UNIVERSIDAD DE ORIENTE
NÚCLEO DE SUCRE
ESCUELA DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DE LA LICENCIATURA EN INFORMÁTICA

# IMPLEMENTACIÓN DE LA ARQUITECTURA DE CONTROL DE ACCESO BASADA EN EL ESTÁNDAR DE SEGURIDAD IEEE 802.1X PARA LA RED ETHERNET DE PETRÓLEOS DE VENEZUELA SOCIEDAD ANÓNIMA, UBICADA EN EL EDIFICIO ESEM, MATURÍN, ESTADO MONAGAS

(Modalidad: Pasantía)

Migdalis del Valle Mago Rodríguez

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE LICENCIADA EN INFORMÁTICA

CUMANÁ, 2010

**IMPLEMENTACIÓN DE LA ARQUITECTURA DE CONTROL DE ACCESO BASADA EN EL ESTÁNDAR DE SEGURIDAD IEEE 802.1X PARA LA RED ETHERNET DE PETRÓLEOS DE VENEZUELA SOCIEDAD ANÓNIMA, UBICADA EN EL EDIFICIO ESEM, MATURÍN, ESTADO MONAGAS**

APROBADO POR:

Prof. Daniel Geremia
Asesor Académico

Asesor Industrial

(Jurado)

(Jurado)

## DEDICATORIA

A:

Jehová mi Dios por ser mi padre y creador, por darme a conocer las promesas que Él tiene para mí y ser mi fortaleza frente a las adversidades, a nuestro Señor Jesucristo mi único Salvador por estar en cada momento de mi vida, porque a través de Él conocí el verdadero amor y la verdadera amistad, llena de fidelidad, comprensión, firmeza y nuevas oportunidades que me permitieron avanzar cada día y seguir en su camino, al Espíritu Santo porque desde que llegó a mi vida ha sido mi guía y mi consolador en todo tiempo.

Mis padres Rosa Migdalia Rodríguez y Pedro Félix Mago, quienes me apoyaron siempre de forma incondicional, a ellos debo todo lo que soy, gracias Mamá y Papá por su amor, dedicación, paciencia y sus valiosos consejos llenos de sabiduría.

Mis hermanas Rosemigd Beatriz y Rosmary Paola, amigas muy importantes en mi vida, quienes son un gran ejemplo a seguir y con las que he compartido los mejores momentos de mi vida, llenos de sonrisas, lágrimas y valiosos consejos que le dieron dirección a mi vida.

Misael Ferrer, mi gran amigo, compañero de estudio, mi amor y mi futuro esposo, que ha estado en momentos muy importantes de mi vida llenándolos de amor, confianza y respeto.

Mi amiga Hecnellys Bastardo quien con sus consejos, amor y constancia, me motivó a seguir en los caminos de Dios.

Mi linda sobrina Samantha Valentina, el regalo de Dios que le da alegría a mi familia.

¡Todo esto se lo dedico a Ustedes!

## AGRADECIMIENTO

Agradezco a:

La Universidad de Oriente, Núcleo de Sucre, por ser la casa de estudios que permitió realizarme como profesional.

El profesor Daniel Geremia, por haberme orientado durante el desarrollo de este proyecto y por ser un buen ejemplo a seguir como profesional y como persona. Muchas gracias.

El licenciado Aníbal Vera, Superintendente de Seguridad AIT Oriente de PDVSA por haberme dado la oportunidad de realizar mi trabajo de grado en esta empresa, y por haberme brindado la asesoría y amistad de forma incondicional.

Todos las personas que laboran en Seguridad AIT Oriente Karin Pérez, María Villasana, Yeritson Pernía, Pedro Salazar, Alex Contreras, Renato Mateluna, Carlota Moreno, Carlos Molinos, Mónica Rivas, Marcelo Velasco, Yrma Gil, Ofelia Brito y Alfonso Belisario por su apoyo y valiosa amistad.

Mis amigos y compañeros de clases: Ines, Hecnellys, Merys, Misael, Charli, Ingrid, Beira, Francisco Tayupo, Silvio, Emerson, y demás compañeros de clases, por haber compartido momentos llenos de alegría y satisfacción.

La profesora Alejandra Galantón por guiarme y ser un modelo a seguir durante el desarrollo de mi carrera universitaria.

Todas aquellas personas que de alguna u otra forma contribuyeron al logro de esta meta.

Gracias a todos.

**ÍNDICE**

## LISTA DE TABLAS

## LISTA DE FIGURAS

Pág.

## RESUMEN

Mediante la ejecución del presente Trabajo de Grado, se logró la implementación de una arquitectura de control de acceso basada en el estándar IEEE 802.1x para la red *Ethernet* de Petróleos de Venezuela, Sociedad Anónima (PDVSA), ubicada en el edificio ESEM de la ciudad de Maturín. La metodología de investigación utilizada fue un híbrido, compuesto por algunos métodos utilizados por James McCabe, (1998), Manuel Sánchez, (2003) e INTEL *Corporation*, (2003); quedando comprendida por cinco (5) fases: determinación de los requerimientos, análisis de las tecnologías, diseño de la arquitectura de control de acceso, ejecución del diseño y pruebas de la arquitectura. Mediante la determinación de los requerimientos se emplearon entrevistas a los usuarios y observación directa de los hechos, con la finalidad de identificar los problemas presentes y visualizar las posibles mejoras; en la fase de análisis de las tecnologías, se procedió a seleccionar entre varias alternativas existentes, el mecanismo de autenticación y autorización, el protocolo de autenticación, el mecanismo de cifrado, y el servidor de autenticación, tomando en cuenta diversos aspectos de seguridad en la red y los requerimientos emitidos por la Gerencia de Seguridad Lógica de PDVSA; en la siguiente fase, se realizó el diseño de la arquitectura de control de acceso, mediante el uso del Lenguaje Unificado de Modelado; seguidamente se procedió con la ejecución del diseño, mediante la instalación y configuración de todos los elementos que intervienen en la arquitectura y finalmente la realización de pruebas de conexión y autenticación tanto en la red cableada como en la red inalámbrica. Esta arquitectura de seguridad, permitió controlar el acceso lógico a los recursos de la red de PDVSA, a través de un proceso de autenticación que permite validar las credenciales que son enviadas al servidor de autenticación, siendo éste el encargado de aceptar o denegar el acceso; con el fin de evitar la manipulación directa de información confidencial de PDVSA a terceros, de igual forma se evita que un dispositivo de un tercero pueda conectarse a la red.



Palabras claves: seguridad en redes LAN, control de acceso, IEEE 802.1x

# INTRODUCCIÓN

La utilización de las tecnologías de información y comunicación dentro de cualquier organización representan el avance y desarrollo de sus procesos en el mundo competitivo, manteniendo una firme presencia y una amplia relación comercial con sus socios y con aquellas naciones poseedoras de un extenso potencial para invertir en el negocio de la empresa; utilizando mecanismos de interconexión de redes en el ámbito mundial. Por tal motivo, las redes y las comunicaciones nunca habían sido tan vitales para las organizaciones que afrontan el reto de competir en el mercado global (Microsoft *Corporation*, 2007).

Este entorno de interconexión tan complejo, se encuentra unido a una gran cantidad de datos críticos que poseen las organizaciones, y a la necesidad de acceso a éstos desde cualquier dispositivo y ubicación, todo ello sin comprometer la integridad y confidencialidad de la información, lo cual ha provocado la aparición de innumerables y nuevos puntos débiles de acceso (García, 2007). Así como también, ha generado nuevas oportunidades para el surgimiento de problemas relacionados con la tecnología, tales como el robo de datos, ataques maliciosos mediante virus, negación de servicios, acceso sin autorización a los equipos de cómputo y a las redes de telecomunicaciones, entre otros, que en particular y en conjunto constituyen riesgos de este entorno de interconexión (Contraloría General de México, 2007). Todos estos problemas pueden presentarse en una red de una forma incontrolable, ocasionando fallas y daños considerables a la plataforma tecnológica de una organización.

Las fallas de seguridad pueden ser costosas para las organizaciones, las pérdidas pueden ocurrir como resultado de la falla misma o pueden derivarse de la recuperación del incidente, es por ello que es necesario definir un conjunto de políticas y procedimientos de seguridad, con el fin de prevenir daños en la reputación

de la empresa y pérdidas financieras (Contraloría General de México, 2007). Por consiguiente, cualquier empresa que desee ser exitosa necesita estar en la capacidad de proteger la información confidencial, con el fin de no dar ventajas a sus competidores (Microsoft *Corporation*, 2007). Tal es el caso de Petróleos de Venezuela Sociedad Anónima (PDVSA), la cual es una organización que dispone de una gran cantidad de información confidencial, que necesita ser protegida de usuarios malintencionados, lo cual es indispensable para el desempeño de todas sus actividades permitiendo así el avance y desarrollo de todas las gerencias y procesos que en ésta se encuentran.

Por lo antes expuesto, el propósito fundamental de este trabajo, fue la implementación de una arquitectura de control de acceso basada en puertos de conexión a la red, utilizando el estándar IEEE 802.1X que permite autenticar, autorizar y realizar la trazabilidad de las conexiones de usuarios, que intenten conectarse a la red de la Corporación, negando el acceso a aquellas personas que no pertenezcan al directorio activo de PDVSA. Para lograr este objetivo, se utilizaron las fases determinación de los requerimientos y ejecución del diseño, de la metodología propuesta por James McCabe (1998); las fases análisis de las tecnologías y diseño de la arquitectura de control de acceso de la metodología utilizada por Manuel Sánchez (2003) e igualmente se consideró la fase prueba de la arquitectura de la metodología de INTEL *Corporation* (2003); obteniendo una metodología híbrida cuyas fases quedan ordenadas de la siguiente manera: determinación de los requerimientos, análisis de las tecnologías, diseño de la arquitectura de control de acceso, ejecución del diseño y pruebas de la arquitectura.

La estructura del presente trabajo, se expuso en tres (03) capítulos principales, tal como sigue a continuación:

Capítulo I. Presentación: describe la problemática presente en la empresa, así como el alcance del trabajo y las limitaciones encontradas durante el desarrollo del mismo.

Capítulo II. Marco de Referencia: describe los antecedentes tanto de la investigación como de la organización, el área de estudio y de investigación y la metodología utilizada para lograr el objetivo propuesto.

Capítulo III. Desarrollo: describe la aplicación de las fases que conforman la metodología y los resultados de la ejecución de las mismas.

Finalmente se presentan las conclusiones y recomendaciones del trabajo realizado.

# CAPÍTULO I. PRESENTACIÓN

## PLANTEAMIENTO DEL PROBLEMA

Para PDVSA la defensa de la Soberanía Nacional es uno de los pilares fundamentales de la política petrolera nacional, popular y revolucionaria desplegada por el Gobierno Bolivariano de Venezuela. Esta línea estratégica, orientada a concretar una auténtica nacionalización petrolera, pasa por la reafirmación de la propiedad de los hidrocarburos que se encuentran en el subsuelo de la nación y el rescate del control de la actividad petrolera, tanto desde el punto de vista del régimen tributario y legal como en el total dominio de la industria petrolera nacional; es por ello que PDVSA, cuenta con la Gerencia de Prevención y Control de Pérdidas (PCP), el cual tiene como función principal diseñar, planificar, implantar y mantener la seguridad de toda la Corporación frente a las diferentes amenazas que existen actualmente y a futuro (Petróleos de Venezuela S.A, 2005).

Para una empresa como ésta, el buen manejo de la información juega un papel importante para el progreso y futuro de su organización; por tal motivo cada día surgen mayores exigencias en el contexto de seguridad en la red, teniendo la necesidad de supervisar cada una de las operaciones que se realizan para mantener la integridad y confiablidad de la información, utilizando tecnologías de alta capacidad que garanticen su óptimo control.

En la actualidad, PDVSA emplea mecanismos de control del acceso físico de equipos computacionales tales como computadores portátiles y de escritorio a la Corporación, sin embargo este control, en algunas oportunidades, se hace insuficiente, ya que no existe control alguno sobre equipos electrónicos como por ejemplo: palm, handhelp, y teléfonos celulares, entre otros, que pueden ser conectados a la red *Ethernet* de

PDVSA y así obtener un identificador de conexión, que le permita adquirir recursos de la red sin previa autorización.

En el mismo sentido, el acceso al nivel de capa de enlace de datos a la red *Ethernet* de la Corporación no está siendo totalmente controlado, debido a que no existe ningún método de autenticación que permita filtrar el acceso a la red, lo cual representa un punto de vulnerabilidad en la plataforma tecnológica, por tal motivo, cualquier equipo que no pertenezca al dominio de PDVSA puede conectarse a algún punto de acceso, permitiendo el uso sin autorización de la red, esto puede ser utilizado por personas ajenas a la Corporación para acceder a sistemas internos pertenecientes a sectores críticos y no críticos de la empresa, tales como, localidades de alta rotación de personal, administración, finanzas, entre otros, normalmente no accesibles desde el exterior y, de esta forma, tener acceso a modificaciones y difusión de toda la información confidencial de PDVSA.

Consciente de esta vulnerabilidad, la Gerencia de Seguridad Lógica de PCP, decide implementar una arquitectura de seguridad basada en el estándar IEEE 802.1X, el cual proporciona una autenticación a nivel de capa de enlace de datos, con el fin de obtener un proceso de conexión, evitando el problema de seguridad antes mencionado. Este estándar de seguridad define el control de acceso a redes basadas en puertos de red LAN, exigiendo una autenticación antes de dar acceso a las redes *Ethernet* y se efectúa la variación dinámica de claves, todo ello ajustado a un protocolo, denominado EAP (*Extensible Authentication Protocol*); por tal motivo, todo usuario que esté empleando la red se encuentra autentificado con una clave única, que se va modificando de manera automática y que es negociada por el servidor y el cliente de manera transparente para el usuario. Este protocolo soporta múltiples métodos de autenticación tales como kerberos, certificados públicos, tarjetas inteligentes o credenciales, claves o contraseñas, entre otros, abarcando distintos escenarios entre los cuales se encuentran: identificar los usuarios que se

conectan a un punto de la red, detectar posibles intentos de intrusión en la red, generar claves de cifrado de la comunicación entre el usuario y el punto de acceso, llevar el registro de los usuarios que se conectan a la red en un periodo determinado, entre otros.

## ALCANCE

El alcance de este trabajo consistió en implementar una arquitectura de seguridad, que permita tener un mayor control a nivel de capa de enlace de datos, del acceso a equipos de terceras personas, tales como: proveedores, contratistas, entre otros, a la plataforma tecnológica de PDVSA, donde sólo las personas que se encuentran registradas en el directorio activo pueden tener acceso a recursos de la red, por ejemplo: internet, archivos compartidos, accesos a sistemas informáticos, entre otros. Además permite contabilizar el tráfico de red y generar diversas estadísticas sobre conexiones.

## LIMITACIONES

No se contó con la adquisición de todos los equipos de red necesarios para llevar a cabo la implementación de la arquitectura de seguridad, debido a que no se pudo efectuar la compra de los equipos de red que soportan el protocolo 802.1x en el periodo de tiempo en el cual se realizó esta implementación.

# CAPÍTULO II. MARCO REFERENCIA

## MARCO TEÓRICO

### Antecedentes de la investigación

Detrás de los servicios usados en una infraestructura de sistemas basados en la autenticación, existen mecanismos que permiten gestionar todos los datos de identificación de forma segura y eficiente. Estas infraestructuras pueden ser sencillas o extremadamente complejas, según el número de usuarios y localizaciones que manejan y según sus niveles de garantía de seguridad; debido a esto, se ha profundizado en el estudio de la seguridad en las redes tanto cableadas como inalámbricas, surgiendo y desarrollándose trabajos de investigación en diversas áreas de estudios, siendo algunos ejemplos de estas investigaciones los siguientes trabajos que han sido desarrollados por estudiantes universitarios e investigadores tales como:

En el año 2003, Sánchez desarrolló una arquitectura de control de acceso a redes de área local inalámbricas 802.11, mediante este trabajo, se tomó algunos métodos para la selección de las tecnologías a utilizar, con el fin de diseñar la arquitectura de control de acceso adaptándola a las necesidades de la organización.

En el año 2006, Matanzo implementa el protocolo CHAP en un sistema de seguridad para redes WLAN, este trabajo permitió la utilización de algunas técnicas de implementación de protocolos de seguridad, con el fin de darle solución a la problemática existente en la Corporación.

### Antecedentes de la organización

Petróleos de Venezuela S.A (PDVSA), es la corporación estatal de la República Bolivariana de Venezuela que se encarga de la exploración, producción, manufactura, transporte y mercadeo de los hidrocarburos, de manera eficiente, rentable, segura,

transparente y comprometida con la protección ambiental; con la finalidad de motorizar el desarrollo armónico del país, afianzar el uso soberano de los recursos, potenciar el desarrollo endógeno y propiciar una existencia digna y provechosa para el pueblo venezolano, propietario de la riqueza del subsuelo nacional y único dueño de esta empresa operadora (Petróleos de Venezuela S.A, 2005).

Por mandato de la Constitución de la República Bolivariana de Venezuela, la totalidad de las acciones de Petróleos de Venezuela S.A. pertenecen al Estado Venezolano, en razón de la estrategia nacional y la soberanía económica y política, ejercida por el pueblo venezolano. En ese sentido, PDVSA está subordinada al Estado Venezolano y por lo tanto actúa bajo los lineamientos trazados en los planes de desarrollo nacional y de acuerdo a las políticas, directrices, planes y estrategias para el sector de los hidrocarburos, dictadas por el Ministerio del Poder Popular para la Energía y Petróleo.

Motivado a la paralización de PDVSA por parte de sus empleados durante el año 2002 y 2003, la empresa realizó una reestructuración de su organización con la finalidad de afrontar esta nueva etapa e impulsar la creación de la Gerencia de Automatización, Informática y Telecomunicaciones (AIT) para encargarse de la administración de toda la plataforma tecnológica de PDVSA, sustituyendo de esta forma a la empresa INTESA. Luego de dos (2) años, se realizó un análisis exhaustivo de la Gerencia de AIT, donde se hizo palpable la necesidad de segregar sus funciones para mantener la transparencia en los procesos que se llevaban a cabo, traspasando la función de Seguridad AIT para la Gerencia de PCP, cambiando su denominación actual a Seguridad Lógica PCP la cual provee actualmente a nivel nacional e internacional una serie de servicios de seguridad a la plataforma tecnológica de la Corporación tales como: control de acceso lógico, tratamiento de incidentes, consultorías de seguridad lógica, educación en seguridad de información, evaluación de seguridad lógica, análisis de riesgo lógico y planificación de la continuidad todos

estos, en conformidad con las políticas diseñadas para el resguardo de la información dentro de la Corporación. En la figura 1, se presenta la estructura organizativa de la Gerencia de PCP Oriente, dentro de la cual se encuentran la Gerencia de Seguridad Lógica, Gerencia donde se realizó el presente trabajo.

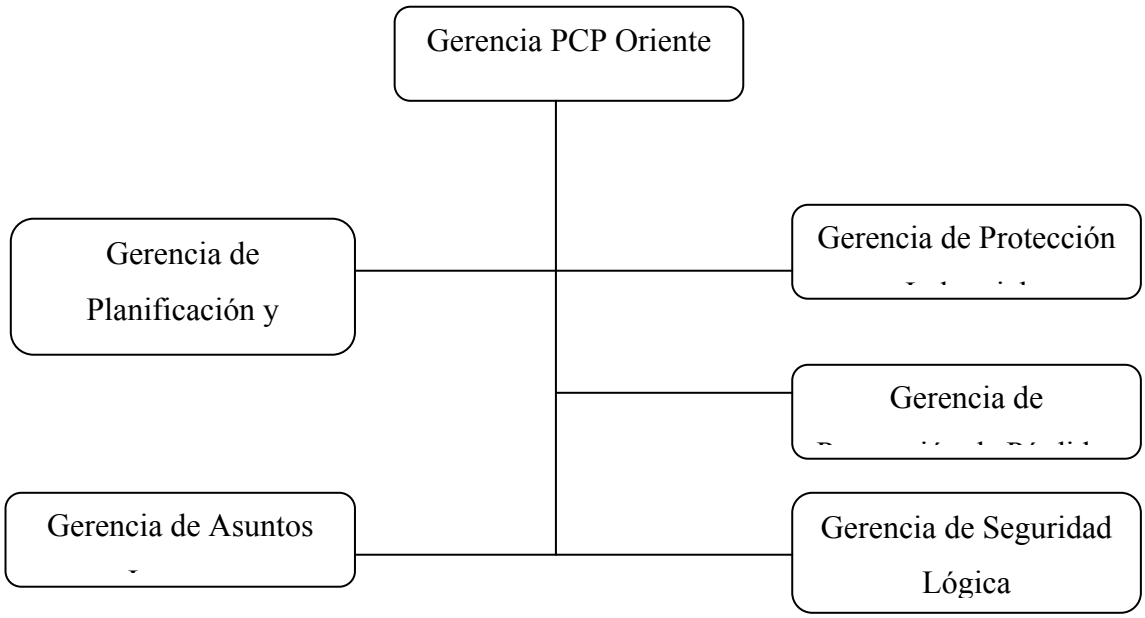



Figura 1. Estructura organizativa de la Gerencia de PCP división Oriente.

En la figura 2, se muestra el organigrama funcional de la Gerencia de Seguridad Lógica y los procesos que ésta realiza; entre ellos se tienen: Arquitectura y Gestión de Seguridad, Evaluación Respuesta y Contingencia, Protección Lógica.

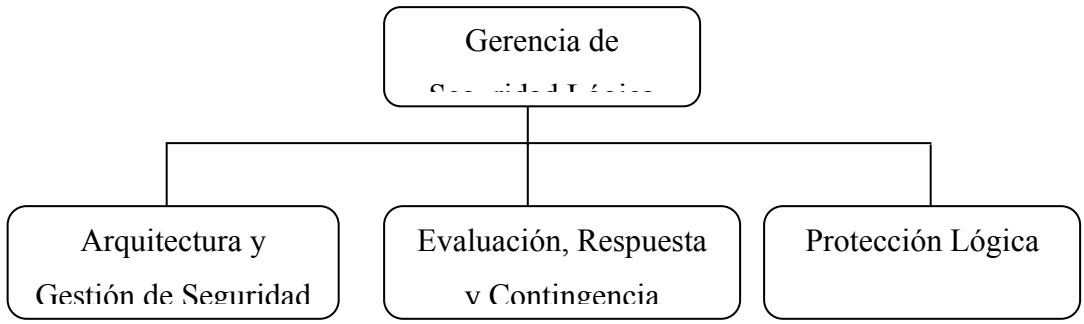



Figura 2. Organigrama funcional de la Gerencia de Seguridad Lógica.

La misión de la Gerencia de Seguridad Lógica división Oriente es diseñar, operar, evaluar soluciones y mecanismos de seguridad que permitan resguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Plataforma Tecnológica de PDVSA, contra amenazas internas y externas, a fin de contribuir con la continuidad de sus operaciones. Sus bases están fundamentadas en trabajo en equipo, honestidad, disciplina, excelencia y lealtad.

**Área de estudio**

El área de estudio esta ubicada en el área de telecomunicaciones, debido a que engloba todos los aspectos relacionados a la transmisión y recepción de información de cualquier tipo, incluyendo datos, utilizando señales eléctricas u ópticas enviadas a través de cable, de fibra o por el aire (Sánchez, 2003). Seguridad Lógica, mantiene una comunicación a distancia entre el recurso humano y los sistemas de información que en ésta se encuentran, mediante el uso de diversos medios de transmisión como lo son: transmisión por cable, fibra e inalámbrica.

A continuación se definen una serie de términos asociados al área de estudio:

Sistema de telecomunicaciones: consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales (Kuhlmann y Alonso, 1996).

Función de una red de telecomunicaciones: consiste en ofrecer servicios a sus usuarios, y cuando ésta es utilizada para que sobre ella se ofrezcan servicios de telecomunicaciones al público en general (por ejemplo, la red telefónica) se le denomina una red pública de telecomunicaciones (Kuhlmann y Alonso, 1996).
Red privada de telecomunicaciones: es una red que establece una persona natural o jurídica con su propia infraestructura para el uso de sus comunicaciones internas o privadas, que le puede permitir comunicaciones no permanente con sus clientes o proveedores. (EFMF, 2004).

Cobertura geográfica de una red de telecomunicaciones: es la que limita el área en que un usuario puede conectarse y tener acceso a la red para utilizar los servicios que ofrece. Por ejemplo, existen redes locales que enlazan computadoras instaladas en un mismo edificio o una sola oficina, conocidas como LAN por su nombre en inglés: *Local Area Network*, pero también existen redes de cobertura más amplia, conocidas como WAN por su nombre en inglés: *Wide Area Network*, redes de cobertura urbana que distribuyen señales de televisión por cable en una ciudad, redes metropolitanas que cubren a toda la población de una ciudad, redes que enlazan redes metropolitanas o redes urbanas formando redes nacionales, y redes que enlazan las redes nacionales, las cuales constituyen una red global de telecomunicaciones (Kuhlmann y Alonso, 1996).

Según Kuhlmann y Alonso (1996), los nodos son los equipos encargados de realizar las diversas funciones de procesamiento que requieren cada una de las señales o mensajes que circulan o transitan a través de los enlaces de la red. Desde un punto de vista topológico, los nodos proveen los enlaces físicos entre los diversos canales que conforman la red.

IEEE: corresponde a las siglas de Instituto de Ingenieros Electricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras

cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros electricistas, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en mecatrónica. En 1963 adoptó el nombre de IEEE al fusionarse asociaciones como el AIEE (*American Institute of Electrical Engineers*) y el IRE (*Institute of Radio Engineers*). Gracias a sus miembros se ha convertido en una de las autoridades principales en todo lo referente al ámbito técnico y tecnológico, abarcando desde la ingeniería informática, biomédica, de telecomunicaciones, aeroespacial y de dispositivos electrónicos, entre otras (Wikipedia, 2005).

Redes de área local (LAN): son las más conocidas en las organizaciones y, de manera creciente, en los hogares. Permiten conectar dispositivos con una cobertura de cientos de metros hasta un par de kilómetros. Históricamente, la tecnología dominante en estas redes ha sido Ethernet, creada por Robert Metcalfe en los laboratorios Xerox PARC a mediados de los años 70 y estandarizada por la IEEE bajo el grupo de trabajo 802.3; En sus primeras versiones, los dispositivos se conectan a un medio compartido (un cable coaxial, o un concentrador) en el que se difunde la señal transmitida, que puede ser escuchada por todos. Cuando un dispositivo desea enviar información, verifica que el medio esté libre y la transmite en una trama que tiene, entre otros campos, identificadores del remitente y del receptor. Este último toma la trama del medio; los demás la ignoran. Existe la posibilidad de que dos dispositivos que deseen transmitir casi al mismo tiempo, escuchen el medio, lo encuentren libre e inicien su transmisión, distorsionando la señal del otro. Los emisores están obligados a detectar este fenómeno, llamado colisión, y en caso de que ocurra, abortan la transmisión y lo intentan nuevamente en un momento posterior. Las nuevas implementaciones del protocolo no utilizan medios compartidos; los dispositivos están conectados directamente a conmutadores que pueden encaminar la información a su destinatario (Metcalfe y Boggs, 1976).

## Área de investigación

Este proyecto se ubica en el área de seguridad en redes LAN, tanto cableadas como inalámbricas, ya que se basa en el uso de redes, sistemas distribuidos y herramientas de comunicación para transportar datos entre el usuario de un terminal y el computador, y entre dos computadores. Las medidas de seguridad de la red son necesarias para proteger los datos durante la transmisión (Stallings, 2004).

Según Stallings (2004), la seguridad es una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, seguro. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros; a continuación se exponen algunas de las razones:

- En el desarrollo de un mecanismo particular de seguridad o algoritmo, siempre se deben tener en cuenta los posibles ataques a esas características de seguridad. En muchos casos, los ataques con éxito están diseñados analizando el problema de una forma totalmente diferente, explotando, por lo tanto, una debilidad inadvertida del mecanismo.
- Los procedimientos empleados para proporcionar servicios particulares no suelen ser intuitivos; es decir, a partir de la afirmación de un requisito particular no es obvio que sean necesarias medidas tan elaboradas. Las medidas empleadas sólo cobran sentido cuando se han considerado las diferentes contramedidas.
- Después de diseñar distintos mecanismos de seguridad, es necesario decidir dónde usarlos, tanto en lo que respecta a la ubicación física (por ejemplo, en qué punto

de una red se necesitan determinados mecanismos de seguridad) como a la ubicación lógica (en qué capa o capas de una arquitectura como la TCP/IP (*Transmission Control Protocol / Internet Protocol*) deberían estar localizados los mecanismos).

- Los mecanismos de seguridad suelen implicar más de un algoritmo o protocolo. Con frecuencia también requieren que los participantes posean alguna información secreta (que podría ser una clave de cifrado), lo que da lugar a cuestiones sobre la creación, distribución y protección de esa información secreta. También hay una dependencia de los protocolos de comunicación cuyo comportamiento puede complicar la tarea de desarrollar mecanismos de seguridad.

Servicio de seguridad: un servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización. Los servicios están diseñados para contrarrestar los ataques a la seguridad, y hacen uso de uno o más mecanismos para proporcionar el servicio (Buster, 2005).

Control de acceso: en el contexto de la seguridad de redes, el control de acceso es la capacidad de limitar y controlar el acceso a sistemas *host* y aplicaciones por medio de enlaces de comunicaciones. Para conseguirlo, cualquier entidad que intente acceder debe antes ser identificada o autentificada, de forma que los derechos de acceso puedan adaptarse de manera individual (Buster, 2005).

Privacidad: esto se hace al encriptar la comunicación, lo que evitará que otras personas puedan usar/leer los datos. El uso de encriptación podría suponer una disminución notable del rendimiento, dependiendo del tipo de implementación y encriptación usados (Buster , 2005).

*Cracker*: es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema (Sánchez, 2003).

*Hacker*: es una persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo (Sánchez, 2003).

Criptoanálisis: es la rama del conocimiento que se encarga de descifrar los mensajes encriptados sin conocer sus llaves. Se dice que determinada clave ha sido "rota" cuando alguien logra descifrar un mensaje sin conocer la clave que le dio origen (Stallings, 2004).

Criptografía: es la rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas (Stallings, 2004).

Clave privada: Una de las dos claves utilizadas en los sistemas de cifrado de clave pública. El usuario mantiene en secreto la clave privada y la utiliza para cifrar firmas digitales y para descifrar los mensajes recibidos (Sánchez, 2003).

Clave pública: Una de las dos claves utilizadas en los sistemas de cifrado de clave pública. El usuario da a conocer esta clave de manera pública, de forma que todo el mundo pueda utilizarla para cifrar los mensajes enviados al usuario y para descifrar las firmas digitales de dicho usuario (Sánchez, 2003).

SSL (*Secure Sockets Layer*): protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP (Sánchez, 2003).

Texto plano: se refiere a un documento antes de ser encriptado. Texto descifrado o que no está cifrado (Sánchez, 2003).

Según McCabe (1998), la seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Confidencialidad: consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial (McCabe, 1998).

Integridad: es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones causadas por errores de hardware y/o software, causadas de forma intencional, de forma accidental, cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia (McCabe, 1998).

Autenticidad: en cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información (Sánchez, 2003).

No repudio: ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa (Sánchez, 2003).

Control de acceso a los recursos: consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace (Sánchez, 2003).

Según Metcalfe y Boggs (1976), TKIP (*Temporal Key Integrity Protocol*) es también llamado *hashing* de clave WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente; el proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los puntos de acceso. Combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que cifrará los datos. Este procedimiento asegura que cada estación utilice diferentes *streams* claves para cifrar los datos. El *hashing* de clave WEP protege a los vectores de inicialización (IV) débiles para que no sean expuestos haciendo *hashing* del IV por cada paquete. Utiliza el RC4 para realizar el cifrado, que es lo mismo que el WEP.

Infraestructura de clave pública: es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. (Metcalfe y Boggs, 1976).

Propósito y funcionalidad: la infraestructura de clave pública permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

Según Stallings (2004), en una operación criptográfica que use infraestructura de clave pública, intervienen conceptualmente como mínimo las siguientes partes:

1. Un usuario iniciador de la operación

2. Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, autoridad de registro y sistema de sellado de tiempo)
3. Un destinatario de los datos cifrados, firmados y enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

La seguridad que puede aportar la infraestructura de clave pública, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o políticas de seguridad aplicados.

Según Metcalfe y Boggs (1976), existen diferentes tipos de certificado digital, en función de la información que contiene cada uno y a nombre de quién se emite el certificado, entre los cuales se encuentran:

- Certificado personal: es el que acredita la identidad del titular.
- Certificado de pertenencia a empresa: es aquel que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de representante: es aquel que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de persona jurídica: es el que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de atributo: el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal.

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos, tales como:

- Certificado de servidor seguro: es utilizado en los servidores Web que quieren proteger ante terceros el intercambio de información con los usuarios.

- Certificado de firma de código: es el que se usa para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Según Stallings (2004), la seguridad en la infraestructura de clave pública depende en parte de cómo se guarden las claves privadas. Existen dispositivos especiales denominados *tokens* de seguridad diseñados para facilitar la integridad y seguridad de la clave privada, así como evitar que ésta pueda ser exportada. Estos dispositivos pueden incorporar medidas biométricas, como la verificación de huella dactilar, que permiten aumentar la confiabilidad, dentro de las limitaciones tecnológicas, en que sólo la persona dueña del certificado pueda utilizarlo.

Cifrado: es el proceso de convertir un mensaje de texto en texto cifrado que puede ser decodificada de nuevo en el mensaje original. Un algoritmo de cifrado con una clave se utiliza para el cifrado y descifrado de datos. Hay varios tipos de encriptaciones de datos que constituyen la base de seguridad de la red. El tipo y la longitud de las claves utilizadas dependerán del algoritmo de cifrado y el grado de seguridad necesario (Stallings, 2004).

Según Stallings (2004), entre los servicios o mecanismos que permiten la construcción de una solución segura para el intercambio de información se encuentran los siguientes:

- Integridad de datos: este mecanismo responde a la pregunta "¿Están mis datos intactos?". Por medio de éste, se asegura que los datos no se han perdido o han sido alterados durante su transferencia. Esto se realiza verificando las características del documento y la transacción. Tales características son inspeccionadas y confirman su contenido y correcta autorización. La integridad de los datos se logra por medio de criptografía electrónica la cual asigna una

identidad única a los datos, como si fuera una huella digital. Cualquier intento de cambiar esta identidad es revelado y proporciona como resultado que el documento (datos) ha sido alterado.

- Autenticación: responde a la pregunta "¿Están los datos correctos y provienen de la entidad correcta?". Este mecanismo verifica las identidades de los usuarios, servidores, dispositivos y sistemas, para asegurar que son genuinos.
- Identificación: responde a la pregunta "¿Quién es o quién está enviando los datos?" Este proceso consiste en reconocer a un individuo en particular. Esto requiere que la persona o proceso encargado de verificar confronte la información presentada con todas las entidades que conoce, para comprobar con quién se está negociando.
- Aceptación: este mecanismo también se le conoce como "no repudio". Asegura la imposibilidad de eludir la responsabilidad en la generación o recepción de una transacción. Esto es, que ninguna de las partes involucradas en una transacción pueda negar el envío o la recepción de información. Este mecanismo utiliza generalmente esquemas basados en firmas digitales.
- Autorización y delegación: responde a la pregunta "¿Puedo compartir de manera segura estos datos si así lo deseo?". El mecanismo permite asignar y administrar privilegios de acceso a usuarios y grupos adicionales. La autorización es el proceso de permitir acceso a datos en específico dentro de un sistema. Delegación es la utilización de un tercero para administrar y certificar cada uno de los usuarios de un sistema (Autoridades de Certificación).
- Auditoria y bitácora: responde a la pregunta "¿Puedo verificar que el sistema esté funcionando?". Este mecanismo provee un monitoreo constante y funciones de asistencia a los sistemas de seguridad. Esta es una examinación y almacenamiento independiente de los registros y actividades para asegurar la conformidad con ciertos controles establecidos, políticas, procedimientos operacionales y recomendar cualquier cambio indicado en estos controles, políticas y

procedimientos.

- Administración: este mecanismo permite la administración del sistema de seguridad. Es la vista general y el diseño de todos los elementos y mecanismos involucrados.
- Privacidad y confiabilidad: este mecanismo asegura que sólo los emisores y receptores tienen acceso a los datos. Esto se realiza generalmente empleando una o más técnicas de encriptación para asegurar los datos. Confiabilidad es el uso de encriptación para proteger la información de accesos no autorizados. El texto original se convierte en texto cifrado por medio de un algoritmo para luego ser descifrado de vuelta al texto original, utilizando el mismo método pero en forma inversa.

Servidor RADIUS: es un dispositivo que recibe y procesa peticiones de conexión o mensajes de contabilidad enviados por clientes RADIUS. En el caso de las peticiones de conexión, el servidor procesa la lista de atributos RADIUS de la petición de conexión. El servidor RADIUS autentica y autoriza la conexión, y a su vez devuelve un mensaje de aceptación rechazo de acceso, basándose en un conjunto de reglas y la información de la base de datos de cuentas de usuario. El mensaje de aceptación de acceso puede contener restricciones de conexión que implementa el servidor de acceso durante el transcurso de conexión (Microsoft *Corporation*, 2007).

Para proporciona un mejor mecanismo en el control y seguridad de acceso, es necesario incluir un protocolo de administración de claves en la especificación. El estándar 802.1x, se desarrolló específicamente para abordar este asunto. Específicamente para el caso de redes inalámbricas, el punto de acceso puede actuar como un autenticador de accesos a la red, utilizando el servidor RADIUS para autenticar las identificaciones del cliente. La comunicación se realiza a través de un "puerto no controlador" o canal lógico en el punto de acceso, con el propósito de

validar las identificaciones y obtener claves de acceso a la red a través de un "puerto lógico controlado". Las claves que están disponibles al punto de acceso y al cliente como resultado de este intercambio, permite que los datos del cliente se encripten y sean identificados por el punto de acceso. De esta manera, se ha agregado el protocolo de administración de claves a la seguridad 802.11 (Kuhlmann y Alonso, 1996).

Servidor AAA: servidor que ofrece servicios de autentificación, autorización y contabilidad (*Accounting*) para realizar transacciones financieras. Estos servidores sirven para desarrollar aplicaciones de comercio electrónico. Por ejemplo, sirven para comprobar que un usuario determinado ha sido autorizado para realizar una transacción en particular, como `puede ser una transacción de débito en un sistema de pagos por tarjeta de crédito (Donoso Cortés, 2002).

Autenticación: es la comprobación de la identidad de una persona o de un objeto. En sí, es el proceso de verificar si la identidad de una persona o una máquina es efectivamente la que declara. Puede basarse en lo que esa persona sabe (contraseña, clave, PIN); lo que la persona posee (tarjeta, certificado digital); lo que la persona es (huella dactilar, cara, mano, voz) (Microsoft *Corporation*, 2007).

Autorización: es el proceso de aceptar o negar el acceso de un usuario a los recursos, una vez haya sido autenticado con éxito. El tipo de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido. Por ejemplo, sólo los usuarios del departamento de nómina podrán tener acceso a los datos de la nómina de la empresa. (Kuhlmann y Alonso, 1996).

Auditoria: es el proceso de supervisar la actividad del usuario durante su acceso, en lo que se refiere al uso de los recursos, la cantidad de tiempo que permanece conectado,

los servicios a los que accede, así como la cantidad de datos transferidos durante la sesión (Microsoft *Corporation*, 2007).

IEEE 802.1x: el estándar 802.1x proporciona control de acceso basado en puerto y la autentificación mutua entre los clientes y los puntos de acceso vía servidor de la autentificación. Este estándar consiste en tres elementos esenciales:

- Un suplicante: es un usuario o un cliente desea ser autenticado. Puede ser el software cliente en la computadora portátil, u otro dispositivo inalámbrico.
- Un servidor de autenticación: es un sistema de autenticación que maneja autenticaciones reales.
- Un autenticador: es un dispositivo actúa como intermediario entre el servidor de autenticación y el solicitante. Generalmente, el dispositivo es un punto de acceso.

La autenticación mutua en 802.1x implica varios pasos, que se describen a continuación:

1. Una vez que el solicitante logra una conexión con un autenticador detecta la inicialización y permite el puerto del solicitante.
2. El autenticador solicita la identidad del solicitante.
3. El solicitante responde con la identidad. El autenticador pasa la identidad a un servidor de la autenticación.
4. El servidor de autenticación autentica la identidad del solicitante. Una vez que este autenticado, un mensaje de "aceptado" se envía al autenticador. El autenticador cambia el estado del puerto del solicitante a estado autorizado.
5. El solicitante entonces solicita la identidad del servidor de autenticación.
6. Una vez que el solicitante autentica la identidad del servidor, todos los tráficos son permitidos.

Según Microsoft *Corporation* (2007), las características que debe cumplir un Servidor AAA son las siguientes:

1. El servidor AAA debe ser capaz de soportar millones de usuarios y cientos de miles de consultas simultáneas.
2. La arquitectura del servidor debe soportar cientos de dispositivos, clientes servidores AAA, entre otros. Debe ser capaz de soportar el mecanismo de autenticación entre el servidor AAA.
3. El servidor AAA debe ser capaz de transportar certificados. Este requerimiento se entiende como una optimización del sistema, debe permitir que la comunicación sea segura. Sin embargo debe permitir que un servicio de seguridad sea utilizado.
4. El servidor AAA debe ser extensible a otros usos para definir las cualidades que son específicas al servicio que es definido, es decir, que este protocolo debe permitir que los grupos definan cualidades estándares. Dentro de los servidores de autenticación que cumplen con estas características, se tiene el servidor RADIUS.

Cliente Servidor: un servidor de acceso de red funciona como un cliente RADIUS. El cliente es responsable de pasar la información del usuario al servidor RADIUS designado. El servidor RADIUS es responsable de recibir peticiones de unión de usuario, certificando al usuario, y luego devolviendo toda la información de configuración necesaria para que el cliente entregue el servicio al usuario. Las transacciones entre el cliente y servidor RADIUS son certificadas por el uso de un secreto compartido, que nunca es enviado sobre la red. Además, cualquier contraseña de usuario es enviada codificada entre el cliente y servidor RADIUS, para eliminar la posibilidad que alguien capture la contraseña de un usuario (Microsoft *Corporation*, 2007).

Servidor de acceso: es un dispositivo que proporciona cierto nivel de acceso a la red. Un servidor de acceso que utiliza una infraestructura RADIUS es un cliente RADIUS y envía peticiones de conexión y mensajes de contabilidad a un servidor RADIUS (Microsoft *Corporation*, 2007).

Servidor de directorio de usuarios: en él se registrarán a todos los usuarios que cuenten con el permiso de acceder al sistema. Se guardará información básica por cada usuario; teniendo desde su nombre de usuario, contraseña, nombres y apellidos y dirección de correo electrónico. Así mismo, es posible poder ampliar estos datos para poder almacenar datos adicionales tales como su edad, fecha de nacimiento, dirección postal, ciudad/país de residencia, área a la que pertenece dentro de la empresa, cargo que desempeña, entre otros (Microsoft *Corporation*, 2007).

Servidor de base de datos: llevará a cabo la contabilidad del sistema. Es decir, dentro de él se almacenarán todos los datos suficientes para poder obtener las estadísticas del sistema por cada usuario; pudiendo conocer cuánto tiempo se ha encontrado conectado, que día y a qué hora se conectó, cuando terminó su sesión, el punto de acceso desde el cual se conectó, entre otros datos ya mencionados anteriormente. Así, por medio de este servidor se podrán conocer los hábitos de conexión a la red por cada usuario; pudiendo así tomar las acciones correspondientes. Adicionalmente, se podría realizar la tarificación por cada usuario por haber hecho uso del sistema; orientando así la solución para mercados comerciales (Microsoft *Corporation*, 2007).

Servidor de gestión Web: este servidor ofrecerá al administrador de la red una interfaz Web de fácil uso con la que podrá llevar a cabo la administración de todo el sistema; pudiendo por medio de ella agregar nuevos usuarios al sistema, editar la información básica correspondiente a cada usuario, restablecer su contraseña, mostrar una lista con todos los usuarios del sistema así como las estadísticas por cada uno de éstos (Microsoft *Corporation*, 2007).

Protocolo RADIUS (Servicio para usuario de Acceso Telefónico de Autenticación Remota): es un protocolo que se utiliza para proporcionar servicios de Autenticación, Autorización y Auditoria del uso de cuentas de usuario, para aplicaciones de acceso a la Red ó movilidad IP (*Internet Protocol*). Este protocolo fue desarrollado originalmente por *Livingston Enterprises* y publicado en 1997. Utiliza el puerto 1812 UDP para los mensajes de Autenticación y el 1813 para los mensajes de *accounting* o administración de cuentas. El protocolo RADIUS tiene un lugar prominente entre los servicios de proveedores de Internet, también pertenece a cualquier ambiente donde sea necesario o deseada, la autenticación central, la autorización regulada y el manejo de cuentas de usuario (Rodríguez, 2007).

Características del protocolo RADIUS: una característica interesante es que el protocolo RADIUS en principio utilizaba segmentos UDP (*User Datagram Protocol*) (Protocolo del nivel de transporte) en lugar de TCP (Protocolo de Control de Transmisión). Esto se debe a que RADIUS tiene algunas propiedades inherentes a los segmentos UDP. RADIUS requiere que las consultas fallidas de un servidor sean redirigidas a un segundo servidor, y para hacer esto, una copia del pedido original debe existir sobre la capa de transporte del modelo de red (modelo OSI), esto en efecto obliga a usar tiempo de retransmisión (Rodríguez, 2007).

Según Rodríguez, 2007 otra propiedad, es que no se ve afectado por el estado del equipo como pérdida de poder, reinicio y tráfico pesado en el sistema. UDP previene todas esas dificultades ya que permite que una sesión se abra y se mantenga abierta durante toda la transacción. UDP permite que RADIUS despache múltiples pedidos al mismo tiempo, además en cada sesión posee habilidades de comunicación sin restricciones entre el equipo de red y los clientes. La única desventaja de utilizar segmentos UDP, es que los desarrolladores por sí mismos deben crear y administrar

tiempos de retransmisión, pero esta desventaja no se compara con la conveniencia y simplicidad de usar estos segmentos de transporte de red.

Según Rodríguez, 2007 las características de los Paquetes RADIUS son las siguientes:

- Transportan mensajes entre el cliente y el servidor RADIUS.
- Siguen una convención de petición/respuesta: El cliente envía una petición y espera una respuesta del servidor. Si la respuesta no llega, el cliente puede reintentar la petición periódicamente.
- Cada paquete sirve para un propósito específico: autenticación o contabilidad.
- Un paquete consta de la cabecera, donde se presenta el código o tipo de mensaje, el identificador del mensaje y la longitud y el autenticador del mensaje, así como también de una serie de cero o más atributos codificados según la convención de tipo, longitud, valor.
- Los atributos específicos que contiene un mensaje dependen del tipo de paquete (contabilidad o autenticación) y del cliente que lo envía.
- Los paquetes RADIUS se transportan usando el protocolo UDP (no orientado a conexión y recepción no garantizada), por lo que si la respuesta no llega en un tiempo determinado, se pueden producir retransmisiones.

Según Hassell (2002), un mensaje RADIUS está formado por un encabezado RADIUS y cero o más atributos RADIUS. Cada atributo RADIUS especifica una información determinada acerca del intento de conexión. Los mensajes RADIUS se envían sobre UDP (*User Datagram Protocol*) para pasar transmisiones entre el cliente y el servidor. El protocolo se comunica por el puerto UDP 1812 (o 1645) para los mensajes de autenticación y el puerto 1813 (o 1646) para los mensajes de contabilidad. Se utiliza UDP en vez de TCP para acelerar el proceso de autenticación.

Ya que normalmente no hace falta la retransmisión de datos ni tampoco la confirmación que brinda TCP. En el caso de no tener respuesta por parte del servidor RADIUS primario, las solicitudes suelen ser redirigidas a un servidor alterno. La carga útil que sigue al encabezado está formada por una secuencia de parejas de atributos y valores (AVP). Para cada atributo se especifica el tipo, la longitud y el valor, de acuerdo a un diccionario previamente establecido. Los atributos son opcionales y se utilizan para proporcionar información entre clientes RADIUS y servidores RADIUS. El mensaje está dividido en cinco partes, como se observa en la figura 3.

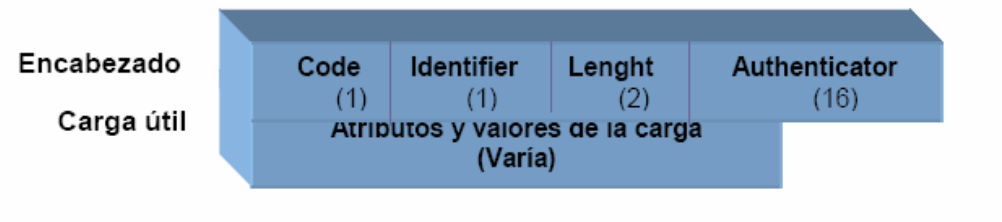



Figura 3. Paquete RADIUS.

*Code* (Código): la región de código tiene una longitud de un byte y sirve para distinguir que tipo de mensaje RADIUS ha sido enviado en el paquete. Los paquetes con campos inválidos son desechados sin notificación; Los códigos válidos son: *Access-Request* (petición de acceso), □*Access-Accept* (acceso aceptado), □*Access-Reject* (acceso denegado), □*Accounting-Request* (pedido de cuenta), □*Accounting-Response* (respuesta de cuenta), □*Access-Challenge* (desafío de acceso), (Hassell, 2002).

*Identifier* (Identificador): el identificador tiene una longitud de un byte y es usado para hacer *threading* (secuencias), o enlace automático de los pedidos iniciales y contestaciones subsecuentes. El servidor RADIUS generalmente puede interceptar mensajes duplicados para examinar factores como el origen de la dirección IP, el

origen del puerto UDP, la duración entre los mensajes sospechosos, y el campo de identificación, (Hassell, 2002).

*Length* (Longitud): la región de longitud es de dos (2) bytes y se usa para especificar el tamaño del mensaje RADIUS. El valor de este campo se calcula al analizar los campos de: código, identificador, longitud, autenticador y haciendo la suma de sus atributos. El campo de longitud se chequea cuando el servidor RADIUS recibe un paquete para asegurar la integridad de los datos. El rango de tamaño válido esta entre los 20 y 4096. Si el servidor recibe un paquete fuera del rango permitido, este es ignorado (Hassell, 2002).

*Authenticator* (Autenticador): la región de autenticación tiene una longitud por lo regular de 16 bytes, este es el campo en que la integridad de la carga útil del mensaje se inspecciona y verifica. En este campo el byte más importante es transmitido antes que cualquier otro. El valor usado para autenticar es contestado por el servidor RADIUS. Este valor también es usado en el mecanismo para conceder contraseñas. Hay dos tipos específicos de valores de autenticación: los valores de pedido y respuesta. Los de pedido son usados con los paquetes de *Authentification-Request* y *Accounting-Request*. El valor de pedido es de 16 bytes y es generado aleatoriamente para prevenir cualquier ataque. El autenticador de respuesta es usado en los paquetes *Access-Accept y Access-Challenge*. El valor es calculado con una función *hash* generada por los valores en las regiones del paquete: código, identificador, longitud, y la región de autenticador de pedido, seguido por la carga útil del paquete y el secreto compartido (Hassell, 2002).

Según Hassell (2002), existen cuatros tipos de mensajes que son relevantes para las fases de Autenticación y Autorización. En los documentos RFC 2865 y 2866 se definen los siguientes tipos de mensajes RADIUS:

*Access-Request* (solicitud de acceso): enviado por un cliente RADIUS para solicitar autenticación y autorización de un intento de conexión. Lo que caracteriza a un mensaje de petición es que el valor del campo de código en el encabezado es igual a uno (1). La carga útil del mensaje de petición de acceso debe incluir el atributo de: nombre de usuario para identificar a la persona que desea obtener el acceso al recurso de la red. Es necesario que la carga útil contenga la dirección IP o el nombre canónico del equipo de la red que está solicitando el servicio, éste también debe contener la contraseña de usuario, la contraseña basada en CHAP, o el identificador de estado, pero no ambos tipos de contraseñas. La contraseña de usuario debe pasarse por una función *hash* usando MD5 (Hassell, 2002). En la figura 4 se muestra la estructura del paquete RADIUS *Access-Request*.

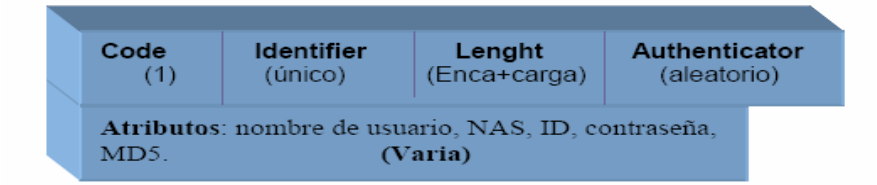



Figura 4. Paquete RADIUS *Access-Request*.

*Access-Accept* (aceptación de acceso): enviado por un servidor RADIUS como respuesta a un mensaje *Access-Request*. En él se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión. Si todas las peticiones en la carga útil que forman la petición de acceso son aceptadas, entonces el servidor RADIUS debe fijar el campo de código a dos (2). El cliente, una vez que recibe el paquete aceptado, comprueba este con el mensaje de respuesta usando el campo de identificación. Los que no sigan este estándar son descartados (Hassell, 2002). En la figura 5, se observa la estructura del paquete *Access-Accept*.

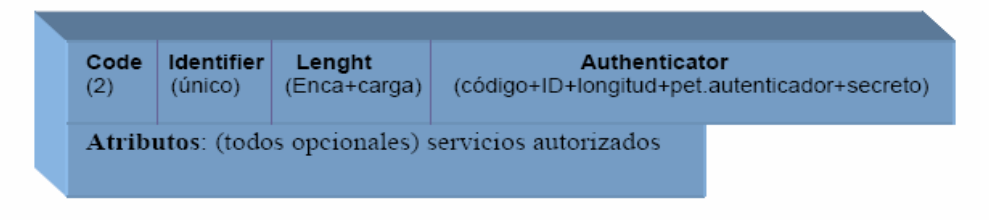



Figura 5. Paquete RADIUS *Access-Accept.*

*Access-Reject* (rechazo de acceso): enviado por un servidor RADIUS como respuesta a un mensaje *Access-Request*. En él se informa al cliente RADIUS de que se ha rechazado el intento de conexión. Un servidor RADIUS envía este mensaje si las credenciales no son auténticas o si no se ha autorizado el intento de conexión. El rechazo puede estar basado en políticas de sistemas, privilegios insuficientes, o cualquier otro criterio. El acceso rechazado puede ser enviado en cualquier momento durante la sesión, lo que se hace ideal para reforzar los tiempos límites de conexión. Sin embargo no todos los equipos soportan recibir el acceso rechazado durante la conexión ya establecida (Hassell, 2002). En la figura 6, se observa la estructura del paquete *Access-Accept*.

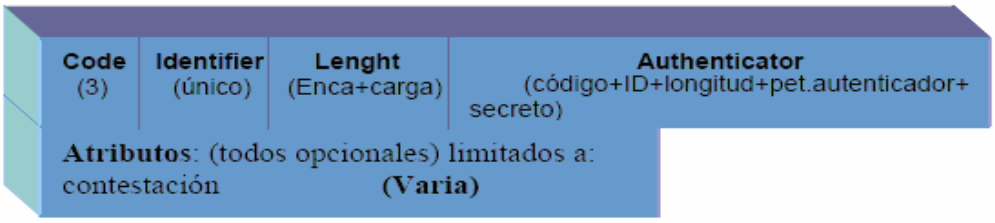



Figura 6. Paquete RADIUS *Access-Reject.*

*Access-Challenge* (desafío de acceso): enviado por un servidor RADIUS como respuesta a un mensaje *Access-Request*. Este mensaje es un desafío al cliente RADIUS que exige una respuesta, esto es, por si el servidor recibe información conflictiva de un usuario, requiere más información, o simplemente desea disminuir el riesgo de una autenticación fraudulenta, puede publicar un paquete de desafío de

acceso al cliente. El cliente una vez que recibe el desafío de acceso debe entonces publicar una nueva petición de acceso con la información apropiada (Hassell, 2002). En la figura 7, se observa la estructura del paquete *Access-Challengue*.

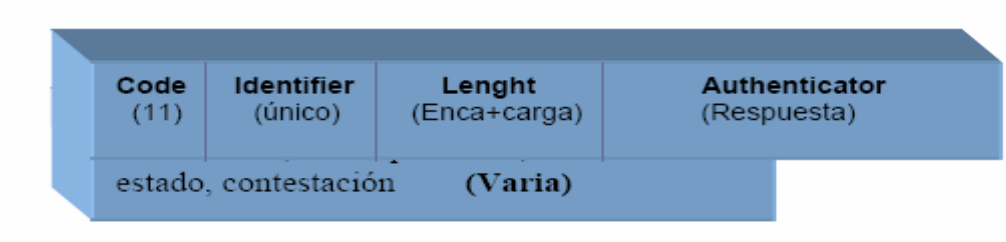



Figura 7. Paquete RADIUS *Access-Challengue.*

El servidor RADIUS también maneja los siguientes mensajes:

*Accounting-Request* (solicitud de administración de cuentas): enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado (Hassell, 2002).

*Accounting-Response* (respuesta de administración de cuentas): enviado por el servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas. En este mensaje se confirman la recepción y el procesamiento correctos del mensaje de Solicitud de administración de cuentas (Hassell, 2002).

Decisión multicriterio: es el conjunto de aproximaciones, métodos, modelos, técnicas y herramientas dirigidas a mejorar la calidad integral de los procesos de decisión seguidos por los individuos y sistemas, esto es a mejorar la efectividad, eficacia y eficiencia de los procesos de decisión y a incrementar el conocimiento de los mismos (valor añadido del conocimiento) (Aznar, 2005).

Método de la ordenación simple: es el método más sencillo de ponderación de criterios, ya que en él lo único que se demanda al decisor es que ordene los criterios

de mayor a menor importancia, de forma que después se otorga el mayor valor al primero y el menor valor al último. En el supuesto de que dos criterios se definan como de la misma importancia a cada uno de ellos se le adjudica el promedio de ambas valoraciones. Puntuados los criterios se normalizan por la suma y el resultado es la ponderación final de los criterios (Aznar, 2005).

Según Aznar (2005), el método de la suma ponderada calcula la ponderación de las alternativas como resultado del sumatorio del producto del peso de cada variable, por el valor que toma para esa alternativa la variable correspondiente. La ponderación de cada alternativa se obtiene mediante la fórmula:

$$W_i = \sum_{ji}^{n} \left( w_j * x_{ij} \right)$$

Siendo cada una de las variables las siguientes:

$W\,i$ = Ponderación final obtenida de cada alternativa.
$w\ j$ = Peso de cada variable obtenido por uno de los métodos conocidos de ponderación
(ordenación simple).
$x\,ij$ = Valor de cada variable para cada alternativa.

## MARCO METODOLÓGICO

### Metodología de la investigación

Forma de la investigación
La forma de investigación fue aplicada debido a que aporta una solución a la problemática planteada en la Gerencia de Seguridad Logica de PCPC (Sabino, 1999).

Tipo de investigación

La investigación que se realizó fue de tipo descriptiva, debido a que se encarga de describir los hechos a partir de un criterio definido previamente. En esta investigación se presenta una descripción completa de la situación actual de la Gerencia de Seguridad Lógica de PCP (Sabino, 1999).

Diseño de la investigación

Esta investigación cumple con un diseño de campo, la cual "estudia los fenómenos sociales en su ambiente natural" (Ramírez, 1995), debido a que la recolección de la información se realizó en el lugar donde se desarrollaron los procesos estudiados.

Técnicas para la recolección de datos

Mediante entrevistas no estructuradas al personal de la Gerencia de Seguridad Lógica de PCP, se obtuvo información clara y precisa, la cual facilitó la determinación de la solución más adecuada, además se aplicó la técnica de observación directa, lo cual permitió percibir los hechos de la realidad sin ningún tipo de intermediario, pudiendo conocer los requerimientos de la plataforma tecnológica de PDVSA, a su vez se realizó se realizó consultas bibliográficas, lo cual permitió establecer el soporte teórico de la investigación.

## Metodología del área aplicada

La metodología utilizada fue híbrida, producto de la configuración de algunos métodos propuestos por James McCabe (1998) de la cual se tomó las fases, determinación de los requerimientos y ejecución del diseño, de igual forma se tomó las fases análisis de las tecnologías y el diseño de la arquitectura de control de acceso, utilizados por Manuel Sánchez (2003); finalmente se consideró la fase denominada prueba de la arquitectura propuesta en la metodología de INTEL *Corporation* (2003),

quedando ordenada de la siguiente manera: determinación de los requerimientos, análisis de las tecnologías, diseño de la arquitectura de control de acceso, ejecución del diseño, pruebas de la arquitectura.

Determinación los requerimientos

Consistió en identificar, capturar y comprender las necesidades de los usuarios, servicios, aplicaciones y dispositivos que conforman el sistema y sus características (interactividad, confiabilidad, seguridad, calidad, adaptabilidad, factibilidad, crecimiento esperado entre otros) para enfocar y mejorar su rendimiento.

Análisis de las tecnologías

En esta fase se examinan diferentes tecnologías existentes, en cuanto a autenticación, protocolos de seguridad, cifrado de datos, mecanismos de autorización y servidor de autenticación, con el fin de seleccionar la alternativa, que mejor se adapte a las necesidades de la organización, permitiendo establecer el control de acceso a la red.

Diseñar la arquitectura de control de acceso

En esta fase se especifica mediante diagramas UML la manera en que los protocolos y aplicaciones de seguridad se comunican, para llevar a cabo la transmisión de los datos en la red.

Ejecución del diseño

Una vez que se propone el diseño debidamente documentado es posible ejecutarlo, definiendo las estrategias de acuerdo a los recursos humanos y computacionales disponibles bajo la supervisión de expertos en el área de redes con la finalidad de que la prueba ofrezca óptimos resultados basados en los requerimientos establecidos.

Pruebas de la arquitectura

En esta fase se llevarán a cabo las pruebas pertinentes que permitirán la verificación la arquitectura de seguridad funciona.

# CAPÍTULO III. DESARROLLO

## DETERMINACIÓN DE LOS REQUERIMIENTOS

El desarrollo de esta fase consistió en analizar y describir la situación actual del sistema de control de acceso empleado en la red PDVSA, para ello se requirió el uso de las técnicas para la recolección de información, tales como la observación directa, realizando un recorrido en las instalaciones del edificio ESEM de Maturín, con el fin de presenciar todo el procedimiento que realizan los usuarios para acceder a la red de datos de PDVSA; sumado a esto se realizaron entrevistas al personal de Seguridad Lógica y al personal de Redes, con el fin de conocer los requerimientos y las necesidades referentes al control de acceso a la plataforma de la red de la corporación.

En la figura 8, se describe mediante un diagrama de casos de usos de UML la situación actual en el sistema de control de acceso a la red *Ethernet* de PDVSA.

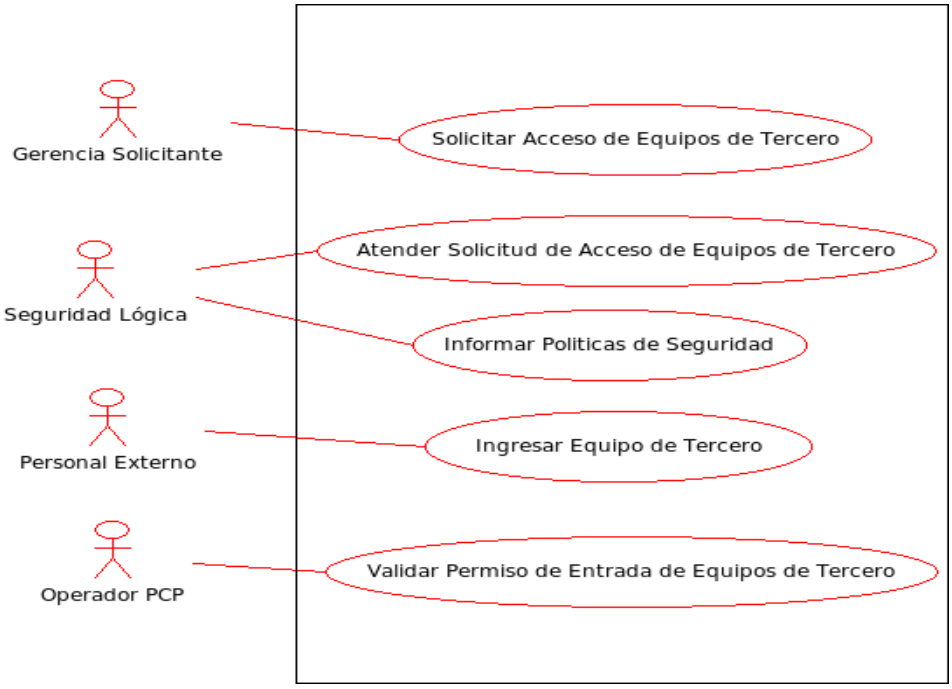


Figura 8. Diagrama de casos de uso para el acceso de equipos de tercero.

En el apéndice A se detalla la descripción de los casos de usos reflejados en la figura 8.

En la figura 9, se presenta mediante un diagrama de flujos, la interacción entre los elementos que intervienen, al momento de permitir o no el acceso a un personal externo (tercero), a las instalaciones de PDVSA, acompañado de un equipo de computación que no es propiedad de la Corporación.

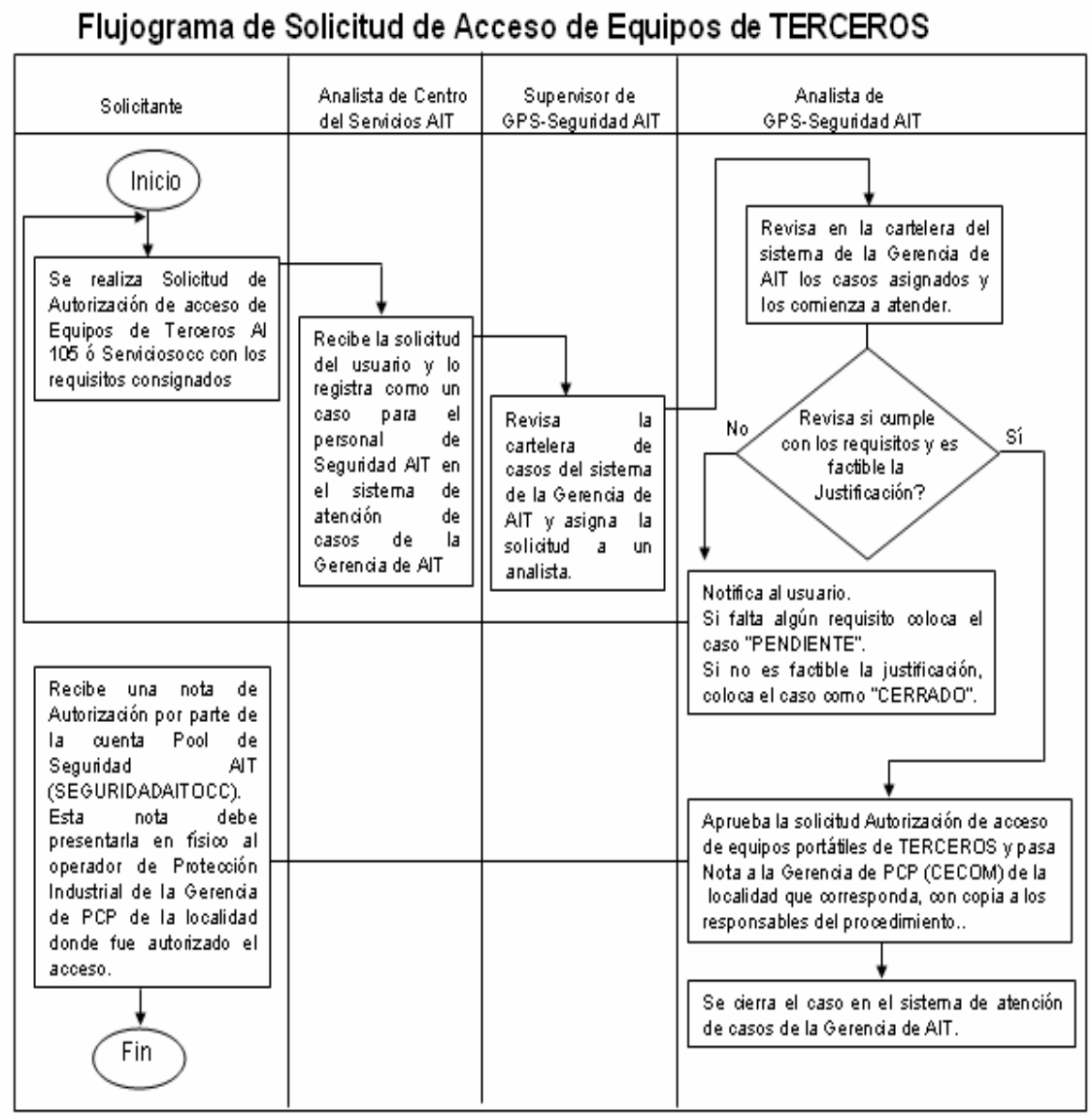



Figura 9. Diagrama de flujos para el acceso de equipos de tercero.

Para que un tercero pueda ingresar a las instalaciones de PDVSA con equipos de computación, que no son propiedad de la Corporación, es necesario que la Gerencia solicitante realice una solicitud de autorización de acceso dirigida al personal que labora en Seguridad Lógica, este personal es el encargado de aprobar dicha solicitud tomando en cuenta una justificación operacional. La Gerencia solicitante es la

encargada de designar a un personal encargado de acompañar al tercero con el fin de prohibir el acceso a la red de datos de la Corporación, evitando de esta forma comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

Mediante este sistema actual no es posible, denegar por completo el uso de puntos de red no seguro, ya que no existe un control de acceso a nivel de capa de enlace de datos que permita bloquear los puertos, usando métodos de cifrado, autorización, autenticación y registros para auditorias que permitan dar el acceso únicamente a los usuarios autorizados pertenecientes al dominio de PDVSA, evitando que personas ajenas a la Corporación hagan uso sin autorización de los recursos de la red, por tal motivo surgió la necesidad de implementar una arquitectura de control de acceso basada en el estándar de Seguridad IEEE 802.1x para el edificio ESEM de Maturín.

## ANÁLISIS DE LAS TECNOLOGÍAS

Durante esta fase se analizaron diferentes tecnologías existentes, referentes a los mecanismos de autenticación, protocolos de seguridad, cifrado de datos, mecanismos de autorización y servidor de autenticación, con el fin de seleccionar la alternativa, que mejor se adapte a las necesidades de la organización y a los requerimientos emitidos por el personal que labora en la Gerencia de Seguridad Lógica de PDVSA.

Para dar inicio a la selección de cada una de las alternativas, se aplicó la escala de evaluación suministrada por el personal de la Gerencia de Seguridad Lógica, tomando en cuenta el nivel de satisfacción, según las apreciaciones deficiente, regular, bueno y excelente y el uso de la escala numérica del uno (1) al ocho (8), tal como se muestra en la Tabla 1.

Tabla 1. Escala de evaluación.

| APRECIACIÓN | PUNTAJE |
|---|---|
| Deficiente | 1 al 2 |
| Regular | 3 al 4 |
| Bueno | 5 al 6 |
| Excelente | 7 al 8 |

La Gerencia de Seguridad Lógica estableció los criterios de evaluación y los valores ponderados que se tomaron en cuenta para escoger el mecanismo de autenticación, protocolo de autenticación, mecanismo de cifrado, el mecanismo de autorización y el servidor de autenticación, basándose en la experiencia que han adquirido en pasadas implementaciones realizadas en la plataforma tecnológica de PDVSA.

**Selección de un mecanismo de autenticación**

Los métodos de autenticación se presentan en función de las credenciales que utilizan los usuarios para la verificación de acceso a la red, actualmente en PDVSA se utiliza en gran manera la autenticación basada en usuario/contraseña para el inicio de sesión en las computadoras de los usuarios, así como también en el ingreso a aplicaciones especializadas propias de la corporación, por consiguiente PDVSA cuenta con una base de datos que contiene todos las credenciales de los usuarios registrados en el directorio activo de PDVSA. A continuación se describen los siguientes mecanismos:

Autenticación basada en usuario y contraseña

Este mecanismo se basa en autenticar al usuario con información que éste conoce, siendo ello un nombre de usuario (*loggin*) y contraseña (*password*) para el inicio de

sesión, con el fin de verificar las credenciales antes de poder disfrutar de los servicios que la red le ofrece.

Autenticación basada en certificados digitales

Este mecanismo consiste en que cada usuario posee una clave privada que se mantiene secreta y una pública que pasa a formar parte de un certificado digital. Dichos certificados son emitidos por una Autoridad Certificadora (CA: *Certification Authority*) quien comprueba la identidad de los usuarios. El certificado es emitido para ser almacenado en la computadora del usuario y es con este archivo que su propietario se identifica cuando realiza operaciones a través de la red.

Autenticación biométrica

Este mecanismo se refiere al uso de tecnologías para medir y analizar las características físicas y del comportamiento humano, con el fin de verificarlas con un patrón establecido y validar el proceso de autenticación en la red, en ocasiones se usa la información referente a huellas dactilares, voz, retina, entre otros.

A continuación se describen los criterios que fueron definidos por la Gerencia de Seguridad Lógica para seleccionar cada alternativa definida según la tecnología evaluada:

Facilidad de implementación: se refiere a la facilidad de ser instalado, administrado, configurado y usado de una manera eficaz.

Robustez: es la capacidad de reaccionar apropiadamente frente a condiciones excepcionales.

Independencia de hardware: se refiere a la capacidad de ser utilizado sin la necesidad de adquirir un nuevo hardware para su implementación.

Reutilización de recursos de red: se refiere a la capacidad de aprovechar los recursos de red existentes y usarlos para futuras implementaciones.

No requiere certificados en el cliente: consiste en no instalar certificados digitales en el equipo del cliente.

Escalabilidad: habilidad para adaptarse a las circunstancias cambiantes sin perder calidad.

Facilidad de mantenimiento: se refiere a la habilidad de administrar y mantener actualizado un software o hardware en forma progresiva.

Seguridad informática: es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida).

Capacidad de procesamiento menor: se refiere a la habilidad que tiene un hardware o software para manejar volúmenes de información sin afectar la calidad del servicio que presta.

Disponibilidad: consiste en garantizar el acceso a un servicio o a los recursos tantas veces el usuario autorizado lo requiera.

Cumplimiento del decreto 3390: consiste en la adopción de software libre desarrollado con estándares abiertos en la administración pública y en los servicios públicos.

Seguidamente el personal de la Gerencia de Seguridad Lógica, asignó un peso porcentual a cada uno de los criterios descritos anteriormente, con el fin de identificar la importancia que tienen dichos criterios para la plataforma tecnológica de PDVSA, tal como se muestra en la Tabla 2

Tabla 2. Matriz de ponderación de criterios del método de autenticación.

| **CRITERIOS** | **PONDERACIÒN** | |
|---|---|---|
| | PESO PORCENTUAL | PESO PONDERADO |
| Facilidad de Implementación | 25 | 0,25 |
| Robustez | 30 | 0,30 |
| Independencia de Hardware | 18 | 0,18 |
| Reutilización de recursos de red | 27 | 0,27 |
| Total | 100 | 1 |

Debido a la gran cantidad de información confidencial que maneja PDVSA entre sus procesos, gerencias y filiales; la Gerencia de Seguridad Lógica establece como criterio de mayor peso porcentual la robustez debido a que busca proteger dicha información de accesos indebidos, así como también se requiere establecer responsabilidades en caso de incidentes de seguridad ocurrido en la red.

La reutilización de recursos de red es el segundo criterio de mayor valor porcentual, debido a que PDVSA desea integrar todos los elementos que se encuentran en la plataforma tecnológica, con el fin de aprovechar cada recurso de la red, evitando

costos adicionales mediante la implementación de métodos de autenticación aislados al que existe actualmente.

La facilidad de implementación no es un criterio tan importante para PDVSA, debido a que ésta posee un recurso humano altamente capacitado, entrenado y dispuesto a desarrollar esta implementación, por consiguiente la Gerencia de Seguridad Lógica estableció un peso porcentual menor para esta implementación.

La independencia de hardware no representa un gran problema para PDVSA, debido a que ésta cuenta con los recursos necesarios para adquirir los equipos requeridos para implementar el método de autenticación, por esta razón la Gerencia de Seguridad Lógica estableció el valor porcentual menor para este criterio.
Seguidamente la Gerencia de Seguridad Lógica estableció para cada alternativa un valor según el grado de satisfacción usando la escala de evaluación descrita en la Tabla 1 y se multiplicó dicho valor por el peso ponderado mostrado en la Tabla 2, el cual nos arroja la calificación individual de cada alternativa y la suma de estas calificaciones da como resultado la calificación ponderada para cada método de autenticación, todos éstos cálculos son necesarios para analizar el método de autenticación que mejor se adapte a la plataforma de PDVSA. Los resultados del cálculo anteriormente expuesto se pueden detallar en el apéndice B.

La tabla que se muestra en el apéndice B indica que la opción que mejor se adapta a la plataforma de PDVSA es el método de autenticación basado en Usuario/Contraseña, debido a que cumple con la mayoría de los requerimientos definidos por la Gerencia de Seguridad Lógica, entre los cuales se encuentran la independencia de hardware y la reutilización de los recursos de red, siendo este último de gran importancia debido a que permite aprovechar la base de datos de las credenciales de los usuarios (usuarios/contraseñas) que se encuentra actualmente implementada en la corporación.

**Selección de un protocolo de autenticación**

En esta fase se realizó una elección del protocolo de autenticación, con el fin de seleccionar aquel que garantice las condiciones necesarias para que el intercambio de mensajes en la comunicación, se realice de forma íntegra y confidencial sin afectar significativamente el rendimiento del hardware disponible. A continuación se describen varias implementaciones del *Extensible Authentication Protocol* (EAP), que es utilizado en el estándar IEEE 802.1x.

EAP-TLS (*Transport Level Security*)

El método TLS utiliza para el procedimiento de autenticación un certificado de clave pública firmado por la misma autoridad de certificación para proporcionar un medio de autenticación mutua entre el cliente y el autenticador. Esta solución tiene fuertes propiedades de autenticación y es muy segura, pero requiere de una infraestructura de clave pública para su uso. EAP-TLS proporciona autenticación mutua, intercambio y establecimiento de claves.

EAP-TTLS o TLS tunelado

Es una extensión de EAP-TLS. En este método de EAP, se establece un túnel seguro entre el servidor y el cliente utilizando un algoritmo de clave pública y los certificados emitidos por una autoridad certificadora de confianza mutua. Una vez que este túnel esté establecido, otro método de autenticación se emplea y la transacción se realiza a través del túnel seguro. Debido a este túnel el método de autenticación interno puede ser menos seguro, como por ejemplo EAP-MD5. EAP-TTLS provee de beneficios de autenticación mutua, instrumentos para una negociación cifrada segura, capacidad para usar certificados y el uso de contraseñas, y mantenimiento de la identidad del usuario en privado, ya que cualquier contraseña de autenticación se producirá dentro del túnel.

EAP-PEAP

Este método tiene un comportamiento parecido a EAP-TTLS. Crea una sesión TLS para transportar otro método de autenticación. Una vez creado el túnel puede utilizarse otro método menos seguro dentro del mismo. La diferencia con EAP-TTLS consiste en que PEAP proporciona un medio de autenticación del autenticador al cliente, pero no en la otra dirección. Esto reduce complejidad y costes. PEAP incluye autenticación y encriptación de mensajes, intercambio seguro de claves.

LEAP (*Lightweight Extensible Authentication Protocol*)

Un nombre de usuario y contraseña se envía a un servidor de autenticación (RADIUS) para la autenticación. LEAP es un protocolo propietario desarrollado por Cisco, y no es considerado seguro.

EAP-FAST (*Flexible Authentication via Secure Tunneling*)

El protocolo fue diseñado para abordar las debilidades de LEAP, preservando el "ligero" de aplicación. El uso de los certificados de servidor es opcional en EAP-FAST. EAP-FAST utiliza una credencial de acceso protegido (PAC) para establecer un túnel de TLS en el que se verifican las credenciales del cliente.

La Gerencia de Seguridad Lógica estableció valores porcentuales a los criterios: facilidad de implementación, robustez, independencia de hardware, no requiere certificados en el cliente y escalabilidad, tomando en cuenta la importancia que posee cada uno para la plataforma de PDVSA. En la Tabla 3 se muestra la matriz de ponderación de criterios definida para el protocolo de autenticación.

Tabla 3. Matriz de ponderación de criterios del protocolo de autenticación.

| | **PONDERACIÒN** |
|---|---|

| **CRITERIOS** | PESO PORCENTUAL | PESO PONDERADO |
|---|---|---|
| Facilidad de Implementación | 15 | 0,15 |
| Robustez | 30 | 0,30 |
| Independencia de Hardware | 12 | 0,12 |
| Escalabilidad | 24 | 0,24 |
| No requiere certificados en el cliente | 19 | 0,19 |
| Total | 100 | 1 |

Debido a que PDVSA maneja gran cantidad de información confidencial, la Gerencia de Seguridad Lógica establece el mayor valor porcentual a la robustez, con el fin de proteger las credenciales de los usuarios que son autenticados en la red de la corporación, evitando que éstas puedan ser capturadas fácilmente.

En la plataforma tecnológica de PDVSA se implementan cambios y mejoras continuas a los servicios de red, por consiguiente la Gerencia de Seguridad Lógica estableció el segundo mayor valor porcentual al criterio escalabilidad con el fin de implementar un método EAP que se adapte al crecimiento y a las mejoras tecnológicas que se presentan en la red de la corporación, manteniendo la calidad del servicio.

La Gerencia de Seguridad Lógica estableció un mayor valor porcentual al criterio no requiere certificados en el cliente, debido a que PDVSA no cuenta con una infraestructura de claves públicas, y la implementación de ésta requerirá de costos adicionales en cuanto a recurso humano, tiempo y adquisición de equipos de hardware, por consiguiente no es de gran importancia la gestión de certificados digitales en los clientes para la implementación de un método EAP.

La facilidad de implementación es un criterio de menor valor porcentual debido a que PDVSA cuenta con personal altamente capacitado y entrenado en el área de telecomunicaciones lo que permitiría la implementación del método EAP en la arquitectura de seguridad.

Debido a que la plataforma tecnológica de PDVSA cuenta con equipos de red de diferentes marcas comerciales, la Gerencia de Seguridad Lógica estableció un menor valor porcentual al criterio independencia de hardware, con el fin de requerir un método EAP que pueda ser instalado y configurado en la mayoría de los equipos de red que existen actualmente en la corporación, evitando costos adicionales mediantela adquisición de nuevos equipos de red.

En el apéndice C, se muestra el resultado de la matriz de evaluación de los protocolo de autenticación estudiados usando el método de suma ponderada.

En el resultado que se muestra en el apéndice C se puede apreciar que es necesario el uso de un protocolo de autenticación que permita la reutilización de componentes de software o hardware presentes en la plataforma de PDVSA y que garantice una comunicación íntegra, haciendo uso de mecanismos de encriptación de mensajes e intercambio seguro de claves. El método de autenticación del protocolo EAP que mejor se ajusta a los requerimientos de esta implementación es el EAP-PEAP, debido a que proporciona seguridad adicional usando el método EAP-MSCHAPv2, el cual puede operar a través del canal cifrado de TLS que proporciona PEAP. En el mismo sentido este método se encuentra integrado en el software para el cliente 802.1x del sistema operativo WindowsXp, siendo éste el sistema operativo que se encuentra implementado en la plataforma tecnológica de PDVSA para las estaciones de trabajo de sus empleados, ofreciendo la facilidad de implementación y la reutilización de componentes debido a que no es necesario realizar alguna instalación adicional de software para usar un cliente 802.1x.

**Selección de un mecanismo de cifrado**

Un factor importante que influye en la seguridad de las redes, es la necesidad de encriptar el contenido de los datos que se transfieren a través de la red, con el fin de que no puedan ser descifrados rápidamente. A continuación se muestra una lista de mecanismos de cifrado que se tomaron en cuenta en esta investigación:

WEP (*Wired Equivalent Privacy*)

Es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11, los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN, utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

WPA (*Wi-Fi Protected Access*)

Es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. El proceso de encriptación de WPA utiliza el protocolo TKIP (Temporal Key Integrity Protocol) y a su vez usa el algoritmo RC4. WPA genera automáticamente nuevas llaves de encriptación únicas para cada uno de los clientes, lo que evita que la misma clave se utilice durante semanas, meses o incluso años, como pasaba con WEP Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de

inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA2 (acceso protegido Wi-Fi 2)

Se basa en la norma IEEE 802.11i y utiliza el protocolo CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), un mecanismo de cifrado que emplea el estándar de cifrado avanzado (AES). Dicho sistema garantiza el nivel de confidencialidad de los datos que demandan muchas instituciones financieras y gubernamentales. El WPA2/802.11i dispone de códigos más actualizados y es compatible con la transmisión de voz en redes inalámbricas, ya que evita el retraso de la señal y los cortes en la conversación en estado de itinerancia, basándose en la autenticación IEEE 802.1x con el Protocolo EAP.

Para PDVSA la capacidad de procesamiento menor, reutilización de recursos de red y robustez, son criterios de gran importancia para la implementación de un mecanismo de cifrado, por tal motivo la Gerencia de Seguridad Lógica estableció diferentes valores porcentuales a cada criterio, con el fin de enmarcar la importancia que tienen cada uno de éstos en la plataforma tecnológica de la corporación.

En la Tabla 4 se muestra la matriz de ponderación de criterios definida para el mecanismo de cifrado.

Tabla 4. Matriz de ponderación de criterios del mecanismo de cifrado.

| **CRITERIOS** | **PONDERACIÒN** | |
|---|---|---|
| | PESO PORCENTUAL | PESO PONDERADO |
| Capacidad de procesamiento menor | 21 | 0,21 |

| | | |
|---|---|---|
| Reutilización de recursos de red | 35 | 0,35 |
| Robustez | 44 | 0,44 |
| Total | 100 | 1 |

La Gerencia de Seguridad Lógica le asignó el mayor valor porcentual a la reutilización de recursos de red, debido que fue necesario integrar e incorporar los mecanismos de cifrados en cada uno de los dispositivos de redes que existen actualmente en la plataforma de la corporación.

Para la Gerencia de Seguridad Lógica es de suma importancia implementar un mecanismo de cifrado que utilice algoritmos robustos y difíciles de romper, con el fin de proteger toda la información que viaja a través de la red de la corporación, asegurando la confidencialidad de la información.

La complejidad de los algoritmos que se utilizan en los mecanismos de cifrado, afecta la capacidad de procesamiento en los equipos de red, por consiguiente la Gerencia de Seguridad Lógica desea implementar un mecanismo de cifrado que degrade en lo menos posible la capacidad de procesamiento de los equipos de red que existen en la plataforma de PDVSA.

La selección del mecanismo de cifrado se realizó mediante el método de la suma ponderada, estableciendo valores para cada mecanismo de cifrado, según la importancia que tienen cada uno de los criterios definidos por el personal de la Gerencia de Seguridad Lógica dentro de la plataforma de PDVSA y realizando cálculos matemáticos que permitieron facilitar el análisis de los resultados obtenidos. En el apéndice D, se muestra la matriz de evaluación de los mecanismos de cifrado estudiados.

Para PDVSA es de gran importancia proteger la información que viaja a través de la red, por tal motivo la Gerencia de Seguridad Lógica, requiere implementar mecanismos de cifrado que sean difíciles de romper y que permitan asegurar la integridad y confidencialidad de la información, incorporando dichos mecanismos en la configuración de los equipos de red que existen actualmente en la corporación, con el fin de no requerir mayor inversión de capital a corto plazo para el suministro de nuevos dispositivos y/o inversión de tiempo para realizar actualizaciones de firmware. En tal sentido se puede observar en el apéndice D, que el mecanismo de cifrado de datos que mejor se adapta a las necesidades de la organización es el WPA.

**Selección de un mecanismo de autorización**

El proceso de autorización se refiere a la concesión de privilegios específicos a un usuario basándose en su identidad previamente usada en el proceso de autenticación, los privilegios que solicita y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, la localidad donde se encuentre el usuario, la prohibición de realizar *login*s simultáneos, entre otras.

A continuación se describen tres elementos que pueden participar en el proceso de autorización basados en el estándar IEEE 802.1x

Base de datos

Una de las formas de proporcionar autorización es por medio de una base de datos que contenga los permisos de cada usuario, permitiendo que una vez autenticados, se verifique a que recursos de la red pueda acceder. Una base de datos está compuesta por una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

Archivos de texto plano

El mecanismo de autorización puede ser empleado usando archivos de texto plano, los cuales están compuestos únicamente por texto sin formato, es decir de sólo caracteres, que se pueden codificar de distintos modos dependiendo de la lengua usada. Algunos de los sistemas de codificación más usados son ASCII, ISO-8859-1 o latín-1, unicode entre otros, este mecanismo de autorización es usado normalmente en sistemas pequeños que no contengan gran cantidad de usuarios.

Directorio activo

El directorio activo es un mecanismo de autorización implementado por Microsoft como servicio de directorio *Lightweight Directory Access Protocol* (LDAP) para ser utilizado en entornos *Windows*, este permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un directorio activo almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios activos con cientos de objetos para una red pequeña hasta directorios activos con millones de objetos, proporcionando información sobre los objetos, los organiza, controla el acceso y establece la seguridad.

El cumplimiento del decreto 3390, la escalabilidad, disponibilidad y reutilización de recursos de red, son criterios de gran importancia para PDVSA durante la selección de un mecanismo de autorización; por tal motivo la Gerencia de Seguridad Lógica estableció diferentes valores porcentuales a cada uno de los criterios mencionados, con la finalidad de priorizar e identificar la importancia que tienen cada uno de los criterios para la plataforma tecnológica de la corporación. En la Tabla 5 se muestra la matriz de ponderación de criterios definida para el mecanismo de autorización.

La Gerencia de Seguridad Lógica considera de suma importancia el criterio reutilización de los recursos de red para el desarrollo de esta implementación, debido a que se requiere aprovechar cada uno de los elementos que se encuentran en la red, con el fin de integrar todos los servicios que se prestan en la plataforma de la corporación.

Tabla 5. Matriz de ponderación de criterios del mecanismo de autorización.

| **CRITERIOS** | **PONDERACIÒN** | |
|---|---|---|
| | PESO PORCENTUAL | PESO PONDERADO |
| Cumplimiento del decreto 3390 | 15 | 0,15 |
| Escalabilidad | 18 | 0,18 |
| Disponibilidad | 27 | 0,27 |
| Reutilización de recursos de red | 40 | 0,40 |
| Total | 100 | 1 |

La Gerencia de Seguridad Lógica es la encargada de garantizar la integridad, confiabilidad y disponibilidad de la información en la red de PDVSA, por consiguiente se le asignó el segundo mayor valor porcentual al criterio disponibilidad, debido a que se requiere que los mecanismos de autorización, mantengan la información accesible para los usuarios autorizados tantas veces sea necesario.

La plataforma de PDVSA se encuentra en continuo crecimiento, debido a la incorporación de nuevas tecnologías que permiten optimizar los servicios que se prestan a los usuarios de la red, por tal motivo la Gerencia de Seguridad Lógica requiere un mecanismo de autorización que se adapte fácilmente al crecimiento y a los avances tecnológicos dentro de la corporación.

Con el fin de seguir las políticas del Gobierno venezolano en materia de soberanía tecnológica, PDVSA se ha propuesto cumplir progresivamente con el decreto 3390, mediante la adopción del software libre en la plataforma de la corporación.

Los resultados mostrados en el apéndice E demuestran que la utilización del directorio activo en la plataforma tecnológica de PDVSA, le proporciona muchas bondades que lo colocan por encima de las otras opciones, entre los cuales se encuentran la escalabilidad y la reutilización de recursos de red, los cuales son criterios que juega un papel fundamental en esta selección.

**Selección de un servidor de autenticación**

Existen multitud de servidores AAA en la actualidad que pueden ser utilizados para llevar a cabo la autenticación de los usuarios, la verificación de sus credenciales y la trazabilidad de sus conexiones en la red de la Corporación, es por ello que en esta fase se describen algunos servidores de autenticación AAA, tomando en cuenta los requisitos suministrados por el personal de Seguridad Lógica con la finalidad de seleccionar el que mejor se adapte a las necesidades de la organización.

FreeRADIUS

Es uno de los servidores RADIUS más populares y versátiles. RADIUS es uno de los protocolos más ampliamente utilizados para realizar la gestión del acceso a redes de área extensa, sobre todo en el ámbito de los ISP (*Internet Service Providers*). Podríamos decir que FreeRADIUS es un producto compuesto tanto por una base de datos de usuarios como por un servidor capaz de atender peticiones de autenticación realizadas por otros elementos de nuestra red. Como indica su nombre, se trata de un producto de código abierto con soporte para gran cantidad de plataformas.

Cisco Secure

Es una plataforma de control de acceso propietaria de Cisco, que le ayuda a cumplir con las políticas y permite gestionar de forma centralizada el acceso a recursos de red para una variedad de dispositivos y grupos de usuarios. Tras confirmar la identidad de un usuario o dispositivo, así como el cumplimiento de las políticas de seguridad de la empresa, puede habilitarse el acceso a determinados recursos o partes de la red. La solución de identidad y confianza de Cisco, denominada ACS, incluye el protocolo de autenticación 802.1x y funciones AAA en los *switch* y *router* de Cisco, tiene la flexibilidad de proporcionar un elevado nivel de derechos de acceso y de crear zonas de cuarentena para los puntos terminales que presenten una no conformidad, además de la posibilidad de bloquear completamente todo acceso no autorizado.

IAS (*Internet Authentication Service*)

Es la implementación de Microsoft de un servidor RADIUS, IAS emplea la autenticación, autorización y seguimiento centralizado de la conexión para varios tipos de acceso a la red, como pueden ser accesos inalámbricos y conexiones por Red Privada Virtual (VPN). El IAS, también cumple funciones de proxy RADIUS, el cual propaga los mensajes de autenticación y seguimiento a otros servidores RADIUS.

Los criterios que la Gerencia de Seguridad Lógica tomó en cuenta para seleccionar el servidor de autenticación fueron: reutilización de recursos de red, disponibilidad, el cumplimiento del decreto 3390, seguridad y capacidad administrativa, siendo éstos dos últimos factores de gran importancia en la implementación del servidor de autenticación, por tal motivo se les asignó un peso porcentual diferente a cada criterio, con el fin de identificar la importancia que tiene cada uno para la plataforma de PDVSA. En la Tabla 6 se muestra la matriz de ponderación de criterios para el servidor de autenticación.

Tabla 6. Matriz de ponderación de criterios del servidor de autenticación.

| CRITERIOS | PONDERACIÒN | |
|---|---|---|
| | PESO PORCENTUAL | PESO PONDERADO |
| Seguridad | 19 | 0,19 |
| Reutilización de recursos de red | 30 | 0,30 |
| Disponibilidad | 22 | 0,22 |
| Facilidad de mantenimiento | 13 | 0,13 |
| Cumplimiento del decreto 3390 | 16 | 0,16 |
| Total | 100 | 1 |

Para PDVSA es de gran importancia implementar un servidor de autenticación que permita ser actualizado progresivamente de forma eficaz y a su vez permita cumplir con la protección de la infraestructura computacional incluyendo la información que viaja a través de la red, por consiguiente la seguridad y la facilidad de mantenimiento.

Actualmente PDVSA cuenta con servidores en entorno Windows y Linux en su plataforma tecnológica, sin embargo la versión de los sistemas operativos Windows no son compatibles con el servidor RADIUS de Microsoft (IAS), mientras que la versión de los sistemas operativos Linux cuentan con el servidor de autenticación FreeRADIUS que además de ser software libre puede ser administrado de una forma eficaz, haciendo uso de los recursos existentes en la red.

Mediante el uso del método de la suma ponderada que se aplicó en el apéndice F, se evidencia que la seguridad, reutilización de recursos de red, disponibilidad y el cumplimiento del decreto 3390, son los criterios de mayor importancia para la Gerencia de Seguridad Lógica y los cuales se ven reflejados en las características que posee el servidor FreeRADIUS, siendo éste el que mejor se adapta a los

requerimientos de la plataforma de PDVSA, suministrado por la Gerencia de Seguridad Lógica.

## DISEÑO DE LA ARQUITECTURA DE CONTROL DE ACCESO

Luego de haber culminado el análisis de las fases anteriores, donde se estableció el mecanismo autenticación, autorización, protocolo EAP, métodos de cifrado y el servidor de autenticación a usar, se procedió a diseñar la arquitectura de control de acceso, que fue implementada en el edificio ESEM de la Ciudad de Maturín, el cual cuenta con cinco (5) puntos de acceso inalámbricos y tres (3) *switch*, que permiten conectar a la red de PDVSA, sesenta (60) usuarios aproximadamente. Este diseño cuenta con la interacción de siete (7) elementos que participan en la arquitectura de control de acceso basada en el estándar de seguridad IEEE 802.1X, los cuales son: personal externo, autenticador, servidor de autenticación, directorio activo, base de datos, aplicación Web y el personal de Seguridad Lógica.

En el mismo sentido esta arquitectura se apoya con la utilización del directorio activo de PDVSA para verificar si las credenciales suministradas por los usuarios son válidas, de igual forma, cuenta con una base de datos donde se almacenan todas las conexiones exitosas o fallidas por un usuario, además de contar con una aplicación Web que permite gestionar de forma sencilla el proceso de *accounting* o trazabilidad de las conexiones de los usuarios que se conectan a la red de la corporación, todo ello se reflejo en un diagrama, que se muestra en el apéndice G.

En el apéndice H, se muestra un diagrama de secuencia de UML, donde se explica la comunicación existente entre las entidades que participan en la arquitectura implementada.

La secuencia del procedimiento por el cual un usuario se conecta a la red *Ethernet* de PDVSA, se describe de la siguiente manera:

1. Un usuario se conecta a través de un cable de red o vía inalámbrica en un punto de red, inicia una sesión y envía sus credenciales (usuario y contraseña).
2. El servidor de autenticación (FreeRADIUS) valida los datos enviados por el punto de acceso a través de una búsqueda en la base de datos del directorio activo, con el fin de brindarle acceso a la red, o en caso contrario, impide su acceso y le envía un mensaje de falla de autenticación.
3. El servidor de autenticación recibe la solicitud por parte del autenticador, verifica que se encuentre registrado como un NAS (*Network Access Server*) autorizado para brindar accesos a la red (mediante una llave compartida entre el autenticador y el servidor FreeRADIUS) y de ser estos correctos, inicia una sesión con el servidor de directorio de usuarios, para enviarle los datos correspondientes al usuario y éste le indique si son correctos de acuerdo a sus registros.
4. El servidor de directorio de usuarios revisa si es que se encuentra registrado el usuario en su sistema y de ser así, procede a verificar si la contraseña ingresada es correcta. En caso que el usuario no se encuentre registrado, envía un mensaje de *Access-Rejected* (acceso rechazado). De ser correcto, devuelve un mensaje de *Access-Accepted* (acceso aceptado); por medio del cual se concede el acceso al usuario.
5. El servidor de autenticación recibe la autorización por parte del servidor de directorio de usuarios y envía un mensaje al autenticador para que le brinde acceso a la red al usuario.
6. El autenticador recibe la autorización para el usuario o cliente e inicia una sesión WPA de intercambio dinámico de llaves, por medio del cual se procederá a utilizar el algoritmo TKIP para cifrar la comunicación de datos entre el cliente y el autenticador.
7. Al momento de recibir la autorización, el autenticador inicia a registrar todas las

actividades de tráfico del usuario y las envía al servidor de base de datos PostgreSQL. En este servidor se registra el momento exacto en el que el usuario inicia su acceso a la red y se registrará el tiempo que estuvo conectado, el momento en el que se desconecta, así como otras estadísticas (número de bytes enviados, número de bytes recibidos, entre otros).

8. Una vez que el usuario cuenta con acceso a la red, iniciará una sesión DHCP para obtener dinámicamente una dirección IP por parte del servidor DHCP y así con estos datos poder utilizar los servicios que le ofrece la red *Ethernet* de PDVSA.

## EJECUCIÓN DEL DISEÑO

Para llevar a cabo la ejecución del diseño de la arquitectura de seguridad basada en el estándar IEEE 802.1X, se contó con el apoyo del personal que labora en el Departamento de Servidores, quienes fueron los responsables de la instalación del sistema operativo GNU/Linux Debian Lenny, en el equipo donde se implementó la aplicación FreeRADIUS, de igual forma se contó con el personal de Redes para obtener el diagrama de conexión de la red *Ethernet* del edificio ESEM de la ciudad de Maturín y el direccionamiento IP de la misma, así como también el acceso a los *switch* y *accesss point*, mediante la creación de un usuario con privilegio para iniciar con la configuración del mismo usando el protocolo 802.1x.

El edificio ESEM cuenta con un centro de computo en condiciones óptimas para que el servidor de autenticación FreeRADIUS trabaje de forma adecuada, además de contar con cuartos de cableados necesarios para la instalación de *switch* y *access point*, con el fin de asegurar el buen funcionamiento de la red y ofrecer mayor seguridad mediante la implementación del estándar IEEE 802.1X, para ello se procedió a ejecutar las siguientes actividades

**Instalación del servidor de autenticación**

Para la instalación de FreeRADIUS en su última versión se 2.1.8, se procedió a realizar los siguientes pasos: primeramente, se agregó el repositorio de *backports* de Debian Lenny tal como sigue a continuación:

En la consola como root editamos el archivo sources.list ubicado en la ruta: /etc/apt, agregamos la línea deb http://www.backports.org/debian lenny-backports main contrib non-free, luego se obtiene la llave, con la siguiente instrucción: apt-get install debian-backports-keyring, y por último se ejecuta la instrucción apt-get update para actualizar los repositorios donde se encuentra el servidor de autenticación.

Luego de esto se procedió a instalar FreeRADIUS con la siguiente instrucción:
apt-get -t lenny-backports install "freeradius"; en el mismo sentido se instalaron los paquetes de FreeRADIUS para postgresql, el cual permite establecer una compatibilidad con la base de datos para realizar el *accounting* y llevar la trazabilidad de las conexiones realizadas por los usuarios, así mismo se instaló el módulo de FreeRADIUS para krb5, esto es para que freeRADIUS pueda realizar la autenticación mediante el directorio activo usando ntlm, el cual es el protocolo de autenticación para equipos que no forman parte de un dominio, como los servidores independientes y los grupos de trabajo, luego de ello se instaló el módulo para FreeRADIUS para dbg, el cual permite establecer los símbolos de depuración del servidor FreeRADIUS y por último se instaló el módulo de FreeRADIUS para iodbc, debido a que el servidor FreeRADIIUS puede usar iODBC para acceder a la base de datos para autenticar usuarios y realizar el *accounting*, todo ello se instaló mediante las instrucciones: apt-get -t lenny-backports install freeradius-postgresql freeradius-krb5, apt-get -t lenny-backports install freeradius-dbg freeradius-iodbc

Una vez instalado el software de FreeRADIUS, se procedió a ejecutar el servicio en modo *debug* con la instrucción radiusd -X, con el fin de verificar si existen errores al iniciar el servicio, cuando la salida del comando radiusd -.X muestra las siguientes líneas, indica que el servicio se inicio correctamente:

Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /var/run/freeradius/freeradius.sock
Listening on proxy address * port 1814
Ready to process requests.

**Configuración del servidor de autenticación**

Antes de iniciar con la configuración de los archivos que conforman la estructura del servidor FreeRADIUS, se unió al servidor FreeRADIUS al dominio de PDVSA, instalando los paquetes Samba, krb5-users, krb5-config, winbind y ntpdate: apt-get install samba samba-client winbind krb5-users krb5-config ntpdate

El paquete Samba proporciona servicios de compartición de ficheros e impresión a clientes en entorno de red Windows a clientes Linux. Samba puede configurarse también como sustituto del Controlador de Dominios de Windows NT 4.0.
El paquete
Luego de la instalación se procedió a realizar la configuración del archivo de configuración de Samba smb.conf, modificando los parámetros necesarios para su correcto funcionamiento. El archivo de configuración smb.conf se muestra en el apéndice I.
Luego se editó el archivo de configuración nsswitch, ubicado en la ruta: /etc/nsswitch.conf, modificando algunos parámetros. Este archivo contiene la configuración de las bases de datos del sistema y del sistema de conmutación de los

servicios de nombres. El archivo de configuración final de nsswitch.conf se encuentra en el apéndice J.

Finalmente se reinician los servicios de samba y winbind, mediante la instrucción: /etc/init.d/samba restart y /etc/init.d/winbind restart

Luego antes de unir el servidor de autenticación al dominio se sincronizó la hora con el controlador de dominio, ejecutando la instrucción: ntpdate -s plcgua95.pdvsa.com

Una vez realizado esto, se procedió con la configuración del archivo krb5.conf, su ubicación en el servidor FreeRADIUS está en la ruta: /etc/krb5.conf. La configuración final del archivo krb5.conf se encuentra en el apéndice K. Continuando con la conexión con el directorio activo mediante la instrucción:

- kinit administradordelAD@PDVSA.COM
- net ads join -U administradordelAD -S plcgua95.PDVSA.COM

Verificamos si un usuario se puede autenticar contra el directorio activo, usando el comando: wbinfo -a indicador%contraseña, al ejecutar la instrucción anterior, el resultado es el siguiente:
plaintext password authentication failed
error code was NT_STATUS_NO_SUCH_USER (0xc0000064)
error messsage was: No such user
Could not authenticate user tuindicador%tucontraseña with plaintext password
challenge/response password authentication succeede
Este error es absolutamente normal, ya que las credenciales no son enviadas al directorio activo en texto plano. Sin embargo lo importante es lo siguiente: challenge/response password authentication suceded. Luego de esto, se verificó que se pudiese obtener información del directorio activo con los siguientes comandos:

- wbinfo –m: lista de dominios de confianza por el servidor.
- wbinfo –g: muestra la información de los Grupos que se encuentran en el directorio activo.
- wbinfo –D: muestra la información que se tiene acerca del dominio.

Una vez, finalizado los pasos anteriores, se procedió a configurar los archivos del servidor FreeRADIUS radiusd.conf, eap.conf, clients.conf, mschap y default, tal como.se describe a continuación:

Configuración del archivo radiusd.conf

En el archivo radiusd.conf se encuentra el cuerpo principal de la configuración del servidor FreeRADIUS, donde se especifican algunos parámetros que permiten el buen funcionamiento del servidor; se modificó las variables *user* y *group* por la cuenta en la que corre el servidor FreeRADIUS.

user = freerad

group = freerad

A través del módulo exec ntlm_auth, se especifica al servidor FreeRADIUS que realice la autenticación contra el directorio activo, utilizando la variable ntlm_auth, basado en nombre de usuario y contraseña pertenecientes al dominio PDVSA2000. En el apéndice L se muestra la configuración final del archivo radiusd.conf.

Generación de certificados para el servidor de autenticación

Para la generación de certificados se procedió a instalar el paquete openssl de los repositorios oficiales de GNU/Linux Debian Lenny y se ejecutó el *script bootstrap.sh* que se encuentra en la carpeta certs del servidor FreeRADIUS. De igual forma para la generación de los certificados, es necesario contar con el archivo xpextensions, el

cual contiene información clave de los certificados para plataforma *windows*, dicho archivo se muestra en el anexo 1.

Al ejecutar el *script* bootstrap.sh, se crean los certificados ca.der, ca.key, ca.pem, server.p12, server.pem, los cuales se muestran en el anexo 2 , anexo 3, anexo 4, anexo 5 y anexo 6 respectivamente.

Las siguientes variables se modificaron en los archivos ca.cnf y server.cnf, con el fin de generar certificados, con información referente a PDVSA.

- input_password y output_password: es aquí, donde se especifica la contraseña del certificado de la entidad certificadora, el cual también es usada en el archivo eap.conf del servidor FreeRADIUS.
- countryName: se coloca las iníciales del país donde se originará el certificado.
- StateOrProvinceName: se coloca el nombre de la ciudad.
- LocalityName: se coloca el nombre de la localidad
- OrganizationName: se indica el nombre de la organización que usará el certificado.
- EmailAddress: se coloca la dirección de correo electrónico del administrador del servidor FreeRADIUS
- commonName: se coloca el nombre del certificado.

En el apéndice M se muestra la configuración final del archivo ca.cnf correspondiente a la entidad certificadora generada para el servidor de autenticación FreeRADIUS.

Configuración del archivo eap.conf

En el archivo eap.conf se especifica el protocolo de autenticación y método que se eligió en la fase selección de tecnologías, siendo éstos el protocolo PEAP y el método Mschapv2; a continuación se describen los parámetros que se modificaron:

En la sección eap se modificó el parámetro default_eap_type con el valor peap, (default_eap_type = peap) el cual es protocolo EAP seleccionado, en el mismo sentido, en la sección tls se modificó el parámetro private_key_password con el valor administrador (private_key_password = administrador), siendo este la clave usada en la generación de los certificados para el servidor.

En la sección peap se modificó los parámetros default_eap_type con el valor mschapv2 (default_eap_type = mschapv2) y copy_request_to_tunnel con el valor *yes* (copy_request_to_tunnel = yes) el cual indica que si algún atributo no están dentro de la solicitud del túnel pero está disponible fuera del túnel, este es copiado dentro del túnel, otro parámetro que se modificó fue use_tunneled_reply.con el valor *yes* (use_tunneled_reply = *yes*) indicando que la respuesta emitida por el autenticador basados en el nombre del usuario serán enviados dentro del túnel.

En el apéndice N, se muestra la configuración final del archivo eap.conf, y en el apéndice O, se encuentra el archivo de configuración mschap.conf, el cual contiene las especificaciones del método EAP que se usó

Configuración del archivo clients.conf

Este archivo contiene la descripción y las credenciales de los diferentes autenticadores que consultan al RADIUS (*access point, switch*, entre otros). Agregando la dirección IP de los autenticadores, el secret que es la clave compartida entre cada autenticador (secret = administrador) y el servidor FreeRADIUS. En el apéndice P se muestra, la configuración final del archivo clients.conf.

Configuración del archivo default

El archivo default se encuentra en la ruta /etc/freeradius/sites-enabled, el cual contiene información referente a los métodos usados en la sección de autorización, autenticación y *accounting*, y este es reflejado en el apéndice Q

Configuración del archivo sql.conf

Este archivo de configuración contiene las especificaciones necesarias para conectar la base de datos de postgresql con el servidor FreeRADIUS, con el fin de almacenar todos los datos necesarios para la realización del *accounting*, para esto se modificó los parámetros driver cuyo valor es "rlm_sql_${database}", siendo ${database} una variable definida anterioremente con el valor database = "postgresql", indicando que el manejador de base de datos es postgresql, en el parámetro server colocamos la dirección IP del servidor FreeRADIUS (server = "10.172.25.84"), también especificamos el nombre del usuario (login = "seguridad") y la contraseña (password = "adminsegaitplc") con que se conecta la base de datos y el parámetro radius_db (radius_db = "plc"), donde le indicamos el nombre de la base de datos para realizar el *accounting*. En el apéndice R, se encuentra reflejado el archivo final de la configuración de sql.conf.

**Configuración de los autenticadotes**

En la implementación del estándar 802.1x del edificio ESEM, se utilizaron *switch* y *access point* para redes cableadas e inalámbricas respectivamente, los cuales se configuraron de la siguiente manera:

Configuración del *switch*

Para la implementación del estándar IEEE 802.1x en el edificio ESEM, se usaron 3 *switch* cisco 3750, cuya configuración es la siguiente:

enable aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius-server host 10.172.25.84 auth-port 1812
acct-port 1813 timeout 3
radius server retransmit 3
radius server key <mysharedsecret>
configure terminal
interface FastEthernet1/0/12
switchport mode access
dot1x port-control auto
end

Configuración del *access point*

Los *access point* que se usaron para las redes inalámbricas ubicadas en el edificio ESEM, fueron marca Cisco modelo aironet 1100. Éstos se configuraron mediante una interfaz gráfica, usando http. En el apéndice N, se muestran las ventanas que se accedieron para la configuración de los mismos.

**Configuración de los suplicantes**

Las plataformas que se usaron durante la implementación del estándar IEEE 802.1x fueron *windows* y Linux, para ello se realizaron las siguientes configuraciones.

Configuración del suplicante WindowsXp para redes inalámbricas y cableadas

En el menú Inicio, Mis sitios de Red luego en el panel ubicado en el lado izquierdo de la ventana y hacer clic en Ver conexiones de Red, se ubicó el icono de Conexiones de Redes Inalámbricas, se realizó clic derecho sobre este, se seleccionó Propiedades y apareció la siguiente ventana:

Se verificó que la Red se encontraba registrada en la lista de Redes preferidas, tal como se muestra en la figura 10, de lo contrario se accedió al botón Agregar, luego se indicó el nombre de la red inalámbrica (SSID), la autenticación de red y el cifrado de datos, como se muestra en la figura 11.

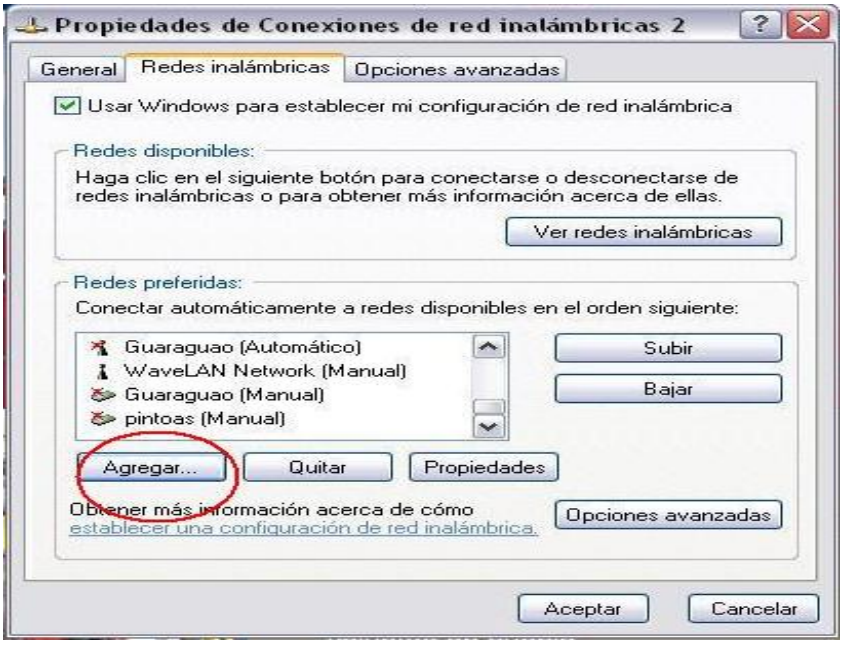



Figura 10. Propiedades de conexión de red.

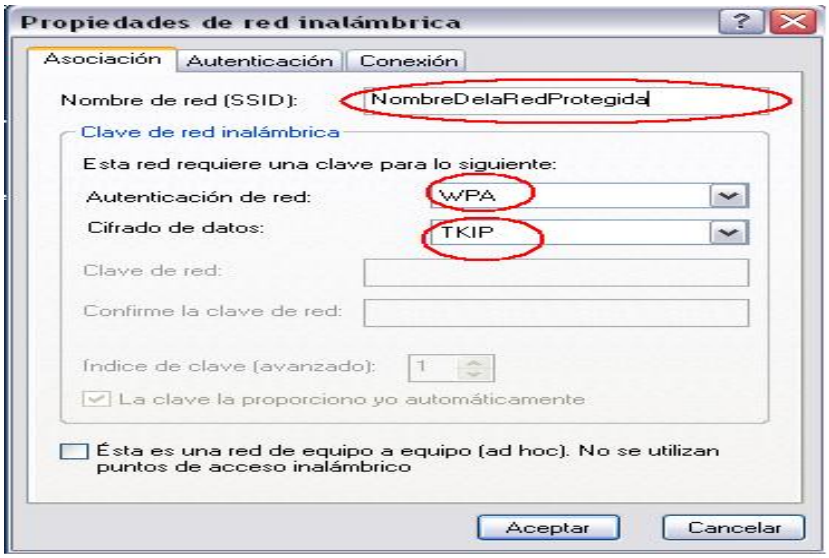



Figura 11. Propiedades de conexión de red con WPA y TKIP

Luego en la siguiente pestaña denominada Autenticación, se seleccionó el tipo de EAP el método PEAP y se habilitó el check que indicá que se autenticará al usuario, cuando la información del equipo esté disponible, tal como se muestra en la Figura 12.

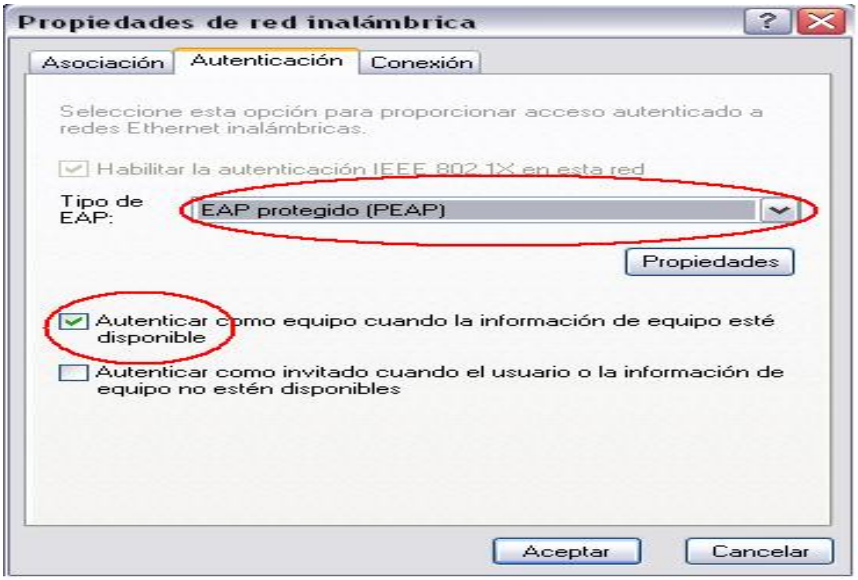


Figura 12. Propiedades de conexión de red con EAP Protegido (PEAP).

Una vez configurada la red inalámbrica protegida por 802.1X, se procedió a visualizar todas las redes inalámbricas disponibles, accediendo mediante el botón ver redes inalámbricas, como se muestra en la Figura 13.

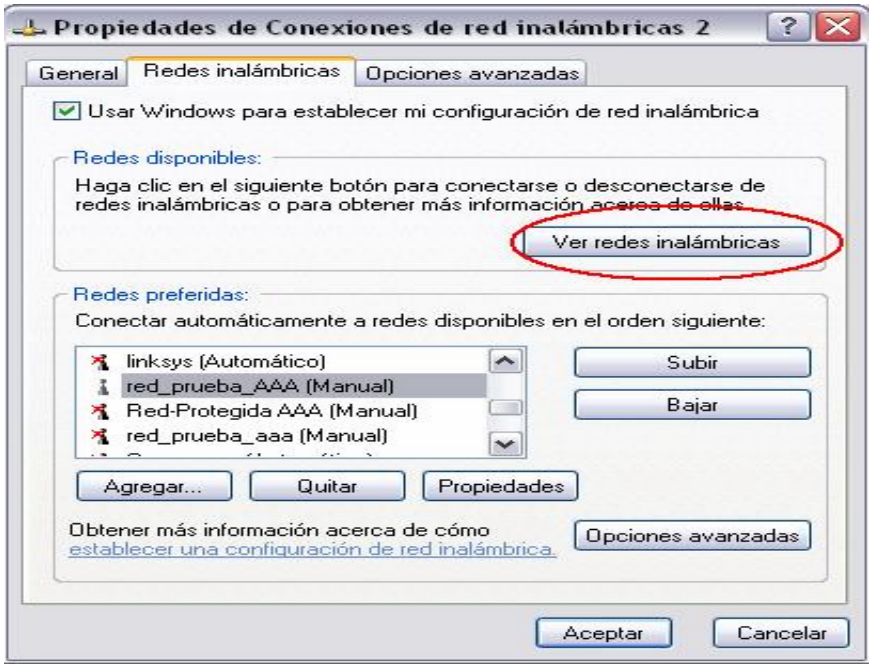



Figura 13. Ver redes inalámbricas disponibles.

Apareciendo la imagen reflejada en la figura 14, donde se procedió a seleccionar la red inalámbrica configurada, mediante el botón conectar.

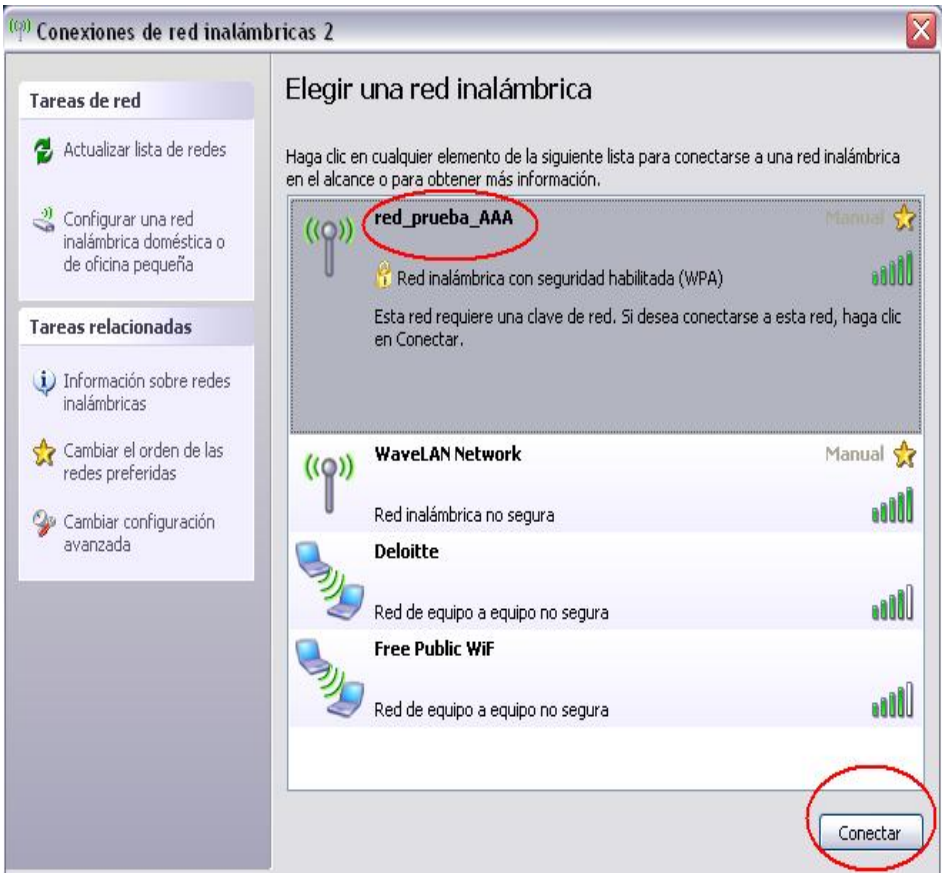



Figura 14. Listado de redes inalámbricas disponibles.

Configuración de los suplicantes Linux

La configuración del suplicante de Linux, consistió en la instalación del paquete wpa_supplicant, desde los repositorios oficiales de GNU/Linux Debian Lenny, mediante el comando apt-get install wpa_supplicant seguido se creó el archivo /etc/wpa_supplicant.conf, mediante la instrucción nano /etc/wpa_supplicant.conf y se procedió a editarlo, con información referente a SSID, el protocolo, usuario y password; la configuración final de este archivo se muestra en el apéndice S.

Luego se ejecutó como root el siguiente comando:

/sbin/wpa_supplicant -c /etc/wpa_supplicant.conf -i wlan0 -D wext -d

Se procedió a ejecutar el commando dhclient wlan0 para que la interfaz tomase dirección IP por DHCP, siendo wlan0 la interfaz de red en este caso y el parámetro -D indica el driver que usará la tarjeta de red el cual soporta 802.1X

**Creación de la base de datos para el *accounting***

El servidor de base de datos se instaló usando un archivo precompilado ubicado en los repositorios de GNU/Linux Debian Lenny, apt-get install postgresql, el cual no requiere realizar ninguna modificación adicional, una vez instalado el servicio, se procedió a crear una tabla, donde se almacena todo el registro de acceso de los usuarios que intentan autenticarse. Para ello, se creó la base de datos plc y dentro de esta se creó la tabla radacct, con los campos que se describen a continuación:

- AcctUniqueId: es el identificador único por cada sesión iniciada de *accounting* entre el servidor de autenticación y el servidor de base de datos.
- UserName: indica el nombre del usuario que se ha autenticado contra el FreeRADIUS.
- NASIPAddress: contiene la dirección IP del punto de acceso inalámbrico desde el cual el usuario ha accedido a la red.
- AcctStartTime: se especifican la fecha y hora en la que el usuario ha iniciado su acceso a la red. El formato de la fecha es el siguiente: aaaa-mm-dd; teniendo por aaaa el año, mm el mes y dd el día. Mientras que el formato de la hora es el siguiente: hh:mm:ss, teniendo por hh la hora, mm el minuto y ss el segundo.
- AcctStopTime: fecha y hora en la que el usuario ha finalizado su acceso a la red. Los formatos de la fecha y hora son los mismos que los de AcctStartTime.
- AcctSessionTime: campo en el que se registra el tiempo que estuvo conectado el usuario a la red. Se contabiliza en segundos.
- AcctInputOctets: número de octetos (bytes) que el usuario ha enviado hacia el

autenticador, o también conocido como el tráfico de subida del usuario.

- AcctOutputOctets: número de octetos (bytes) que el usuario ha recibido del autenticador, o también conocido como el tráfico de bajada o descargado del usuario.
- CalledStationId: contiene la dirección MAC y el SSID registrados en el autenticador por el cual el usuario ha accedido a la red. El formato en el que se guarda la información es el siguiente: aa-bb-cc-dd-ee-ff:ssid, para el cual el primer parámetro representa la dirección MAC del autenticador y el segundo el identificador de la red a la que accedió el usuario.
- CallingStationId: la dirección MAC del equipo desde el cual el usuario ha accedido a la red. El formato es el mismo al anteriormente descrito en el campo CalledStationId.
- AcctTerminateCause: la causa por la cual se finalizó de contabilizar y se terminó la conexión del usuario a la red inalámbrica. Se pueden tener dos posibles causas: NAS-Request, o Lost-Carrier. El primer caso se suele dar cuando el usuario ha terminado la conexión, ya sea cerrándola manualmente o apagando su equipo; mientras que el segundo caso se da cuando el usuario ha dejado el área de cobertura del autenticador.
- AcctStartDelay: campo donde se registra si es que ocurrió algún retraso en atender una solicitud de inicio para contabilizar una sesión. El tiempo de retraso se almacena en segundos.
- AcctStopDelay: campo donde se registra si es que ocurrió algún retraso en atender una solicitud de finalización para contabilizar una sesión. El tiempo que retraso que hubo se almacena en segundos.

Seguidamente, se procedió a configurar el servidor de base de datos, para dar permisología a las direcciones IP del servidor FreeRADIUS y del servidor Web Apache, cuyas IP son 10.172.25.84 y 10.172.25.85 respectivamente, para que

ejecuten operaciones sobre la misma. Para ello accedemos al archivo postgresql.conf ubicado en la siguiente ruta: /etc/postgresql/8.3/main/ modificando la línea #listen_addresses = 'localhost' por la siguiente línea listen_addresses = 10.172.25.84, 10.172.25.85' De igual forma se configuró el archivo pg_hba.conf ubicado en la siguiente ruta: /etc/postgresql/8.3/main/ con el fin de establecer la forma de autenticación de los clientes de la base de datos, cuales direcciones IP son permisadas para conectarse, cuales nombres de usuarios postgresql pueden ser usados y cuales base de datos puedes ser accedidas, los parámetros definidos en este archivo de configuración son tipo de conexión, base de datos, usuario, dirección IP, quedando de la siguiente manera:

```
llocal    all          postgres    ident sameuser
local     all          all         ident sameuser
host      all          all         127.0.0.1/32          md5
host      radius       radius      10.172.25.84/32       md5
host      radius       radius      10.172.25.85/32       md5
host      all          all         ::1/128               md5
```

**Configuración del servidor Web Apache**

El servidor Web apache se instaló usando un archivo precompilado ubicado en los repositorios de GNU/Linux Debian Lenny utilizando el comando apt-get install apache2, el cual no requiere realizar ninguna modificación adicional, para su buen funcionamiento. En el apéndice T, se muestra la configuración final del archivo VirtualHost, donde se público el sistema web PDVRadius.

**Configuración de la aplicación de gestión Web**

En esta etapa, se desarrolló una aplicación para la administración de usuarios conectados mediante el uso del servidor FreeRADIUS, con el fin de poder visualizar los accesos de los usuarios, en caso de ser necesarios para una auditoria futura. A continuación se muestra las ventanas de la aplicación PDVRadius.

La siguiente figura muestra la autenticación de los usuarios administradores del servidor FreeRADIUS.


Figura 15. Autenticación de administradores de FreeRADIUS

La figura 16, muestra los usuarios conectados a la red inalámbrica

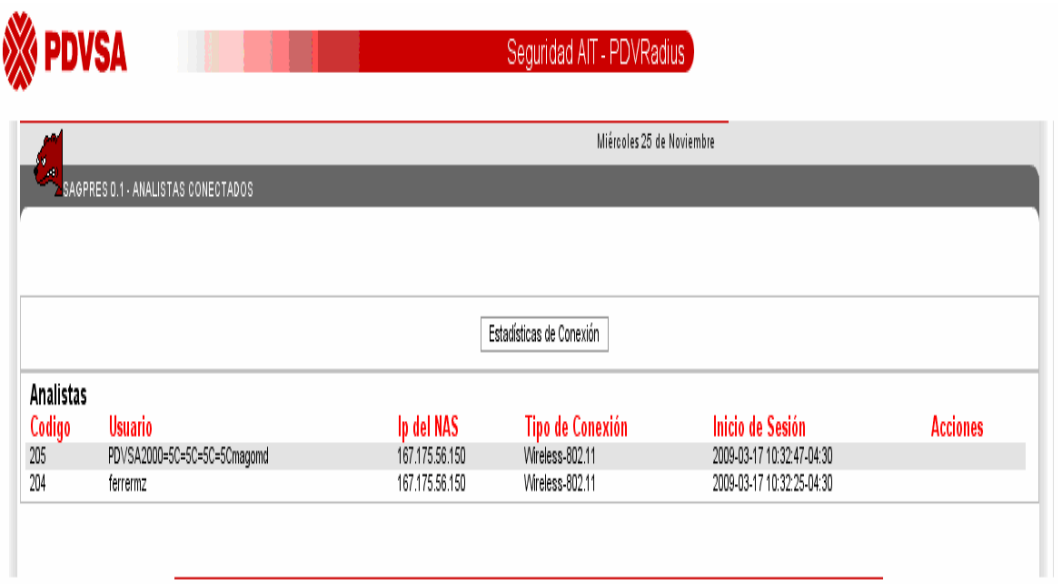



Figura 16. Usuarios conectados a la red.

La figura 17, muestra la cantidad de veces que un usuario se ha autenticado con el Servidor FreeRADIUS.

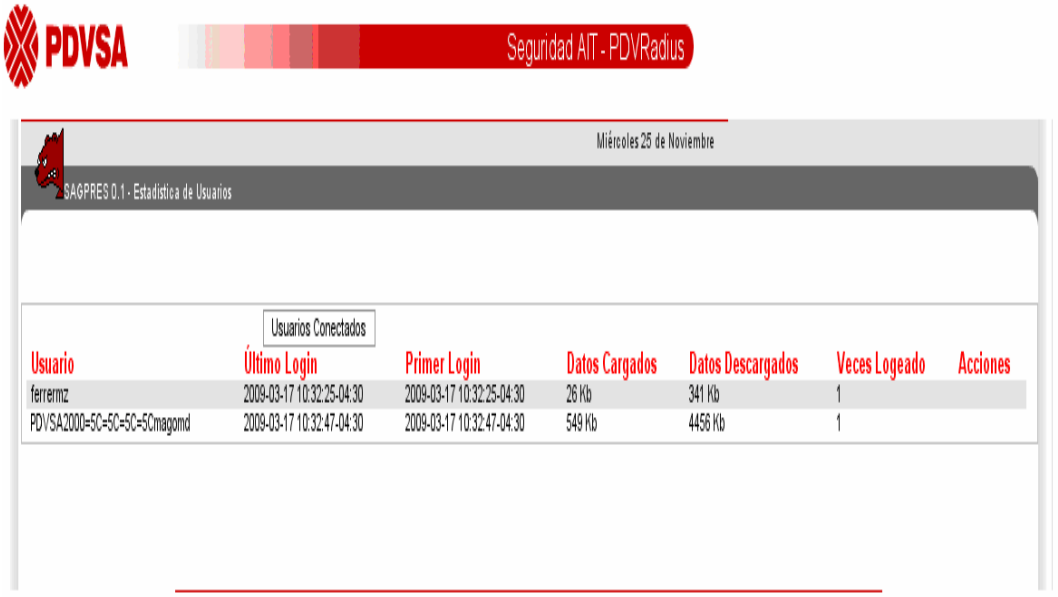


Figura 17. Número de conexiones de un usuario al servidor FreeRADIUS.

## PRUEBAS DE LA ARQUITECTURA

Esta última fase consistió en diagnosticar el comportamiento del servidor de autenticación, una vez instalado, configurado y puesto en funcionamiento. Para ello se realizaron dos pruebas, las cuales se describen a continuación:

### Prueba de conexión

Esta prueba consistió en conectar el servidor FreeRADIUS junto a los *switch y access po*int, para establecer el control de acceso a los clientes tanto inalámbricos como cableados, permitiendo dar inicio a los procesos de autorización, autenticación y contablidad que representa al estándar IEEE 802.1X. Se verificó a través del comando ping la comunicación entre los equipos de red y el servidor FreeRADIUS.

```
FREERADIUS:~# ping 167.175.56.150
PING 167.175.56.150 (167.175.56.150) 56(84) bytes of data.
64 bytes from 167.175.56.150: icmp_seq=1 ttl=251 time=3.92 ms
64 bytes from 167.175.56.150: icmp_seq=2 ttl=251 time=3.87 ms
64 bytes from 167.175.56.150: icmp_seq=3 ttl=251 time=3.99 ms
64 bytes from 167.175.56.150: icmp_seq=4 ttl=251 time=3.87 ms
--- 167.175.56.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 3.854/3.903/3.993/0.084 ms
```

Igualmente se pudó validar la comunicación del autenticador y el servidor FreeRADIUS, si al listar los archivos contenidos en el directorio /var/log/freeradius/radacct se encuentra la IP de los autenticadores.

**Prueba de autenticación**

Esta prueba consistió en definir dos (2) posibles escenarios que pueden presentarse en la red del edificio ESEM, para ello se configuro tres equipos inalámbricos (laptop), dos de los cuales están registrados en el directorio activo y uno que no pertenece a la corporación; A uno de los equipos de la empresa se le configuró el cliente WindowsXp para que pudiese autenticarse contra el servidor FreeRADIUS, a través del uso de usuarios y contraseñas, permitido en el dominio de PDVSA y el segundo equipo laptop no estaba registrado en el dominio y tampoco tenía configurado el cliente para establecer la conexión, todo esto arrojó el siguiente resultado:

A continuación se muestran las líneas obtenidas desde el archivo log de freeradius reply-detail, el cual almacena las conexiones exitosas

Fri Nov 20 10:38:20 2009
	Packet-Type = Access-Accept
	EAP-Message = 0x03090004
	Message-Authenticator = 0x00000000000000000000000000000000
	User-Name = "PDVSA2000\\britoop"
Fri Nov 20 10:38:20 2009
	Packet-Type = Access-Accept
	User-Name = "PDVSA2000\\britoop"
	MS-MPPE-Recv-Key =
0xfda550331eacb76ba1b93be6fe2d5b50bec25d851440eadf34483e4fb28639b7
	MS-MPPE-Send-Key =
0x69d82f93299546f85f1d2deca895447f23ed2919612fcb3f51cff9a4789ad012
	EAP-MSK =
0xfda550331eacb76ba1b93be6fe2d5b50bec25d851440eadf34483e4fb28639b769d82
f93299546f85f1d2deca895447f23ed2919612fcb3f51cff9a47$

EAP-EMSK = 0x40c142422f3400d8f33befd3a368222ee6522ca04a69c5e4899b770d380d3d8f06124a5a91e4f5727623f267a64784a8007810ca658ada364889900b$

EAP-Message = 0x030a0004

Message-Authenticator = 0x00000000000000000000000000000000

A continuación se muestra el intento de conexión del equipo que pertenece a la empresa, sin embargo no tiene configurado el cliente para conectarse a la red mediante el estándar de seguridad IEEE 802.1X y por lo tanto no se permite el acceso debido a que no se envía el mensaje Access-Accept.

rad_recv: Access-Request packet from host 167.175.56.150 port 1645, id=86, length=194

User-Name = "PDVSA2000\\romeroajx"

Framed-MTU = 1400

Called-Station-Id = "0022.90a0.4020"

Calling-Station-Id = "0014.a5de.6a53"

Service-Type = Login-User

Message-Authenticator = 0x50d8f7ef889d1e473b08f2ac3ef4449b

EAP-Message = 0x020a00261900170301001b91169713a97c9a9e3f7dd899dc5dcb106a1d136832982c062bb180

NAS-Port-Type = Wireless-802.11

NAS-Port = 346

NAS-Port-Id = "346"

State = 0xe537419be23d58d69210b8f13d370add

NAS-IP-Address = 167.175.56.150

NAS-Identifier = "PruebaFR"

+- entering group authorize {...}

[auth_log] expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%d -> /var/log/freeradius/radacct/167.175.56.150/auth-detail-20091005

[auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%d expands to /var/log/freeradius/radacct/167.175.56.150/auth-detail-20091005

[auth_log] expand: %t -> Mon Oct 5 15:06:45 2009

++[auth_log] returns ok

[ntdomain] Looking up realm "PDVSA2000" for User-Name = "PDVSA2000\romeroajx"

[ntdomain] No such realm "PDVSA2000"

++[ntdomain] returns noop

[eap] EAP packet type response id 10 length 38

[eap] Continuing tunnel setup.

++[eap] returns ok

++[mschap] returns noop

[suffix] No '@' in User-Name = "PDVSA2000\romeroajx", looking up realm NULL

[suffix] No such realm "NULL"

++[suffix] returns noop

++[files] returns noop

Found Auth-Type = EAP

+- entering group authenticate {...}

[eap] Request found, released from the list

[eap] EAP/peap

[eap] processing type peap

[peap] processing EAP-TLS

[peap] eaptls_verify returned 7

[peap] Done initial handshake

[peap] eaptls_process returned 7

[peap] EAPTLS_OK

[peap] Session established. Decoding tunneled attributes.

[peap] Received EAP-TLV response.

[peap]  Had sent TLV failure.  User was rejected earlier in this session.

[eap] Handler failed in EAP/peap

[eap] Failed in EAP select

++[eap] returns invalid

.....

Failed to authenticate the user.

Login incorrect: [PDVSA2000\\romeroajx/<via Auth-Type = EAP>] (from client PruebaFR port 346 cli 0014.a5de.6a53)

Using Post-Auth-Type Reject

WARNING: Unknown value specified for Post-Auth-Type.  Cannot perform requested action.

…….

Delaying reject of request 27 for 1 seconds

Going to the next request

Waking up in 0.9 seconds.

Sending delayed reject for request 27

Sending Access-Reject of id 86 to 167.175.56.150 port 1645

EAP-Message = 0x040a0004

Message-Authenticator = 0x00000000000000000000000000000000

Sending Access-Reject este mensaje indica que el usuario ha sido rechazado por el servidor Freeradius en vista de que no esta usando el mismo protocolo EAP que el servidor de autenticación esto se evidencia en la siguiente línea [eap] Failed in EAP select.

**Prueba de conexiones simultáneas**

Esta prueba consistió en someter al servidor FreeRADIUS al proceso de autenticación con múltiples solicitudes, en este caso usamos siete (7) suplicantes intentando conectarse desde un mismo autenticador, para verificar el comportamiento del ancho de banda consumido por dichas peticiones hacia el servidor FreeRADIUS, los resultados de esta prueba se muestra en la Tabla 7.

Tabla 7. Especificaciones de conexión de suplicantes

| Cantidad de Usuarios | Tiempo Total | Bytes Total | Mbit/sec | Tiempo por Usuario |
|---|---|---|---|---|
| 1 | 0,311514 | 6147 | 0,158000 | 0,311514 |
| 2 | 1,005349 | 12294 | 0,098000 | 0,502675 |
| 3 | 1,389205 | 18426 | 0,106000 | 0,463068 |
| 4 | 1,583445 | 24573 | 0,124000 | 0,395861 |
| 5 | 2,196661 | 31420 | 0,114000 | 0,439332 |
| 6 | 3,766361 | 37672 | 0,080000 | 0,627727 |
| 7 | 4,087166 | 43819 | 0,081795 | 0,583881 |

En la figura 18, se puede observar el comportamiento del tiempo total de respuesta del Servidor frente a muchas solicitudes concurrentes por parte de los usuarios

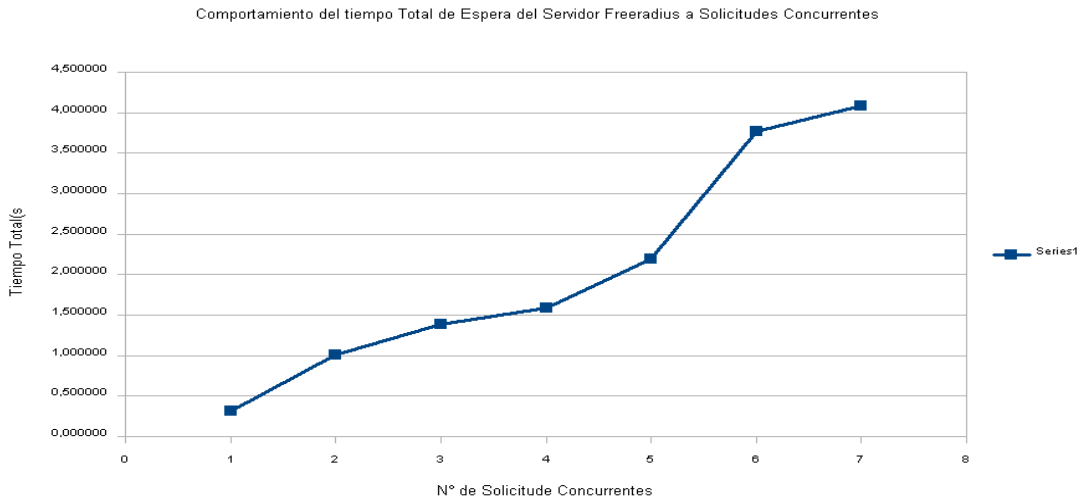



Figura 18. Tiempo de respuesta del servidor FreeRADIUS.

En la figura 19, se puede observar el comportamiento del ancho de banda disminuye leve

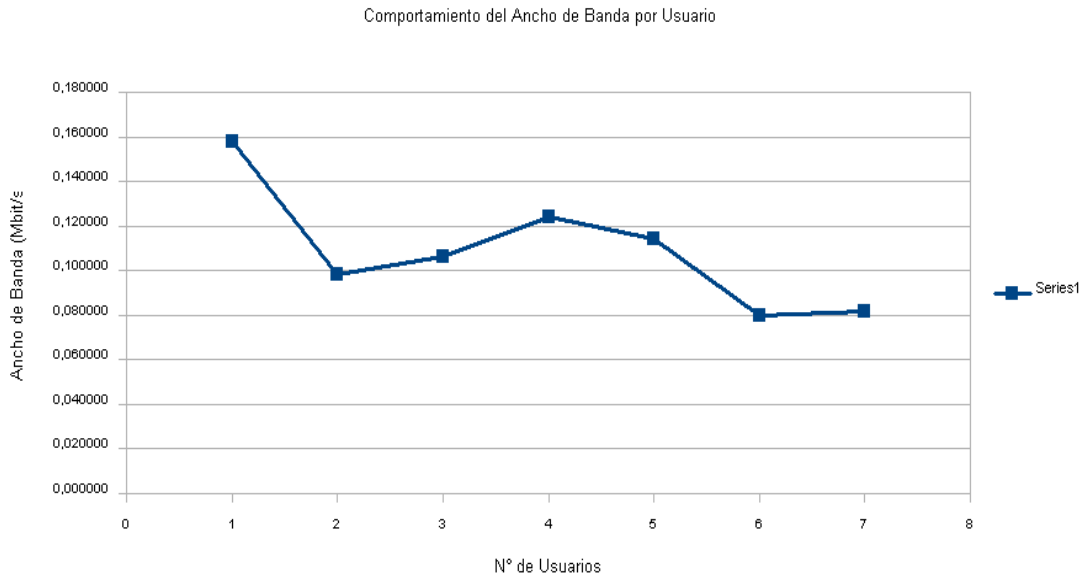



Figura 19. Disminución del ancho de banda

.

# CONCLUSIONES

Después de la culminación de este trabajo, se pudo comprobar que la arquitectura implementada garantiza un mayor control a nivel puertos de red LAN, negando el uso de los recursos a aquellas personas o equipos, que no pertenecen al directorio activo de PDVSA, mediante la utilización del protocolo EAP y el mecanismo de cifrado TKIP; los cuales impiden que la información transmitida por la red pueda ser escuchada y capturada. Además, la configuración del servidor AAA, permitió autenticar, autorizar y llevar la trazabilidad de las conexiones establecidas por los usuarios, estando éstas reflejadas en un sistema Web, que permite visualizar, de forma amigable para los analistas de la Gerencia de Seguridad Lógica, la trazabilidad antes mencionada.

Mediante esta arquitectura, se aprovecha las bondades de otros componentes existentes en la Plataforma Tecnológica de PDVSA, como es el caso del servidor DHCP y el directorio activo de Microsoft.

## RECOMENDACIONES

Implementar la arquitectura de control de acceso basada en el estándar de seguridad IEEE 802.1x en las demás localidades de PDVSA, con la finalidad de autenticar y dar acceso sólo a usuarios pertenecientes al directorio activo de la corporación.

Incorporar a esta arquitectura de seguridad, la infraestructura de claves públicas PKI, añadiendo certificados digitales en los clientes, con la finalidad de garantizar la seguridad en las operaciones o transacciones que precisan de la certificación, de tal forma se incrementarían más puntos de control para poder ingresar a la red *Ethernet* de la empresa

## BIBLIOGRAFÍA


Buster D, 2005. *Towards IP for space based communications systems; a Cisco Systems assessment of a single board router*. EEUU

Contraloría General de México. 2007. "Normas generales que deberán observarse en materia de seguridad de la información en la administración pública del distrito federal". "contraloria.df.gob.mx". <http://www.contraloria.df.gob.mx/htm> (16/09/07).

Donoso Cortés. 2002. "Diccionario de Internet". Primera edición española. Editorial Complutense, S.A.

EFMF, 2004 *IEEE standard.* 802.3 *Ethernet in the First Mile over Fiber*. <http://www.ieee802.org/3/efm/> (23/10/2009)

García P, 2007. "Seguridad y conectividad". "GERMINUS XXI". <http://www.germinus.com/sala_prensa/articulos/SIC73_096-100.pdf> (10/10/07).

Gómez, P 2007. Arquitectura unificada para control de acceso en redes inalámbricas seguras. Tesis de maestría en teleinformática. Universidad de Murcia.

Hernández, M. 2007. Implementación de una red inalámbrica protegida por un sistema de autenticación RADIUS en la planta de mejorado de crudo de petrolera Ameriven (PA), ubicada en el complejo industrial José Antonio Anzoátegui. Trabajo de Grado. Licenciatura en Informática. Universidad de Oriente, Cumaná.

Hassell, J. 2002. RADIUS. Primera Edición. O´Reilly. Estados Unidos.

IIET, 2005. Instituto de Investigaciones en Electrónica y Telecomunicación de Corea del Sur I Body Area Networking.<http://www.boingboing.net/2005/06/23.html> (12/05/2009)

INTEL Corporation, 2003 "intel.com" <http://docs.google.com/ntel.com/thodology.pdf> (22/07/2009)

Kuhlmann F. y Alonso A, 1996. Información y telecomunicaciones. Secretaría de Educación Pública y el Consejo Nacional de Ciencia y Tecnología <http://bibliotecadigital.ilce.edu.mx/sites/ciencia/htm/sec_8.htm> (20/03/2008).

Matanzo, A 2008. Implementación del protocolo CHAP en un sistema de seguridad para redes WLAN. Trabajo de Grado. Universidad de Chile.

McCabe, James. 1998. Introducción al análisis y diseño de redes de computadoras. Morgan Kaufmann Publishers. México.

Metcalfe R y Boggs D, 1976., *Ethernet: Distributed Packet Switching for Local Computer Networks,* Communications of the ACM, Volumen. 19.

Microsoft *Corporation*. 2007, "Redes y telecomunicaciones en las organizaciones" "Microsoft *Corporation*". <http://www.microsoft.com/latam/networking.mspx> (11/06/07).

PDV-PCP-ISL-040, 2007. "Instrucción de trabajo: Manejo de cuentas de red/correo de la plataforma tecnológica de la coorporación" (09/07/07).

Petróleos de Venezuela S.A. 2005. "Exploración y producción". "PDVSA". <http://www.pdvsa.com/ne> (05/07/2007).

Ramírez, T. 1995. “Cómo Hacer un Proyecto de Investigación”. Tercera Edición. Carhel C.A, Caracas.

Rodríguez, E. 2007. “Seguridad de la información: ¿Moda o Necesidad?”. “ISACA”. <http://www.isaca.org.mx/cgi-bin/isaca/mambo451/index.php?optd=2> (16/09/07).

Sabino, C. 1999. “Proceso de Investigación”. Tercera Edición. PANAPO. Caracas.

Sánchez, C. (ed) 2004. Microsoft diccionario de informática e internet. Interamericana de España. Segunda edición McGraw-Hill.

Sánchez, M. 2003. Una arquitectura de control de acceso a redes de área local inalámbricas 802.11. Proyecto Informático. Facultad de Informática. Universidad de Murcia.

Stallings W, 2004. Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. Segunda Edición. Ediciones Pearson Educación, S.A. Madrid.

Wikipedia, 2005 “IEEE” “wikipedia.org”. <http://es.wikipedia.org/wiki/ IEEE> (12/09/2009)

# APÉNDICES

# APENDICE A

## Descripción del caso de uso para el acceso de equipos de tercero

En las siguientes tablas, se describen cada uno de los casos de usos, pertenecientes al caso de uso del sistema de control de acceso actual de la red *Ethernet* de PDVSA, así como los elementos que interactúan en el.

**Tabla 1. Caso de uso, solicitar acceso de equipos de terceros.**

| ELEMENTOS | DESCRIPCIÓN |
|---|---|
| Caso de uso: | Solicitar acceso de equipos de terceros |
| Actor: | Gerencia solicitante |
| Descripción del caso de uso: | Se realiza la solicitud de autorización de acceso de equipos de tercero, consignando los requisitos previos. |
| Precondición: | La Gerencia solicitante, requiere el acceso de equipos de terceros al operador de PCP . |
| Postcondición: | Acceso aceptado o acceso denegado |
| Flujo Normal: | La Gerencia solicitante, muestra información de la solictud para acceso de tercero que es verificado por el personal de PCP. Si el operador de PCP, verifica la solicitud emitida por la Gerencia solicitante y no contiene las firmas de autorización por la Gerencia de Seguridad Lógica, éste rechaza el acceso. |

**Tabla 2. Caso de uso, atender solicitud de acceso de equipos de terceros.**

| ELEMENTOS | DESCRIPCIÓN |
|---|---|
| Caso de uso: | Atender solicitud de acceso de equipos de tercero |
| Actor: | Seguridad Lógica |
| Descripción: | La Gerencia solicitante, solicta la autorización mediante una firma al personal de la Gerencia de Seguridad Lógica y a su vez informa sobre las políticas de seguridad de la información. |
| Precondición: | Estudia el requerimiento de acceso, suministrado por la Gerancia solicitante |
| Postcondición: | Acceso aceptado o rechazado |
| Flujo Normal: | Seguridad Lógica verifica la información de la solictud de acceso y suministra información sobre las políticas de seguridad de la información. Si la solicitud de acceso a equipos de tercero no contiene una justificación importante y no contiene la autorización de la Gerencia que solicita el ingreso, éste rechaza el acceso a la Corporación e informa sobre las políticas de seguridad de la información |

**Tabla 3. Caso de uso, informar políticas de seguridad.**

| ELEMENTOS | DESCRIPCIÓN |
|---|---|
| Caso de Uso: | Informar políticas de seguridad |
| Actor: | Seguridad Lógica |
| Descripción: | Seguridad Lógica informa a la Gerencia solicitante las políticas de seguridad de la información |
| Precondición: | Suministra información sobre las políticas de seguridad de la información. |
| Postcondición: | Suministra información sobre las políticas de seguridad de la información. |
| Flujo Normal: | Seguridad Lógica da a conocer información referente a las normas establecidas en las políticas de seguridad, sobre el acceso de equipos de terceros. |

**Tabla 4. Caso de uso, ingresar equipos de tercero.**

| ELEMENTOS | DESCRIPCIÓN |
|---|---|
| Caso de Uso: | Ingresar equipos de tercero |
| Actor: | Personal externo |
| Descripción: | Se requiere el ingreso del equipo de computación a las instalaciones de PDVSA. |
| Precondición: | El Personal externo, muestra la solicitud de acceso firmada y autorizada por la Gerencia Solicitante y Seguridad Lógica, asi como también muestra el equipo que se requiere accesar a la Corporación. |
| Postcondición: | Acceso aceptado o rechazado |
| Flujo Normal: | El Personal externo ingresa los datos del equipo y la solicitud |

**Tabla 5. Caso de uso, validar permiso de entrada de equipos de tercero.**

| ELEMENTOS | DESCRIPCIÓN |
|---|---|
| Caso de Uso: | Validar permiso de entrada de equipos de tercero |
| Actor: | Operador PCP |
| Descripción: | Se registra los datos que se encuentran en la autorización de equipos de terceros, con el fin de validar la fecha de vigencia de dicha autorización. |
| Precondición: | El operador de PCP, verifica que la autorización de equipos de terceros cuenta con la autorización de Seguridad Lógica y la Gerencia Solicitante, asi como la fecha de vigencia. |
| Postcondición: | Habilitar o negar el acceso |
| Flujo Normal: | El operador de PCP, recuerda que no se puede conectar el equipo de tercero a la red de PDVSA. Si el operador de PCP, visualiza que la autorización de equipos de tercero no posee todos los requisitos, niega el acceso. |

## APENDICE B

## Matriz de evaluación de los mecanismos de autenticación

**Tabla 1. Matriz de evaluación de los mecanismos de autenticación.**

| CRITERIOS | VALOR PONDERADO | MÉTODOS DE AUTENTICACIÓN | | | | | |
|---|---|---|---|---|---|---|---|
| | | USUARIO/CONTRASEÑA | | CERTIFICADOS | | BIOMETRIA | |
| | | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN |
| Facilidad de Implementación | 0,18 | 8 | 1,44 | 7 | 1,26 | 3 | 0,54 |
| Robustez | 0,30 | 5 | 1,50 | 8 | 2,40 | 8 | 2,40 |
| Independencia de Hardware | 0,25 | 8 | 2,00 | 8 | 2,00 | 2 | 0,50 |
| Reutilización de recursos de red | 0,27 | 8 | 2,16 | 1 | 0,27 | 1 | 0,27 |
| **Calificación ponderada** | 1,00 | **7,1** | | 5,93 | | 3,71 | |

# APENDICE C

## Matriz de evaluación de los protocolos de autenticació

**Tabla 2. Matriz de evaluación de los protocolos de autenticación.**

| CRITERIOS | Valor ponderado | MÉTODOS EAP | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EAP-TLS | | EAP-TTLS | | EAP-PEAP | | EAP-FAST | | EAP-LEAP | |
| | | Evaluación | Calificación | Evaluación | Calificación | Evaluación | Calificación | Evaluación | Calificación | Evaluación | Calificación |
| Facilidad de Implementación | 0,15 | 7 | 1,05 | 7 | 1,05 | 8 | 1,2 | 7 | 1,05 | 8 | 1,2 |
| Robustez | 0,30 | 5 | 1,5 | 8 | 2,4 | 8 | 2,4 | 2 | 0,6 | 3 | 0,9 |
| Independencia de Hardware | 0,12 | 3 | 0,36 | 5 | 0,6 | 6 | 0,72 | 1 | 0,12 | 1 | 0,12 |
| No requiere certificados en el cliente. | 0,19 | 1 | 0,19 | 1 | 0,19 | 8 | 1,52 | 8 | 1,52 | 1 | 0,19 |
| Escalabilidad | 0,24 | 4 | 0,96 | 5 | 1,2 | 7 | 1,68 | 3 | 0,72 | 3 | 0,72 |
| **Calificación ponderada** | 1,00 | | 4,06 | | 5,44 | | **7,52** | | 4,01 | | 3,13 |

# APENDICE D

## Matriz de evaluación de los mecanismos de cifrado

**Tabla 3. Matriz de evaluación de los mecanismos de cifrado.**

| CRITERIOS | VALOR PONDERADO | MECANISMO DE CIFRADO | | | | | |
|---|---|---|---|---|---|---|---|
| | | WEP | | WPA | | WPA2 | |
| | | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN |
| Capacidad de procesamiento menor | 0,21 | 8 | 1,68 | 6 | 1,26 | 2 | 0,42 |
| Reutilización de recursos de red | 0,35 | 8 | 2,8 | 8 | 2,8 | 5 | 1,75 |
| Robustez | 0,44 | 1 | 0,44 | 6 | 2,64 | 8 | 3,52 |
| **Calificación ponderada** | 1,00 | | 4,92 | | **6,7** | | 5,69 |

## APENDICE E

**Matriz de evaluación de los mecanismos de autorización.**

**Tabla 4. Matriz de evaluación de los mecanismos de autorización.**

| CRITERIOS | VALOR PONDERADO | MECANISMO DE AUTORIZACIÓN | | | | | |
|---|---|---|---|---|---|---|---|
| | | Base de Datos | | Archivo de Texto Plano | | Directorio Activo | |
| | | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN |
| Cumplimiento del decreto 3390 | 0,15 | 8 | 1,20 | 8 | 1,20 | 1 | 0,15 |
| Escalabilidad | 0,18 | 8 | 1,44 | 1 | 0,18 | 8 | 1,44 |
| Disponibilidad | 0,27 | 8 | 2,16 | 1 | 0,27 | 8 | 2,16 |
| Reutilización de componentes | 0,40 | 2 | 0,80 | 1 | 0,40 | 8 | 3,20 |
| **Calificación ponderada** | 1,00 | | 5,60 | | 2,05 | | **6,95** |

# APENDICE F

## Matriz de evaluación de los servidores de autenticación

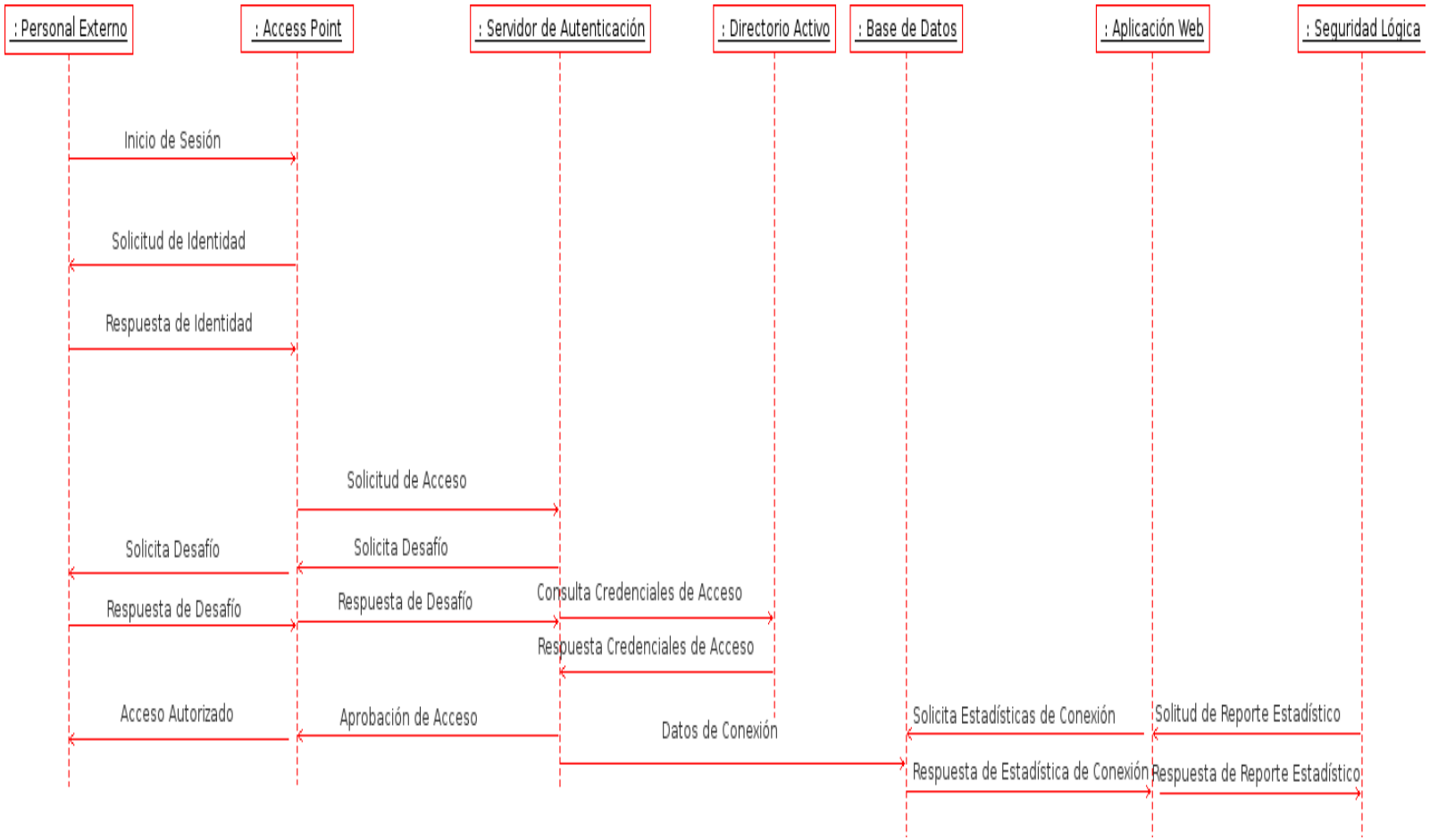
**Tabla 5. Matriz de evaluación de los servidores de autenticación.**

| CRITERIOS | VALOR PONDERADO | SERVIDOR DE AUTENTICACIÓN | | | | | |
|---|---|---|---|---|---|---|---|
| | | Cisco Secure Access | | FreeRADIUS | | Micrososft IAS | |
| | | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN | EVALUACIÓN | CALIFICACIÓN |
| Seguridad | 0,19 | 8 | 1,52 | 8 | 1,52 | 7 | 1,33 |
| Reutilización de recursos de red | 0,30 | 1 | 0,30 | 8 | 2,4 | 7 | 2,1 |
| Disponibilidad | 0,22 | 3 | 0,66 | 8 | 1,76 | 8 | 1,76 |
| Facilidad de mantenimiento | 0,13 | 3 | 0,39 | 6 | 0,78 | 6 | 0,78 |
| Cumplimiento del decreto 3390 | 0,16 | 1 | 0,16 | 8 | 1,28 | 1 | 0,16 |
| **Calificación ponderada** | 1 | | 3,03 | | **7,74** | | 6,13 |

# APENDICE H

## Diagrama de secuencia de UML de la arquitectura de control de acceso basada en el estándar IEEE 802.1x implementada en la red *Ethernet* de PDVSA

**Figura 1. Diagrama de secuencia UML de la arquitectura de control de acceso, basada en el estándar de seguridad IEEE 802.1x implementada en la red *Ethernet* de PDVSA**



# APENDICE I

## Archivo de configuración smb.conf del servidor FreeRADIUS.

```
[global]
workgroup = PDVSA2000
server string = %h server
dns proxy = no
log file = /var/log/samba/log.%m
max log size = 1000
syslog = 0
panic action = /usr/share/samba/panic-action %d
security = ads
encrypt passwords = true
passdb backend = tdbsam
obey pam restrictions = yes
invalid users = root
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* %n\n
*Retype\snew\sUNIX\spassword:* %n\n *password\supdated\ssuccessfully* .
socket options = TCP_NODELAY
idmap uid = 10000-20000
idmap gid = 10000-20000
template shell = /bin/bash
winbind use default domain = no
winbind separator = +
password server = matsed14.pdvsa.com
realm = PDVSA.COM
[homes]
  comment = Home Directories
  browseable = no
  writable = yes
  create mask = 0700
```

```
   directory mask = 0700
   valid users = %S
[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   public = no
   writable = no
   create mode = 0700
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
```

## APENDICE J

## Archivo de configuración nsswitch.conf del servidor FreeRADIUS.

```
passwd:         files winbind
group:          files winbind
shadow:         files winbind

hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4 winbindx
networks:       files

protocols:      files winbind
services:       files winbind
netgroup:       files winbind
automount:      files winbind
ethers:         db files
rpc:            files winbind
```

## APENDICE U

## Archivo de configuración krb5.conf del servidor FreeRADIUS.

```
[libdefaults]
  default_realm = PDVSA.COM
  krb4_config = /etc/krb.conf
  krb4_realms = /etc/krb.realms
  kdc_timesync = 1
  ccache_type = 4
  forwardable = true
  proxiable = true
  default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
  default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
  v4_instance_resolve = false
  v4_name_convert = {
    host = {
      rcmd = host
      ftp = ftp
    }
    plain = {
      something = something-else
    }
  }
  fcc-mit-ticketflags = true

[realms]
  ORI.PDVSA.COM = {
    kdc = matsed14:88
    admin_server = matsed14:749
    default_domain = pdvsa.com
  }
  PDVSA.COM = {
```

```
    kdc = matsed14:88
    admin_server = matsed14:749
    default_domain = pdvsa.com
  }
[domain_realm]
  .ori.pdvsa.com = ORI.PDVSA.COM
  ori.pdvsa.com = ORI.PDVSA.COM
  .pdvsa.com = PDVSA.COM
  pdvsa.com = PDVSA.COM

[login]
  krb4_convert = true
  krb4_get_tickets = false

[appdefaults]
  pam = {
    ticket_lifetime = 1d
    renew_lifetime = 1d
    forwardable = true
    proxiable = false
    retain_after_close = false
    minimum_uid = 0
    try_first_pass = true
  }
```

## APENDICE K

## Archivo de configuración radiusd.conf del servidor FreeRADIUS.

```
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius
radacctdir = ${logdir}/radacct
name = freeradius
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}
db_dir = ${raddbdir}
libdir = /usr/lib/freeradius
pidfile = ${run_dir}/${name}.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 1024
listen {
        type = auth
        ipaddr = *
        port = 1812
}
listen {
        ipaddr = *
        port = 1813
        type = acct
}
```

```
hostname_lookups = no
allow_core_dumps = no
regular_expressions    = yes
extended_expressions= yes
log {
        destination = files
        file = ${logdir}/radius.log
        syslog_facility = daemon
        stripped_names = no
        auth = yes
        auth_badpass = yes
        auth_goodpass = yes
}
checkrad = ${sbindir}/checkrad
security {
        max_attributes = 200
        reject_delay = 1
        status_server = yes
}
proxy_requests  = yes
$INCLUDE proxy.conf
$INCLUDE clients.conf
thread pool {
        start_servers = 5
        max_servers = 32
        min_spare_servers = 3
        max_spare_servers = 10
        max_requests_per_server = 0
}
```

```
modules {
        $INCLUDE ${confdir}/modules/
        $INCLUDE eap.conf
        exec ntlm_auth {
          wait = yes
           program = "/usr/bin/ntlm_auth ntlm_auth --request-nt-key --
domain=PDVSA2000 --username=%{mschap:User-Name} --password=%{User-
Password}"
      }
        $INCLUDE sql.conf
        $INCLUDE sql/postgresql/counter.conf

}
instantiate {
        exec
        expr
        expiration
        logintime
}
$INCLUDE policy.conf
$INCLUDE sites-enabled/
```

# APENDICE L

## Archivo de configuración de la entidad certificadora CA.cnf

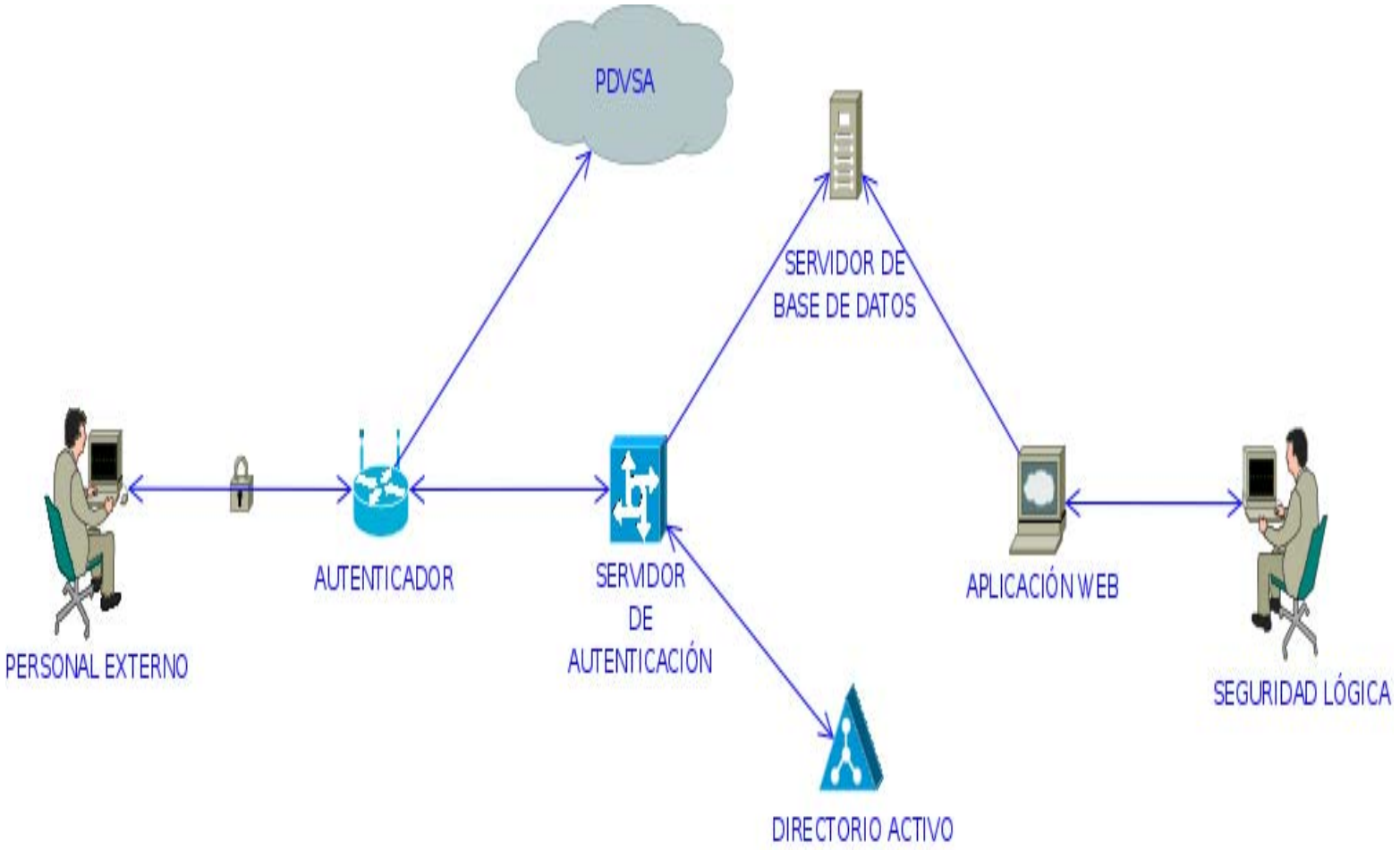
```
[ ca ]
default_ca              = CA_default
[ CA_default ]
dir                     = ./
certs                   = $dir
crl_dir                 = $dir/crl
database                = $dir/index.txt
new_certs_dir           = $dir
certificate             = $dir/ca.pem
serial                  = $dir/serial
crl                     = $dir/crl.pem
private_key             = $dir/ca.key
RANDFILE                = $dir/.rand
name_opt                = ca_default
cert_opt                = ca_default
default_days            = 365
default_crl_days        = 30
default_md              = md5
preserve                = no
policy                  = policy_match
[ policy_match ]
countryName             = match
stateOrProvinceName= match
organizationName        = match
organizationalUnitName      = optional
commonName              = supplied
emailAddress            = optional
[ policy_anything ]
countryName             = optional
```

```
stateOrProvinceName= optional
localityName            = optional
organizationName        = optional
organizationalUnitName      = optional
commonName              = supplied
emailAddress            = optional

[ req ]
prompt                  = no
distinguished_name      = certificate_authority
default_bits            = 2048
input_password                  = administrador
output_password                 = administrador
x509_extensions                 = v3_ca

[certificate_authority]
countryName             = VE
stateOrProvinceName= MATURIN
localityName            = PDVSA
organizationName        = SEGURIDAD AIT ORIENTE
emailAddress            = seguridadaitori@pdvsa.com
commonName              = "AUTORIDAD CERTIFICADORA PDVSA"

[v3_ca]
subjectKeyIdentifier    = hash
authorityKeyIdentifier          = keyid:always,issuer:always
basicConstraints        = CA:true
```

# APENDICE G

## Arquitectura de control de acceso implementada en la red de PDVSA, basada en el estándar de seguridad IEEE 802.1x

**Figura 2. Arquitectura de control de acceso implementada en la red de PDVSA, basada en el estándar de seguridad IEEE 802.1x**



## APENDICE M

## Archivo de configuración eap.conf del servidor FreeRADIUS.

```
eap {
        default_eap_type = peap
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = 2048
        tls {
                certdir = ${confdir}/certs
                cadir = ${confdir}/certs
                private_key_password = whatever
                private_key_file = ${certdir}/server.pem
                certificate_file = ${certdir}/server.pem
                CA_file = ${cadir}/ca.pem
                dh_file = ${certdir}/dh
                random_file = ${certdir}/random
                fragment_size = 1024
                include_length = yes
                make_cert_command = "${certdir}/bootstrap"
                cache {
            enable = no
                        lifetime = 24 # hours
            max_entries = 255
                }
        }
        peap {

                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
```

```
                proxy_tunneled_request_as_eap = yes
                }
        mschapv2 {
        }
}
```

## APENDICE N

## Archivo de configuración mschap.conf del servidor FreeRADIUS.

```
mschap {

        authtype = MS-CHAP
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
        with_ntdomain_hack = yes
        ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{mschap:User-
Name:-None}          --domain=%{mschap:NT-Domain:-PDVSA2000}          --
challenge=%{mschap:Challenge:-00} --nt-response=%{mschap:NT-Response:-00}"
}
```

## APENDICE O

## Archivo de configuración clients.conf del servidor FreeRADIUS.

```
client 127.0.0.1 {
        secret          = testing123
        shortname       = localhost
        nastype     = other      # localhost isn't usually a NAS...
}

client 167.175.56.150 {
        secret          = administrador
        shortname       = aironet
}
client 167.175.56.124 {
        secret          = administrador
        shortname       = es-plcoficina61
}
client 167.175.56.136 {
        secret          = administrador
        shortname       = es-plcoficina66
}
client 10.172.20.45 {
        secret          = administrador
        shortname       = es-plcoficina59
}
```

**APENDICE P**

**Archivo de configuración default del servidor FreeRADIUS.**

```
authorize {
auth_log
        ntdomain
    eap
    mschap
    suffix
        files
}
authenticate {
ntlm_auth
Auth-Type MS-CHAP {
            mschap
     }
eap

}
preacct {
suffix
}

accounting {
acct_unique
    detail
}
session {
}
post-auth {
     reply_log
}
```

## APENDICE Q

## Archivo de configuración sql.conf del servidor FreeRADIUS.

```
sql {
        driver = "rlm_sql_postgresql"
        server = "localhost"
        login = "seguridad"
        password = "segaitradiusplc"
        radius_db = "plc"
        acct_table1 = "radacct"
        acct_table2 = "radacct"
        postauth_table = "radpostauth"
        authcheck_table = "radcheck"
        authreply_table = "radreply"
        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply"
        usergroup_table = "usergroup"
        deletestalesessions = yes
        sqltrace = yes
        sqltracefile = ${logdir}/sqltrace.sql
        num_sql_socks = 5
        sql_user_name = "%{User-Name}"
        authorize_check_query = "SELECT id, UserName, Attribute, Value, Op \
                FROM ${authcheck_table} \
                WHERE Username = '%{SQL-User-Name}' \
                ORDER BY id"
        authorize_reply_query = "SELECT id, UserName, Attribute, Value, Op \
                FROM ${authreply_table} \
                WHERE Username = '%{SQL-User-Name}' \
                ORDER BY id"
                authorize_group_check_query = "SELECT ${groupcheck_table}.id,
${groupcheck_table}.GroupName, \
```

```
                ${groupcheck_table}.Attribute,
${groupcheck_table}.Value,${groupcheck_table}.Op \
                FROM ${groupcheck_table}, ${usergroup_table} \
                WHERE ${usergroup_table}.Username = '%{SQL-User-Name}' AND
${usergroup_table}.GroupName = ${groupcheck_table}.GroupName \
                ORDER BY ${groupcheck_table}.id"
        authorize_group_reply_query = "SELECT ${groupreply_table}.id,
${groupreply_table}.GroupName, ${groupreply_table}.Attribute, \
                ${groupreply_table}.Value, ${groupreply_table}.Op \
                FROM ${groupreply_table},${usergroup_table} \
                WHERE ${usergroup_table}.Username = '%{SQL-User-Name}' AND
${usergroup_table}.GroupName = ${groupreply_table}.GroupName \
                ORDER BY ${groupreply_table}.id"
        authenticate_query = "SELECT Value,Attribute FROM ${authcheck_table} \
                WHERE UserName = '%{User-Name}' AND ( Attribute = 'User-
Password' OR Attribute = 'Crypt-Password' ) \
                ORDER BY Attribute DESC"
accounting_onoff_query = "UPDATE ${acct_table1} \
  SET AcctStopTime = ('%S'::timestamp - '%{Acct-Delay-Time:-0}'::interval), \
  AcctSessionTime = (EXTRACT(EPOCH FROM('%S'::timestamp with time zone - \
            AcctStartTime::timestamp with time zone - \
            '%{Acct-Delay-Time:-0}'::interval)))::BIGINT, \
  AcctTerminateCause='%{Acct-Terminate-Cause}', \
  AcctStopDelay = 0 \
  WHERE AcctSessionTime IS NULL \
  AND AcctStopTime IS NULL \
  AND NASIPAddress= '%{NAS-IP-Address}' \
  AND AcctStartTime <= '%S'::timestamp"
accounting_update_query = "UPDATE ${acct_table1} \
```

```
  SET FramedIPAddress = NULLIF('%{Framed-IP-Address}', '')::inet, \
  AcctSessionTime = (EXTRACT(EPOCH FROM('%S'::timestamp with time zone - \
                AcctStartTime::timestamp with time zone - \
                '%{Acct-Delay-Time:-0}'::interval)))::BIGINT, \
  AcctInputOctets = (('%{Acct-Input-Gigawords:-0}'::bigint << 32) + \
                '%{Acct-Input-Octets:-0}'::bigint), \
  AcctOutputOctets = (('%{Acct-Output-Gigawords:-0}'::bigint << 32) + \
                '%{Acct-Output-Octets:-0}'::bigint) \
  WHERE AcctSessionId = '%{Acct-Session-Id}' \
  AND UserName = '%{SQL-User-Name}' \
  AND NASIPAddress= '%{NAS-IP-Address}' \
  AND AcctStopTime IS NULL"
accounting_update_query_alt = "INSERT into ${acct_table1} \
  (AcctSessionId, AcctUniqueId, UserName, Realm, NASIPAddress, NASPortId,
NASPortType, AcctStartTime, \
  AcctSessionTime, AcctAuthentic, AcctInputOctets, AcctOutputOctets,
CalledStationId, CallingStationId, \
                ServiceType, FramedProtocol, FramedIPAddress,
XAscendSessionSvrKey) \
                values('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-
User-Name}', '%{Realm}', '%{NAS-IP-Address}', \
                '%{NAS-Port}', '%{NAS-Port-Type}', \
            ('%S'::timestamp - '%{Acct-Delay-Time:-0}'::interval - '%{Acct-Session-
Time:-0}'::interval), \
                '%{Acct-Session-Time}', '%{Acct-Authentic}', \
                (('%{Acct-Input-Gigawords:-0}'::bigint << 32) + '%{Acct-Input-
Octets:-0}'::bigint), \
                (('%{Acct-Output-Gigawords:-0}'::bigint << 32) + '%{Acct-Output-
Octets:-0}'::bigint), '%{Called-Station-Id}', \
```

```
                '%{Calling-Station-Id}', '%{Service-Type}', '%{Framed-Protocol}', \
                NULLIF('%{Framed-IP-Address}', '')::inet, '%{X-Ascend-Session-
Svr-Key}')"
        accounting_start_query = "INSERT into ${acct_table1} \
                (AcctSessionId, AcctUniqueId, UserName, Realm, NASIPAddress,
NASPortId, NASPortType, AcctStartTime, AcctAuthentic, \
                ConnectInfo_start, CalledStationId, CallingStationId, ServiceType,
FramedProtocol, FramedIPAddress, AcctStartDelay, XAscendSessionSvrKey) \
                values('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-
User-Name}', '%{Realm}', '%{NAS-IP-Address}', \
                '%{NAS-Port}', '%{NAS-Port-Type}', ('%S'::timestamp - '%{Acct-
Delay-Time:-0}'::interval), '%{Acct-Authentic}', '%{Connect-Info}', \
                '%{Called-Station-Id}', '%{Calling-Station-Id}', '%{Service-Type}',
'%{Framed-Protocol}', \
                NULLIF('%{Framed-IP-Address}', '')::inet, 0, '%{X-Ascend-Session-
Svr-Key}')"
        accounting_start_query_alt = "UPDATE ${acct_table1} \
                SET AcctStartTime = ('%S'::timestamp - '%{Acct-Delay-Time:-
0}'::interval), AcctStartDelay = 0, \
                ConnectInfo_start = '%{Connect-Info}' WHERE AcctSessionId =
'%{Acct-Session-Id}' AND UserName = '%{SQL-User-Name}' \
                AND NASIPAddress = '%{NAS-IP-Address}' AND AcctStopTime IS
NULL"
        accounting_stop_query = "UPDATE ${acct_table2} \
                SET AcctStopTime = ('%S'::timestamp - '%{Acct-Delay-Time:-
0}'::interval), \
                AcctSessionTime = NULLIF('%{Acct-Session-Time}', '')::bigint, \
                AcctInputOctets = (('%{Acct-Input-Gigawords:-0}'::bigint << 32) +
'%{Acct-Input-Octets:-0}'::bigint), \
```

AcctOutputOctets = (('%{Acct-Output-Gigawords:-0}'::bigint << 32) + '%{Acct-Output-Octets:-0}'::bigint), \

AcctTerminateCause = '%{Acct-Terminate-Cause}', AcctStopDelay = 0, \

FramedIPAddress = NULLIF('%{Framed-IP-Address}', '')::inet, ConnectInfo_stop = '%{Connect-Info}' \

WHERE AcctSessionId = '%{Acct-Session-Id}' AND UserName = '%{SQL-User-Name}' \

AND NASIPAddress = '%{NAS-IP-Address}' AND AcctStopTime IS NULL"

accounting_stop_query_alt = "INSERT into ${acct_table2} \

(AcctSessionId, AcctUniqueId, UserName, Realm, NASIPAddress, NASPortId, NASPortType, AcctStartTime, AcctStopTime, \

AcctSessionTime, AcctAuthentic, ConnectInfo_stop, AcctInputOctets, AcctOutputOctets, CalledStationId, CallingStationId, \

AcctTerminateCause, ServiceType, FramedProtocol, FramedIPAddress, AcctStopDelay) \

values('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-User-Name}', '%{Realm}', '%{NAS-IP-Address}', \

'%{NAS-Port}', '%{NAS-Port-Type}', ('%S'::timestamp - '%{Acct-Delay-Time:-0}'::interval - '%{Acct-Session-Time:-0}'::interval), \

('%S'::timestamp - '%{Acct-Delay-Time:-0}'::interval), NULLIF('%{Acct-Session-Time}', '')::bigint, \

'%{Acct-Authentic}', '%{Connect-Info}', \

(('%{Acct-Input-Gigawords:-0}'::bigint << 32) + '%{Acct-Input-Octets:-0}'::bigint), \

(('%{Acct-Output-Gigawords:-0}'::bigint << 32) + '%{Acct-Output-Octets:-0}'::bigint), '%{Called-Station-Id}', \

```
                '%{Calling-Station-Id}', '%{Acct-Terminate-Cause}', '%{Service-
Type}', '%{Framed-Protocol}', \
                NULLIF('%{Framed-IP-Address}', '')::inet, 0)"
        group_membership_query = "SELECT GroupName FROM
${usergroup_table} WHERE UserName='%{SQL-User-Name}'"
        postauth_query = "INSERT INTO ${postauth_table} (username, pass, reply,
authdate) VALUES ('%{User-Name}', '%{User-Password:-Chap-Password}',
'%{reply:Packet-Type}', NOW())"
}
```

# APENDICE R

## Configuración del *access point*

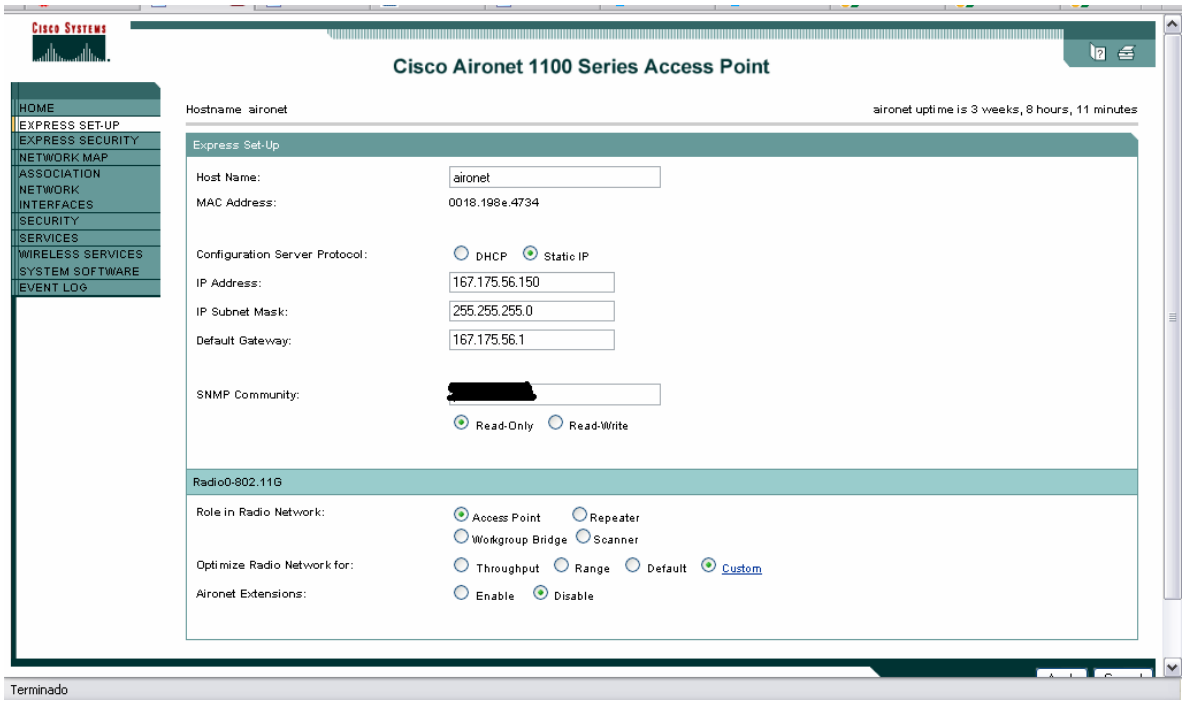



**Figura 1. Configuración de la comunidad SNMP y de la dirección IP del Access point**

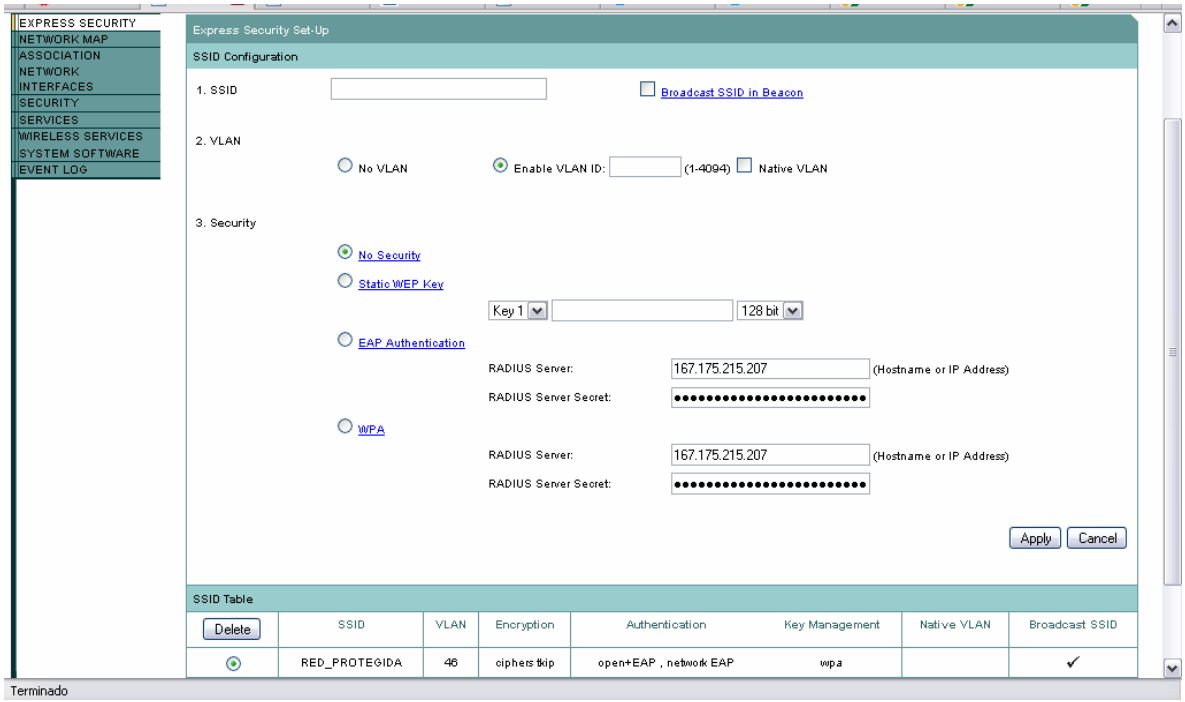


**Figura 2. Configuración del secreto compratido entre el FreeRADIUS y el access point.**

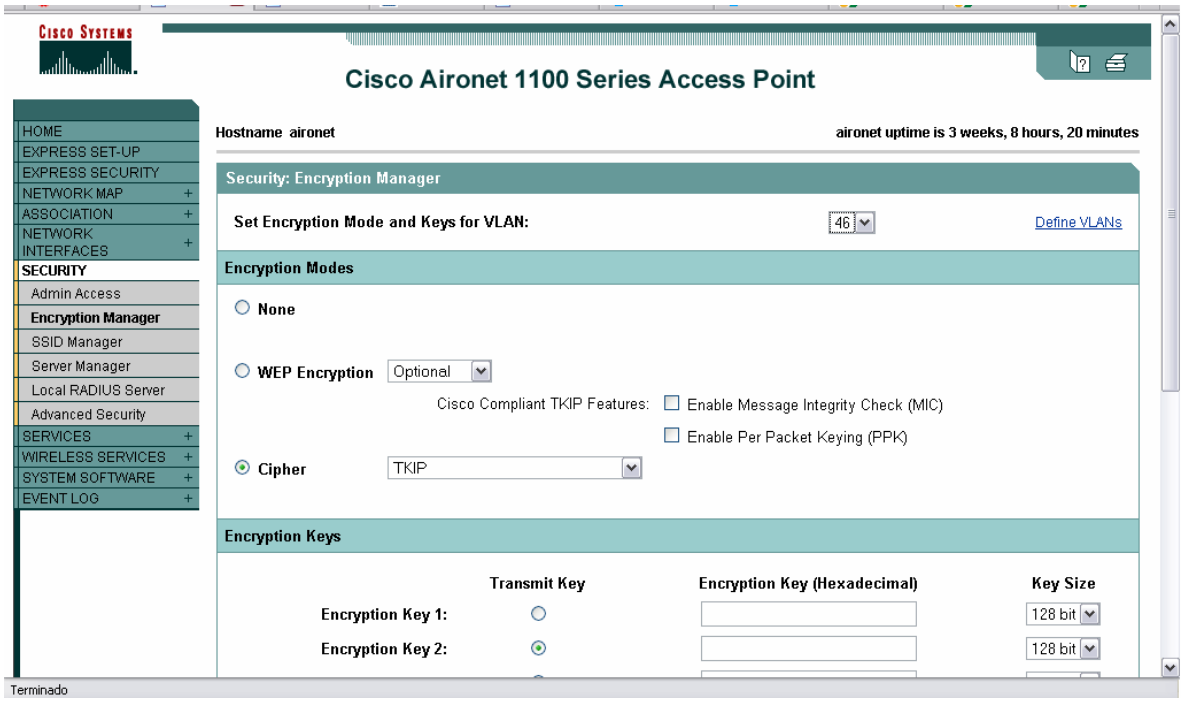



**Figura 3. Configuración del cifrado TKIP.**

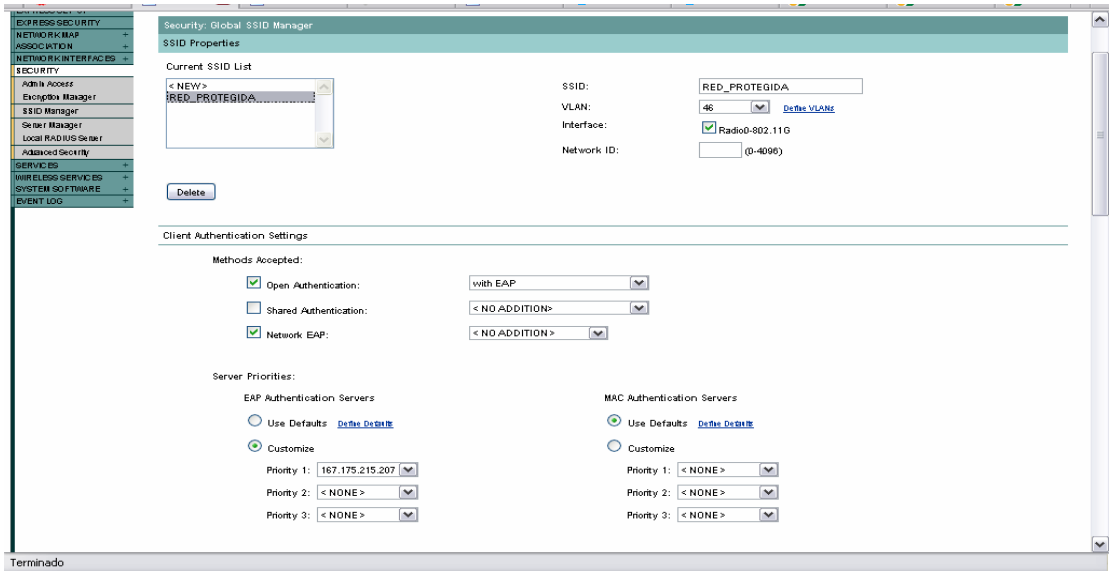


**Figura 4. Configuración del protocolo EAP.**

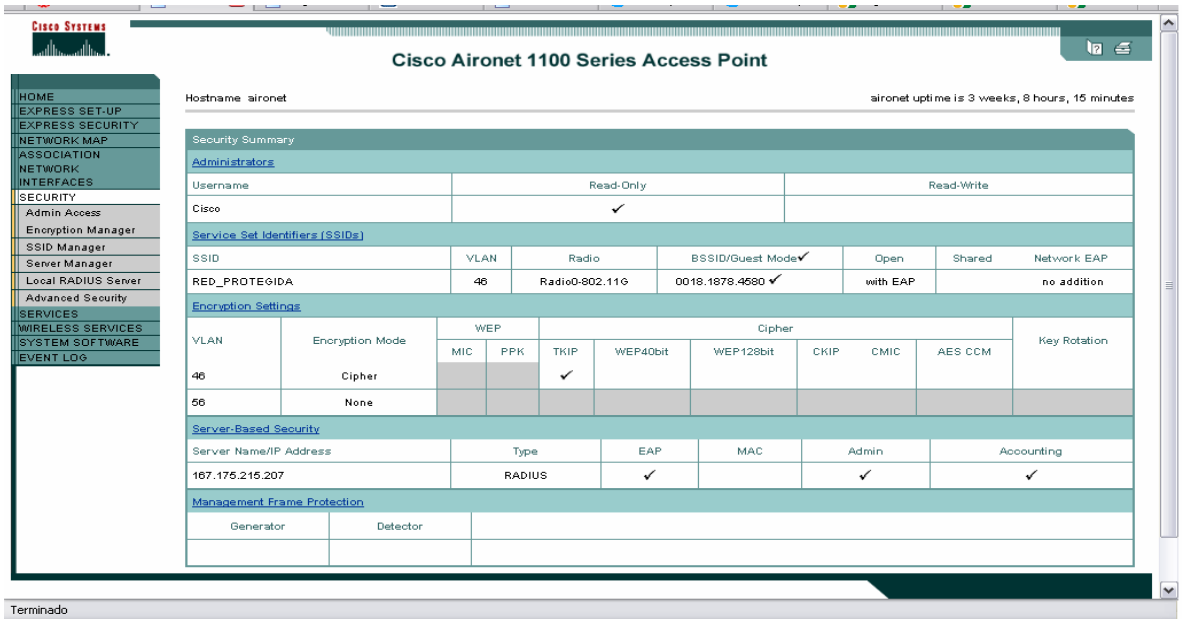



**Figura 5. Visualización del servidor de autenticación y el cifrado TKIP.**

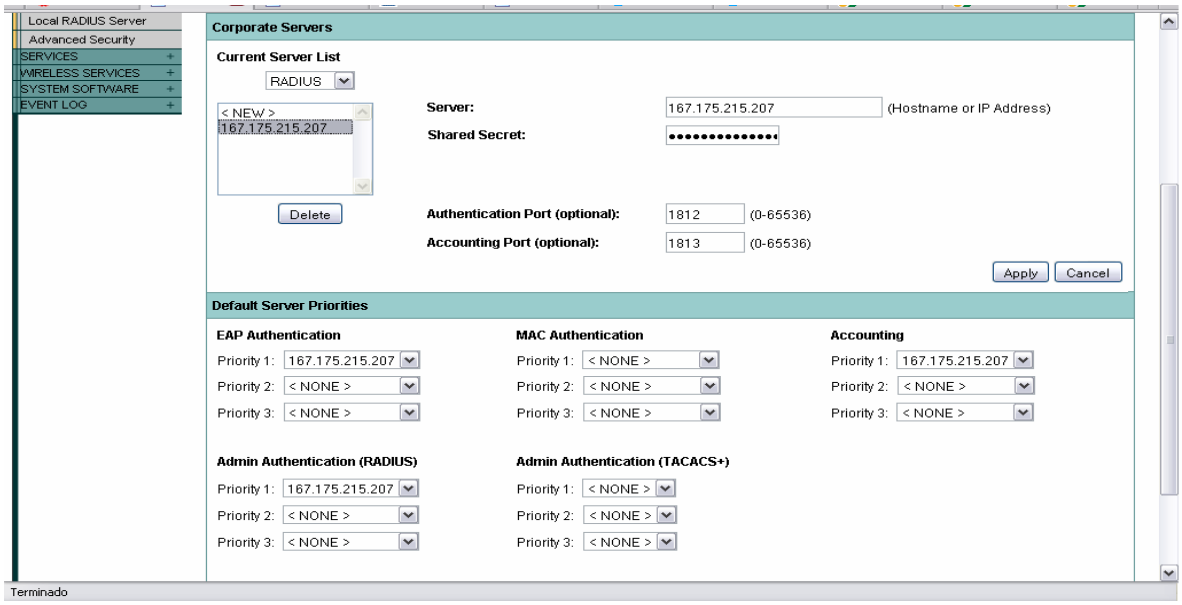



**Figura 6. Configuración de los puertos de autenticación (1812) y accounting (1813).**

## APENDICE S

**Archivo de configuración wpa_supplicant.conf del servidor FreeRADIUS.**

```
ctrl_interface=/var/run/wpa_supplicant
eapol_version=1
ap_scan=1
fast_reauth=1
network={
  ssid="RED_PROTEGIDA"
  scan_ssid=1
  proto=WPA
  key_mgmt=WPA-EAP
  pairwise=TKIP
  group=TKIP
  eap=PEAP
  identity="usuario"
  password="password"
  phase2="auth=MSCHAPV2"
}
```

## APENDICE T

## Archivo de configuración VirtualHost del servidor Web Apache.

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/
  <Directory />
     Options FollowSymLinks
     AllowOverride None
  </Directory>
  <Directory /var/www/>
     Options FollowSymLinks MultiViews
     AllowOverride None
     Order allow,deny
     allow from all
  </Directory>
  ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
  <Directory "/usr/lib/cgi-bin">
     AllowOverride None
     Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
     Order allow,deny
     Allow from all
  </Directory>
  ErrorLog /var/log/apache2/error.log
  LogLevel warn
  CustomLog /var/log/apache2/access.log combined
  Alias /doc/ "/usr/share/doc/"
  <Directory "/usr/share/doc/">
     Options Indexes MultiViews FollowSymLinks
     AllowOverride None
     Order deny,allow
     Deny from all
```

```
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>
</VirtualHost>
```

**ANEXOS**

# ANEXO 1

## Archivo Xpextensions

```
[ xpclient_ext]
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
[ xpserver_ext]
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

**ANEXO 2**

**Archivo CA.der**

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F524084FF2801EC3

/tNnWz3FQSbyXBD+Mr66JCPQyKNJ80vir6pZ7w704OEokUMJ2PmcVvZlZk9Oc
oIJ
zNfY2hHpxEGWAUryVznnCxcn8L3GZfITwUfxulnyj8BFrtnuZ7NL1/tHi+bY24Hl
T1aet9KzDGaiNFT+b5tsIVDeLZ5CCIdxx8WmZMCfIjqcfgXVOSZVqT+LQcNx+
Ori
KYtcTBZt5cPT8NosVdFCge/gcAli63HNmUvSRVMkTJZDU580Mb4DNS9rPtt5P9l
M
lLrc9P16kO3jVfjfYdkT3C4QBiHbtcSzGuQbS1RGXgJgBiC7nuTak2r0f0ABYQEd
MXoWqpAiuQLLoNdenF0tJjykqFvXkvdV95GW1alAuxuHbOoiP8L1MsrE37J7IXl
x
bcIt313HseMUj4KNZUgtKVwNFJOj7P3Fr4mbFO8kbOJxLtj/hkUYon3LJy/npqA+
FgTzpiEAYj9KyfYfLlpMMmnUBCtoLZHCc+CIPo39lvJGzAYMqvjId7rXz/y/2BsQ
LqhNkXSk5UQOWtspe+wysGeoHvLolnrRMQPvG/Yyj+xLecvphp1GIKBh6MAmb
OcU
lQviAMybk/koJ39OYdOyvxISVyT2N+cFiq/14CfiEM+KDcH+lnLRhLdkwncznlz/
8PJW6zxDJYvqscT7Z3iBIe426lpIUPi1PXhu5ATJwEGbRkeiZmyFgxzt6JOkIv/C
SgRtJ4MarnDRC/mhNrh/MvzRNTq6itAsP6Y+n+Lgqn/4aQTI1o0mSjSkCHu+Czmz
OxesmY3Vr0Hu9jOl6qUlJZRCFIp3roP05zmZU8x/Osk2rVxYwWSAlViFt181YaCs
8cnhaoQdLe06XgSa9PeD2QDoqUaJqtLbi+JLCvO5+B4ju12B6v2YRJcOTE7O5Ik0
K78eptepK0mtGhgOUZcnwZ59qh24j9NIOAdMA+klYw3Qd2dlUKr9vfZ4a+QJCN
Ni
DIF/x2A9WG/KQqqBKf+lVEvjyXfzhWx2CY5j1Q8EK4PHwz/WGO/QFJTqklJsr+1
s
Vk8jIDnDNwnvOTXr7/Z/nXgj3ncsBHw4Ftw3zm1d7D2J7ATJ26e6dFd0vIFLQB3v
kHmu+51euDKBocjlywwT+Pl5ZFSexv7ORgbiITCd6vczAkN47rmofx84b1Ibl+sA
kC8qmWLsmDMrfmYr19u4vSw7fb3OYH5EV8wwOLEq3283iB1gtrXiQtHtr4Mw
tq566xuAZ3tq9tQpH9sA8kaUQbmbrFdYcCRHgKP+gQZGdZsCLXdYZI/rUnut3LI
C
7E59JgsKEw7ZBh2ciyyTgaSX+84g4RhgV/af56XuxJ4z4GqImwbZiFaCW9WBdw
mM
EUq1eltHMnEApCOlh2zmuIA60Nh3bLJVqMJaoGlujfa277HVxQWOD2dWTwU7
qiyiMcWU+d0mkNhP0yVpxsSl5RH07sfPbuF9NnZjwoNlsbD2NNUbAG8vyvWOZ
HRp
WrHoM19Bxoypzna9LvGbm99OI+JYMDn9Mzj55OYq1EkmPmWdVlyNTdwQTA
LmpDOs
Y00CyvVMF+kqOSHJxG+qiGCnyiycRHu5xSTkx956dwkyERuOqIuQddoYXdjlc9
Us
-----END RSA PRIVATE KEY-----
```

**ANEXO 3**

**Archivo CA.key**

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIJAPkw+SzKs3Q1MA0GCSqGSIb3DQEBBQUAMIGhM
QswCQYDVQQG
EwJWRTEQMA4GA1UECBMHTUFUVVJJTjEOMAwGA1UEBxMFUERWU0Ex
HjAcBgNVBAoTFVNFR
1VSSURBRCBBSVQgT1JJRU5URTEoMCYGCSqGSIb3DQEJARYZc2VndX
JpZGFkYWl0b3
JpQHBkdnNhLmNvbTEmMCQGA1UEAxMdQVVUT1JJREFEIENFUlRJRklDQU
RPUk
EgUERWU0EwHhcNMDkxMDIwMTk0MTA0WhcNMTAxMDIwMTk0MTA0Wj
CBoTEL
MAkGA1UEBhMCVkUxEDAOBgNVBAgTB01BVFVSSU4xDjAMBgNVBAcTB
VBEVlNBMR4w
HAYDVQQKExVTRUdVUklEQUQgQUlUIE9SSUVOVEUxKDAmBgkqhkiG9w0
BCQEWGXNl
Z3VyaWRhZGFpdG9yaUBwZHZzYS5jb20xJjAkBgNVBAMTHUFVVE9SSURBR
CBDRVJSUZJQ0FET1JBIFBEVlNBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA7XJ4wBLq00U+bohhUjqL1TEg3lBJdKPro9kyd6VMPnPpy4OnI
HuQB6X8PFoeAh1z
18lB3POL0PE3eDH9SrR1wJp+tSjYcLMeTLTamSk21fBsWjMsmtFPY1SSH7Tfm
G6YvnzpBNteheMehpGxZG7J4k8VbeFmIJT4LRYWZ//2kF/q9Z3zW47v/RWSO0q
ePliBhlUveKXbwHIoz9voe+5Ogm2SsZHGwGBEh2T3IhS3ZfuILP2nSe/9SjDmHV
QLyYyViL0HVzrNfhLqKpao2KK+4k2HpH89YubRARl/4qAREq31x7ABsr+nOIw
Mf92zSNh+jo1CBSFhW0W0EPTWMGYY9wIDAQABo4IBCjCCAQYwHQYDVR
0OBBYEFOISqDaJgKj2
agCq2amHQcBCa39vMIHWBgNVHSMEgc4wgcuAFOISqDaJgKj2agCq2amHQcB
Ca39oYGnpIGkMIGhMQswCQYDVQQGEwJWRTEQMA4GA1UECBMHTUFUV
VJJTjEOMAwGA1UE
BxMFUERWU0ExHjAcBgNVBAoTFVNFR1VSSURBRCBBSVQgT1JJRU5URTE
oMCYGCSqG
SIb3DQEJARYZc2VndXJpZGFkYWl0b3JpQHBkdnNhLmNvbTEmMCQGA1UEA
xMdQVVUT1JJREFEIENFUlRJRklDQURPUkEgUERWU0GCCQD5MPksyrN0NT
AMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBBQUAA4IBAQDLR3oMYRDZ4uTfGa+CPjjVBdfY8
iQI1NlRAJqM9Zht7+rk/6u4Uy0kgNGpSo4HxIpjsy2DiabhrdfhQ6gHQhyPRoOxrXv
cZooG
YzSRhBLjGFxWQbelbiO5b0TpPys40g0fzXVyRfTU+4n8p1qWqnQjwVBnWcSwA
zeu3c0GpX+ZTu4fjC7cjToROIA5vE2pgwjXeNk0RnFs08voMYN+AXyfFguiXBaln
gQW
POuIDCV3dYBPPwnsmE1FFSsLPRu8v3hbzde7Nzo1w9pYctzg6c9BlhZbB6bW0b
HW6SFUEj5NNTo+aVogID97bR2jwCrWiBXZV1CjY1ey7vcR7/17CEZr
-----END CERTIFICATE-----

**ANEXO 4**

**Archivo CA.pem**

Bag Attributes
localKeyID: 64 E4 76 2C 7C 18 3E F1 70 A8 C5 F6 C0 F5 E7 6B 4B DC D4 2D
subject=/C=VE/ST=MATURIN/O=SEGURIDAD AIT ORIENTE/CN=CERTFICADO SERVIDOR RADIUS/emailAddress=seguridadaitori@pdvsa.com
issuer=/C=VE/ST=MATURIN/L=PDVSA/O=SEGURIDAD AIT ORIENTE/emailAddress=seguridadaitori@pdvsa.com/CN=AUTORIDAD CERTIFICADORA PDVSA
-----BEGIN CERTIFICATE-----
MIIDwzCCAqugAwIBAgIBATANBgkqhkiG9w0BAQQFADCBoTELMAkGA1UEBhMCVkUx
EDAOBgNVBAgTB01BVFVSSU4xDjAMBgNVBAcTBVBEVlNBMR4wHAYDVQQKExVTRUdV
UklEQUQgQUlUIE9SSUVOVEUxKDAmBgkqhkiG9w0BCQEWGXNlZ3VyaWRhZGFpdG9y
aUBwZHZzYS5jb20xJjAkBgNVBAMTHUFVVE9SSURBRCBDRVJUSUZJQ0FET1JBIFBE
VlNBMB4XDTA5MTAyMDE5NDEzMFoXDTEwMTAyMDE5NDEzMFowgY4xCzAJBgNVBAYT
AlZFMRAwDgYDVQQIEwdNQVRVUklOMR4wHAYDVQQKExVTRUdVUklEQUQgQUlUIE9S
SUVOVEUxIzAhBgNVBAMTGkNFUlRGSUNBRE8gU0VSVklET1IgUkFESVVTMSgwJgYJ
KoZIhvcNAQkBFhlzZWd1cmlkYWRhaXRvcmlAcGR2c2EuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqf+XqFhx8Wr1I/nzW1E3AufKk8oGU/MmCtra
OYUaOP8zD3CDDxuiozvWIUKx+kiDuMApb8sz1mTbBL0VanQbVIpUGiU3qJYU0WgA
2JxyY2VGX9CA1YMjt296KRVBLmqCKLTEu/ouIpasOHcFWIitGzRA+1aNQzxRi9Nl
Ob0iWn3lnbUWYLY2r4KZySqAWhl0+W7t/j9E1paddUFr8fhf3IU52u2i6705rToV
8AOB1yy4oQmqRl3HdKAc/+5m6zFmt/+3RsbkAzLQUI7oHu6X4LZGW3Asw7U13vHX
K2CWoTZksAtW4b+EJqkWo+Qy8hQ95HpDfHePPPPoxI6Xp5mUKwIDAQABoxcwFTAT
BgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQQFAAOCAQEAy1REPBGbzFNH
1tVa2+WZm9PV4wib9JzW1s0zvzw1gRA0LAXPDkOHsnnZxs7NIQJAnqrF1EcN8ObT
Gt/LzVYs3aezOIYMdVTByTzEhDgoWZ4kAaaBICD+xzr3bKMdQtdklMdsQwYTJpXC

hKZth+GV5QOhEE9gBMz+QdWranQ9VcUPtWgBajtNjmh7NPFFmjdNna3GDIT4
Eqe0
/dPH7yn5i4SwicYuedrx1N6nJjBuPQhycUML6SSNLbvvsKDqyO0mLLEiuHvUA7
MB
lgR+M95kjXkv+R0Mr7LKDnT+mV/Pv937k5I19O4Pc0vC/mklgn3SElAVGmWDm
oy9
0+WMS5hv+Q==
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 64 E4 76 2C 7C 18 3E F1 70 A8 C5 F6 C0 F5 E7 6B 4B DC D4 2D
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,AA5FF17446FBF17A
KZUAK58iinr4rEKDSmFb3J11ICc2Q0T5lEVSlEHABZBEJAQB4/8SXrAcLX8Ku
78S
IL7KWN4IsgSh9FkMmxoPHEiG8pfxol+YDds0vAfjFRymD+Usqe0KWEL3E3wrR
+Ku
Um0UX93dsXA5YbLdPUnFYZ3Qka22MMLmcN5qSaMVPBoVszanHQSgpK6eG
gxovYvg
Crw5ulTTWx3JT0mwKjSPFR3ObGg6nDvKlVAd841kVi+1tn/ZJbS0sW42S9UkPk
W1
RUww34lIGKmrJBH1V4sAWFBkyq0mJEGCI4ievxh77V6pJ4KQYsbrtiMgBuUea/c
h
xbg7rIeQczshr0axreOP0ZBNyfLDZRTfsr0K/ZKY+jUw2RBd5QO2y37DDgji9IAp
alTzrnrBx6wb22PIA2DJAZqmz2LlCZg3g6wTqajhAGAWiDIXySRR8ExhA1yiCSC
8
Z9YtvxfCeeR7HXEMbPKypbrro/bPYm+nw1oK+vfMdpGeBrID2RXvtUUAMffKw
ECb
BBCgg4n6K3ELyQ7Xc+JKQiVwzc7tU/xkIY9RQnek/h5JBwms2lZnpPi2Zy/98MIZ
RQl+ikMLBYHzA3Mmcogv7px5ohxYVQArfcPxklSIJV30hohCmgulsQo/xf2Yfuui
Bh9CgG9h6ENdKEM7cyDyWJTmhz/P7+JKW/xEn3jVbgaPJGUHwdAUp/QRPrLZ
IG9G
06Ams18Ro8oig8q29hs7GO3wWEhmpX26EQ6FQJ5zdyty/V0FcNwKnbvuGJeApa
VC
RG5nF016k40SetEWKXm/yRDOP/0wE14sHn70iPHZe45Q5KTyzXF/mTJBboy0H
Cza
gBbfhJxdBXebMasRM3htUPCSwUP9q1g9kovEhFwrlK0uQsRlQ0QsYBVo/LGonc
da
SzjLS1Kg0Wr2dgLKGEyZwCqRIE8Cy8pvVZo61Go2+jxyDkhS9YmlmFTcGJ8G
WLrA
KhPGhOFekhDUeayURV2epu/0HRvbfmhGRV77EwOeImonyGkpsilB5e73a41eifs7

/dNFGoH29YAJCdhtZDmFu+Rufvts3OztXLDZuSN4VZQ3xZP7F8TUaWrpUUmP
DE9KlmJL0iJJRxbxPGHhy+CK6aFFhNm66HgeaEa7aruQQiAVuP+cPb7w
5WMO4C+2jpc8KQgHmv3qqBEkRYdYWG8kBfdnGI9WheJdDys/AXYpalUX6Kz
2mOoV
ekGvfaZe5BBq6IBYSr0J8Wm4KhDthO2HuUELBJYJ0SadAbFo3Jq82NTEJLeSf/d
R
53st7FBoWfAB/OUa714loPP92QxJy0znSZvH4WcVsdMoTqD2/KV8njuUM2xnH+
xv
96DT/czaENWJF8ZbRHV7T3jzy/Ziz1pAPT6Qoh1Y1NQ6DD3rIQk/zeV/ZZampYB
o
TWFtGzeAAqLkrlnPEsXlYfRoJgjt2vEGYFhd6irdMhfKYSiU0JeXtg==
-----END RSA PRIVATE KEY-----

# Hoja de Metadatos

# Hoja de Metadatos para Tesis y Trabajos de Ascenso – 1/5

| | |
|---|---|
| **Título** | IMPLEMENTACIÓN DE LA ARQUITECTURA DE CONTROL DE ACCESO BASADA EN EL ESTÁNDAR DE SEGURIDAD IEEE 802.1X PARA LA RED ETHERNET DE PETRÓLEOS DE VENEZUELA SOCIEDAD ANÓNIMA, UBICADA EN EL EDIFICIO ESEM, MATURÍN, ESTADO MONAGAS |
| **Subtítulo** | |

**Autor(es)**

| Apellidos y Nombres | Código CVLAC / e-mail | |
|---|---|---|
| **Migdalis del Valle. Mago R.** | **CVLAC** | |
| | **e-mail** | **Migdalis.mago@gmail.com** |
| | **e-mail** | |
| | **CVLAC** | |
| | **e-mail** | |
| | **e-mail** | |
| | **CVLAC** | |
| | **e-mail** | |
| | **e-mail** | |

| | | |
|---|---|---|
| | **CVLAC** | |
| | **e-mail** | |
| | **e-mail** | |

**Palabras o frases claves:**

| |
|---|
| **Control de acceso, IEEE 802.1x, Servidor AAA.** |
| |
| |
| |
| |
| |
| |
| |
| |

# Hoja de Metadatos para Tesis y Trabajos de Ascenso – 2/5

**Líneas y sublíneas de investigación:**

| Área | Subárea |
|---|---|
| **Ciencias Aplicadas** | **INFORMÁTICA.** |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**Resumen (abstract):**

Mediante la ejecución del presente Trabajo de Grado, se logró la implementación de una arquitectura de control de acceso basada en el estándar IEEE 802.1x para la red *Ethernet* de Petróleos de Venezuela, Sociedad Anónima (PDVSA), ubicada en el edificio ESEM de la ciudad de Maturín. La metodología de investigación utilizada fue un híbrido, compuesto por algunos métodos utilizados por James McCabe, (1998), Manuel Sánchez, (2003) e INTEL *Corporation*, (2003); quedando comprendida por cinco (5) fases: determinación de los requerimientos, análisis de las tecnologías, diseño de la arquitectura de control de acceso, ejecución del diseño y pruebas de la arquitectura. Mediante la determinación de los requerimientos se emplearon entrevistas a los usuarios y observación directa de los hechos, con la finalidad de identificar los problemas presentes y visualizar las posibles mejoras; en la fase de análisis de las tecnologías, se procedió a seleccionar entre varias alternativas existentes, el mecanismo de autenticación y autorización, el protocolo de autenticación, el mecanismo de cifrado, y el servidor de autenticación, tomando en cuenta diversos aspectos de seguridad en la red y los requerimientos emitidos por la Gerencia de Seguridad Lógica de PDVSA; en la siguiente fase, se realizó el diseño de la arquitectura de control de acceso, mediante el uso del Lenguaje Unificado de Modelado; seguidamente se procedió con la ejecución del diseño, mediante la instalación y configuración de todos los elementos que intervienen en la arquitectura y finalmente la realización de pruebas de conexión y autenticación tanto en la red cableada como en la red inalámbrica. Esta arquitectura de seguridad, permitió controlar el acceso lógico a los recursos de la red de PDVSA, a través de un proceso de autenticación que permite validar las credenciales que son enviadas al servidor de autenticación, siendo éste el encargado de aceptar o denegar el acceso; con el fin de evitar la manipulación directa de información confidencial de PDVSA a terceros, de igual forma se evita que un dispositivo de un tercero pueda conectarse a la red y propicie ataques maliciosos.

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 3/5

**Contribuidores:**

| Apellidos y Nombres | ROL / Código CVLAC / e-mail | |
|---|---|---|
| **Daniel Geremias.** | **ROL** | **CA** [ ] **AS** [X] **TU** [ ] **JU** [ ] |
| | **CVLAC** | |
| | **e-mail** | **geremiada@hotmail.com** |
| | **e-mail** | |
| **Aníbal Vera** | **ROL** | **CA** [ ] **AS** [X] **TU** [ ] **JU** [ ] |
| | **CVLAC** | |
| | **e-mail** | **veraaq@pdvsa.com** |
| | **e-mail** | |
| **José Sifontes** | **ROL** | **CA** [ ] **AS** [ ] **TU** [ ] **JU** [X] |

| | | |
|---|---|---|
| | CVLAC | |
| | e-mail | jasinfontes@yahoo.com |
| | e-mail | |
| Carmelys Rodríguez | ROL | CA [ ] AS [ ] TU [ ] JU [X] |
| | CVLAC | |
| | e-mail | carmelysrodriguez@gmail.com |
| | e-mail | |

**Fecha de discusión y aprobación:**

| Año | Mes | Día |
|---|---|---|
| 2010 | 08 | 05 |

**Lenguaje:** spa

# Hoja de Metadatos para Tesis y Trabajos de Ascenso – 4/5

**Archivo(s):**

| Nombre de archivo | Tipo MIME |
|---|---|
| **Tesis_migdalis.doc** | **Aplication / Word** |
| | |
| | |
| | |
| | |
| | |

**Alcance:**

**Espacial :** _____ (Opcional)

**Temporal:** _____ (Opcional)

**Título o Grado asociado con el trabajo:** Licenciatura en Informática.

**Nivel Asociado con el Trabajo:** Pregrado.

## Área de Estudio:

Ciencias Aplicadas.

## Institución(es) que garantiza(n) el Título o grado:

Universidad de Oriente Núcleo de Sucre.

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 5/5

**Derechos:**
**Yo Migdalis Mago como autora intelectual de esta tesis le doy el derecho a la Universidad de Oriente para divulgar esta tesis siempre y cuando resguardando la patente de industria y comercio si se diera el caso**

**AUTOR**

**TUTOR** **JURADO 1** **JURADO 2**

**POR LA COMISIÓN DE TRABAJO DE GRADO:**