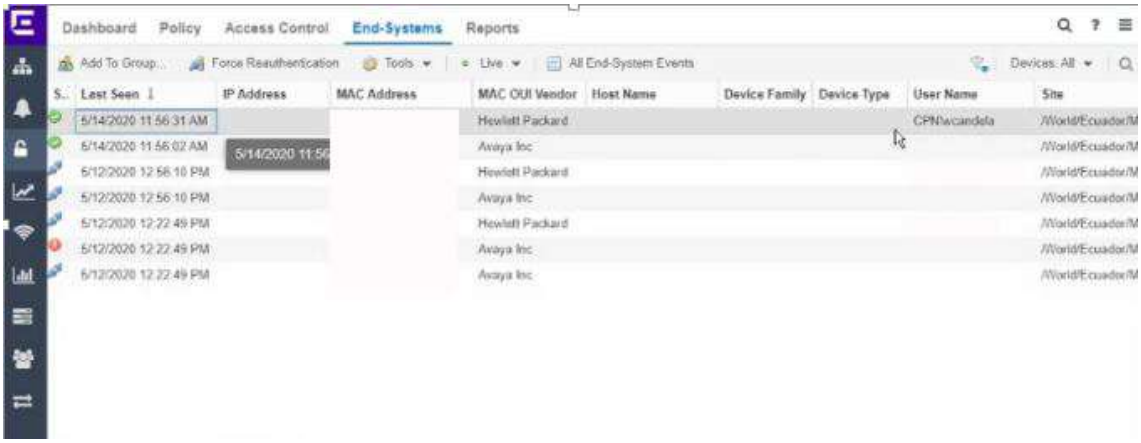

Figura 82. *Autentificación del host*

En la plataforma de extreme se puede observar el registro con hora y fecha del proceso de autentificación la MAC del equipo y el usuario que solicito el proceso de acceso a la red mediante la autentificación NAC con las credenciales de usuario.

Figura 83. *El host responde con las credenciales*

Podemos validar el usuario que se autentifica, el sitio Ecuador Matriz la ip del switch, y la ubicación del switch. La evaluación se aplica al dispositivo que pretende acceder a la red, las políticas y reglas establecidas en el capítulo III, subtitulo 3.2.5 y 3.2.7.

***Figura 84**. Postura local*

El servidor AAA agrega resultados individuales sobre la postura resultante en base al cumplimiento de las políticas y procede asignar las VLANS correspondiente para el host de acuerdo a la postura de autorización o la denegación. La evaluación se aplica al dispositivo que pretende acceder a la red, las reglas establecidas en el capítulo III, subtitulo 3.2.7.

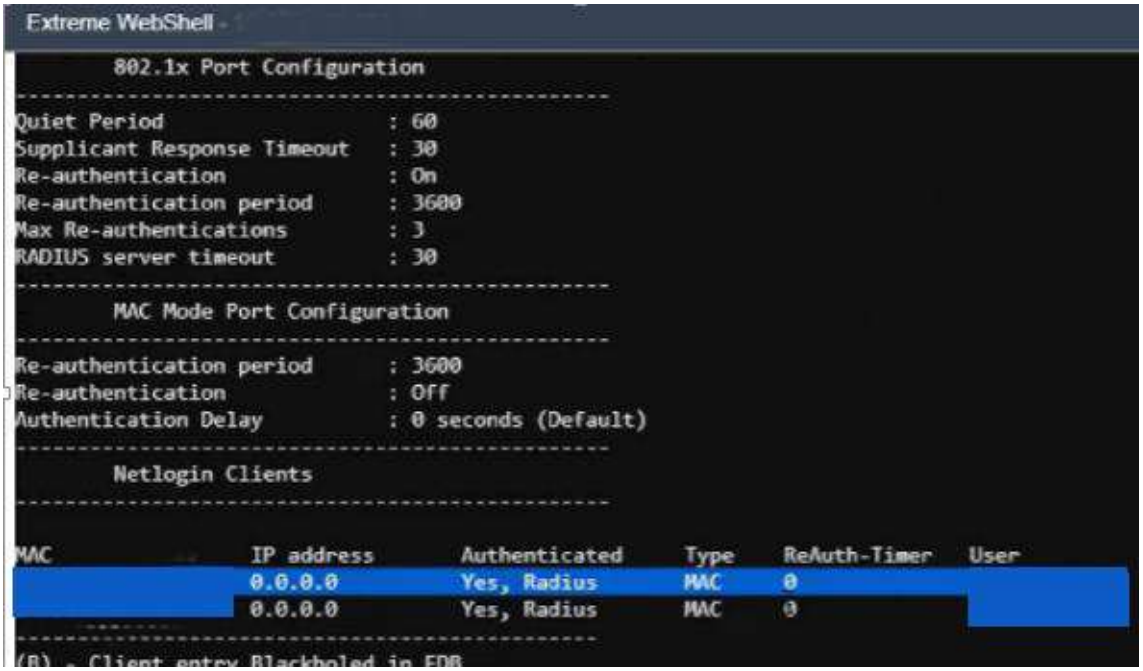

***Figura 85.** Validación de autentificación*

Se valida efectivamente mediante extreme que el usuario logro autentificar y obtener acceso.

4.2.4 Autoriza.

En el Control de acceso al obtener la autorización, la tarjeta de red realiza el proceso de autentificación y se obtiene la VLANS con los permisos correspondientes para hacer huso del internet.

Figura 86. *Vista de postura de autorización*

De acuerdo al perfil y política correspondiente con la autentificación 802.1x y el teléfono.

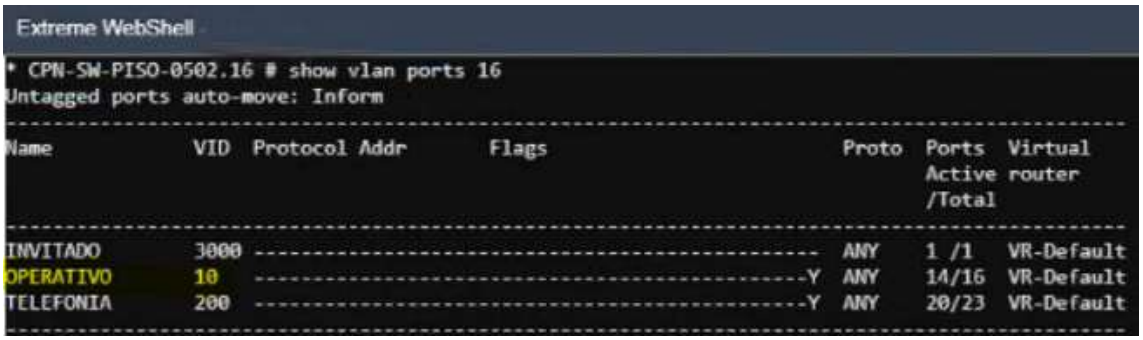

Figura 87. *Postura de autorización*

Luego de ser autentificado, se autoriza y se asigna el perfil se entrega la VLAN a la que corresponde el equipo se asigna al usuario la red operativo 10.1.10 vlan 10.

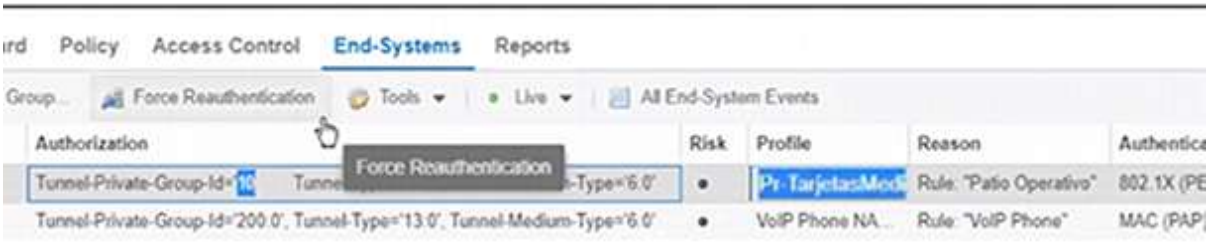

Figura 88. *Autentificación e identidad*

En la gráfica anterior se realiza el proceso de autentificación mediante el túnel de seguridad de 802.1x (PEAP), se valida el perfil asignado al usuario (TarjetaMediosdePagos), se asigna el id 10 para VLANS, y se obtiene el acceso a la red en base a las reglas establecidas en el capítulo III, subtitulo 3.2.7.

4.2.5 Remediación.

La remediación está compuesta por dos posturas asignar la ***VLANS*** de invitado o la denegación del acceso a la red.

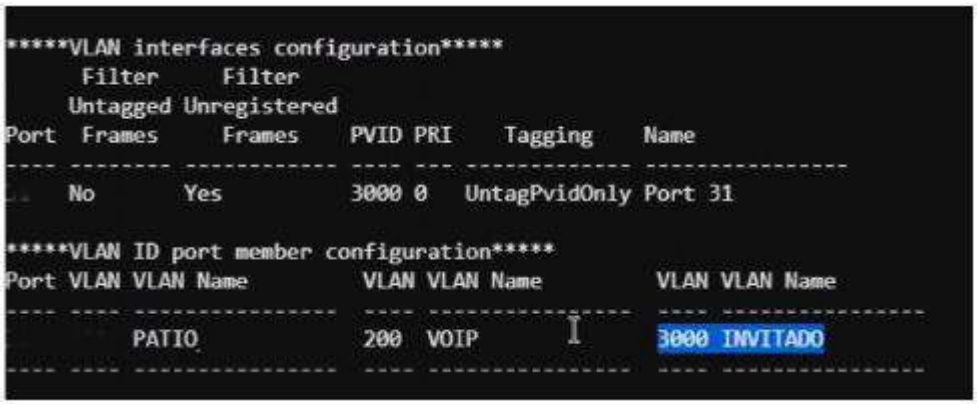

Figura 89.*Postura acceso invitado*

El proceso de aislar o reparar cuando los dispositivos no cumplen con las políticas de autentificación es asignarles una red de invitados, en este caso se configura la VLAN 3000 para usuarios invitados.

Figura 90*.Resultados de postura para denegación*

La denegación ocurre cuando no se cumple ninguna política o regla, el perfil denegar no asigna ninguna VLANs. La función de esta postura es impedir el acceso a la red, esto es en base a las reglas establecidas en el capítulo III, subtitulo 3.2.7.

5. CAPÍTULO V

5. Evaluación.

En el siguiente capítulo se detalla la evaluación de la tecnología NAC del prototipo aplicado en la red de la CPN, se puntualiza aspectos referentes a la seguridad de la red contemplados a través de los tres pilares de la seguridad. Los indicadores son Autorización, Auditabilidad, Autenticación.

5.1. Metodología.

La investigación se desarrolla en base al diseño cuasi experimental, aquello para estudiar el NAC y demostrar como mejora la seguridad en redes de área local. Esta investigación es tipo descriptiva aplicada.

Métodos.

La evaluación es desarrollada en base a tres indicadores usados en seguridad para redes de área local, se aplica los métodos de investigación tales como el analítico y sintético, los indicadores son Autorización, Auditabilidad, Autenticación. En cada indicador se realiza la evaluación con dos criterios, utilizando la tecnología NAC y sin ella basándose en los estudios de los CAP II, III y IV.

Método Analítico.

El método analítico es utilizado para la demostración de un todo, permite analizar y profundizar la información requerida y analizada basándose en los antecedentes y el examen minucioso a través de la investigación.

Método sintético.

El método sintético es el proceso del razonamiento que permite construir un todo en base a los elementos analizados. La síntesis es un proceso mental que tiene como finalidad la comprensión de un todo, sus partes y particularidades del objeto de estudio como lo es el ***NAC***.

Análisis y evaluación.

Se plantea el escenario de evaluación, indicando cuatro criterios, la categoría de cumplimiento en su totalidad representa el 100% y la de no cumplimiento 1 %. Para cuantificar los indicadores se utiliza los valores de la tabla 5.

Tabla5. Parámetros de evaluación NAC

CRITERIOS	VALOR	PORCENTAJE
CUMPLE	4	100%
MEDIANAMANETE CUMPLE	3	75%
PARCIALMENTE CUMPLE	2	50%
NO CUMPLE	1	25 %

Autorización.

Autorización

Este indicador permite evaluar los aspectos referentes al control de acceso a la red por parte de los usuarios.

Accesos sin NAC, evaluación en base al Capítulo II.

- ✓ Control de los accesos en función del rol del usuario, hora del día, localización y aplicación.

No existe ningún proceso de autenticación.

- ✓ Control del acceso de los usuarios no conocidos o con menos garantías de seguridad, como proveedores, clientes o usuarios remotos.

No se cuenta con una herramienta de ese tipo para la red ***LAN*** de la ***CPN***.

- ✓ Cumplir con políticas de seguridad.

  En la red de la ***CPN*** no se cuenta con una herramienta tecnología que permita establecer políticas de acceso a la red ***LAN***.

Accesos con NAC, evaluación en base al Capítulo III y IV.

- ✓ Control de los accesos en función del rol del usuario, hora del día, localización y aplicación

Mediante el ***NAC*** se puede controlar los acceso a la red mediante perfiles y políticas para el control y seguridad de las conexiones, verificar usuario, hora y switch en cual se realizó la autentificación.

- ✓ Control del acceso de los usuarios no conocidos o con menos garantías de seguridad, como proveedores, clientes o usuarios remotos.

La implementación del ***NAC*** aporta seguridad en la red, al poder autenticar las conexiones, asignación de permisos y políticas, monitoreo y administración de los equipos y usuarios que realizan las peticiones de conexión y acceso a la red.

- ✓ Cumplir con políticas de seguridad.

Mediante el ***NAC*** en la red de la ***CPN***, se puede administrar y establecer políticas de acceso a la red ***LAN***, mismas que sean validadas cuando un usuario intenta acceder a la red mediante un host.

Tabla 6. *Autorización.*

CRITERIOS	ACCESOS SIN NAC	ACCESOS CON NAC
Detección de cada dispositivo conectado a la red y control de su comportamiento - Productividad sin riesgos.	NO CUMPLE	CUMPLE
Control de los accesos en función del rol del usuario, hora del día, localización y aplicación	NO CUMPLE	CUMPLE
Control del acceso de los usuarios no conocidos o con menos garantías de seguridad, como proveedores, clientes o usuarios remotos.	NO CUMPLE	CUMPLE

La tabla 6. Hace referencia a la evaluación en base al indicador autorización, aplicando los parámetros de la tabla 5 se obtiene los resultados mostrados en la tabla, evaluando los criterios planteados sobre el acceso a la red sin NAC CAP II, y accesos a la red utilizando la tecnología NAC CAP III y IV.

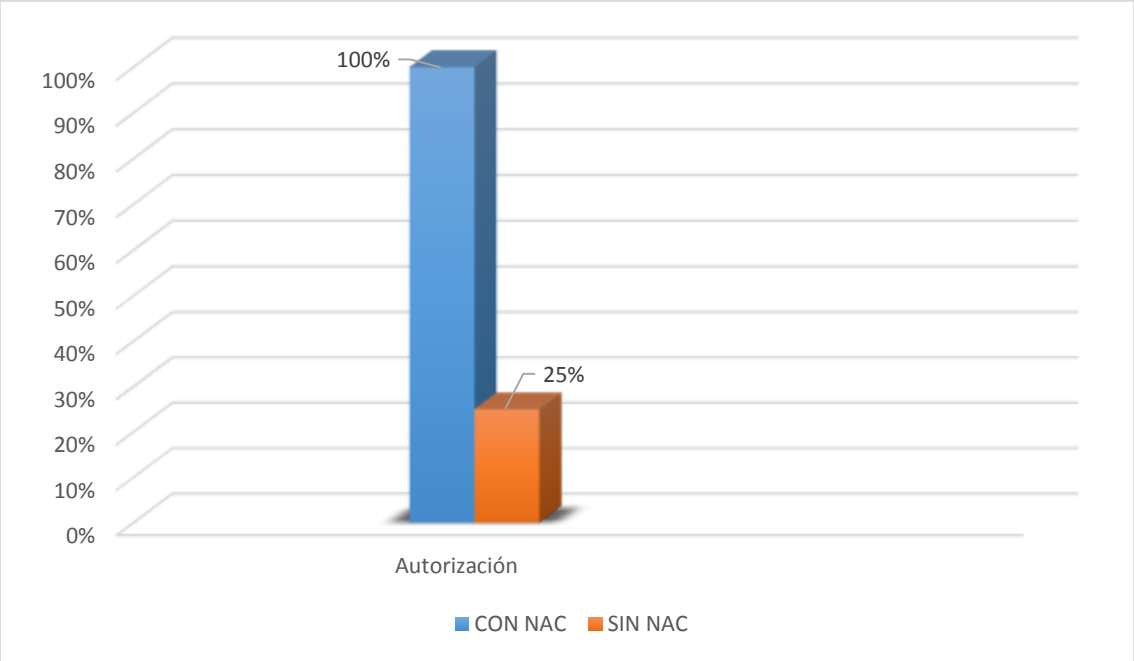

Gráfico 1 *Seguridad en cuanto a la Autorización*

Gráfico 1. En base a los datos obtenidos de la tabla 6 para el indicador de autorización, gráficamente se evidencia que mediante la tecnología NAC se logra un mayor control de acceso a la red.

Auditabilidad

Auditabilidad.

Aquí se evalúa los aspectos referentes al registro del acceso a la red y la monitorización correspondiente.

Accesos sin NAC, evaluación en base al Capítulo II.

- ✓ Restricción del acceso a información.

Si es posible que pueda encontrar un punto de red por ejemplo sala de juntas, sin embargo, necesitaría tener más datos como la red y ***VLANs*** a la cual pueda conectarse a través del puerto de red que haya podido tener acceso.

- ✓ Control de quién accede a la red y restricción del número de recursos con los que puede operar.

Por medio de la ***IP*** los usuarios cuentan con accesos a navegación y accesos algunos servicios y aplicaciones que están protegidos por firewall de perímetro y datacenter respectivamente, sin embargo no hay un control de acceso a la red automático o centralizado.

- ✓ Detección de cada dispositivo conectado a la red y control de su comportamiento. - Productividad sin riesgos.

No existe un control automático, se mantiene una división de ***VLANs*** por Gestiones.

Accesos con NAC, evaluación en base al Capítulo III y IV.

- ✓ Restricción del acceso a información.

En base a la validación de la identidad del usuario y el dispositivo conectado a la red se restringe y audita la utilización de los diferentes recursos de la red mediante una administración centralizada.

- ✓ Control de quién accede a la red y restricción del número de recursos con los que puede operar.

Mediante el ***NAC*** se puede administrar y auditar de manera centralizada los usuarios que acceden a la red, de acuerdo a cumplimiento de políticas si los procesos de autentificación de ser correcta se habilita el puerto con la ***VLANs*** correspondiente, caso contrario de enviará a remediación con ***VLANs*** de invitado y recursos limitados.

- ✓ Detección de cada dispositivo conectado a la red y control de su comportamiento. - Productividad sin riesgos.

Con el NAC se obtiene un control sobre equipos y usuarios que se conecten a la red.

Tabla7. *Auditabilidad*

CRITERIOS	ACCESOS SIN NAC	ACCESOS CON NAC
Restricción del acceso a información.	MEDIANAMENTE CUMPLE	CUMPLE
Control de quién accede a la red y restricción del número de recursos con los que puede operar.	MEDIANAMENTE CUMPLE	CUMPLE
Detección de cada dispositivo conectado a la red y control de su comportamiento.- Productividad sin riesgos.	MEDIANAMENTE CUMPLE	CUMPLE

La tabla 7. Hace referencia a la evaluación del indicador Auditabilidad, aplicando los parámetros de la tabla 5 se obtienen los resultados mostrados en la tabla , en base a los criterios planteados sobre el acceso a la red sin NAC CAP II, y accesos a la red utilizando la tecnología NAC CAP III y IV.

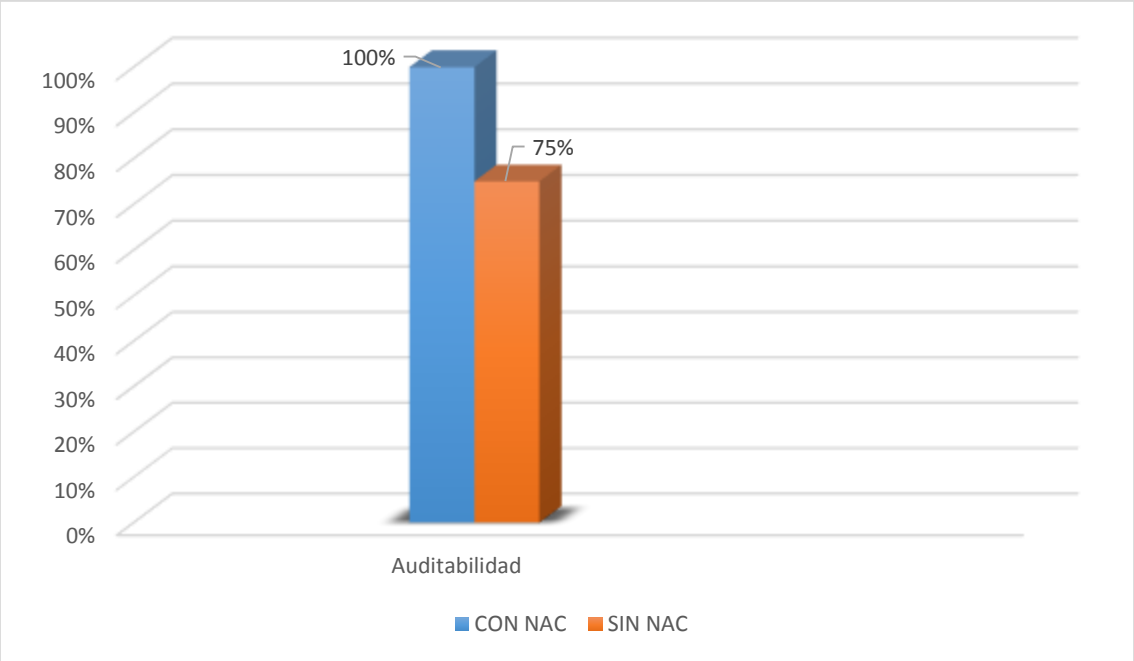

Gráfico 2. Seguridad en cuanto a la Auditabilidad

Gráfico 2. En base a los resultados obtenidos de la tabla 7 se puede representar gráficamente, y comprobar que la tecnología ***NAC*** aporta significativamente para realizar el proceso de auditar los dispositivos que está conectado a la red, logrando un mejor control de acceso.

Autenticación

Autenticación

Aquí se evalúan los aspectos como la verificación de la identidad de los usuarios antes de permitirles acceder a la red.

Accesos sin NAC, evaluación en base al Capítulo II.

- ✓ Segmentación de usuarios en función del cumplimiento normativo.

En la red de la ***CPN*** se mantiene una segmentación de usuario manualmente, por ejemplo se tiene segmentadas la ***VLANs*** y se asignan ***IP*** al usuario acorde al área, también se tienen destinadas ***IP*** para asignar a un proveedor que hace las veces de invitado en la red.

- ✓ Protección de red IP - Adapta y configura la red dinámicamente.

Actualmente se mantiene direccionamiento ***IP*** estático, acorde al área en la cual está conectado el host se realiza la configuración del puerto en el switch y se asigna la ***VLANs*** respectiva.

Accesos con NAC, evaluación en base al Capítulo IV.

- ✓ Segmentación de usuarios en función del cumplimiento normativo.

Mediante la utilización del ***NAC*** se establecen previamente los entornos de red para que pueda acceder cada usuario automáticamente, por ejemplo los proveedores o invitados se asignara la ***VLANs*** 3000 en la cual se establecen permisos concretos para que no puedan acceder en su totalidad a la red.

- ✓ Protección de red IP - Adapta y configura la red dinámicamente.

De acuerdo a la segmentación de la red en función de perfil de usuario se garantiza la disponibilidad de la red, sin descuidar el control de acceso a la red y las conexiones.

Mediante el control de acceso a la red con ***NAC*** la asignación de ***VLANs*** se puede realizar de manera dinámica, es decir el direccionamiento de IP se puede establecer mediante DHCP siendo una forma flexible en la utilización de computadoras.

Tabla 8. *Autenticación*

CRITERIOS	ACCESOS SIN NAC	ACCESOS CON NAC
Segmentación de usuarios en función del cumplimiento normativo	MEDIANAMENTE	CUMPLE
Control de quién accede a la red y restricción del número de recursos con los que puede operar.	MEDIANAMENTE	CUMPLE

La tabla 8. Hace referencia a la evaluación del indicador Autenticación, aplicando los parámetros de la tabla 5 se obtiene los resultados mostrados en la tabla 8, en base a los criterios planteados sobre el acceso a la red sin NAC CAP II, y accesos a la red utilizando la tecnología NAC CAP III y IV.

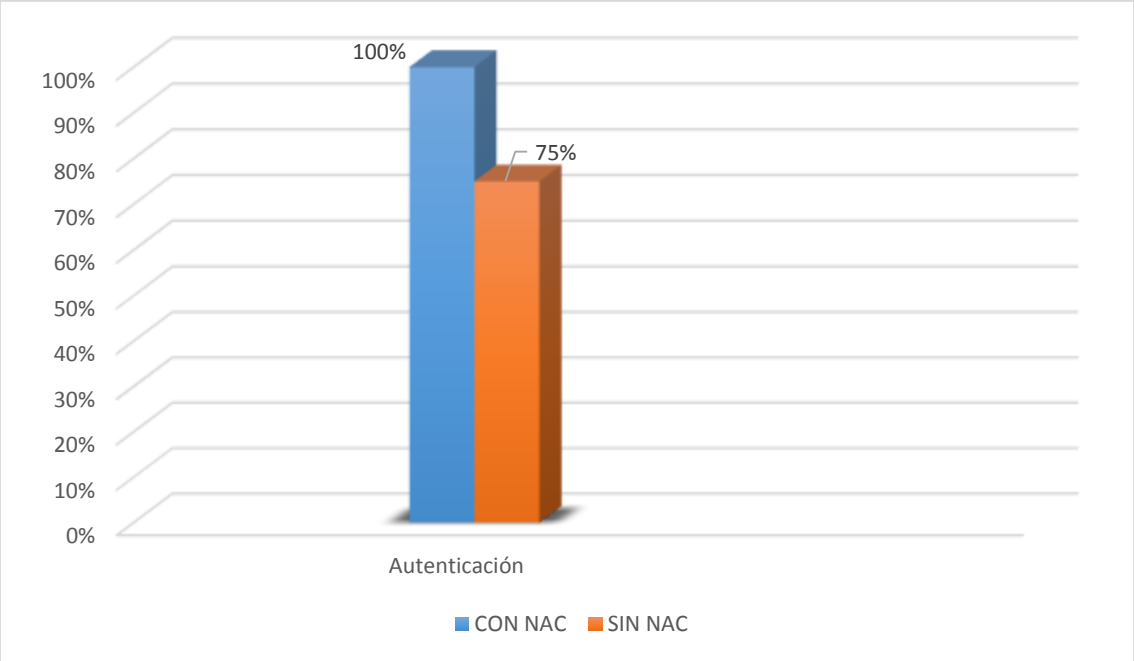

Gráfico 3. *Seguridad en cuanto a la Autenticación*

Gráfico 3. Para el proceso de autentificación se basa en los datos obtenidos de la tabla 8, se logra validar en base a los criterios planteados sobre el acceso a la red sin NAC CAP II, y accesos a la red utilizando la tecnología NAC CAP III y IV, mediante el NAC se puede realizar una mejor Autenticación con administración centralizada, automática y dinámica.

5.2. Instrumento operacional.

Encuesta.

Respecto a los instrumentos de recolección de información se utiliza la encuesta, como parte del método analítico y sintético, mismos que permiten la comprensión y razonamiento a partir de los elementos distinguidos. La encuesta es orientada hacia los miembros del departamento de TIC de la CPN Matriz, cuyos integrantes son 20, aquello para conocer los criterios que demuestren el grado de importancia de la tecnología NAC para la red de la CPN Matriz.

Datos.

La estructura de las preguntas es de carácter cerradas, con el fin de obtener respuesta de manera concreta. Las tablas están compuestas por tres columnas en las cuales se detalla las alternativas, la frecuencia y el porcentaje respectivo. Aquellos se logran en base al proceso de tabulación realizado de los resultados la encuesta aplicada.

¿Conoce sobre el NAC?

Tabla 5. Conocimiento sobre el NAC

Opciones	Frecuencia	Porcentaje
NADA	1	5%
ALGO	6	30%
POCO	2	10%
MUCHO	11	55%
Total	20	100 %

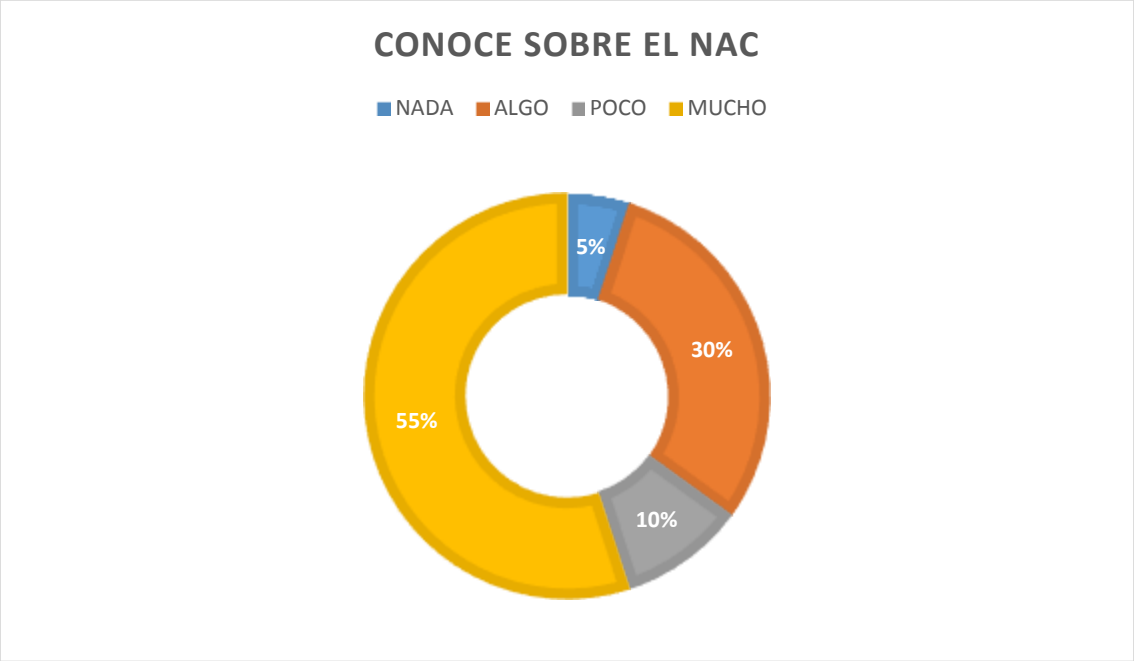

Gráfico 4. Conocimiento sobre el NAC

Análisis. El gráfico 4 representa el portaje de cada alternativas planteada, representa el conocimiento sobre la Tecnología NAC en la CPN la mayoría de los encuestados un 55% conoce mucho sobre tecnología NAC, un 30% conoce algo, un 10% conoce poco sobre el NAC y un 5% no tiene conocimiento sobre esta tecnología.

¿En qué medida considera necesaria la tecnología NAC en la red de la CPN?

Tabla 6. *Necesidad del NAC en la CPN*

Opciones	Frecuencia	Porcentaje
Altamente necesario	10	50%
Medianamente necesario	6	30%
Poco necesario	3	15%
Innecesario	1	5%
Total	20	100 %

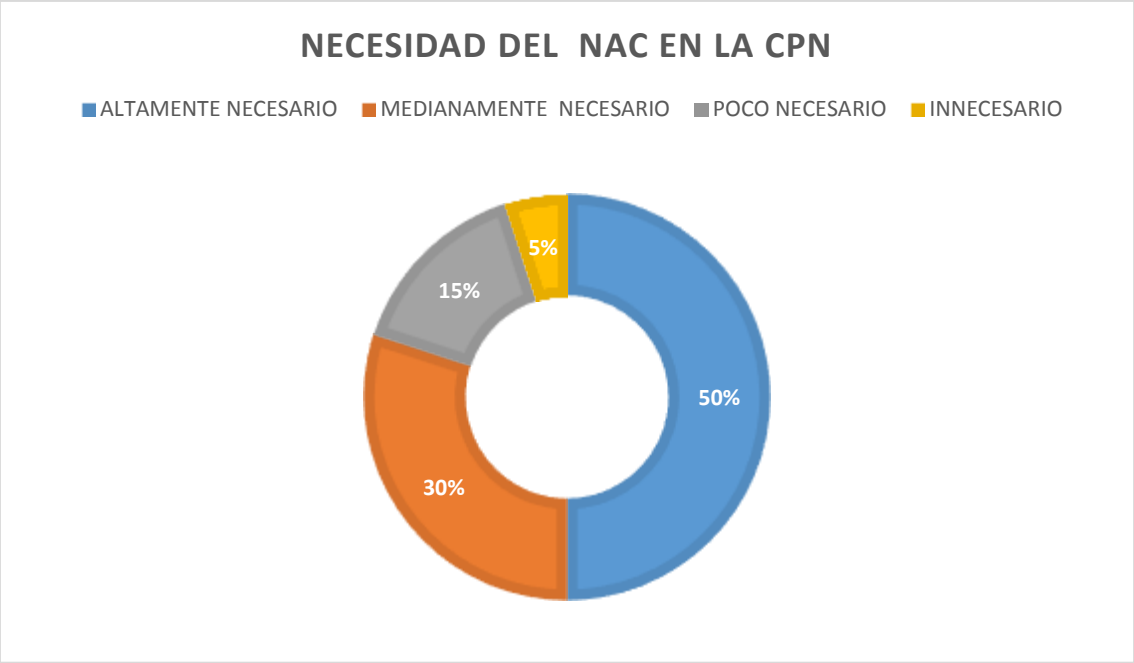

Gráfico 5. *Necesidad del NAC en la CPN*

Análisis. En esta gráfica podemos ver el nivel acorde a la necesidad de implementar el NAC en la CPN, se considerada cuatro alternativas para los encuestados, un 5% considero innecesario el NAC en la red de la CPN, un 15% lo considera poco necesario, el 30% medianamente necesario y el 50% del total de los encuetados considera altamente necesario implementar en la NAC en la red de la CPN para realizar optimizar el control de acceso a la red.

De los siguientes aspectos de seguridad, que irrupción de seguridad considera Ud. se puede prevenir mediante el NAC.

Tabla 7. *NAC en la CPN*

OPCIONES	FRECUENCIA	PORCENTAJE
Obtener acceso a la red sin autorización	17	85%
Ejecutar transacciones	0	0%
Alterar servicios	3	15%
Obtener permisos y roles	0	0%
TOTAL	20	100%

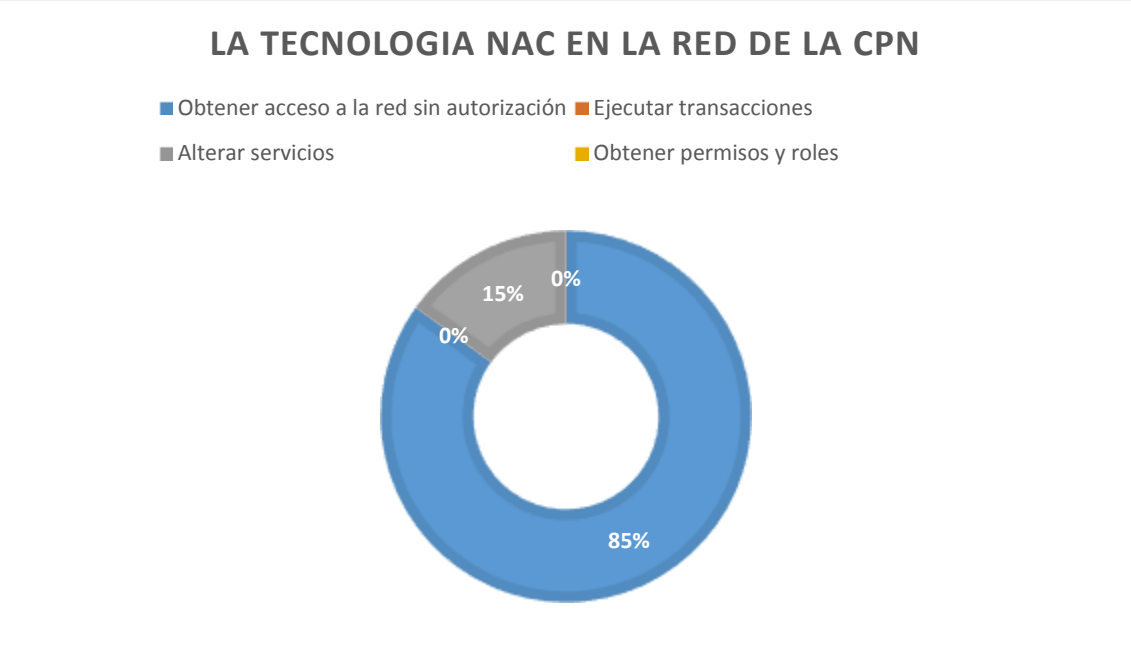

Gráfico 6. *NAC en la CPN*

Análisis. En la gráfica se representan cuatro alternativas referentes a los aspectos de seguridad en los cuales el NAC aportaría para evitar irrupciones, sin embargo dos tuvieron mayor acogida por los encuestados, con un 15% consideran que el NAC podría ayudar a evitar alteraciones de servicios y con un 85% la mayoría de los encuestados mencionan que el NAC permite controla el acceso a la red por lo tanto evita obtener acceso a la red sin autorización brindado mayor seguridad a la red de la CPN.

¿Qué ventajas aportaría el NAC en la CPN?

Tabla 8. *Aportes del NAC en la CPN*

OPCIONES	FRECUENCIA	PORCENTAJE
Controlar el acceso a la red e identificar usuarios	14	70%
Administrar los recursos de la red	4	20%
Despliegue de Firewall y Antivirus	1	5%
Administrar Permisos	1	5%
TOTAL	20	100%

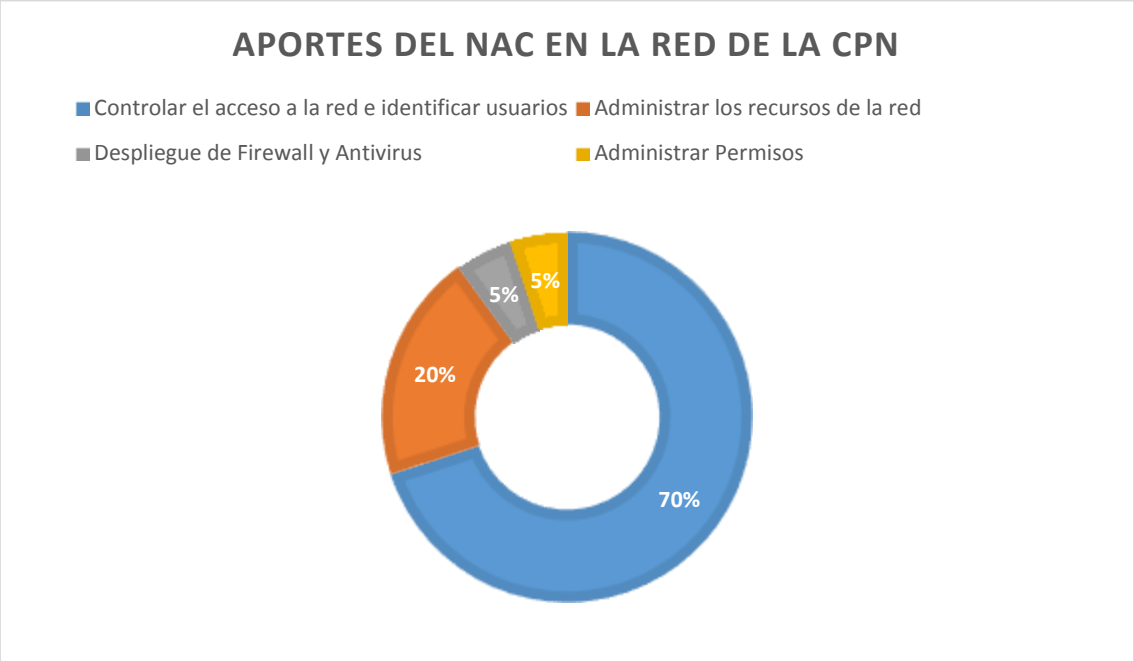

Gráfico 7. *Aportes del NAC en la CPN*

Análisis. En cuanto aportes de NAC para la red de la CPN la gráfica anterior muestra que en base a las cuatro alternativas, un 5% menciono que el NAC podría facilitar la administración de permisos, con el mismos porcentaje también opinaron que el NAC contribuye a la seguridad de la red mediante firewall y antivirus, un 20% menciona que mejoraría la administración de la red mediante el NAC, y la mayoría de los encuetados con un 70% consideran que el NAC aportaría a la seguridad de la red controlando el acceso e inidentificado los usuarios que acceden a la red.

¿Seleccione que tipo de Soluciones NAC recomendaría Ud. para la institución?

Tabla 9. *Solución NAC*

OPCIONES	FRECUENCIA	PORCENTAJE
Nac de cisco	1	5%
Nap de microsoft	4	20%
Tecnologías con funcionalidad NAC/NAP: 802.1X , IPSEC VPN Y SSL VPN	14	70%
Alternativas de código Abierto	1	5%
TOTAL	20	100%

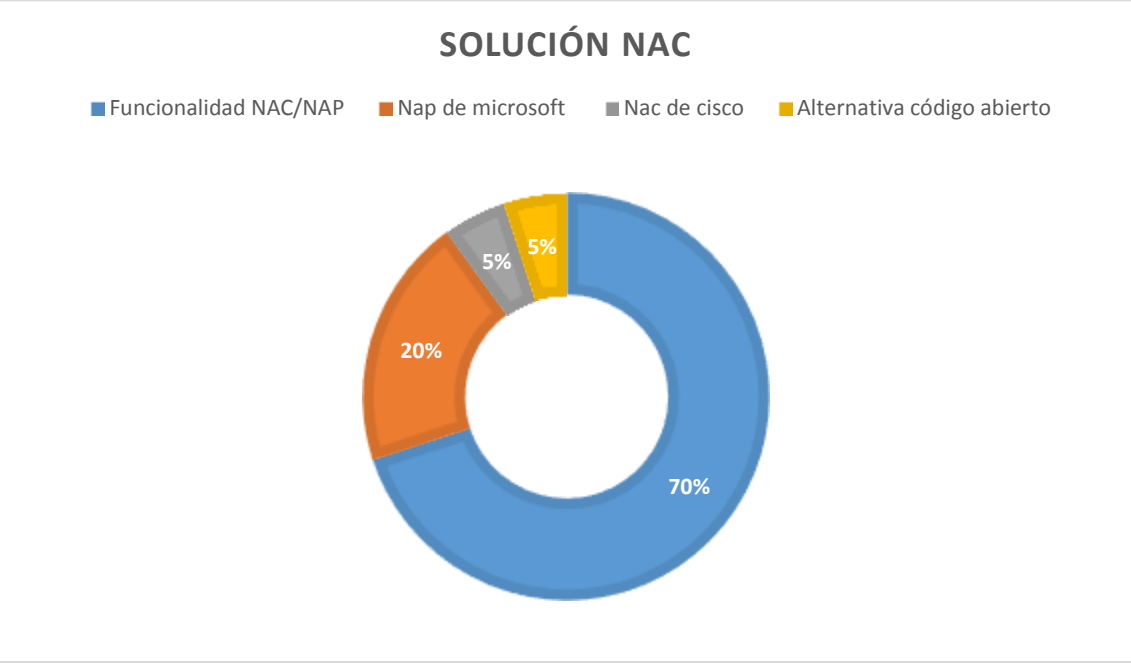

Gráfico 8. *Solución NAC*

Análisis. En la gráfica se representan cuatro alternativas de soluciones NAC, sin embargo la mayor acogida por los encuestados con un 70% consideran que la funcionalidad NAC/NAP se apega a la infraestructura AVAYA de la institución, con un 20% los encuestados mencionan que el Nap de microsoft permite controlar el acceso a la red, un 5 % mencionaron que Nac de cisco es una alternativa, y con el mismo porcentaje se refirieron a la alternativa de código abierto.

Conclusiones.

- ✓ De acuerdo al estudio realizado se determina que en la red de la ***CPN*** no existe un control automático y centralizado que autentifique al usuario que intenta acceder a la red, aquello la deja expuesta a irrupciones tales como obtener acceso a la red sin autorización.
- ✓ Se comprueba que la tecnología ***NAC*** mejora la seguridad en la red de la ***CPN*** mediante el cumplimiento de políticas que permiten autentificar, auditar y autorizar el acceso a la red.
- ✓ Luego del estudio realizado se considera que es altamente necesaria la tecnología ***NAC*** en la red de la ***CPN***, ya que permite controlar el acceso a la red de manera automática y centralizada.
- ✓ El ***NAC*** está acto para ser implementado en la red de la ***CPN*** ya que se adapta a la infraestructura tecnología de la red de la ***CPN***.

Recomendaciones.

- ✓ En base a la utilización de la tecnología ***NAC*** se recomienda considerar la migración de asignación IP estática por DHCP en la red de la ***CPN.***
- ✓ Es importante ir implementado paulatinamente el ***NAC*** ya que puede provocar incomodidad en la prestación de servicio de los usuarios.

Bibliografía

Avaya In. (2015). *www.cdcgroup.mx*. Obtenido de https://www.cdcgroup.mx/download/ERS4800.pdf

Allied Telesis. (2016). *alliedtelesis.com.* Recuperado el 27 de Junio de 2020, de alliedtelesis.com: https://www.alliedtelesis.com/sites/default/files/documents/solutions-guides/network_access_control_nac_revf.pdf

Alternativas en Computación S.A. (2019). *ALTERNATIVAS EN COMPUTACIÓN*. Recuperado el 11 de 07 de 2020, de https://altcomp.mx/que-es-un-dispositivo-de-control-de-acceso-a-la-red-network-access-control-o-simplemente-nac/

Bonete, S. (2008). *Ponencia, consultor preventa de Seguridad para el Sur de Emea de ENTERASYS.* Obtenido de www.rediris.es: https://www.rediris.es/difusion/publicaciones/boletin/82-83/ponencia1.3D.pdf

Cisco. (2020). *CISCO*. Obtenido de https://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/index.html

De la Cruz, H. B. (2013). *HACKING & CRACKING.* Lima: Macro EIRL. Obtenido de https://books.google.com.ec/books?id=G0YwDwAAQBAJ&pg=PT119&dq=protocolo+eap+EN+802.1X&hl=es-419&sa=X&ved=0ahUKEwilt9TD37TpAhWsmuAKHcSsDP4Q6AEIQzAD#v=onepage&q=protocolo%20eap%20EN%20802.1X&f=false

Ekos. (2018). *Ekosnegocios*. Recuperado el 10 de 07 de 2020, de https://www.ekosnegocios.com/: https://www.ekosnegocios.com/articulo/cpn-4-decadas-generando-solvencia-y-confianza.

Esmoris, D. O. (2014). *Control de Acceso a Redes.* La Plata. Obtenido de https://postgrado.info.unlp.edu.ar/wp-content/uploads/2014/07/Esmoris.pdf

Esmoris, D. O. (2014). *Control de Acceso a Redes.* La Plata. Obtenido de https://postgrado.info.unlp.edu.ar/wp-content/uploads/2014/07/Esmoris.pdf

Extreme. (2019). *AIDC*. Obtenido de AIDC Online: https://aidc-online.com/redes-inalambricas/231-switch-extreme-networks-16533.html

Fortinet. (2018). *NETWORK ACCESS CONTROL.* California. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-nac-in-the-era-of-iot-and-byod.pdf

Gámez, P. (2017). *Conasa itworks*. Obtenido de CONASA MADRID: https://www.conasa.es/blog/soluciones-nac-network-access-control-2/

García, A. (2020). *SEGURIDAD DE REDES DE.* Perú. Recuperado el 23 de Junio de 2020, de https://www.google.com/search?ei=N6nyXrGTDuSi_QaG5ISoBA&q=seguridad

+en+redes+informaticas.+pdf&oq=seguridad+en+redes+informaticas.+pdf&gs_lcp=CgZwc3ktYWIQAzIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjoECAAQR1DHpwJYra0CYOmuAmgAcAF4AIABxAGIAd8GkgEDMC41mAEAoAEBqgEHZ3dzL

Guerra Mantilla, A. R. (2018). Gestión de seguridad de lainformación con la norma ISO27001:2013. *ESPACIOS*. Obtenido de https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf

ISO Tools Excellence. (2016). *SGSI*. Recuperado el 27 de Junio de 2020, de Sistemas de Gestión: https://www.pmg-ssi.com/2016/07/como-administrar-la-seguridad-de-red-segun-la-norma-iso-27001/

Jimenez Perez, L. A., & Joanny, U. R. (2017). *Migracion de Servicios Cisco NAC.* Quito. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/13662/1/T-ESPE-053915.pdf

Loredo, E. M. (2010). *Magazcitum*. Recuperado el 27 de Junio de 2020, de https://www.magazcitum.com.mx/?p=249#.Xvf65m1Kjcd

Murillo, M. (2020). *Control de Acceso a La Red (NAC).* Recuperado el 28 de Junio de 2020, de https://es.scribd.com/document/248164840/Control-de-Acceso-a-La-Red-NAC

Pello, G. (2017). *Soluciones NAC (Network Access Control)*. Obtenido de Conasa Itworks: https://www.conasa.es/blog/soluciones-nac-network-access-control/

Pérez, A. (2020). *La seguridad de las redes.* Reino Unido: Science Publishing. Obtenido de https://books.google.com.ec/books?id=tbzTDwAAQBAJ&pg=PA6&dq=protocolo+eap+EN+802.1X&hl=es-419&sa=X&ved=0ahUKEwilt9TD37TpAhWsmuAKHcSsDP4Q6AEISzAE#v=onepage&q=protocolo%20eap%20EN%20802.1X&f=false

Ramos, A. &. (2011). *Seguridad informática.* Madrid: Paraninfo. Recuperado el 23 de Junio de 2020, de https://books.google.com.ec/books?id=c8kni5g2Yv8C&pg=PA1&dq=gesti%C3%B3n+activa+de+la+seguridad+informatica&hl=es-419&sa=X&ved=2ahUKEwi8ibzlgZTqAhUCTDABHS1MAQAQ6AEwBHoECAEQAg#v=onepage&q=gesti%C3%B3n%20activa%20de%20la%20seguridad%20informatica&f=false

Romero Castro, M. I. (2018). *INTRODUCCIÓN A LA SEGURIDAD.* Jipijapa: Els Alzamora. Recuperado el 23 de Junio de 2020, de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Telesis Allied. (2016). *Network Access Control (NAC).* Obtenido de https://www.alliedtelesis.com/sites/default/files/documents/solutions-guides/network_access_control_nac_revf.pdf

Universidad Internacional de la Rioja. (2019 de Diciembre de 2019). *Unir Revista*. Recuperado el 27 de Junio de 2020, de ¿Qué es la certificación ISO 27001 y para qué sirve?: https://www.unir.net/ingenieria/revista/noticias/iso-27001/549204720236/

Vieites, Á. G. (2015). Seguridad informática. *STARBOOK*, 5. Obtenido de https://www.ecoeediciones.com/wp-content/uploads/2015/08/seguridad-informatica-basico.pdf

Waldo de la Ossa, J. (s.f.). *INTRODUCCION A LA SEGURIDAD EN REDES.* Obtenido de http://networkingsignora.pbworks.com/f/Unidad%201%20-%20Introduccion%20Seguridad%20Redes.pdf

Anexos.

Anexo 1. Norma ISO 27001 CPN.

ID	Código	Procedimiento de aplicación	Requerimiento
2	1.1.1.a	Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente:	• Conexiones de red • Cambios en las configuraciones de firewalls y routers
3	1.1.1.b	Para obtener una muestra de las conexiones de red, entreviste al personal responsable y revise los registros para verificar que se hayan aprobado y probado las conexiones de red.	
12	1.1.5.b	Entreviste al personal responsable de administrar los componentes de la red para confirmar que las funciones y las responsabilidades se hayan asignado según lo documentando.	
14	1.1.6.b	Identifique los servicios, protocolos y puertos inseguros permitidos y verifique que se hayan documentado las funciones de seguridad de cada servicio.	
15	1.1.6.c	Revise las configuraciones de firewalls y routers para verificar que se hayan implementado las funciones de seguridad para cada servicio, protocolo y puerto inseguros.	
	6.1.b	Entreviste al personal y observe el proceso para verificar lo siguiente:	Se identifiquen nuevas vulnerabilidades de seguridad. • Se asigne una clasificación de riesgo a las vulnerabilidades que identifique todas las vulnerabilidades
	10.	Rastree y supervise todos los accesos a los recursos de red y a los datos.	

Anexo 2.

Encuestas aplicadas.

ENCUESTA

La presente encuesta pretende recabar información sobre la situación actual de la red de la CPN.

Indicaciones: Sombrear la respuesta que considere pertinente.

¿Conoce sobre el NAC?

- Nada
- Algo
- Poco
- Mucho

¿En qué medida considera necesaria la tecnología NAC en la red de la CPN?

- Altamente necesario
- Medianamente necesario
- Poco necesario
- Innecesario

De los siguientes aspectos de seguridad, que irrupción de seguridad considera Ud. se puede prevenir mediante el NAC.

- Obtener acceso a la red sin autorización
- Ejecutar transacciones
- Alterar servicios
- Obtener permisos y roles

¿Qué ventajas aportaría el NAC en la CPN?

- Controlar el acceso a la red e identificar usuarios
- Administrar los recursos de la red
- Despliegue de Firewall y Antivirus
- Administrar Permisos

¿Seleccione que tipo de Soluciones NAC recomendaría Ud. para la institución?

- Nac de cisco
- Nap de microsoft
- Tecnologías con funcionalidad NAC/NAP: 802.1X , IPSEC VPN Y SSL VPN
- Alternativas de código Abierto

ENTREVISTA

La presente entrevista pretende recabar información sobre la situación actual de la red de la CPN.

1. **¿Actualmente existe algún control automático para acceder a la red?**

2. **¿En la administración de la red, existe algún proceso de autentificación de usuarios, se tiene definidas políticas de seguridad para acceder a la red?**

3. **¿Al momento en la institución aplican alguna norma ISO respecto a la seguridad de red?**

4. **¿Actualmente se pueden establecer políticas, perfiles, permisos de usuario al entorno que se le asigna para el uso de la red de manera automática?**

5. **¿La institución está en la capacidad de implementar un servidor y tecnología de administración de políticas para controlar el acceso a la red?**