DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED SEGURA CON UN SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS

JOSUE LOBO CONTRERAS
RAFAEL SANDOVAL MORALES

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2013

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED SEGURA CON UN SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS

JOSUE LOBO CONTRERAS
RAFAEL SANDOVAL MORALES

Trabajo de grado para optar el título de
Especialista en Seguridad Informática

Director:
Esp. César Iván Rodríguez Sánchez

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2013

Nota de aceptación

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá, D.C. 2 de Octubre de 2013

DEDICATORIAS

Dedico este trabajo de grado, en primer lugar a Dios y a la virgen de Torcoroma, por regalarme el más valioso detalle, la vida. Gracias por el inmenso amor e incondicional compañía, por haberme dado la paciencia, la fe, la fortaleza, la sabiduría, la salud y concederme este gran logró que colma mi corazón de alegría y felicidad.

A mis padres EDUARDO LUIS LOBO AMAYA y ARGENIDA CONTRERAS SUAREZ que gracias a su compañía excepcional e incondicional y a sus innumerables consejos, me han enseñado el verdadero valor de la vida. Seres maravillosos que día tras día luchan por darme lo mejor y moldearme como una persona que refleje sus sueños.

A mi tía SUGEIDY CONTRERAS SUAREZ que además de ser como mi segunda madre, ha sido mi amiga y compañera incondicional, gracias por todo su apoyo y sus consejos eres un ejemplo a seguir, todo lo que se quiere se puede.

A mis abuelos, LUBIN LOBO QUINTERO y MARGARITA AMAYA VERGEL, ROBERTO CONTRERAS ALFONSO y ROSALIA SUAREZ PAEZ, Que hoy no están conmigo pero que dejaron huellas imborrables en mi corazón.

A mi hermanita, MARGARITA ROSA LOBO CONTRERAS, que es un regalo de DIOS, gracias por hacerme sonreír día tras día, que aunque a veces la regaño y pasamos malos ratos, la quiero mucho.

A toda mi familia que siempre ha estado conmigo, brindándome su apoyo en los buenos y malos momentos, regalándome momentos de alegría, su inmenso cariño, sus significativos consejos y sus experiencias que tanto me gusta escuchar.

Josue Lobo Contreras

Esta tesis se la dedico a mi DIOS quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mis padres HERCILIA HORTENCIA MORALES DE SANDOVAL y RAFAEL SANDOVAL ESPEJO por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos. *Hoy les quiero decir nuevamente, que soy lo que soy como persona y profesionalmente únicamente por ustedes.*

A mi amada esposa MÓNICA CRISTINA ORTIZ TABARES, que ha estado a mi lado dándome cariño, amor, confianza y apoyo incondicional para seguir adelante para cumplir otra etapa en mi vida.

A mis hijos RAFAEL AUGUSTO SANDOVAL ORTIZ y SAMUEL JOSÉ SANDOVAL ORTIZ, que son el motivo y la razón que me ha llevado a seguir superándome día a día, para alcanzar mis más apreciados ideales de superación, ellos fueron quienes en los momentos más difíciles me dieron su amor y compresión para poderlos superar, quiero también dejar a cada uno de ellos una enseñanza que cuando se quiere alcanzar algo en la vida, no hay tiempo ni obstáculo que lo impida para poderlo LOGRAR.

A toda mi FAMILIA que es la joya más preciada que uno puede tener, sin la familia uno no puede conseguir la fuerza necesaria para lograr las metas propuestas. Los AMO.

Rafael Sandoval Morales

"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar"
Thomas Chalmers

AGRADECIMIENTOS

A DIOS y a la virgen de Torcoroma por ser parte de mi vida y guiarme por el sendero del bien.

A César Iván Rodríguez Sánchez, por ser el asesor del presente trabajo de grado. Gracias por su apoyo incondicional en la realización de esta investigación, por sus consejos, sugerencias, mi respeto y admiración para él.

A Orlando Gómez Quintero, gracias por confiar en mí y haberme dado la oportunidad de cursar el presente postgrado en tan prestigiosa institución.

A la facultad de Ingenierías, especialmente al plan de estudios de la Especialización en Seguridad Informática, gracias por aceptarme como estudiante y por la formación recibida durante el proceso de enseñanza, que es base fundamental para alcanzar esta meta.

A los profesores por compartir su conocimiento conmigo.

A la UNIVERSIDAD PILOTO DE COLOMBIA, por darme la oportunidad de estudiar mi Postgrado en Seguridad Informática y haber contribuido a mi conocimiento durante el proceso de enseñanza, me enorgullezco de ser parte de esta Institución, muchas gracias por apoyarme.

A mis amigos y demás personas que en algún momento de su vida han compartido su tiempo conmigo y han dejado su aporte para mi crecimiento personal y profesional.

A todos los docentes de la Especialización en Seguridad Informática de la Universidad Piloto de Colombia.

Josue Lobo Contreras

El presente trabajo de tesis primeramente me gustaría agradecerte a ti DIOS por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado.

A mi mamá y mi papá, por contar con su apoyo de forma incondicional y darme palabras de aliento para alcanzar mis metas propuestas, Los Amo.

A mi amada Esposa, por su amor y apoyo incondicional en todos los momentos de mi vida, Te amo.

A mis Hijos, que son el motivo y la razón que me ha llevado a seguir superándome día a día, Los Amo.

A la UNIVERSIDAD PILOTO DE COLOMBIA por darme la oportunidad de estudiar mi Postgrado en Seguridad Informática.

Al Ing. César Iván Rodríguez Sánchez, director de tesis, por su valiosa guía y asesoramiento a la realización de la misma.

A todos los docentes de la Especialización en Seguridad Informática de la Universidad Piloto de Colombia.

Rafael Sandoval Morales

REFLEXIÓN

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados"

Gene Spafford

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores"

Kevin Mitnick

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

Bruce Schneier

RESUMEN EJECUTIVO

El presente proyecto se fundamenta en el diseño e implementación de una infraestructura red segura LAN (Local Area Ne.|++- twork) y WLAN (Wireless Local Area Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting). El primer paso fue analizar y determinar que la red LAN actual de Unisys de Colombia una red LAN utiliza el servicio de PortChannel[1] y Hot Stand-by Redundancy Protocol[2] (HSRP) también conocido como Protocolo de Redundancia para equipos de Comunicación para optimizar el uso de recursos de la red. Luego se implementó el servidor ACS (Access Control Server) que utiliza el protocolo TACACS+ para centralizar todo el acceso de los administradores y usuarios de lectura a los equipos de la red. En lo que compete a las redes WLAN, se instaló e implementó el servidor de Microsoft IAS en plataforma Windows 2003 Server, luego se verificó que el punto de acceso inalámbrico (Access Point - AP) cumpla con el estándar de autenticación IEEE 802.1x[3] que se usó como intermediario entre la capa de acceso (L2) y el algoritmo de autenticación, finalmente se configuró con el mecanismo de autenticación WPA-Enterprise y WPA2-Enterprise.

El primer capítulo especifica la Infraestructura Tecnológica que utilizó en la implementación de la solución expuesta y toda su evolución tecnológica para llegar a esta.

El estudio del arte se hizo de manera separada para la red LAN y para la red WLAN porque al tratarse de redes de conexiones diferentes, cada una tiene definida de forma independiente métodos y estándares de seguridad para su acceso a la red.

El segundo capítulo proyecta el estudio del problema y se dispuso un escenario real en UNISYS de Colombia con el fin de especificar los requerimientos necesarios a utilizar dentro de la empresa, la cual requiere una solución de una red LAN y WLAN que garantice la seguridad de la información y el uso adecuado de los recursos de la red teniendo en cuenta los roles y responsabilidades de cada uno de los miembros de Red.

El tercer capítulo se diseñó la solución de la implementación, realizando un análisis de vulnerabilidades de los requerimientos propuestos en el segundo

[1] Cisco System. Trabajo sin fronteras. Disponible en http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/EtherChannel.html

[2] Cisco System. Soluciones de red. Disponible en http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml

[3] Microsoft Corporation. Disponible en http://windows.microsoft.com/es-co/windows-vista/enable-802-1x-authentication

capítulo del proyecto. Una vez terminado el análisis de vulnerabilidades se decidió cuáles de los métodos y estándares estudiados en la fase uno se usaría en la implementación real.

El cuarto capítulo muestra cada uno de los resultados obtenidos, como también el análisis de la implementación de la solución diseñada con la red operativa de Unisys de Colombia[4].

El quinto capítulo se realiza el análisis financiero para medir la rentabilidad del proyecto.

[4] Unisys Corporation. (Mayo, 2013). Disponible en http://www.unisys.com/unisys/home.jsp

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCIÓN

Actualmente los avances tecnológicos de comunicación han desarrollado nuevas formas de conectividad al mundo exterior conocido hoy en día como la Internet. Teniendo en cuenta lo anterior, se hace más dispendioso a los seres humanos del planeta mundo estar a la par de las infraestructuras tecnológicas dentro de nuestras empresas, tanto para la red cableada como en la red inalámbrica. Debido al incremento tecnológico, muchas de las empresa en nuestro medio laboral no tienen en cuenta que los nuevos avances de infraestructura presentan vulnerabilidades de acceso no autorizado, por lo que es necesario la implementación de sistemas de control de acceso a la red que nos permita asegurar el método CID (Confidencialidad, Integridad y Disponibilidad) de nuestra información más confiable de posibles ataques de personas ajenas a ella mediante métodos de suplantación de identidad, lo cual conllevaría a perdida de Información confidencial de nuestra empresa. Para mitigar todo lo anterior, existen protocolos, estándares y equipos de comunicación que nos permiten diseñar e implementar soluciones de seguridad más robustas.

El presente proyecto de grado busca diseñar e implementar una infraestructura de red LAN, WLAN segura que sea capaz de evitar la suplantación de credenciales de acceso; así como afinar el hueco entre una red cableada y una red inalámbrica, en términos de seguridad. Además de optimizar los recursos de la red usando PortChannel y el protocolo HSRP como mecanismos de redundancia y control de tráfico de los datos.

Un sistema de control de acceso basado en el protocolo AAA[5] (Authentication, Authorization and Accounting) se implementó haciendo uso de los protocolos RADIUS y TACACS+, ambos protocolos son del tipo cliente/servidor. El servidor RADIUS tiene la función de autenticar y controlar a los usuarios que accedan a la red inalámbrica mientras que el servidor TACACS+ tendrá la función de administrar los perfiles de los administradores de red y registrar sus eventos de forma controlada, mediante su base de datos local. Para lograr un acceso controlado y seguro a la red inalámbrica se utilizó el estándar IEEE 802.11i (RSN, Robust Security Network) que se basa en encriptación AES (Advanced Encryption Standard)[6], TKIP (Temporal Key Integrity Protocol)[7] y el mecanismo de autenticación WPA-Enterprise como también WPA2-Enterprise.

[5] En seguridad informática, el significado de **AAA** corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting). La expresión *protocolo AAA* no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los *tres servicios citados*.

[6] AES ofrece un nivel más alto de seguridad y está aprobado para uso del gobierno, sino que requiere una actualización de hardware para la implementación. Como organizaciones de remplazar los antiguos equipos inalámbricos, AES se espera para convertirse en el estándar de cifrado aceptado para la seguridad de WLAN.

1. DISEÑO E IMPLEMENCIÓN DE UNA INFRAESTRUCTURA DE RED SEGURA CON UN SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS

1.1 PLANTEAMIENTO DEL PROBLEMA

Los sistemas informáticos se han convertido en una parte fundamental de las organizaciones a nivel mundial, ya que permiten gestionar y manejar la información de una manera ágil y eficaz. Las compañías soportan sus procesos bajos redes de comunicaciones ya que ayuden a garantizar el aumento de la productividad y la facilidad de acceso a la información por los usuarios.

En relación a la información confidencial que se maneja en las compañías, los recursos tecnológicos están expuestos a ser accedidos por personas ajenas, que buscan sustraer, modificar o eliminar información con la finalidad de comprometer la seguridad; Estas personas emplean diversas técnicas para obtener accesos no autorizados a los sistemas y tomar el control de los mismos con fines personales o de terceros.

Debido a la falta de controles de seguridad en las infraestructuras de redes tecnológicas, se generan eventos indeseados que pretenden atentar contra la integridad de la información, por lo que se determina que si una persona ilegitima accede a la red empresarial, la información que circula a través de la misma, se ve comprometida la mayoría de las veces por los atacantes.

El no controlar estos eventos maliciosos, donde la información confidencial es accedida por terceros, puede generar desde pérdidas de la misma información, hasta pérdidas económicas que conllevan a bajar la reputación de la compañía. Desde este punto de vista, se deben implementar controles de autorización y autenticación en donde los sistemas reconozcan los usuarios de la compañía y se establezcan relaciones de confianzas entre sistemas. Por lo tanto, que en el momento que una persona quiera acceder a recursos que no esté autorizada, se rechace la conexión y además, se registren alertas de seguridad que indiquen que se están generando eventos indeseados que pretenden atentar contra la integridad de la información empresarial.

En relación a las consideraciones anteriormente planteadas, se genera el siguiente cuestionamiento: ¿Cómo garantizar la confidencialidad e integridad de la información empresarial implementando mecanismos de seguridad criptográfica

[7] TKIP es útil para mejorar la seguridad en los dispositivos equipados originalmente con WEP, no se ocupa de todos los problemas de seguridad que enfrentan las redes WLAN y pueden no ser confiables o suficientemente eficiente para la transmisión confidencial de la empresa.

para mitigar accesos no autorizados a la red corporativa del NOC de UNISYS de Colombia?

1.2 OBJETIVOS

1.2.1 **General.** Diseñar e implementar una infraestructura de red segura con un servidor de autenticación AAA basado en el protocolo TACACS, para mejorar el control de acceso a los recursos tecnológicos y aumentar los niveles de seguridad en la red corporativa.

1.2.2 Objetivos específicos

- Documentar y recopilar información acerca del estado del arte sobre servidores de autenticación AAA basados en el protocolo TACACS.
- Estudiar los protocolos de autenticación TACACS y AAA enfocados hacía las herramientas de criptográficas empleadas por los mismos.
- Realizar un análisis de riesgos de la red del NOC de UNISYS
- Implementar y configurar el servidor de autenticación AAA basado en el protocolo TACACS en el NOC de UNISYS para el control de acceso de los usuarios.
- Evaluar la efectividad de los controles implementados para mitigar los riesgos identificados en la red del NOC de UNISYS.
- Realizar un análisis financiero para medir la rentabilidad del proyecto

1.3 JUSTIFICACIÓN

La seguridad informática es una ciencia en relación a la tecnología, que nace con el fin de proporcionar directrices y buenas prácticas de seguridad que garanticen el funcionamiento adecuado de los recursos tecnológicos y además, garanticen la confidencialidad, Integridad y Disponibilidad de la información en las redes de comunicación de las organizaciones.

Día a día se descubren nuevos fallos de seguridad en los sistemas, los cuales son utilizados por los atacantes cibernéticos para acceder a las infraestructuras tecnológicas y manipular la información a su conveniencia en relación a fines personales que pueden llevar a las compañías a pérdidas económicas y atentar contra el buen nombre de las organizaciones.

Un factor significativo para las empresas que apoyan sus procesos de negocio en las tecnologías de la información y la comunicación, es ver la seguridad informática como uno de los factores significativos de éxito para la operación de negocio. Por lo tanto, se debe analizar la infraestructura tecnológica y determinar los procedimientos que se requieren para asegurar el buen funcionamiento de los procesos tecnológicos y garantizar el mejor uso de la información.

La implementación del servidor de autenticación TACACS basado en el protocolo AAA en la red empresarial del NOC de UNISYS, va a garantizar el control de acceso a los recursos tecnológicos de esta área de negocio, generando controles de seguridad que permitan establecer el reconocimiento de los usuario legítimos proporcionando un filtro de acceso a las personas no autorizadas que mediante técnicas de hacking, deseen atentar contra el buen nombre de la institución y acceder a información confidencial del core de negocio.

1.4 ALCANCE

El alcance del proyecto comprende el diseño e implementación de un servidor de autenticación AAA basado en el protocolo TACACS, enmarcado sobre las mejores prácticas de seguridad informática, para controlar los accesos a la red corporativa del NOC de UNISYS y garantizar la seguridad en el uso eficiente de los recursos tecnológicos de la compañía mediante niveles de acceso a la información solo por usuarios autorizados y así aumentar el nivel de seguridad de la infraestructura tecnológica y prevenir eventos indeseados que atenten contra el buen funcionamiento de la red de la organización.

La presente investigación estará enmarcada en la línea de investigación de criptografía de la especialización en Seguridad Informática de la Universidad Piloto de Colombia.

2. MARCO REFERENCIAL

2.1 ESTADO DEL ARTE

Nuttsy Aurora Lazo García, estudiante de Ingeniería de Telecomunicaciones de la Pontificia Universidad Católica del Perú, desarrollo el proyecto de grado denominado “DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA” Lima, Perú Julio de 2012.

La presente tesis consiste en el diseño e implementación de una red LAN (Local Area Network) y WLAN (Wireless Local Area Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting). El primer paso fue implementar una red LAN utilizando el mecanismo Etherchannel y el protocolo de balanceo de carga en la puerta de enlace GLBP (Gateway Load Balancing Protocol) para optimizar el uso de recursos de la red. Luego se implementó el servidor ACS (Access Control Server) que utiliza el protocolo TACACS+ para centralizar el acceso de los administradores de los equipos de la red. En lo que concierne a la WLAN, se instaló el servidor IAS de Windows, luego se verificó que el punto de acceso inalámbrico (Access Point - AP) cumpla con el estándar de autenticación IEEE 802.1x que se usó como intermediario entre la capa de acceso y el algoritmo de autenticación, finalmente se configuró con el mecanismo de autenticación WPA-Enterprise.

En el primer capítulo se definió todas las tecnologías que se emplearon en la implementación de la solución y cuál fue la evolución tecnológica para llegar a ellas. El estudio se hizo de manera separada para la LAN y para la WLAN porque al tratarse de redes con interfaces diferentes, cada una tiene definida de forma independiente métodos y estándares de seguridad para el acceso a la red.

En el segundo capítulo se planteó un estudio del problema y se le ubicó en un escenario real con el fin de especificar las exigencias de la empresa, la cual requiere una solución de una red LAN y WLAN que garantice la seguridad de la información y el uso adecuado de los recursos de la red.

En el tercer capítulo se diseñó la solución, realizando un análisis de los requerimientos propuestos en el segundo capítulo. Una vez terminado el análisis se decidió cuáles de los métodos y estándares estudiados en el capítulo uno se usarían en la implementación.

En el cuarto capítulo se muestran los resultados y el análisis de la implementación de la solución diseñada en el laboratorio de redes de la especialidad. En el quinto capítulo se realizó el análisis económico para medir la rentabilidad del proyecto

haciendo uso de la tasa interna de retorno (TIR) y el valor actual neto (VAN) como métodos financieros de inversión.

Luis Carlos Plasencia Bedón, estudiante de Ingeniería en Electrónica y Redes de Comunicación, perteneciente a la Facultad de Ciencias Aplicadas de la Universidad Técnica del Norte, elaboro la investigación *denominada "servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de Networking de un ente del Ministerio de Defensa Nacion*al".

En los tiempos actuales la seguridad de la información es un tema de suma importancia para cualquier organización o institución, debido a las facilidades de las comunicaciones que se brinda a los usuarios a través de servicios internos y públicos (Internet) para el desarrollo de sus actividades laborales, por tal motivo no se debe descuidar la protección de los datos que circulan por la red. El presente proyecto mediante la implementación de un servidor AAA valida el acceso de los usuarios que ingresan a la infraestructura de networking del ente del Ministerio de Defensa Nacional con la finalidad de asegurar la conexión a la red sólo a usuarios autorizados y complementariamente a la solución se utiliza infraestructura UTM desarrollada sobre software libre que controla el acceso de usuarios a los recursos de red de la institución.

Angél Vinicio Maldonado Tapia, estudiante de Ingeniería de Sistemas de la Universidad Politécnica Salesiana, elaboro la tesis de grado "*implementación de un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del colegio San Luis Gonzaga a través de una autenticación de los usuarios mediante un servicio AAA implementado en un servidor que trabaje con protocolos radius".*

El presente proyecto describe el problema y la solución planteada para habilitar la conexión de los distintos dispositivos inalámbricos de los estudiantes del colegio San Luis Gonzaga hacia Internet.

En vista al continuo cambio en la aplicación de la tecnología dentro de la pedagogía, hace que las necesidades de conectividad, por parte de dispositivos móviles de los estudiantes a la red mundial de Internet, como medio de consulta académica, herramienta de comunicación virtual, método complementario de aprendizaje, etc. Sean más necesarias dentro del colegio San Luis Gozaga.

Al ser este servicio un medio de acceso público y dispuesto para que se utilice con cierta cantidad de seguridad entre el estudiantado, deberá contar con un control y registro de los dispositivos que usan el servicio.

Al habilitar un servicio DHCP en una red inalámbrica se corre el riesgo de que personas ajenas a la institución obtengan la clave de acceso a la red, utilizando un

software especial y utilicen un servicio que es de uso exclusivo para el estudiantado y personal laboral del Colegio Gonzaga.

El mencionado control se logrará utilizando un portal cautivo gestionado por el software Chillispot, este portal cautivo se comunicara internamente, con el servidor RADIUS que es el encargado de permitir el acceso al servicio de Internet mediante un “Nombre de usuario y password”, estas referencias del usuario son consultadas en una base de datos especifica diseñada en MySQL, la cual almacenará los registros de los usuarios en cuanto a datos de identificación y registro de utilización del portal cautivo.

Todo este proceso se logra a través de un protocolo de tipo AAA (Autenticación, Autorización y Registro), el cual verifica la identidad del usuario, autoriza que el usuario acceda a un servicio específico y registra el uso que el usuario ha tenido sobre el servicio.

Se plantea esta solución, incluso para centralizar el espacio de uso de Internet por parte de los estudiantes de la institución. La Biblioteca Gonzalo Romero S.J será el lugar destinado para instalar e implementar el portal cautivo con todos los componentes de Hardware y Software.

Paul Asadoorian, miembro del instituto SANS (SysAdmin Audit, Networking and Security Institute), elaboro la guía “IMPLEMENTING SECURE ACCESS TO CISCO DEVICES USING TACACS+ AND SSH” Mayo de 2003.

Esta guía pretende proporcionar a los administradores de red un referente para implementar políticas de acceso a los equipos de comunicación CISCO de las infraestructuras tecnológicas de las compañías, mediante la autenticación de conexiones mediante el protocolo TACACS+ de Cisco.

Steve Ingram, miembro del instituto SANS (SysAdmin Audit, Networking and Security Institute), realizo un documento denominado “CASE STUDY IN IMPLEMENTING AAA SERVERS USING TACACS+” Diciembre de 2003.

Este caso de estudio cubre las temáticas de las consideraciones que deben tener las organizaciones en el procesos de toma de decisiones para implementar soluciones de seguridad informática, basadas en servidores AAA que funcionen bajo el protocolo TACACS+ de Cisco para autenticar, autorizar y auditar clientes de la infraestructura de red.

Cisco Systems, Inc. Genero una guía de soluciones de internetworking denominada “CISCO AAA IMPLMENTATION CASE STUDY” USA, Mayo del 2000.

Esta guía se genera con el fin de proporcionar información acerca de ejemplos que se constituyan en modelos para la construcción de entornos de seguridad

eficaces basados en soluciones AAA de Cisco. Además, se pretende mostrar el funcionamiento esta solución de seguridad, configuración y como solucionar los problemas comunes que se encuentran en este tipos de ambientes.

3. PROSPERIDAD DE LAS INFRAESTRUCTURAS TECNOLÓGICAS UTILIZADAS EN LA SEGURIDAD DE LA INFORMACIÓN Y EL AFINAMIENTO DE LAS REDES CABLEADAS E INALÁMBRICAS

3.1 SEGURIDAD EN REDES INALÁMBRICAS

Hoy en día las redes WLAN también conocidas como redes Inalámbricas son muy vulnerables a infinidades de ataques desde el Interior como también del exterior de los diferentes puntos de cobertura de acceso a la red, permitiendo poder realizar test de vulnerabilidades en la transmisión de los datos. Para garantizar la seguridad en este tipo de redes se necesita cifrar la información antes de ser enviada por el medio de comunicación, pero a su vez, el usuario final debe autenticarse con el servidor AAA antes de acceder a la red.

A continuación damos a conocer los protocolos, métodos y estándares que fueron utilizados para la elaboración de la implementación del proyecto de grado.

3.1.1 Estándar de Autenticación y Cifrado IEEE 802.11i. En el año de 2001 IEEE creó un grupo de trabajo para proponer mejoras en la autenticación y el proceso de encriptación de datos. Dicho grupo implementó mejoras que la Wi-Fi Alliance emitió recomendaciones en contestación de las distintas preocupaciones de distintas organizaciones por la seguridad de redes inalámbricas. Pero aún con esto, el equipo de trabajo estaba convencido que los usuarios no querrían cambiar su equipos.

Finalmente en el año de 2004 se publicó la versión final del estándar 802.11i y fue denominada comercialmente como WPA2 por parte de la alianza Wi-Fi.

Con la llegada del estándar IEEE 802.11i se dieron cambios elementales, como por ejemplo el hecho de separar la autenticación de usuario con la integridad y privacidad de los mensajes, construyendo una arquitectura con estructura más robusta y escalable, que puede ser aplicada de igual forma en redes domésticas como en escenarios grandes de redes corporativas.

Robust Security Network (RSN) es la denominación para la nueva arquitectura de las redes WLAN que implementa una autenticación por medio de 802.1X, entrega de claves robustas y nuevas implementaciones de integridad y privacidad. Una arquitectura inalámbrica RSN, sin importar que sea compleja, es segura y escalable. Redes RSN admitirán únicamente equipos operables con RSN, sin embargo el estándar IEEE 802.11i define también una red de transición de seguridad – Transitional Security Network (TSN), permitiendo la operatividad de sistemas bajo RSN y WEP, dando la posibilidad de no requerir actualización de

equipo. Cuando se utiliza autenticación mediante 4-Way handshake, la asociación se denomina RSNA (Robust Security Network Association).

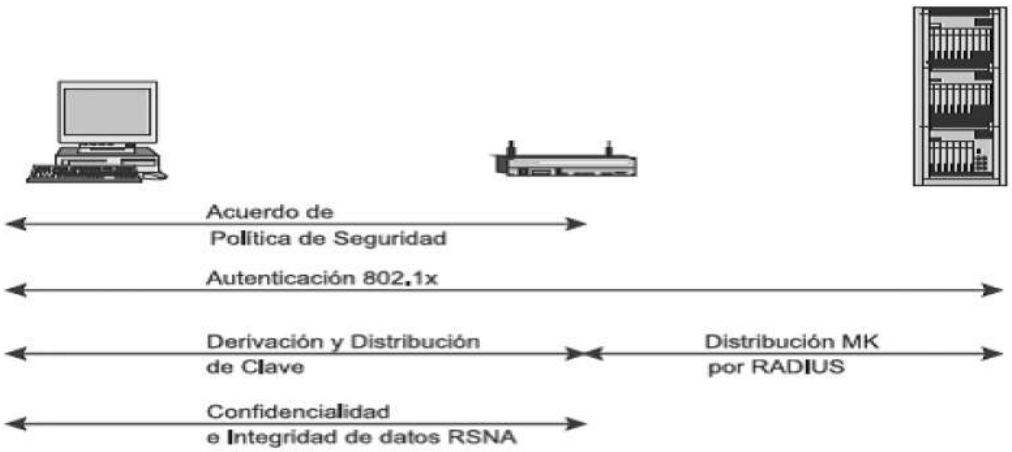
Fases de la Operación de IEEE 802.11i

El estándar IEEE 802.11i envuelve 4 fases que se describen a detalle a continuación:

- Convenio sobre política de seguridad, se da entre el AP y el equipo.
- Autenticación 802.1X, se da entre el AP, el servidor de claves y el equipo.
- Derivación y distribución de las claves, servidor de claves, AP y equipo.
- Confidencialidad e integridad de los datos RSNA, entre el AP y el equipo.

En la siguiente figura se describe las fases de la Operación de IEEE 802.11i:

Figura 1. Fases de la Operación de IEEE 802.11i



Fuente**:** Los autores

3.1.2 Protocolos de Cifrado. Hoy en día los protocolos de cifrado han desarrollado una prospectiva de seguridad al ser más fiables y seguros en la transmisión de los datos, en otras palabras de pasar de cifrado WEP a lo que actualmente conocemos como cifrado WPA2 siendo este último desarrollado dentro del estándar IEEE 802.11i.

3.1.2.1 Cifrado WEP (Wired Equivalent Privacy). El cifrado de los datos inalámbricos, el estándar 802.11 original definió la privacidad equivalente por cable (WEP). Debido a la naturaleza de las redes inalámbricas, la protección del acceso físico a la red resulta difícil. A diferencia de una red con cables donde se requiere una conexión física directa, cabe la posibilidad de que cualquier usuario dentro del alcance de un punto de acceso inalámbrico o un cliente inalámbrico pueda enviar y recibir tramas, así como escuchar otras tramas que se envían, con lo que la interceptación y el espionaje remoto de tramas de red inalámbrica resultan muy sencillos.

WEP utiliza una clave compartida y secreta para cifrar los datos del nodo emisor. El nodo receptor utiliza la misma clave WEP para descifrar los datos. Para el modo de infraestructura, la clave WEP debe estar configurada en el punto de acceso inalámbrico y en todos los clientes inalámbricos. Para el modo ad hoc, la clave WEP debe estar configurada en todos los clientes inalámbricos.

Tal como se especifica en los estándares de IEEE 802.11, WEP utiliza una clave secreta de 40 bits. La mayor parte del hardware inalámbrico para IEEE 802.11 también admite el uso de una clave WEP de 104 bits. Si su hardware admite ambas, utilice una clave de 104 bits.

3.1.3 Proceso de Cifrado y Descifrado WEP. Es importante definir el proceso de cifrado y descifrado de WEP, debido a su constante utilización en todo el proceso de autenticación y operación.

El proceso de cifrado se puede explicar en los siguientes pasos:

Paso 1: Se genera un nuevo vector de inicialización (IV) y se selecciona para ser utilizado. Es importante mencionar que en el estándar no se define una fórmula concreta.

Paso 2: Se procede a concatenar la clave WEP y el vector de inicialización (IV) del paso 1. Esto generará una secuencia de 64 ó 128 bits. Dicho valor es denominado RC4 Keystream.

Paso 3: A la secuencia generada, o RC4 Keystream, se le aplica un algoritmo RC4 que producirá valor cifrado de la clave específica.

Paso 4: Un valor de integridad (ICV) es generado para el mensaje que se va a transmitir y se añade al final del mensaje. El ICV será utilizado para cerciorarse que el mensaje haya sido descifrado correctamente.

Paso 5: Se aplica la función XOR (OR Exclusivo) al mensaje y al RC4 Keystream, de esta forma se genera el mensaje cifrado.

Paso 6: Al mensaje transmitido se le añade el IV utilizado, para asegurarse que el recipiente del mensaje sea capaz de descifrar su contenido.

El proceso de descifrado es exactamente el inverso:

Paso 1: Se hace lectura del vector de inicialización (IV) en el mensaje recibido.
Paso 2: Se concatena el IV y la clave WEP conocida.
Paso 3: Como consecuencia, el RC4 Keystream es generado.
Paso 4: Se aplica función XOR entre el RC4 Keystream y el mensaje cifrado, obteniendo así el mensaje y el ICV[8].

Paso 5: Se verifica el mensaje haciendo uso del ICV.

3.1.3.1 Amenazas al cifrado WEP. Examinando el cifrado WEP a detalle, existe una serie de amenazas y riesgos que lo vuelven vulnerable ante determinadas condiciones. En esta sección se resumirán todas las vulnerabilidades y así como las principales causas que hacen de este cifrado un sistema inseguro de protección para comunicaciones críticas.

3.1.3.2 Longitud de cifrado poco efectiva. Hace ya algunos años se demostró que el algoritmo RC4 sufre múltiples vulnerabilidades, entre las cuales destacan las que prácticamente reducen la longitud efectiva del cifrado a 24 bits, en lugar de los 128 que se pueden definir como máximo en WEP.

WEP utiliza 24 bits y 40 bits de clave para el caso de un cifrado de 64 bits, pero para un cifrado de 128 bits también utiliza 24 bits para el IV y 104 bits para de clave. Por tanto, el cifrado WEP ofrece únicamente seguridad de 24 bits en cualquiera de sus longitudes. Erróneamente, muchos administradores de red con WEP con seguridad de 128 bits, con la noción de duplicar la seguridad del cifrado WEP. Esto no es un razonamiento completamente cierto. Debe hacerse hincapié en el hecho de que un cifrado de 64 bits no es la mitad de débil que uno de 128, la mitad de uno de 128, en cambio, sería uno de 127 bits.

Figura 2. Longitud de cifrado

$$2^{128} / 2^{1} = 2^{(128-1)} = 2^{127}$$

Fuente: Los autores

[8] Campo de datos unido a los datos de texto para la integridad (basado en el algoritmo débil CRC32).

Por lo que un cifrado de 24 bits es 2104 veces la mitad de débil que uno de 128. Al no utilizar el máximo posible de 128 bits en el cifrado WEP, y utilizar únicamente 24 bits para su seguridad, se puede afirmar que un ataque que rompa una clave de 64 bits, será igualmente efectivo para romper un cifrado de 128 bits, esto porque la seguridad implementada en ambos casos es únicamente de 24 bits.

3.1.3.3 Amenazas a la conexión. Como consecuencia de que el punto de acceso anuncia el SSID cada intervalo corto de tiempo, cualquier atacante puede captar (o escuchar) la red inalámbrica aunque cuente con seguridad. Unos pocos segundos son suficientes para que cualquier equipo detecte el canal de operación y el nombre de la red.

Debido a esta situación de inseguridad, el fabricante Lucent fue de los primeros en tomar medidas correctivas para paliar esta situación, dicha medida fue denominada Red Cerrada (Closed Network). Esta medida, de red cerrada consistió únicamente en cesar el anuncio de la red por medio del frame de beacon, es decir, no difundir el SSID.

Sin embargo, en la actualidad esta medida es simplemente una pequeña dificultad añadida para el atacante, quien deberá realizar un pequeño procedimiento adicional para descubrir los datos de la red. Día a día han ido apareciendo nuevo software que convierte el adaptador inalámbrico del equipo en un sniffer, tales como AirSnort o AirTraf, que permiten descubrir, escuchar y analizar redes de inalámbricas de área local.

3.1.3.4 Amenazas a la autentificación. La autentificación por clave compartida del cifrado WEP envía textos claros entre los equipos a través del canal de comunicación, luego dichos textos son encriptados y nuevamente transmitidos a través del mismo canal de comunicación. Por tanto, haciendo uso de un ataque de fuerza bruta es posible llegar a descubrir la clave compartida si se tienen suficientes muestras de paquetes de texto claros enviados y sus respectivas contrapartes cifradas. De esta forma un atacante puede ejecutar un ataque pasivo para averiguar la clave secreta, debido a que la comunicación se transmite en el canal sin ningún control por parte de cualquiera de los participantes legítimos de la red.

Cuando la clave secreta es descubierta, la red y la comunicación entre sus participantes estarán completamente expuestas, ya que el atacante será capaz de encriptar y desencriptar todo el tráfico, a causa de que en el cifrado WEP la clave de autentificación es la misma clave de encriptación.

Lucent, como fabricante preocupado por la seguridad, nuevamente trato de combatir este problema al implementar la seguridad WEP de 128 bits. En esta seguridad la clave WEP pasa de 40 a 104 bits, haciéndola más fuerte ante el ataque mencionado.

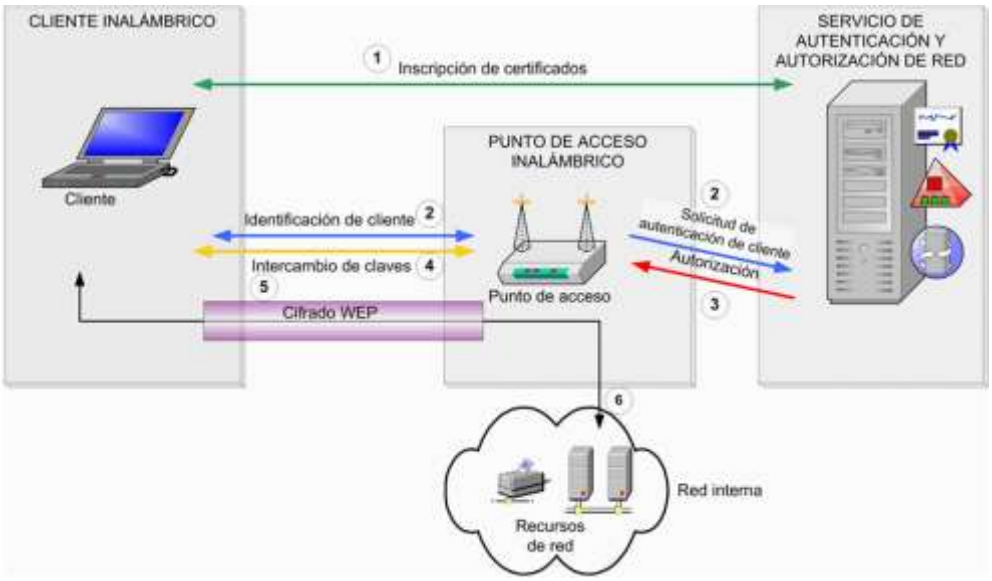
Finalmente, algunos administradores de red consideran que es más seguro desactivar la autentificación mediante este protocolo, ya que de esta forma se protege más la clave de encriptación WEP. Lamentablemente, la mayoría de equipos tienen la autentificación WEP por defecto y son instalados sin modificar dicha característica.

3.1.3.5 Proceso de Autenticación. Cada cliente que desee conectarse o unirse a cualquier red inalámbrica de área local o WLAN, debe autenticado previo a su otorgarle el acceso. Dicha autenticación puede ser de dos tipos:

- **Abierta**, se autentica a todos sin ninguna discriminación, es decir que no existen requerimientos especiales ni medida de exclusión alguna para asociarse a esa red.
- **Cerrada**, se autentica a los usuarios mediante a reglas establecidas por el punto de acceso, dichas reglas tratan de asegurarse que se autentique únicamente a un cliente autorizado.

En la siguiente figura se describe el proceso de autenticación de cifrado WEP:

Figura 3. Proceso de Autenticación con Cifrado WEP



Fuente: Los autores

3.1.3.6 Diccionarios de descifrado. Luego que se haya recuperado con éxito el texto plano de un mensaje determinado, es posible separar el valor del Keystream, aplicando la técnica de análisis de IV o mediante otros procedimientos. Esto habilita al atacante para utilizar este Keystream con el fin de descifrar cualquier paquete que tenga un IV similar.

Debido a que las claves privadas compartidas k son cambiadas alguna vez, el atacante, a través de la captura masiva de información, puede formar un arreglo de Keystreams que pertenezcan a distintas IV. Cuando se ha construido la tabla, descifrar cada texto cifrado es una tarea poco complicada y relativamente fácil.

Esta situación no depende en ningún momento de la longitud de clave de cifrado, debido a que el tamaño de las entradas del diccionario estará fijado a 24 bits, porque depende del IV y este no varía su longitud. Incluso, el diccionario utilizado en el ataque se hará más práctico al aprovechar el modo de operación de las tarjetas PCMCIA ya que estas establecen el IV a 0 cada vez que son reseteadas.

Debido a la mayoría de casos habituales donde las tarjetas se arrancan al menos una vez diaria, el atacante podría establecer un diccionario limitado únicamente a los primeros millares de valores de IV, esto le habilitaría descifrar casi todos los paquetes transmitidos por el punto de acceso. La ventaja en este caso es, como se ha explicado anteriormente, que en una red bajo el estándar 802.11 con bastantes clientes, se presentan colisiones en los primeros miles de valores de IV muchas veces.

3.1.3.7 Gestión de claves. Para iniciar este tema, es importante mencionar que el estándar 802.11 no cuenta con una definición formal de un procedimiento para distribuir las claves. Al contrario, la distribución utiliza un procedimiento externo para llenar la matriz de cuatro claves compartida globalmente. Todos los mensajes incluyen un campo para la identificación de clave donde se especifica la posición de la clave dentro de la matriz que se usó para el proceso de cifrado.

Finalmente se pueden destacar las vulnerabilidades más grandes tal como sigue:

- Implementación del algoritmo RC4 que es débil a razón de la generación de la clave

- La longitud del IV es bastante corta (24 bits) lo que nos brinda una probabilidad de 50% de averiguar la clave, con únicamente 5000 paquetes, además que es permitida la reutilización de IV (no existe ninguna implementación para proteger la repetición de mensajes)

- No se implementa una comprobación de integridad correcta (es utilizado el algoritmo CRC32 para tratar de detectar errores y este algoritmo no es, desde un punto de vista criptográfico seguro debido a su linealidad)

- No hay implementado ningún método integrado que permita actualizar las claves.

3.1.4 Cifrado WAP (Wi-Fi Protected Access). IEEE 802.11i diseña y patenta su nuevo estándar que especifica mejoras en la seguridad de las redes locales inalámbricas. El estándar 802.11i soluciona muchos de los problemas de seguridad del estándar 802.11 original. Mientras se ratifica el nuevo estándar IEEE 802.11i, los proveedores de productos inalámbricos han acordado un estándar intermedio interoperable denominado WPA™ (acceso protegido Wi-Fi).

WPA es, entonces, una solución a los problemas que se presentaron con el sistema WEP y es el eslabón entre el estándar 802.11i y WEP. WPA fue concebido para interactuar con un servidor de autenticación (generalmente un servidor RADIUS), que es el encargado de entregar claves diferentes a cada usuario, haciendo uso del protocolo 802.1x, esto debido a que fue diseñado para ser bastante seguro. Sin embargo, es posible implementarlo en un escenario de seguridad disminuida, donde las condiciones no permiten o no requieren utilizar un servidor de autenticación, esto se logra utilizando PSK (Pre-Shared Key) o clave pre-compartida.

Los mensajes son cifrados por medio del algoritmo RC4, esto debido a que el sistema WPA brinda mayor fortaleza y poder al proceso de de cifrado de WEP, y no lo elimina. Específicamente WPA trabaja como el sistema WEP con una clave de 128 bits y un vector de inicialización de 48 bits.

Aunque WPA opera como un sistema WEP, existen distintas mejoras que lo hacen potencialmente seguro, entre ellas es importante mencionar que implementa el Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que genera claves de manera aleatoria conforme el sistema es utilizado. Al observar en conjunto esta situación, con el vector de inicialización más grande, se distingue claramente que existe más protección a los ataques de recuperación de clave (estadísticos o de fuerza bruta) a los que WEP ha estado expuesto durante muchos años.

Además de las mejoras en la autenticación y en el cifrado, el sistema WPA implementa mejoras en la integridad de la información que se cifra. La verificación de redundancia cíclica (CRC[9]) implementada por WEP es altamente insegura, debido a que el contenido de las tramas puede ser modificado y el CRC actualizado sin conocer la clave WEP. Por ello, WPA implementa un código de

[9] Pseudo-algoritmo de integridad usado en el protocolo WEP, bastante cuestionado debido a su debilidad.

integridad del mensaje (MIC), que también es denominado como "Michael". Otra mejora del sistema WPA sobre WEP, es que previene ataques de repetición implementando un contador de tramas.

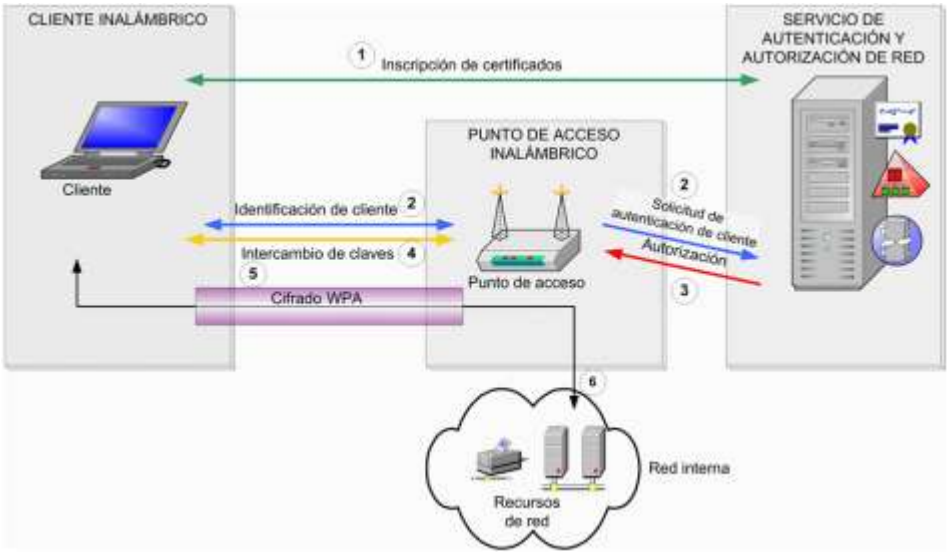
Implementando estas mejoras, claves más grandes, mayor número de llaves usadas y el sistema de verificación de mensajes, el sistema WPA complica de manera muy grande el acceso no autorizado a las redes inalámbricas de área local WLAN.

Los diseñadores del sistema WPA idearon el algoritmo mas poderoso que fuera compatible con dispositivos antiguos existentes en los equipos, como consecuencia el algoritmo Michael a pesar de ser bastante fuerte, también es susceptible a ataques. Para tratar de paliar esta situación de riesgo, las redes con seguridad WPA se desconectan por un intervalo de 60 segundos al detectar dos intentos de ataque en menos de un minuto.

La vulnerabilidad con más probabilidades de éxito consiste en un ataque contra la clave PSK (Pre Shared Key) de WPA/WPA2.

En la siguiente figura se describe el proceso de autenticación de cifrado WAP:

Figura 4. Proceso de Autenticación con Cifrado WAP



Fuente: Los autores

3.1.4.1 Ataque contra la clave PSK. La PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación. La PSK es una cadena con longitud de 256 bits o bien una frase de 8 a 63 caracteres, y es utilizada para generar una cadena de texto usando un algoritmo sabido:

Figura 5. Algoritmo PSK

PSK = PMK = PBKDF2 (frase, SSID, SSID length, 4096, 256)

Fuente: Los autores

La PTK se origina de la PMK haciendo uso del 4-Way Handshake y la totalidad de la información usada para el cálculo de su valor es transmitida con formato texto. El poder de la PTK se encuentra en el valor de PMK, que para PSK representa de manera exacta una frase sólida[10].

3.1.5 Cifrado WAP2 (Wi-Fi Protected Access 2). WPA2 (o Acceso Protegido Wi-Fi 2 por sus siglas en inglés) es un sistema que se implementa para protección de redes inalámbricas que cumplen con el estándar 802.11 Wi-Fi. La creación de este sistema representa la corrección de una lista de vulnerabilidades existentes en su predecesor, WPA.

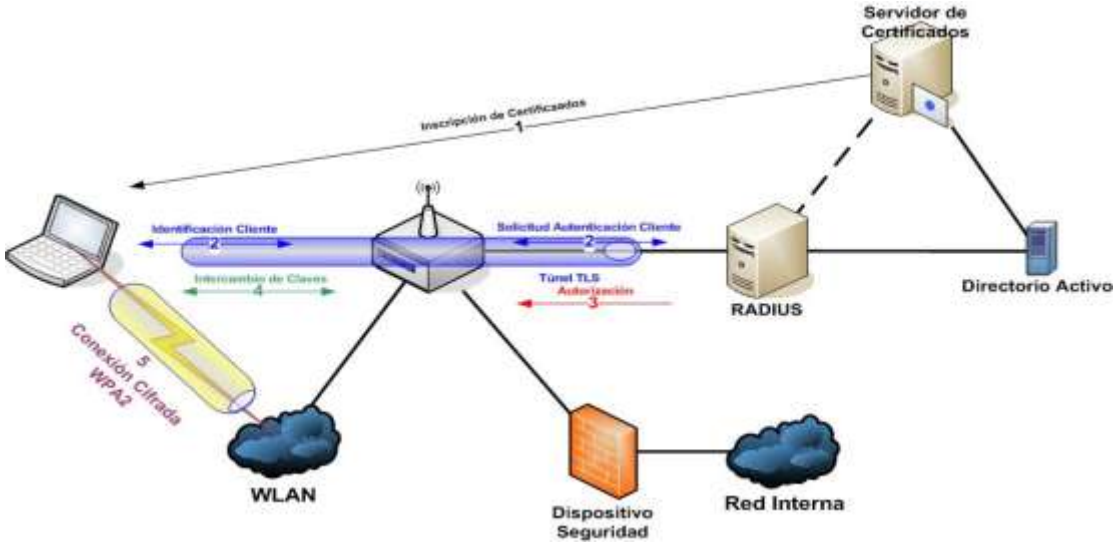
WPA2 es una implementación temprana del estándar 802.11i, pues a pesar de estar basado en este nuevo estándar, no implementa todas sus funcionalidades y procedimientos, por lo que es considerada como una transición de las redes bajo el estándar WI-FI hacia la próxima generación de redes inalámbricas, es decir el estándar 802.11i. Es común que se mencione a WPA2 como la versión certificada de 802.11i, a pesar de no incluir todas sus características. Según las normas de la alianza WI-FI, la autenticación por clave pre-compartida es denominada WPA-Personal y WPA2-Personal, mientras que la autenticación por 802.1x/EAP son denominadas WPA-Enterprise y WPA2-Enterprise.

Los puntos de acceso con capacidad para soportar WPA2 son una nueva generación de puntos de acceso fabricados para utilizar el algoritmo de encriptación AES (Advanced Encryption Standard). Dichos puntos de acceso, al implementar AES para WPA2, permitirán que se cumpla con la norma de seguridad del gobierno de los Estados Unidos FIPS140-2. Sin embargo, aunque los dispositivos de última generación que implementan AES son esperados con muchas ansias, es necesario resaltar que los productos WPA certificados son todavía seguros conforme las especificaciones del estándar 802.11i.

[10] PTK y PMK. Disponible en http://www.hsc-labs.com/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

En la siguiente figura se describe el proceso de autenticación de cifrado WAP2:

Figura 6. Proceso de Autenticación con Cifrado WAP2

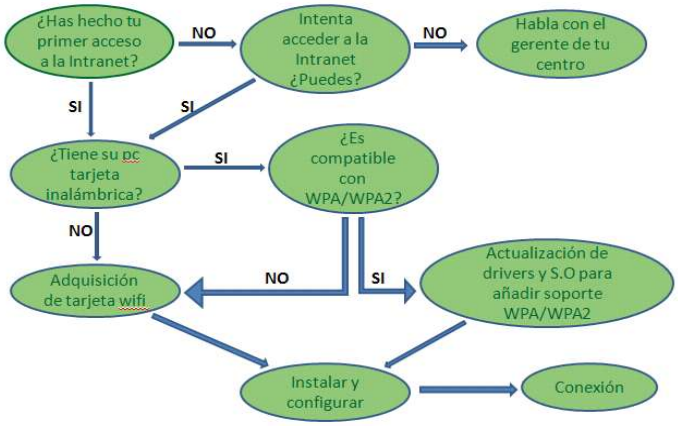


Fuente**:** Los autores

Diagrama de Flujo de los diferentes Cifrados de Autenticación WAP/WAP2:

En la siguiente figura se describe el proceso de autenticación de cifrado WEP:

Figura 7. Diagrama de Flujo Cifrados WAP/WAP2



Fuente: Los autores

3.1.6 Protocolos Seguros de Confidencialidad e Integridad en la Seguridad de la Información

Cada uno de los protocolos seguros de confidencialidad e integridad en la seguridad de la información han iniciado la prospectiva con TKIP incorporado en el cifrado WAP hasta hoy día con el último protocolo de cifrado robusto conocido como CCMP[11] que se encuentra incorporado en el cifrado WPA2.

3.1.6.1 TKIP (Temporal Key Integrity Protocol). El protocolo TKIP (Temporal Key Integrity Protocol por sus siglas en inglés), también es conocido hashing de Clave WEP. TKIP resuelve de forma temporal el problema que presenta WEP al reutilizar la clave, pues se usa periódicamente la misma clave para cifrar datos.

La operación de TKIP se inicia con la compartición de una clave temporal de 128 bits entre los clientes y los puntos de acceso, y TKIP realiza una combinación de la clave temporal con la dirección MAC del cliente. Entonces se adiciona un vector de inicialización relativamente largo, de 16 octetos, para generar la clave que se utilizará para el cifrado de datos.

Con este conjunto de operaciones se intenta asegurar que las estaciones utilicen diferentes streams claves para el cifrado de datos. Por tanto, el hashing de clave WEP brinda protección a los Vectores de Inicialización (IV) ya que no los expone, pues se implementa hashing del IV por cada paquete.

TKIP hace uso del algoritmo RC4[12] para cifrar los datos, por lo que es equivalente al modo de encriptación de WEP. Sin embargo, la gran diferencia es que TKIP sustituye las claves temporales a cada cierto número de paquetes (10.000). Con esto se consigue un procedimiento de distribución dinámico y se mejora grandemente la red.

3.1.7 WRAP (Wireless Robust Authenticated Protocol). Este sistema de cifrado se basa también en el algoritmo de encriptación AES, fue el primer protocolo elegido por el estándar IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias.

3.1.7.1 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Este protocolo no nació para acomodarse al

[11] CCMP es obligatorio en el estándar WPA2, opcional en WPA y obligatorio en las redes RSN (Robust Security Network).

[12] El algoritmo RC4 es el sistema de cifrado de flujo más utilizado y es implementado en algunos de los protocolos de seguridad más importantes como TLS/SSL que protege el tráfico de red en Internet, y el protocolo de seguridad más usado en las redes inalámbricas de área local.

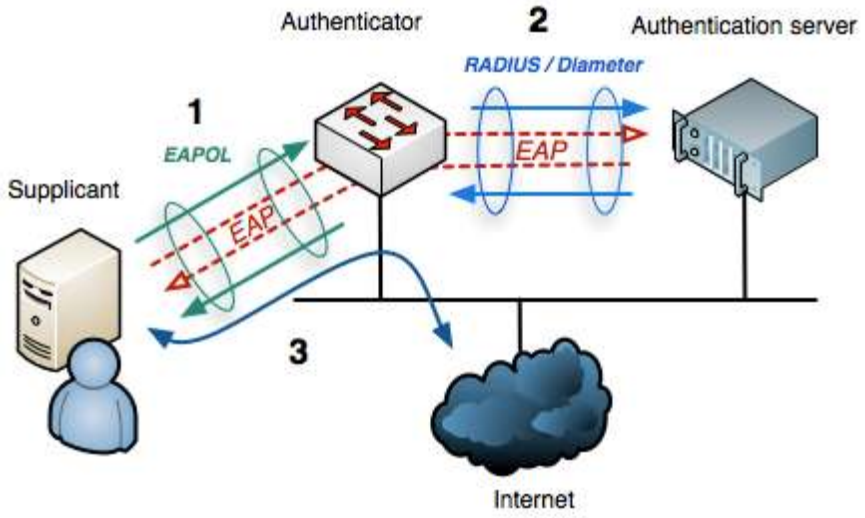
hardware WEP, por ello tiene un nuevo diseño basado en el algoritmo de encriptación de bloques AES (cuenta con un contador extra inicializado en 1 y se incrementa en cada bloque). Además utiliza el método de autenticación de mensajes CBC – MAC (Cipher Block Chaining) para producir un MIC[13]. Usa una clave única pero con diferentes vectores de inicialización, el vector es incrementado en cada fragmento del paquete. La cabecera CCMP no viaja cifrada pero los datos si, incluido el vector.

3.1.8 Protocolo de Autenticación IEEE 802.1x. Este protocolo también es conocido como Port Based Network Access Control, la implementación original fue para redes cableadas. Este protocolo incluye la implementación de mecanismos de autenticación, autorización y distribución de claves. Así mismo contiene un control de acceso de equipos que accedan a la red. La arquitectura de este protocolo está compuesta por tres entidades funcionales[14]:

- El suplicante (equipo que intenta unirse a la red).
- El autenticador (encargado de conceder de acceso. En las WLAN es el AP quien cumple esta función).
- El servidor de autenticación (que toma las decisiones de autorización).

En la siguiente figura se muestra la interconexión de los protocolos de autenticación y las diversas redes mediante 802.1x

Figura 8. Modelo IEEE 802.1x teniendo en cuenta las especificaciones IEEE 802.1x



Fuente: Los autores

[13] Campo de datos unido a los datos de texto para la integridad, está basado en el algoritmo Michael.
[14] WPA. Disponible en http://www.hsc-labs.com/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

3.1.8.1 PAE - Entidad de acceso a Puertos. PAE Port Access Entity por sus siglas en inglés, es la entidad de acceso a puertos. Cada puerto físico (o virtual en las WLAN) está compuesto de dos puertos lógicos, la PAE de autenticación y la PAE de servicio. En el caso de la primera, siempre está a la escucha y abierta, permitiendo el paso a procesos de autenticación. En el caso de la segunda, únicamente será abierta cuando se haya efectuado una autenticación exitosa y por un tiempo limitado (por defecto 3600 segundos).

Finalmente quien otorga el permiso para el acceso es por lo general una tercera entidad, llamada servidor de autenticación. Esta función la puede cumplir un servidor RADIUS dedicado, en el caso de soluciones robustas y que requieran mayor seguridad, o puede ser un proceso ejecutándose en el punto de acceso, en el caso de las redes domésticas. La siguiente ilustra el modo de comunicación entre estas entidades.

El nuevo estándar 802.11i presenta ligeros cambios frente al robo de identidades en relación a su predecesor IEEE 802.1X. Se ha implementado una autenticación de mensajes para garantizar que ambos, el suplicante y el autenticador, activan la encriptación de datos con claves secretas previo al acceso a la red.

Ambos, suplicante y autenticador establecen comunicación haciendo uso de un protocolo basado en EAP. Debido a que el autenticador únicamente envía mensajes al servidor de autenticación, se podría decir que tiene un rol pasivo. EAP es una implementación para transportar distintos métodos de autenticación, permitiendo únicamente un número definido de mensajes, siendo ellos:

- Request (mensaje de solicitud)
- Response (mensaje de respuesta)
- Success (mensaje de solicitud exitosa o aprobada)
- Failure (mensaje de fallo)

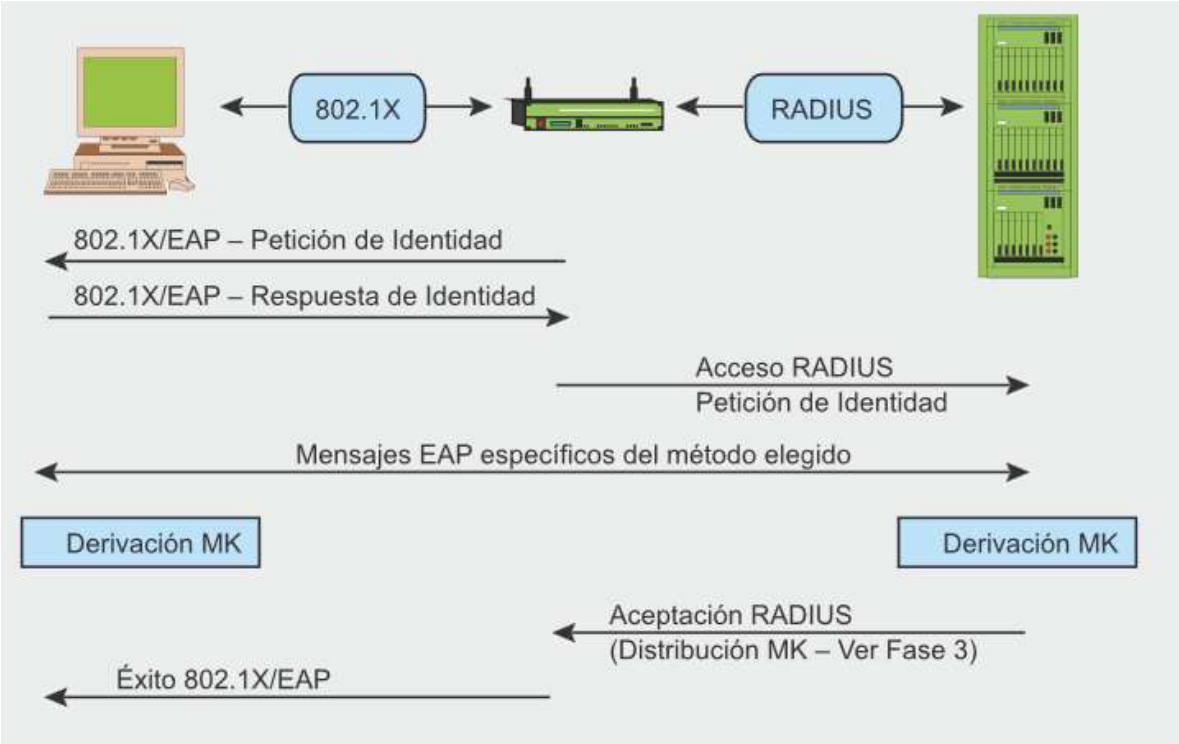
Existen otros mensajes intermedios, pero no se mencionan debido a que son propios de cada implementación de EAP.

La comunicación entre NAS[15] y servidor de autenticación requiere un protocolo de capa más alta, como RADIUS si usamos un servidor RADIUS. Este proceso finaliza cuando el servidor envíe un mensaje “Radius Accept” que contiene la MK y un mensaje final “EAP Success” para el usuario.

En la siguiente figura se muestra todo el proceso de autenticación IEEE 802.1x

[15] También denominado NAS, es un equipo de comunicación, puede ser un access point, un switch, un RAS entre otros, los cuales serán la puerta de ingreso a la red, al cual los usuarios se conectan físicamente por medio de cable, wireless o ADSL.

Figura 9. Proceso de Autenticación IEEE 802.1x



Fuente: Los autores

Al anterior estándar tiene las siguientes ventajas principales:

- Certificados de usuario
- Cifrado más seguro
- Autenticación y cohesión a la WLAN transparentes
- Alto nivel de seguridad porque puede usar nombres de usuarios y contraseñas
- Autenticación por separado de usuarios y de equipos
- Bajo costo de hardware de red
- Alto rendimiento porque el cifrado se lleva a cabo en el hardware de la WLAN y no en el procesador del equipo cliente.

3.1.8.2 Autenticación EAP. EAP Extensible Access Protocol por sus siglas en inglés o protocolo extensible de autentificación, es un protocolo utilizado para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos. La autentificación por EAP implementa dos cifrados WEP que los equipos utilizan como claves de sesión que y que son acordados en la autentificación y que cambia cada cierto tiempo conforme al punto de acceso.

De los dos cifrados WEP implementados, uno es utilizado para el broadcast o anuncio de la red en el punto de acceso, y otro se implementa en la comunicación con cada cliente, de tal forma que los clientes no se escuchen entre sí.

3.1.8.3 RADIUS (Remote Authentication Dial-In User Server). Es un protocolo cliente/servidor, donde el cliente es un NAS (Network Access Server) y el servidor es un software ejecutado en un equipo UNIX, LINUX o Windows. Como protocolo de transporte emplea puertos UDP, para establecer comunicación utiliza dos puertos: el 1813 - 1645 para contabilidad y el 1812 - 1646 para autenticación y autorización.

Para el correcto funcionamiento el cliente se requiere los siguientes datos:

- Dirección IP o nombre del servidor RADIUS
- Puerto de autenticación y autorización
- Puerto de contabilidad, por donde recibe los eventos de conexión
- Clave de autorización, que codifica la información enviada en la negociación con el servidor.

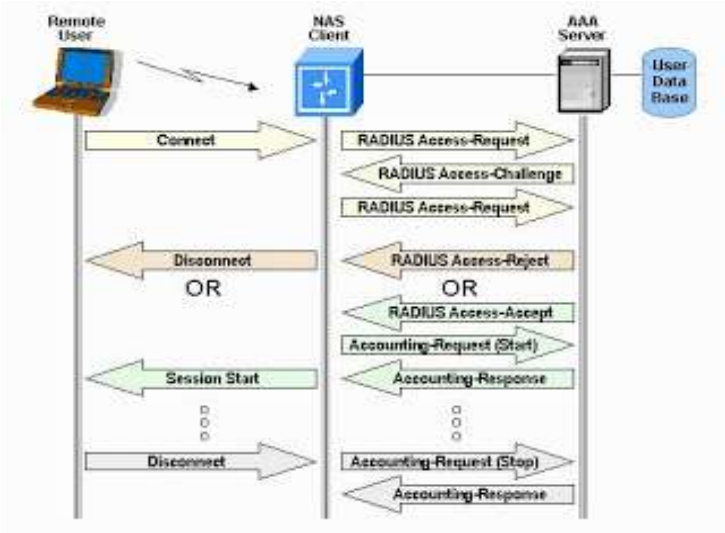
3.1.8.4 Server RADIUS. El Software se instala como un servicio en el sistema operativo actual de una computadora, es el encargado de administrar todo el sistema de acceso. Recibe la autenticación y luego de realizar la comparación con sus registros envía un mensaje permitiendo o negando el acceso, además ira almacenando los eventos de dichos procesos. Para aceptar las consultas del cliente debe tener un perfil del NAS con la dirección IP del cliente y la clave de autorización.

En la comunicación con el cliente, se intercambian los siguientes mensajes:

- **Access - Request:** Solicitud de atención para autenticación
- **Access - Accept:** Acepta la autenticación
- **Access - Reject:** No acepta la autenticación
- **Accounting - Request:** Registra eventos
- **Accounting – Response:** Confirmación de evento registrado

En la siguiente figura se muestra todo el proceso Intercambio de Mensaje en un Servidor Radius:

Figura 10. Proceso Intercambio de Mensaje en un Servidor Radius



Fuente**:** Servidores Radius[16]

A continuación se detalla los atributos que son transportados en cada mensaje:

Access – Request

- **User - Name:** Cuenta del usuario
- **User - Password:** Pasword del usuario

Access – Accept

- **Frame - IP - Address:** Dirección IP a entregar
- **Frame - IP - Netmask:** Mascara de la dirección IP a entregar

Accounting – Request

- **Acct - Status - Type:** Estado de conexión
- **Acct - session Time:** Tiempo de sesión
- **Acct - Terminate - Cause:** Causa de desconexión

[16] http://trabajotele08.blogspot.com/

En la tabla se hace una breve comparación de los principales servidores de autenticación AAA

Tabla 1. Comparación Entre Servidores AAA de Autenticación

Nombre	Sistema Operativo	Protocolo 802.1x	Libre
IAS Windows	Windows	TLS, PEAP Y LEAP	No
Odyssey	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
FreeRadius	Linux Windows	MD5, TLS, PEAP, TTLS y LEAP	Si
EmeraldV5	Linux Windows	PEAP, TTLS y LEAP	No

Fuente: Los autores

3.2 SEGURIDAD EN REDES DE ÁREA LOCAL (LAN)

La administración de cada una de las conexiones que se estarán realizando desde la Red LAN, se implementará un sistema centralizado de control de acceso para los usuarios de la red, como también de los dispositivos de red. lo cual provee una mayor escalabilidad y administración rápida y precisa de cada uno de los usuarios de red.

Todo el proceso de autenticación y administración será efectuado por el servidor de autenticación TACACS+, este fue desarrollado por la multinacional Cisco Systems. Al Igual que RADIUS se basan en protocolos de control de acceso, y operan bajo el modelo cliente/servidor. Los cliente serán todos los equipos de comunicaciones de la red (Switches, Access Point y Routers) que soporten integrarse un cliente AAA, de esa manera lo obliga a establecer comunicación con el servidor AAA, dado que solamente utilizara un puerto único de autenticación y autorización.

3.2.1 **TACACS+ .** Es un protocolo de la capa de aplicación, usa TCP como protocolo de transporte (garantizando la transmisión de paquete) que tiene como puerto asociado al 49, este cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Separa cada uno de sus procesos autenticación, autorización, y contabilidad.

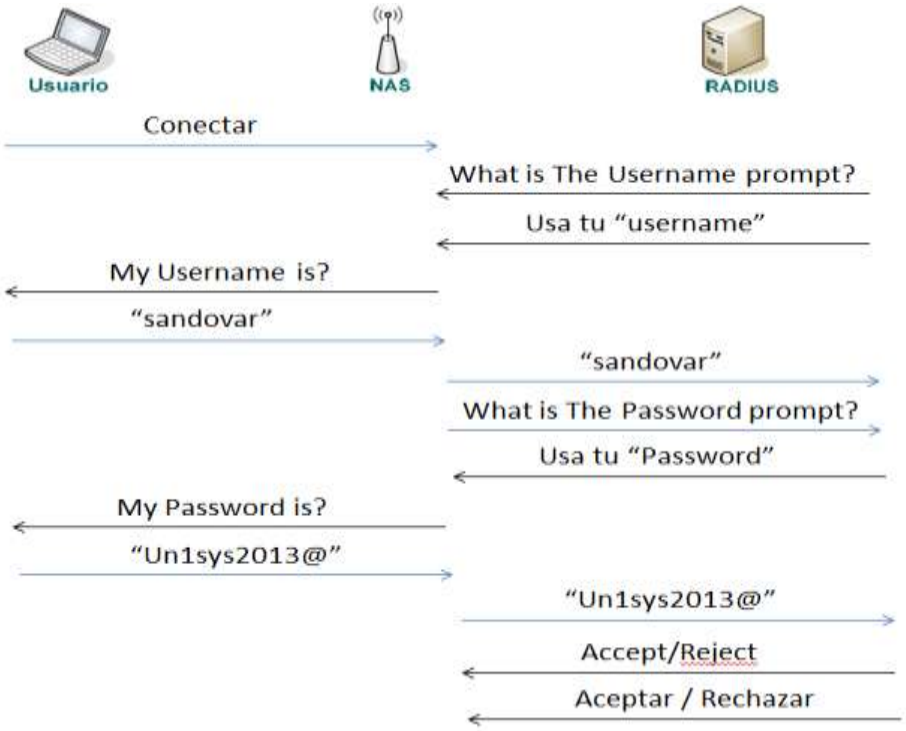
Cada comunicación entre el cliente y servidor AAA usa una conexión dedicada TCP. Pero para tener menos carga en el servidor y una mejor detección de caídas en la comunicación también una sola sesión puede ser establecida. Esta sesión

permanece establecida mientras el servidor o el dispositivo de red se encuentren siendo gestionado por el personal encargado.

3.2.2 **Autenticación TACACS+.** Todo este proceso es únicamente establecido por el servidor de TACACS+, este se efectúa por medio de una comunicación parcial que recopila suficiente información del usuario para poderse autenticar. Eventualmente la información solicitada son las credenciales del usuario.

En la siguiente figura se muestra todo la secuencia del mensaje TACACS+ cuando son intercambiados entre el usuario, el equipo de comunicación (NAS) y el servidor AAA cuando se produce la autenticación de un usuario.

Figura 11**.** Proceso Autenticación TACACS+



Fuente: Los autores

3.2.1.1 Autorización TACACS+. Si el proceso de autenticación se realizó de manera correcta y el cliente tiene habilitada la fase de autorización, el usuario no tendría problema en conectarse con su sesión.

Para ello el cliente se contacta nuevamente con el servidor, para recibir una respuesta que puede ser de la siguiente manera:

- ACCEPT: Acepta la autorización, y contiene información en forma de atributos que determinaran a que servicios puede acceder el usuario.

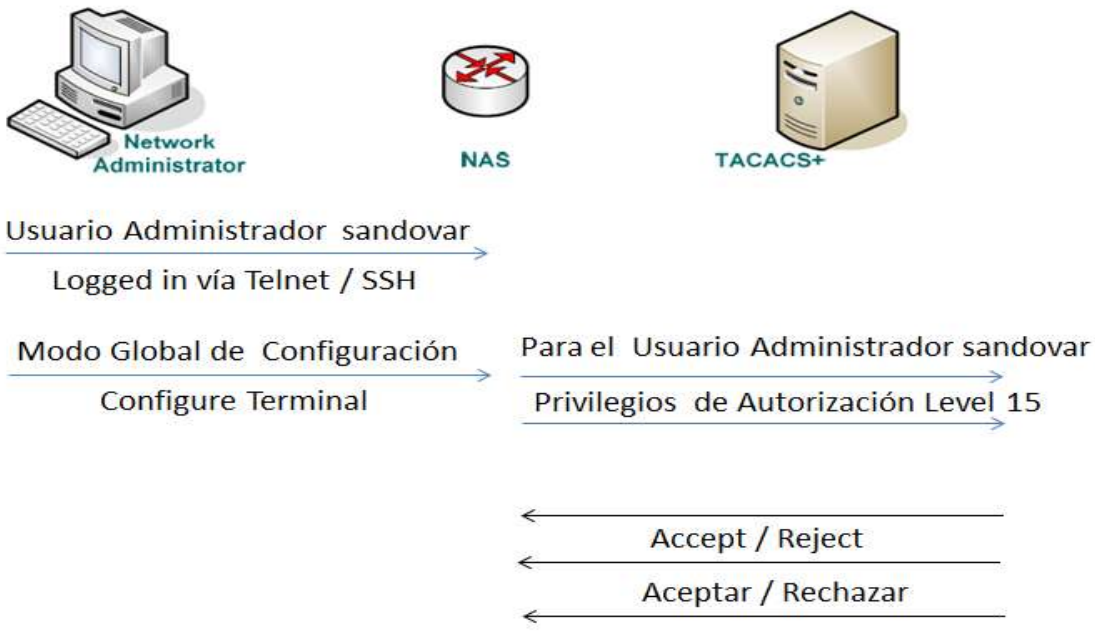
- REJECT: Autorización denegada

Entre los atributos contenidos en el mensaje ACCEPT están: parámetros de conexión, nombre del host o dirección IP, ACL, Timeouts para el usuario, en otras palabras toda la información del perfil del usuario.

Este control de acceso a los servicios de la red representa una gran medida de seguridad. Además el contar con un control de acceso a comandos de configuración restringe de manera significativa los ataques internos. El proceso de autorización de comandos se realizara cada vez que el usuario ingrese un comando, para que el servidor pueda determinar si es aceptado o rechazado de acuerdo al perfil del usuario.

En la siguiente figura se muestra el proceso de autorización para comandos ingresaron en los equipos de comunicación:

Figura 12. Proceso Autorización para las líneas de comando Mediante el Servidor TACACS+



Fuente: Los autores

3.2.1.2 Proceso de Trazabilidad y Responsabilidad TACACS+. El servidor AAA se encarga de registrar todos los diversos eventos, para de esa manera poder realizar un seguimiento detallado a cada sesión que se establece o rechaza a través de este servicio, dado que este log son almacenados en archivos .log o en una base de datos dependiendo de la configuración establecida. Los archivos log son fácilmente exportables a a diferentes tipos de bases de datos, archivos de hoja de cálculo o texto plano. La anterior información es muy útil para la administración y gestión de la red, para tener respaldo en las auditorias de las cuentas, los sistemas billing y generación de reportes que se requieran.

3.2.2 Sistema de Control de Acceso (ACS). El sistema de control de acceso es una solución óptima en cada una de las empresas, por qué provee un servidor AAA altamente escalable y robusto, su optimo control de acceso opera como servidor centralizado RADIUS o TACACS+, para su implementación se requiere el sistema operativo WINDOWS 2003 Server en cualquiera de sus versiones, además de las características solicitadas por el protocolo AAA con que decida trabajar, además cuenta con las siguientes características:

- Maneja diferentes niveles de acceso por usuario o por grupo, una vez que la autenticación se ha dado de manera correcta, ACS envía un profile del usuario al cliente, conteniendo políticas que indicaran a que servicios de la red puede acceder dicho usuario.

- Los accesos pueden ser diferenciados por: servicios, tiempo de acceso, y niveles de seguridad. Además puede aplicar políticas de control acceso ACL, restringiendo el acceso a determinadas áreas.

- Puede deshabilitar cuentas cuando se producen reintentos fallidos de ingreso o por vencimiento en la fecha.

- Los usuarios no podrá realizar el cambio de sus contraseña individualmente, el administrador de la gestión de la red es el único que podrá realizar este cambio.

Componentes Internos del Sistema de Control de Acceso (ACS):

El Sistema de Control de Acceso está desarrollado por 7 capas las cuales son instaladas como servicios en Windows al momento de instalar el programa:

- **CSAdmin:** Provee la interfaz web para la administración, soporta múltiples procesos que permiten múltiples sesiones, por defecto usa el protocolo HTTP en el puerto 2002.
- **CSAuth:** Provee el servicio de autenticación, permitiendo o negando el acceso, maneja la base de datos local ACS.

- **CSDBSync:** Maneja la sincronización y replicación de la base de datos hacia otros servidores AAA ACS.
- **CSLog:** Provee el servicio de logging, para la contabilidad y actividad del sistema. Para ello monitorea y registra: actividades de los usuarios y administradores, backups y restauraciones, replicación de bases de datos, sincronización, servicios centrales de ACS, contabilidad TACACS+, contabilidad VoIP.
- **CSTacacs:** Provee comunicación entre clientes TACACS+ y el servicio CSAuth.
- **CSRadius:** Provee comunicación entre clientes RADIUS y el servicio CSAuth.
- **CSMon:** Monitorea el estado de los servicios ACS y los recursos, registra y reporta todos los errores críticos, envía alertas vía e-mail al administrador, realiza test de login.

3.2.3 Comparación Servidor TACACS+ y RADIUS. Una de las diferencias entre TACACS+ y RADIUS, es que TACACS+ utiliza TCP como protocolo de transporte mientras que RADIUS utiliza UDP. Debido a esto el protocolo TACACS+ es más confiable que el protocolo RADIUS porque tendrá retransmisión de mensajes en caso se produzca una pérdida.

Otras diferencias importante entre RADIUS y TACACS+ está en que RADIUS sólo cifra la contraseña en la petición de acceso hasta un máximo de 16 bytes TACACS +, por otra parte, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Por ello podemos decir que el cifrado que maneja el protocolo TACACS+ es más robusta que el cifrado usado por el protocolo RADIUS.

RADIUS combina la autenticación y la autorización como un solo servicio, mientras TACACS+ los ofrece como servicios independientes. Esto hace que TACACS+ pueda ser utilizado en implementaciones donde no solo se requiera autenticarse sino que se requiera definir diversos niveles de autorización.

Tabla 2. Comparación Servidor TACACS+ y RADIUS

Nombre	Protocolo de Transporte	Datos Cifrados	Autenticación y Autorización
TACACS+	TCP	Cuerpo del Paquete TACACS+	Servicios Indenpendientes
RADIUS	UDP	La Contraseña	Se combina como un solo servicio

Fuente: Los autores

4. ANÁLISIS DE RIESGOS DE LA RED DEL NOC DE UNISYS

El presente análisis de riesgos se realiza enfocado en la metodología MAGERIT la cual permite realizar una aproximación sobre los riesgos informáticos que se tiene en la presente compañía de estudio, para identificar las debilidades a las que están expuestos los activos informáticos.

4.1 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

El Consejo Superior de Administración Electrónica, ha elaborado y promueve la Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos (MAGERIT) como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

La metodología MAGERIT consta de tres volúmenes:

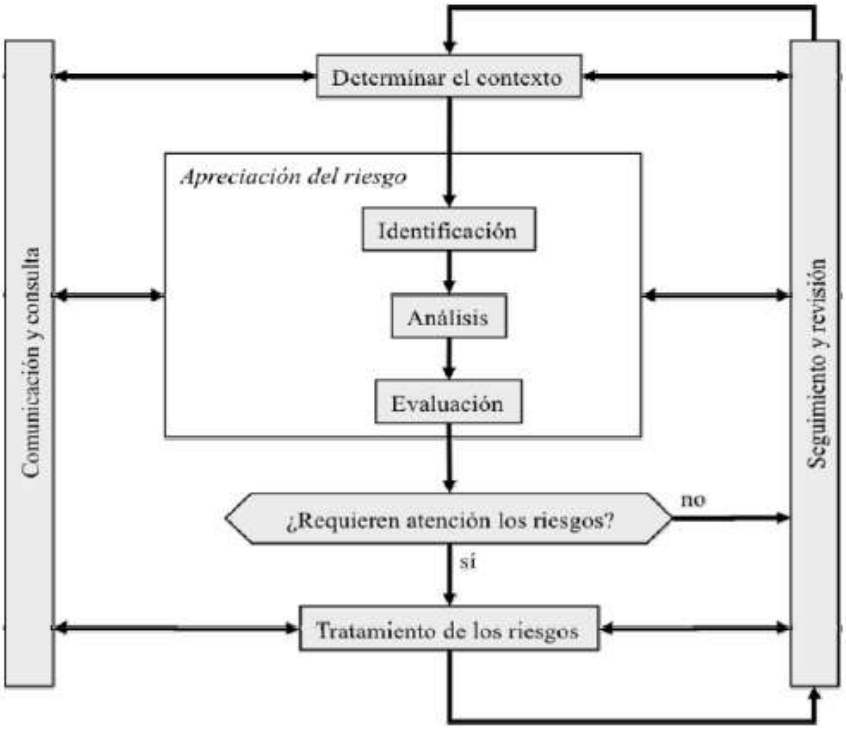
Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.

Volumen II – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que se incluyen son:

- Tipos de activos
- Dimensiones y criterios de evaluación
- Amenazas
- Salvaguardas

Volumen III – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas técnicas a utilizar en las distintas fases del análisis de riesgo

Figura 13. Proceso de gestión de riesgos (fuente: ISO 31000)



Fuente: MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Página 20.

La **determinación del contexto** lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. Véase la norma [ISO 31000] para un mayor desarrollo de los factores que determinan el contexto.

La **identificación de los riesgos** busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado.

El **análisis de los riesgos** busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

La **evaluación de los riesgos** va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

El **tratamiento de los riesgos** recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante.

Comunicación y consulta. Es importante no olvidar nunca que los sistemas de información de-ben ser soporte de la productividad de la Organización. Es absurdo un sistema muy seguro pero que impide que la Organización alcance sus objetivos. Siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores.

- los usuarios cuyas necesidades deben ser tenidas en cuenta y a los que hay que informar para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad determinados por la Dirección
- los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigir-les tanto el cumplimiento de los niveles de servicio requeridos, como la gestión de los incidentes de seguridad que pudieran acaecer
- los órganos de gobierno para establecer canales de comunicación que consoliden la con-fianza de que el sistema de información responderá sin sorpresas para atender a la misión de la Organización y que los incidentes serán atajados de acuerdo el plan previsto

Seguimiento y revisión. Es importante no olvidar nunca que el análisis de riesgos es una actividad de despacho y que es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

4.1.1 Determinación del contexto. El NOC es un área fundamental de UNISYS ya que desde el mismo, se proporciona la asesoría y apoyo a los clientes a asegurar sus operaciones, aumentar la eficiencia y utilización de sus centros de cómputo, mejorar el apoyo a sus usuarios finales y componentes.

Enfocados en los procesos que se ejecutan desde el NOC de UNISYS y la gran importancia que tiene los mismos, para alcanzar los objetivos de la organización, se pretende realizar un análisis de riesgos informáticos que permita identificar las causas de posibles amenazas, estimar el impacto que estos eventos indeseados pueden generar contra el buen funcionamiento de los procesos de esta área de negocio de la organización y posteriormente plantear medidas de protección que

permitan mitigar o minimizar el nivel de afectación a la realización de los procesos diarios de negocio y por ende, a la buena imagen de la organización.

4.2.1 Apreciación del riesgo

4.2.1.1 Identificación de amenazas. Teniendo en cuenta que en la metodología MAGERIT establece, que un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Por lo tanto, el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Entonces, en esta etapa se identificaron las posibles amenazas que pueden afectar los procesos de negocio diario del NOC de UNISYS, estos puntos críticos de esta importante área de la organización, se determinaron enfocados hacía la temática de seguridad informática. A continuación, en la tabla 3 se muestra los resultados de esta etapa del análisis de riesgos.

Tabla 3. Matriz de identificación de amenazas

No.	Amenaza	Causas
1	**Inadecuado control de acceso lógico**	Ingreso de usuarios no autorizados
		Uso inapropiado del software
		Manipulación, borrado, alteración de datos
2	**Niveles de acceso no establecidos**	Acceso a información confidencial
		Abuso de privilegios de acceso
		Instalación de software
		Manejo inadecuado de información confidencial
3	**Asignación inadecuada de perfiles de usuarios**	Acceso a información restringida
		Manipulación de la configuración
		Instalación de software malicioso
4	**Gestión deficiente de password**	Descifrado sistemático de passwords
		Suplantación de usuario
5	**Suplantación IP**	Ataques de denegación de servicios
		Análisis de tráfico

		Interceptación de información
		Ataque man in the middle
		Suplantación router o gateway
6	**Información sin clasificación**	Información confidencial de acceso público
		Divulgación de información secreta a terceros
7	**Instalación por defecto de sistemas y aplicaciones**	Puertos lógicos en desuso abiertos
		Servicios no utilizados
8	**Recursos compartidos en red no protegidos**	Fuga de información
		Modificación de información
		Difusión de software dañino
9	**Uso de recursos sin monitoreo**	Inadecuado uso de recursos
10	**Intercambio de información sin cifrar**	Revelación de información confidencial
		Conexiones no seguras
11	**No registro de Logs de acceso**	Ataques de denegación de servicios DOS
		Ataques de diccionario de datos
		Ataques XSS
		Ataques de SQL Injection
12	**No registro de logs del sistema**	Instalación de software espías
		Puertas traseras o backdoors
		Indisponibilidad de recursos
		Deficiencia para restaurar el sistema
13	**Conexiones externas sin autenticación**	Acceso a información restringida de la compañía
14	**Grupos no establecidos para roles de usuarios**	Error en asignación de privilegios de usuarios
15	**Múltiples conexiones por usuario**	Suplantación de identidad de usuario
16	**No verificar la complejidad de**	Contraseñas débiles
		Descifrado de contraseñas

	contraseñas	Ingeniería social
17	**No restringir horarios de conexión**	Capturas de cookies de sesión
		Secuestros de sesiones TCP
		Acceso a recursos para actividades no laborales
18	**Uso de controles criptográficos deficiente**	Protocolos criptográficos descifrables
		Cifrado de conexiones con errores
		Autenticación de usuarios no autorizados
		Suplantación de autoridades certificadoras
19	**Crecimiento del negocio**	Degradación del servicio
		Servicio no confiable
		Degradación de la disponibilidad
		Pérdida de capacidad
20	**Instalación no controlada de software**	Uso ilegal de software
		Uso inapropiado del software
		Descarga no controlada de software
		Violación derechos de autor
		Uso de software sin licencias
21	**Administración deficiente**	Incompletitud
		Inexactitud
		Incorrección
		Desactualización
		Pérdida de disponibilidad
		Deterioro de medio de almacenamiento

Fuente: Los autores

4.2.1.2 Análisis de los riesgos. En esta sección se busca calificar los riesgos encontrados en la etapa anterior, para este proceso utilizaremos las siguientes tablas de probabilidad e impacto, las cuales tiene escalas de medición establecidas. Además, el riesgo se calcula mediante la siguiente fórmula:

Tabla 4. Matriz estimación del impacto

Impacto		Degradación		
		1%	10%	100%
Valor	MA	**M**	**A**	**MA**
	A	**B**	**M**	**A**
	M	**MB**	**B**	**M**
	B	**MB**	**MB**	**B**
	MB	**MB**	**MB**	**MB**

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. Página 6.

Tabla 5. Definición de niveles de impacto en términos de negocio

Impactos en términos de negocio			
Valor Cualitativo	**Denominación**	**Descripción**	**Valor Cuantitativo**
MA	Muy Alta	Indisponibilidad total y compromiso total	5
A	Alta	Perdida de la conectividad, integridad de información y disponibilidad de servicios	4
M	Media	Se requieren controles, daño de la reputación organizacional y la confidencialidad de la información	3
B	Baja	Se requieren controles para mitigar la severidad	2
MB	Muy Baja	No se requieren controles para mitigar la severidad	1

Fuente: Los autores

Tabla 6. Escalas de evaluación

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: Muy Alto	**MA:** Prácticamente seguro	**MA:** Crítico
A: Alto	**A:** Probable	**A:** Importante
M: Medio	**M:** Posible	**M:** Apreciable
B: Bajo	**B:** Poco probable	**B:** Bajo
MB: Muy Bajo	**MB:** Muy raro	**MB:** Despreciable

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. p. 7.

Tabla 7. Probabilidad de ocurrencia de los riesgos

Matriz de Probabilidad			
Valor Cualitativo	**Denominación**	**Descripción**	**Valor Cuantitativo**
MA	Muy Alta	Prácticamente seguro	5
A	Alta	Probable	4
M	Media	Posible	3
B	Baja	Poco Probable	2
MB	Muy Baja	Muy raro	1

Fuente: Los autores

Tabla 8. Matriz estimación del riesgo

Riesgo		**probabilidad**				
		MB	B	M	A	MA
Impacto	MA	**A**	**MA**	**MA**	**MA**	**MA**
	A	**M**	**A**	**A**	**MA**	**MA**
	M	**B**	**M**	**M**	**A**	**A**
	B	**MB**	**B**	**B**	**M**	**M**
	MB	**MB**	**MB**	**MB**	**B**	**B**

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. p. 7.

En relación a la Matriz de estimación de riesgo, la junta directiva de la compañía estableció que los niveles de riesgo del NOC de UNISYS, se manejarán como se muestra en la tabla X.

Tabla 9. Valoración de riesgo

	Riesgos	Decisión Gerencial	Rangos
MA	**Crítico**	La organización TOMARÁ MEDIDAS DRÁSTICAS para hacer tratamiento de este riesgo, dándole máxima prioridad.	**23 a 25**
A	**Importante**	La organización TOMARÁ MEDIDAS MAYORES para hacer tratamiento de este riesgo, dándole una alta prioridad.	**18 a 22**
M	**Apreciable**	La organización TOMARÁ MEDIDAS CONSIDERABLES, para hacer tratamiento de este riesgo.	**12 a 17**
B	**Bajo**	La organización TOMARÁ MEDIDAS MÍNIMAS para hacer tratamiento de este riesgo.	**06 a 11**
MB	**Despreciable**	La organización NO TOMARA MEDIDAS al respecto. Ningún control será aplicado. La gerencia acepta este nivel de riesgo.	**01 a 05**

No.	Nombre del Riesgo	Causas	PROBABILIDAD		IMPACTO		VALORACIÓN DEL RIESGO
			Criterio cualitativo	Factor cuantitativo	Criterio cualitativo	Factor cuantitativo	
1	Inadecuado control de acceso lógico	Ingreso de usuarios no autorizados	MA	5	M	4	20
		Uso inapropiado del software	MA	5	A	4	20
		Manipulación, borrado, alteración de datos	MA	5	A	4	20
2	Niveles de acceso no establecidos	Acceso a información confidencial	MA	5	A	4	20
		Abuso de privilegios de acceso	MA	5	A	5	25
		Instalación de software	MA	5	M	3	15
		Manejo inadecuado de información confidencial	MA	5	M	3	15
3	Asignación inadecuada de perfiles de usuarios	Acceso a información restringida	MA	5	A	4	20
		Manipulación de la configuración	MA	5	MA	5	25
		Instalación de software malicioso	MA	5	MA	5	25
4	Gestión deficiente de password	Descifrado sistemático de passwords	MA	5	M	3	15
		Suplantación de usuario	A	4	A	4	16
5	Suplantación IP	Ataques de denegación de servicios	MA	5	MA	5	25
		Análisis de tráfico	MA	5	M	3	15
		Interceptación de información	MA	5	A	4	20
		Ataque man in the middle	MA	5	MA	5	25
		Suplantación router o	MA	5	MA	5	25

		gateway					
6	**Información sin clasificación**	Información confidencial de acceso público	**MA**	**5**	**M**	**3**	**15**
		Divulgación de información secreta a terceros	**MA**	**5**	**A**	**4**	**20**
7	**Instalación por defecto de sistemas y aplicaciones**	Puertos lógicos en desuso abiertos	**A**	**4**	**A**	**4**	**16**
		Servicios no utilizados	**A**	**4**	**A**	**4**	**16**
8	**Recursos compartidos en red no protegidos**	Fuga de información	**MA**	**5**	**M**	**3**	**15**
		Modificación de información	**MA**	**5**	**A**	**4**	**20**
		Difusión de software dañino	**MA**	**5**	**MA**	**5**	**25**
9	**Uso de recursos sin monitoreo**	Inadecuado uso de recursos	**MA**	**5**	**A**	**4**	**20**
10	**Intercambio de información sin cifrar**	Revelación de información confidencial	**MA**	**5**	**M**	**3**	**15**
		Conexiones no seguras	**MA**	**5**	**A**	**4**	**20**
11	**No registro de Logs de acceso**	Ataques de denegación de servicios DOS	**MA**	**5**	**MA**	**5**	**25**
		Ataques de diccionario de datos	**MA**	**5**	**A**	**4**	**20**
		Ataques XSS	**A**	**4**	**M**	**3**	**12**
		Ataques de SQL Injection	**A**	**4**	**A**	**4**	**16**
12	**No registro de logs del sistema**	Instalación de software espías	**MA**	**5**	**M**	**3**	**15**
		Puertas traseras o backdoors	**MA**	**5**	**MA**	**5**	**25**
		Indisponibilidad de recursos	**MA**	**5**	**MA**	**5**	**25**
		Deficiencia para restaurar el sistema	**MA**	**5**	**MA**	**5**	**25**

13	**Conexiones externas sin autenticación**	Acceso a información restringida de la compañía	**MA**	**5**	**M**	**3**	**15**
14	**Grupos no establecidos para roles de usuarios**	Error en asignación de privilegios de usuarios	**A**	**4**	**M**	**5**	**20**
15	**Múltiples conexiones por usuario**	Suplantación de identidad de usuario	**MA**	**5**	**M**	**3**	**15**
16	**No verificar la complejidad de contraseñas**	Contraseñas débiles	**MA**	**5**	**M**	**3**	**15**
		Descifrado de contraseñas	**MA**	**5**	**M**	**4**	**20**
		Ingeniería social	**MA**	**5**	**M**	**4**	**20**
17	**No restringir horarios de conexión**	Capturas de cookies de sesión	**MA**	**5**	**MA**	**5**	**25**
		Secuestros de sesiones TCP	**MA**	**5**	**M**	**4**	**20**
		Acceso a recursos para actividades no laborales	**MA**	**5**	**B**	**2**	**10**
18	**Uso de controles criptográficos deficiente**	Protocolos criptográficos descifrables	**MA**	**5**	**M**	**3**	**15**
		Cifrado de conexiones con errores	**MA**	**5**	**A**	**4**	**20**
		Autenticación de usuarios no autorizados	**MA**	**5**	**M**	**3**	**15**
		Suplantación de autoridades certificadoras	**MA**	**5**	**M**	**3**	**15**
19	**Crecimiento del negocio**	Degradación del servicio	**A**	**4**	**M**	**3**	**12**
		Servicio no confiable	**MA**	**5**	**M**	**3**	**15**
		Degradación de la disponibilidad	**MA**	**5**	**MA**	**5**	**25**
		Pérdida de capacidad	**MB**	**1**	**A**	**4**	**4**
20	**Instalación no controlada de**	Uso ilegal de software	**MA**	**5**	**M**	**3**	**15**
		Uso inapropiado del	**MA**	**5**	**F**	**4**	**20**

	software	software					
		Descarga no controlada de software	**A**	**4**	**M**	**3**	**12**
		Violación derechos de autor	**MA**	**5**	**M**	**3**	**15**
		Uso de software sin licencias	**MA**	**5**	**M**	**3**	**15**
21	**Administración deficiente**	Incompletitud	**A**	**4**	**MA**	**5**	**20**
		Inexactitud	**A**	**4**	**MA**	**5**	**20**
		Incorrección	**A**	**4**	**MA**	**5**	**20**
		Desactualización	**A**	**4**	**MA**	**5**	**20**
		Pérdida de disponibilidad	**MA**	**5**	**A**	**4**	**20**
		Deterioro de medio de almacenamiento	**MA**	**5**	**A**	**4**	**20**

Fuente: Los autores

4.2.1.3 Evaluación de los riesgos

Tabla 10. Efectos en términos de negocio

No.	Nombre del Riesgo	Causas	Efecto
1	**Inadecuado control de acceso lógico**	Ingreso de usuarios no autorizados	Reputación de la organización
		Uso inapropiado del software	Incumplimiento cláusulas de servicio con terceros
		Manipulación, borrado, alteración de datos	Información no confiable para operaciones de negocio
2	**Niveles de acceso no establecidos**	Acceso a información confidencial	Perdida de la confidencialidad de la información
		Abuso de privilegios de acceso	Suplantación de usuarios administradores de red
		Instalación de software	Uso de software no permitido por la compañía
		Manejo inadecuado de información confidencial	Divulgación de información confidencial a terceros
3	**Asignación inadecuada de perfiles de usuarios**	Acceso a información restringida	Perdida de la confidencialidad de la información
		Manipulación de la configuración	Errores de configuración en los sistemas de gestión
		Instalación de software malicioso	Denegación de servicios a recursos informáticos
4	**Gestión deficiente de password**	Descifrado sistemático de passwords	Accesos no autorizados mediante usuarios legítimos
		Suplantación de usuario	
5	**Suplantación IP**	Ataques de denegación de servicios	Indisponibilidad en los recursos tecnológicos
		Análisis de tráfico	Perdida de la confidencialidad de la información
		Interceptación de información	

		Ataque man in the middle	Perdida de la integridad de la información
		Suplantación router o Gateway	
6	**Información sin clasificación**	Información confidencial de acceso público	Perdida de la confidencialidad de la información
		Divulgación de información secreta a terceros	Divulgación de información confidencial
7	**Instalación por defecto de sistemas y aplicaciones**	Puertos lógicos en desuso abiertos	Generación de puntos débiles de seguridad
		Servicios no utilizados	
8	**Recursos compartidos en red no protegidos**	Fuga de información	Perdida de la confidencialidad de la información
		Modificación de información	Perdida de la integridad de la información
		Difusión de software dañino	Denegación de servicios a recursos informáticos
9	**Uso de recursos sin monitoreo**	Inadecuado uso de recursos	Administración deficiente de recursos de monitoreo
10	**Intercambio de información sin cifrar**	Revelación de información confidencial	Perdida de la confidencialidad de la información
		Conexiones no seguras	Interceptación de información sensible de
11	**No registro de Logs de acceso**	Ataques de denegación de servicios DOS	Indisponibilidad en los recursos tecnológicos
		Ataques de diccionario de datos	Accesos no autorizados
		Ataques XSS	Reputación de la organización
		Ataques de SQL Injection	Accesos no autorizados
12	**No registro de logs del sistema**	Instalación de software espías	Vigilancia tecnológica de terceros
		Puertas traseras o backdoors	Servicio desconfiable
		Indisponibilidad de recursos	Perdida de monitoreo y gestión de recursos
		Deficiencia para restaurar el sistema	Interrupción para continuar las operaciones de negocio

13	**Conexiones externas sin autenticación**	Acceso a información restringida de la compañía	Perdida de la confidencialidad de la información
14	**Grupos no establecidos para roles de usuarios**	Error en asignación de privilegios de usuarios	Labores de administración por personas no autorizadas
15	**Multiples conexionnes por usuario**	Suplantación de identidad de usuario	Accesos no autorizados mediante usuarios legítimos
16	**No verificar la complejidad de contraseñas**	Contraseñas débiles	Descifrado sistemático de contraseñas
		Descifrado de contraseñas	Accesos no autorizados median usuarios legítimos
		Ingeniería social	Descifrado de contraseñas mediante el entorno del usuario
17	**No restringir horarios de conexión**	Capturas de cookies de sesión	Accesos no autorizados a los recursos del NOC mediante sesiones establecidas por usuarios legítimos
		Secuestros de sesiones TCP	
		Acceso a recursos para actividades no laborales	Uso inadecuado de los recursos informáticos que afecta las operaciones diarias del NOC
18	**Uso de controles criptográficos deficiente**	Protocolos criptográficos descifrables	Confidencialidad e integridad de la información comprometida
		Cifrado de conexiones con errores	Indisponibilidad en los servicios ofrecidos
		Autenticación de usuarios no autorizados	Accesos no autorizados
		Suplantación de autoridades certificadoras	Re direccionamiento de tráfico de red hacía fuentes no confiables
19	**Crecimiento del negocio**	Degradación del servicio	La calidad de los servicios disminuye y por ende la satisfacción del cliente

		Servico no confiable	Los clientes no confían procesos del NOC
		Degradación de la disponibilidad	Monitoreo ineficiente y resolución de problemas con tiempos excedidos
		Pérdida de capacidad	El NOC no podrá cumplir con lo establecido en la cláusula de servicios
20	**Instalación no controlada de software**	Uso ilegal de software	Incumplimiento de leyes de derecho de autor
		Uso inapropiado del software	Uso del software no enfocado a las actividades de negocio
		Descarga no controlada de software	Descargar de virus, spyware y adware
		Violación derechos de autor	Multas y sanciones
		Uso de software sin licencias	
21	**Administración deficiente**	Incompletitud	Servicios generador sin cumplir a totalidad los objetivos acordados
		Inexactitud	Se realizan los procesos de negocio de manera oportuna pero se dejan brechas de servicio
		Incorrección	Se generan inconsistencia en procedimientos y no se corrigen
		Desactualización	Se ofrece el servicio mediante recursos desactualizados
		Pérdida de disponibilidad	Recursos de gestión no funcionales
		Deterioro de medio de almacenamiento	Actividades que afectan medios de almacenamiento de gestión de las operaciones del NOC

Fuente: Autores de la investigación

4.2.1.4 Tratamiento de los riesgos

Tabla 11. Matriz de tratamiento de riesgos

No.	Nombre del Riesgo	Causas	CONTROLES	DESCRIPCIÓN DEL CONTROL
1	**Inadecuado control de acceso lógico**	Ingreso de usuarios no autorizados	**Autenticación de usuarios**	**El servidor generará la autenticación de los usuarios mediante las credenciales de los mismos y aumentará el nivel de seguridad en el acceso a los activos de la red de la compañía**
		Uso inapropiado del software		
		Manipulación, borrado, alteración de datos		
2	**Niveles de acceso no establecidos**	Acceso a información confidencial	**Perfiles de usuarios**	**Entre las funcionalidades del servidor de autenticación se encuentra la función de crear usuarios con distintos perfiles de acceso**
		Abuso de privilegios de acceso		
		Instalación de software		
		Manejo inadecuado de información confidencial		
3	**Asignación inadecuada de perfiles de usuarios**	Acceso a información restringida	**Roles de usuario establecidos**	**Mensualmente se estará realizando auditoria a la base de datos del servidor TACACS, para efecto de validar el perfil y permisos de cada usuario.**
		Manipulación de la configuración		
		Instalación de software malicioso		
4	**Gestión deficiente de password**	Descifrado sistemático de passwords	**Políticas de contraseñas**	**El servidor tiene establecidas un nivel de complejidad aceptable para que las contraseñas de los usuarios no sean débiles**
		Suplantación de usuario		
5	**Suplantación IP**	Ataques de denegación de servicios	**Autenticación por usuario y contraseña**	**El servidor realiza la autenticación a nivel de capa de aplicación por lo que no hay riesgos de acceso por suplantación a nivel de IP**
		Análisis de tráfico		
		Interceptación de información		
		Ataque man in the middle		

		Suplantación router o Gateway		
6	**Información sin clasificación**	Información confidencial de acceso público Divulgación de información secreta a terceros	**Niveles de acceso a la información**	**La solución de seguridad a implementar maneja un nivel de jerarquía para acceso a la información establecida en cada perfil de usuario**
7	**Instalación por defecto de sistemas y aplicaciones**	Puertos lógicos en desuso abiertos Servicios no utilizados	**Autorización de usuarios**	**Cada vez que un usuario desee realizar un cambio en el sistema el servidor validará con el servidor si tiene las permisos y decidirá si permitir o rechazar la petición**
8	**Recursos compartidos en red no protegidos**	Fuga de información Modificación de información Difusión de software dañino	**Permisos de usuarios**	**La información contenida en recursos de red compartidos estará protegida, ya que solo podrá ser accedida por usuarios autorizados**
9	**Uso de recursos sin monitoreo**	Inadecuado uso de recursos	**Auditoría de sesiones**	**El servidor a implementar proporciona la utilidad de generar un log por cada sesión en donde se almacena todas las actividades realizadas por los usuarios**
10	**Intercambio de información sin cifrar**	Revelación de información confidencial Conexiones no seguras	**Conexiones cifradas**	**El servidor de autenticación cifra la información mediante protocolos criptográficos**
11	**No registro de Logs de acceso**	Ataques de denegación de servicios DOS Ataques de diccionario de datos Ataques XSS Ataques de SQL Injection	**Generación de logs de acceso**	**Cuando un usuario intenta conectarse al servidor de gestión de redes del NOC de UNISYS cada petición de conexión o de acceso queda registrada en los logs del servidor TACACS**
12	**No registro de logs del sistema**	Instalación de software espías Puertas traseras o backdoors Indisponibilidad de recursos	**Instalar aplicación server syslog para efectuar backup de**	**La Aplicación Server Syslog, estará unidad a recolectar todos los log de eventos del servidor Windows.**

		Deficiencia para restaurar el sistema	**los log de Eventos**	
13	**Conexiones externas sin autenticación**	Acceso a información restringida de la compañía	**Control de Acceso Por perfil de Usuario**	**Los usuarios que se logueen con el Servidor de TACACS no tendrán acceso a los recurso internos de la compañía, debido a los control establecidos en cada uno de los perfiles.**
14	**Grupos no establecidos para roles de usuarios**	Error en asignación de privilegios de usuarios	**Generación de Bitácora de Creación de Usuarios**	**Cada vez que un usuario ingrese o renuncie de la compañía y se encuentre en el NOC de UNISYS, se procederá a realizar backup de todo su perfil y posteriormente a su eliminación.**
15	**Múltiples conexiones por usuario**	Suplantación de identidad de usuario	**Limite se sesiones activas por usuario**	**Para brindar mayor nivel de seguridad y confiabilidad en las conexiones el servidor de autenticación permite solo una sesión activa por usuario**
16	**No verificar la complejidad de contraseñas**	Contraseñas débiles Descifrado de contraseñas Ingeniería social	**Políticas de contraseñas seguras y complejas**	**Todo miembro del NOC de UNISYS, deberá firmar un acuerdo de confidencialidad**
17	**No restringir horarios de conexión**	Capturas de cookies de sesión Secuestros de sesiones TCP Acceso a recursos para actividades no laborales	**Horarios por tipos de usuarios establecidos**	**Aquellos usuarios que se conecten desde Internet, se les hará backup de los log el cual quedaría plasmado, todos sus acceso y acciones realizadas.**
18	**Uso de controles criptográficos deficiente**	Protocolos criptográficos descifrables Cifrado de conexiones con errores Autenticación de usuarios no autorizados Suplantación de autoridades certificadoras	**Autenticación por algoritmos de cifrado robustos**	**Las Contraseñas y los sistemas de Cifrado, tales como los accesos a los equipos de comunicación se harán por medio del protocolo SSH.**
19	**Crecimiento**	Degradación del servicio	**Servidor de**	**La solución de seguridad a**

	del negocio	Servicio no confiable	**autenticación, autorización y auditoría**	**implementar garantizará la Confidencialidad, Integridad y Disponibilidad de la información y los activos tecnológicos utilizados para gestionar el buen funcionamiento de las redes de las compañías desde el NOC de UNISYS**
		Degradación de la disponibilidad		
		Pérdida de capacidad		
20	**Instalación no controlada de software**	Uso ilegal de software	**Privilegios de usuarios**	**El servidor de autenticación establece una jerarquía de niveles de ejecución de las distintas tareas de administración**
		Uso inapropiado del software		
		Descarga no controlada de software		
		Violación derechos de autor		
		Uso de software sin licencias		
21	**Administración deficiente**	Incompletitud	**Control sobre los recursos tecnológicos**	**El servidor gestionará el debido uso de los activos tecnológicos, contribuyendo a una administración eficiente de los dispositivos del NOC de UNISYS**
		Inexactitud		
		Incorrección		
		Desactualización		
		Pérdida de disponibilidad		
		Deterioro de medio de almacenamiento		

Fuente: Los autores

5. ANÁLISIS Y PLANTEAMIENTO DE LOS REQUERIMIENTOS QUE NECESITAN PARA SU IMPLEMENTACIÓN

5.1 TIPIFICACIÓN DEL PROBLEMA

La prospectiva de la seguridad informática es fácilmente vulnerada en la mayoría empresas y actualmente han surgido nuevas técnicas de robo informático: técnicas de suplantación de identidad, donde individuos u organizaciones ajenas acceden a la red para manipular información confidencial que son de la empresa, trayendo pérdidas financieras.

Actualmente la vulnerabilidad en las redes inalámbricas WLAN es el medio de transporte de la información, ya que el aire es un medio de acceso para cualquier persona. Por lo tanto cualquiera que capte señal del punto de acceso, podrá acceder a la red si tiene todos los elementos y herramientas para poder romper esa barrera de acceso. Con la posibilidad de navegar en la Intranet de la empresa como también navegar gratis en Internet, emplear la red como punto de ataque hacia otras redes, robar información, introducir virus o software maligno, entre muchas otras cosas.

Además los dispositivos de acceso son manejados con niveles de autorización de forma individual, donde es necesario registrar a los usuarios en cada dispositivo con la dirección MAC de los equipos inalámbricos. Lo cual demanda al administrador mayor tiempo para gestionar el acceso de autorización, ocasionando que con el tiempo se pierda este control y eso causa que se dejen puertos abiertos para el ingreso de usuarios no autorizados o de usuarios con cuentas caducadas.

5.2 ANÁLISIS DEL PROBLEMA EN EL ESCENARIO REAL

La empresa multinacional UNISYS de Colombia lleva más de 60 años en el mercado colombiano, compitiendo y siendo una empresa líder en sus productos que presta actualmente, requiere diseñar e implementar mayor seguridad en su red local, por eso se cuenta con un edificio central de 6 pisos en la Ciudad de Bogotá y otro en la ciudad de Medellín, donde trabajan aproximadamente 400 empleados directamente, y más de 600 usuarios indirectamente, ubicados en diversas áreas de trabajo.

Cada uno de los usuarios tendrá asignado una computadora para realizar sus labores diarias, dependiendo de sus necesidades algunos tendrán Desktop y otros Laptops:

Tabla 12**.** Tamaño de la red de UNISYS

Área	Números de Computadoras Personales	Número de Laptops
Networking Administrator	15	10
Systems Administrator	15	20
HelpDesk	320	40
Administración	15	10
Marketing	20	10
Ventas	10	15
Recursos Humanos	10	5

Fuente: Los autores

Los usuarios podrán acceder a los equipos de la red de acuerdo al nivel de privilegios de autorización, definidos de la siguiente manera grupal:

Tabla 13. Niveles de Control de Autorización

Usuarios Locales	Acceso a Equipos de Comunicación	Nivel de Privilegio de Acceso
Networking Administrator	Toda la Red	Privilegios 15 (Mayor Acceso)
Systems Administrator	Ninguno	Privilegios 0 (Menor Acceso)
NOC Unisys (Monitore)	Toda la Red	Privilegios 15 (Mayor Acceso)

Fuente: Los autores

La infraestructura del local, no permite realizar un cableado horizontal en todas las áreas de trabajo, y por ello se ha decidido implementar un red inalámbrica para que pueda cubrir dichas áreas, además será utilizada por usuarios que tengan dispositivos portátiles como, laptops, Iphone, BlackBerry, Ipad y en lugares donde los puntos de red no sean suficientes, como en la sala de reuniones. Esta red debe estar oculta y contar con un sistema de gestión de control de acceso a los usuarios por seguridad.

El administrador de la red será el encargado de otorgar privilegios a los grupos, o de manera individual a los usuarios que lo requieran, además debe estar informado de todos los eventos de la red. Por seguridad se requiere que la topología de la red no sea descubierta. También se requiere optimizar el uso de recursos a través de la implementación de un adecuado balanceo de carga.

6. DISEÑO DE LA SOLUCIÓN MEDIANTE EL ANÁLISIS PROSPECTIVO DE LOS REQUERIMIENTOS PROPUESTOS

Actualmente la implementación de una red segura consiste en separar la Red Cableada y la Red Inalámbrica debido que ambas usan interfaces de comunicación diferentes, por su esquema tecnológico, protocolos y estándares que las rigen. El sistema de seguridad deber ser diseñado de acuerdo a la infraestructura de la organización.

6.1 DISEÑO RED LAN

La topología conocida como Red LAN, el servidor AAA de autenticación a utilizar la implementación, distribución de direcciones IP dentro de la red y la configuración adecuada para su óptimo funcionamiento.

UNISYS de Colombia cuenta con 400 empleados, para que esta red se escalable en 4 años se debe tomar el 45% de crecimiento, con lo que tendremos que realizar el dimensionamiento para 300 usuarios. Además se tendrá en cuenta los nuevos proyectos y equipos que ingresaran bajo nuestra gestión y monitoreo para la adecuada segmentación y ordenamiento de la red, se ha considerado que en cada área habrá aproximadamente 50 usuarios y 10 usuarios inalámbricos.

Respecto al direccionamiento IP, se decidió utilizar dos redes clase B tomando en cuenta el número de usuarios de la empresa, una para la red LAN y otra para la red WLAN. La red LAN estará dividida en subredes mediante un mecanismo de subneteo, asimismo se implementará un sistema de VLANs para segmentar la red de manera más óptima y segura. A cada VLAN le corresponderá una subred.

Se tiene que como máximo van a haber 25 usuarios por cada área, lo que quiere decir que se deberá usar 5 bits para el host. Esto nos da un total de 30 direcciones IP para cada departamento, de las cuales se reservarán 3 direcciones para el gateway, la red y el broadcast.

129.222.128.129 / 27
129.222.128.1 1 0 0 0 0 0 0 / 27

Por ejemplo para la primera subred 129.222.128.129/27, que corresponde a la VLAN 20 - NET_MANAGER, se tiene el siguiente direccionamiento IP:

Tabla 14. Asignación de IPs en VLAN de administración de red**.**

IP Address: 129.222.128.192
Subnet Mask: 255.255.255.224

IP	Mask	Notes ...
129.222.128.192	255.255.255.224	Subnet Address
129.222.128.193	255.255.255.224	
129.222.128.194	255.255.255.224	
129.222.128.195	255.255.255.224	
129.222.128.196	255.255.255.224	
129.222.128.197	255.255.255.224	
129.222.128.198	255.255.255.224	
129.222.128.199	255.255.255.224	
129.222.128.200	255.255.255.224	
129.222.128.201	255.255.255.224	
129.222.128.202	255.255.255.224	
129.222.128.203	255.255.255.224	
129.222.128.204	255.255.255.224	
129.222.128.205	255.255.255.224	
129.222.128.206	255.255.255.224	
129.222.128.207	255.255.255.224	
129.222.128.208	255.255.255.224	
129.222.128.209	255.255.255.224	
129.222.128.210	255.255.255.224	
129.222.128.211	255.255.255.224	
129.222.128.212	255.255.255.224	
129.222.128.213	255.255.255.224	
129.222.128.214	255.255.255.224	
129.222.128.215	255.255.255.224	
129.222.128.216	255.255.255.224	
129.222.128.217	255.255.255.224	
129.222.128.218	255.255.255.224	
129.222.128.219	255.255.255.224	
129.222.128.220	255.255.255.224	
129.222.128.221	255.255.255.224	
129.222.128.222	255.255.255.224	Default-Gateway
129.222.128.223	255.255.255.224	Broadcast Address

Fuente: Los autores

Referenciando el ejemplo anterior la segmentación de la red y la asignación de dirección IPs para las diversas áreas de la red LAC y para las WLAN se realizará de la siguiente manera:

Tabla 15. Asignación de subredes por VLAN

VLAN SEGMENTATION		
VLAN ID	**Description**	**IP Segment**
10	GESTION	129.222.131.0 /27
20	NET_MANAGER	129.222.128.192 /27
30	SYS_MANAGER	129.222.128.224 /27
40	CARREFOUR	129.222.130.0 /27
50	ISA_BELCORP	129.222.129.32 /27
60	HENKEL	129.222.129.64 /27
70	AC_CRC	129.222.129.128 /25
80	LIBRE	129.222.129.0 /27
90	NOVARTIS	129.222.130.32 /27
110	MSC_UNI	129.222.130.64 /26
120	HENKEL-FLOWSERVE	129.222.130.128 /27
140	LIBRE	129.222.130.160 /27
150	TELEFONIA	129.222.134.0 /24
160	UNILEVER	129.222.131.192 /26
170	MICROSOFT	129.222.132.128 /27
180	BANCOLOMBIA	129.222.132.0 /25
500	DSM-ROYAL	192.168.0.0 /24
600	PUBLICA_NOVARTIS	186.116.9.208 /28
200	OUTSIDE_UNISYS	129.222.128.0 /28
400	VPN_CLIENTES	129.222.128.16 /28
100	OUTSIDE_TOOLS	129.222.128.32 /28

Fuente: Los autores

Tabla 16**.** Asignación de subredes con retalles

VLAN SEGMENTATION							
VLAN ID	Description	IP Segment	IP Red - IP Broadcast	IP Virtual Gateway	HSRP	IPs Failover Active - Standby	DHCP Server
10	GESTION	129.222.131.0 /27	129.222.131.0 - 129.222.131.31	N/A	N/A	129.222.131.1 - 129.222.131.30	N/A
20	NET_MANAGER	129.222.128.192 /27	129.222.128.192 - 129.222.128.223	129.222.128.193	129.222.128.194 - 129.222.128.195	129.222.128.196 - 129.222.128.197	129.224.76.20
30	SYS_MANAGER	129.222.128.224 /27	129.222.128.224 - 129.222.128.255	129.222.128.225	129.222.128.226 - 129.222.128.227	129.222.128.228 - 129.222.128.229	129.224.76.20
40	CARREFOUR	129.222.130.0 /27	129.222.130.0 - 129.222.130.31	129.222.130.1	129.222.130.2 - 129.222.130.3	129.222.130.4 - 129.222.130.5	129.224.76.20
50	ISA_BELCORP	129.222.129.32 /27	129.222.129.32 - 129.222.129.63	129.222.129.33	129.222.129.34 - 129.222.129.35	129.222.129.36 - 129.222.129.37	129.224.76.20
60	HENKEL	129.222.129.64 /27	129.222.129.64 - 129.222.129.95	129.222.129.65	129.222.129.66 - 129.222.129.67	129.222.129.68 - 129.222.129.69	129.222.131.2 - 129.222.131.3
70	AC_CRC	129.222.129.128 /25	129.222.129.128 - 129.222.129.255	129.222.129.129	129.222.129.130 - 129.222.129.131	129.222.129.132 - 129.222.129.133	129.224.76.20
80	LIBRE	129.222.129.0 /27	129.222.129.0 - 129.222.129.31	129.222.129.1	129.222.129.2 - 129.222.129.3	129.222.129.4 - 129.222.129.5	129.224.76.20
90	NOVARTIS	129.222.130.32 /27	129.222.130.32 - 129.222.130.63	129.222.130.33	129.222.130.34 - 129.222.130.35	129.222.130.36 - 129.222.130.37	129.224.76.20
110	MSC_UNI	129.222.130.64 /26	129.222.130.64 - 129.222.130.127	129.222.130.65	129.222.130.66 - 129.222.130.67	129.222.130.68 - 129.222.130.69	129.224.76.20
120	HENKEL-FLOWSERVE	129.222.130.128 /27	129.222.130.128 - 129.222.130.159	129.222.130.129	129.222.130.130 - 129.222.130.131	129.222.130.132 - 129.222.130.133	129.224.76.20
140	LIBRE	129.222.130.160 /27	129.222.130.160 - 129.222.130.191	129.222.130.161	129.222.130.162 - 129.222.130.163	129.222.130.164 - 129.222.130.165	129.224.76.20
150	TELEFONIA	129.222.134.0 /24	129.222.134.0 - 129.222.134.255	129.222.134.1	129.222.134.2 - 129.222.134.3	129.222.134.4 - 129.222.134.5	129.224.76.20
160	UNILEVER	129.222.131.192 /26	129.222.131.192 - 129.222.131.255	129.222.131.193	129.222.131.194 - 129.222.134.195	129.222.131.196 - 129.222.131.197	129.222.131.2 - 129.222.131.3
170	MICROSOFT	129.222.132.128 /27	129.222.132.128 - 129.222.132.159	129.222.152.129	129.222.152.130 - 129.222.132.131	129.222.132.132 - 129.222.132.133	129.222.131.2 - 129.222.131.3
180	BANCOLOMBIA	129.222.132.0 /25	129.222.132.0 - 129.222.132.127	129.222.132.1	129.222.132.2 - 129.222.132.3	129.222.132.4 - 129.222.132.5	129.222.131.2 - 129.222.131.3
500	DSM-ROYAL	192.168.0.0 /24	192.168.0.0 - 192.168.0.255	192.168.0.1	N/A	N/A	192.168.0.1
600	PUBLICA_NOVARTIS	186.116.9.208 /28	186.116.9.208 - 186.116.9. 223	186.116.9.209	N/A	N/A	186.116.9.209
200	OUTSIDE_UNISYS	129.222.128.0 /28	129.222.128. 0 - 129.222.128. 15	129.222.128.1	N/A	129.222.128.2 - 129.222.128.3	N/A
400	VPN_CLIENTES	129.222.128.16 /28	129.222.128.16 - 129.222.128.31	129.222.128.15	N/A	129.222.128.26 - 129.222.128.27	N/A
100	OUTSIDE_TOOLS	129.222.128.32 /28	129.222.128.32 - 129.222.128.47	129.222.128.33	N/A	129.222.128.34 - 129.222.128.35	N/A

Fuente: Los autores

Para evitar los bucles lógicos en la red LAN se implementará el protocolo RSTP (Rapid Spanning Tree Protocol) para conseguir una convergencia rápida para optimizar la red. Además implementaremos Etherchannel para optimizar los enlaces de los switches, agrupando dos enlaces FastEthernet en una solo interfaz lógica (Port-channel), con ello podremos ampliar el ancho de banda a 400 Mbps, obtener balanceo de carga entre las interfaces físicas del Port-channel y redundancia de enlace, ya que si una interfaz física deja de funcionar las tramas serán recibidas por el enlace restante. Como protocolos de negociación tenemos: PAgP (Port Aggregation Protocol) propietario de Cisco y LACP (Link Aggregation Control Protocol) descrito en la norma IEEE 802.3ad, ambos protocolos se configuran de forma similar; sin embargo, usaremos PAgP porque tiene como ventaja la modificación automática del Portchannel en un extremo si el otro extremo es modificado.[17]

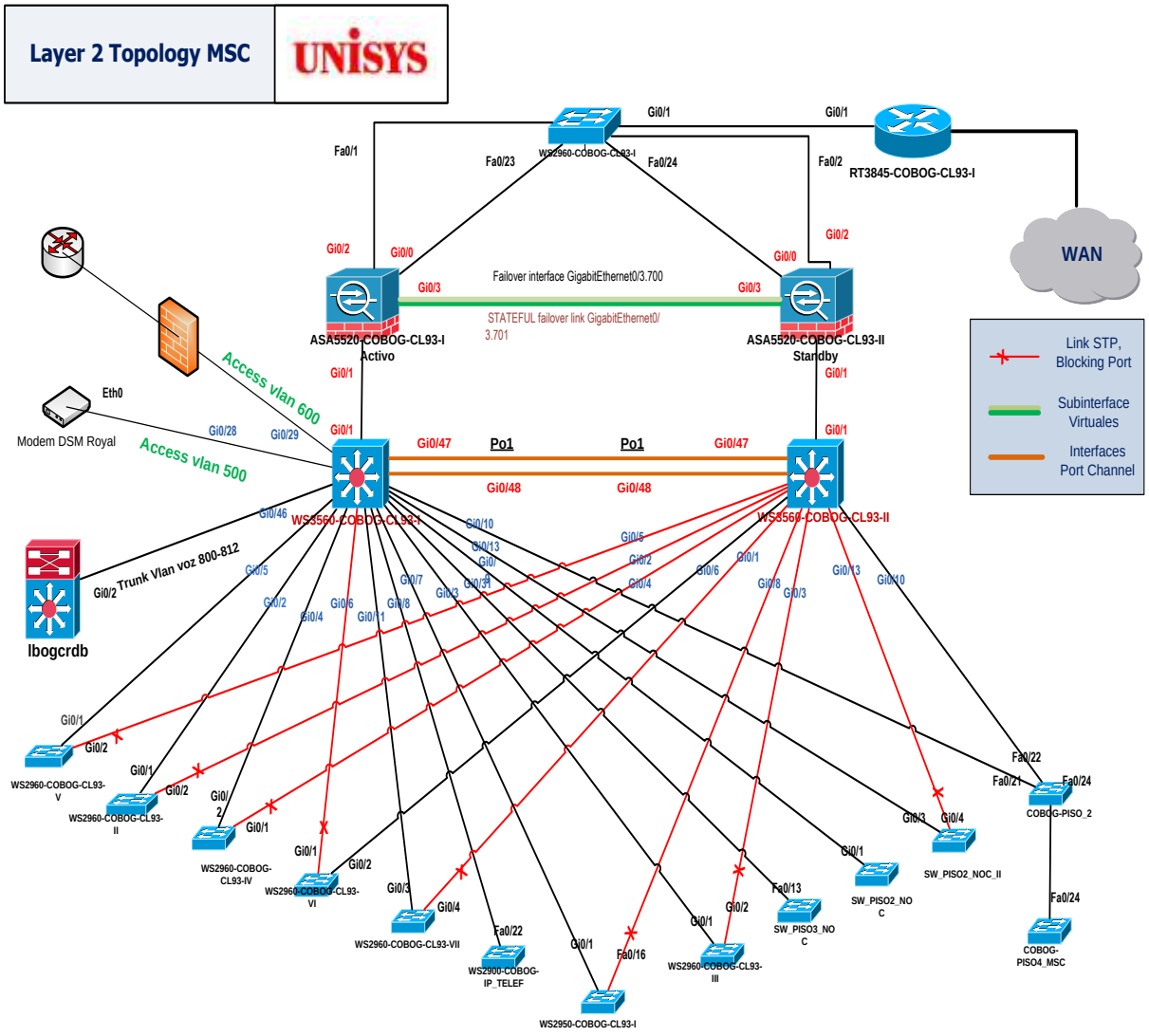
Para implementar redundancia al gateway de la red tenemos dos protocolos: Protocolo de intercambio para Router HSRP (Hot Standby Router Protocol) y GLBP (Gateway Load Balacing Protocol), usaremos GLBP porque además de brindar redundancia como HSRP, ofrece balanceo de carga. Asociaremos dos routers en un grupo GLBP y funcionarán como un solo router virtual, haciendo ambos el trabajo de reenvío de paquetes de manera balanceada. Utilizaremos Round Robin como tipo de balanceo de carga, esto será transparente para los usuarios porque ellos direccionan a una misma puerta de enlace (IP virtual de router), pero el balanceo se dará por las MACs virtuales que el protocolo GLBP enviará como respuesta a los mensajes ARP de los clientes.[18]

[17] LAZO GARCIA, Nuttsy Aurora. Diseño e implementación de una red LAN y WLAN con Sistema de control de acceso mediante servidores AAA. Tesis de grado.
[18] Ibid.

Para autenticar a los usuarios y centralizar el control de acceso a los equipos de la red instalaremos un servidor AAA, pues soporta el protocolo TACACS+. Su principal función es la gestión de acceso de acuerdo al nivel de autorización de cada usuario o grupo de usuarios, esto gracias que tiene separada la autenticación de la autorización permitiendo el filtrado de comandos, además debe registrar todos estos eventos para que el administrador pueda acceder a ellos.

La topología de la red será la siguiente:

Figura 14. Topología Física de la red LAN



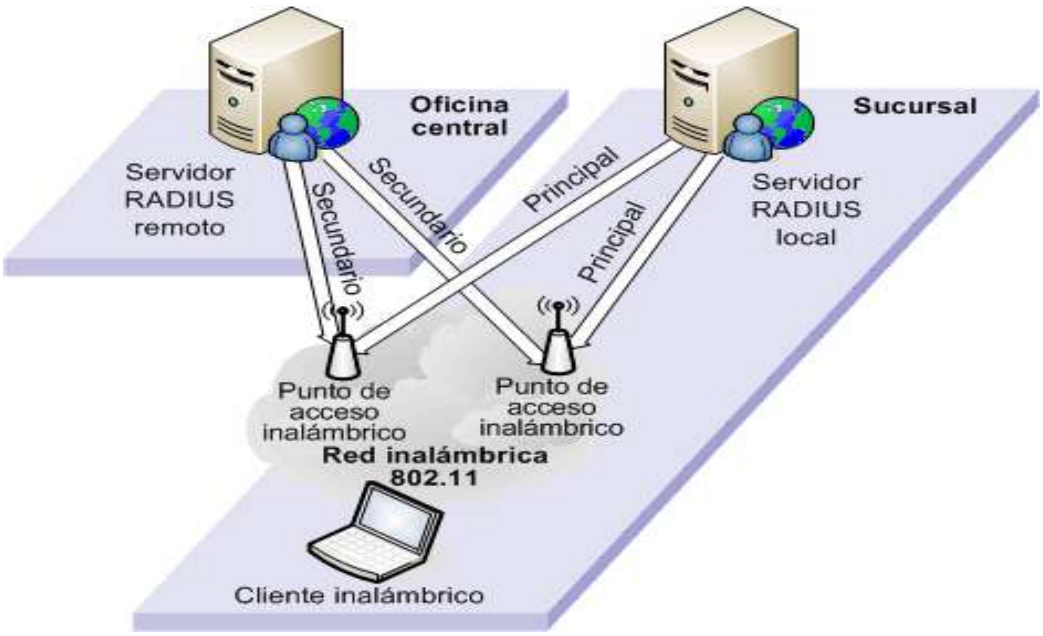
Fuente: Los autores

6.2 DISEÑO RED WLAN

Luego de tener clara la topología LAN a implementar, definiremos la topología de la WLAN, los servidores a utilizar en la implementación, el access point y la configuración adecuada para su funcionamiento. Cuando la red LAN ya esta implementada y la WLAN cuenta con una VLAN debemos implementar el servidor AAA de autenticación. Tomando en cuenta el análisis comparativo de los diversos servidores TACACS+ vs RADIUS realizado en los capítulos anteriores.

El AP (Access Point) será el cliente RADIUS, es decir será el encargado de establecer la comunicación entre el usuario inalámbrico y el servidor AAA de autenticación. Para ello debe ser configurado con los mismos protocolos de autenticación y cifrado que se configuro en el servidor RADIUS, debido que ya se configuró los parámetros del Servidor TACACS+ en lo Equipos de Comunicación. Para que la autenticación se realice de manera exitosa el usuario debe contar previamente con un certificado de autenticación otorgado por el servidor de certificados.
La siguiente será la topología de la WLAN:

Figura 15. Topología física de la red WLAN



Fuente: Los autores

6.3 REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DEL DISEÑO PROPUESTO

6.3.1 Punto de Acceso Inalámbrico (Access Point – AP). Para el acceso inalámbrico se va contar con varios Access Point que será el encargado de comunicar a los usuarios con el servidor AAA de autenticación (RADIUS-TACACS+), cumplirá el rol de cliente RADIUS, este deberá soportar como mecanismo de autenticación a WPA2-Enterprise (basado en el estándar IEEE 802.11i y cifrado AES/TKIP) y su mecanismo de autenticación debe estar basado en el estándar IEEE 802.1x (con EAP y PAE). La empresa cuenta con 50 usuarios inalámbricos.

6.3.2 Servidor AAA Autenticación RADIUS. El encargado de autenticar a los usuarios antes de permitir su acceso a la red va ser el servidor RADIUS, para ello se va instalar el servicio IAS en una PC con sistema operativo Windows Server 2003.

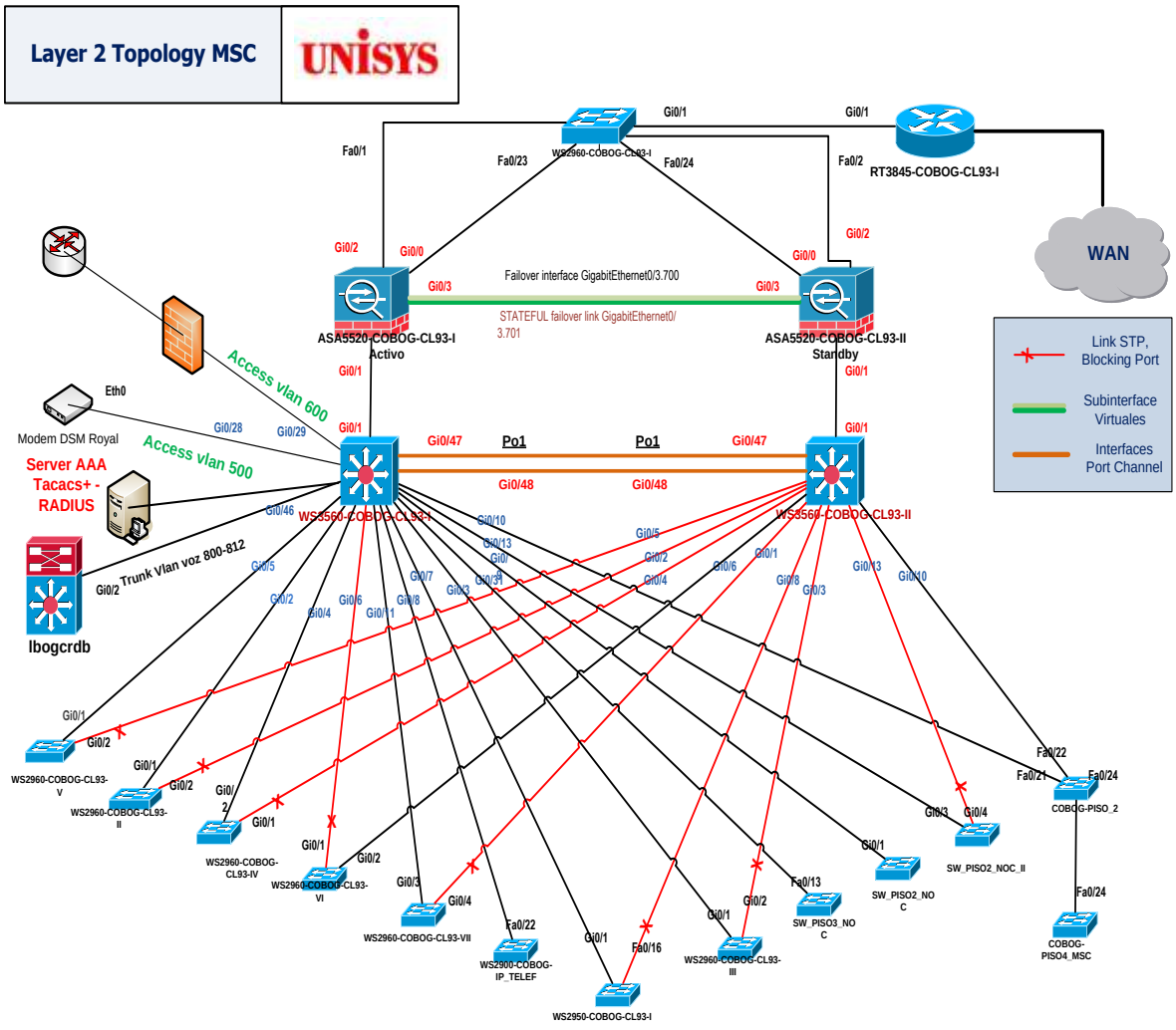
6.3.3 Servidor AAA Autenticación TACACS+. Este servidor será el encargado de centralizar los perfiles de los administradores de red y realizar el registro de eventos, para su implementarlo se requiere una PC con sistema operativo Windows Server 2003. Se usó una versión del software ACS 4.2 Licenciada descargado de la página WEB de Cisco, para este tipo de implementación, la configuración y el rendimiento de ambos (software y hardware) es similar.

6.3.4 Switches Acceso (Capa 2). La empresa cuenta con 400 usuarios cada uno cuenta con una PC o Laptop, tomando en consideración el crecimiento de la red a 4 años se contara con 300 usuarios. Para cubrir dicho número de usuarios vamos a necesitar 6 switches de 48 puertos, por donde se comunicarán el servidor AAA de Autenticación (usando el protocolo TACACS+) y los equipos de la LAN. También se comunicarán por ahí el servidor AAA de Autenticación RADIUS y el Cliente RADIUS y los usuarios inalámbricos.

6.3.5 Switches CORE – Distribución – Router (Capa 3). Tendrá la función de puerta de enlace de la red y de servidor DHCP, se usarán dos Switches CORE, dos Switches de Dsitribución en redundancia de acceso con balanceo de carga para ofrecer mayor calidad de servicio mediante GLBP.

La siguiente topología de la red en conjunto será la siguiente:

Figura 16. Topología física de la red LAN



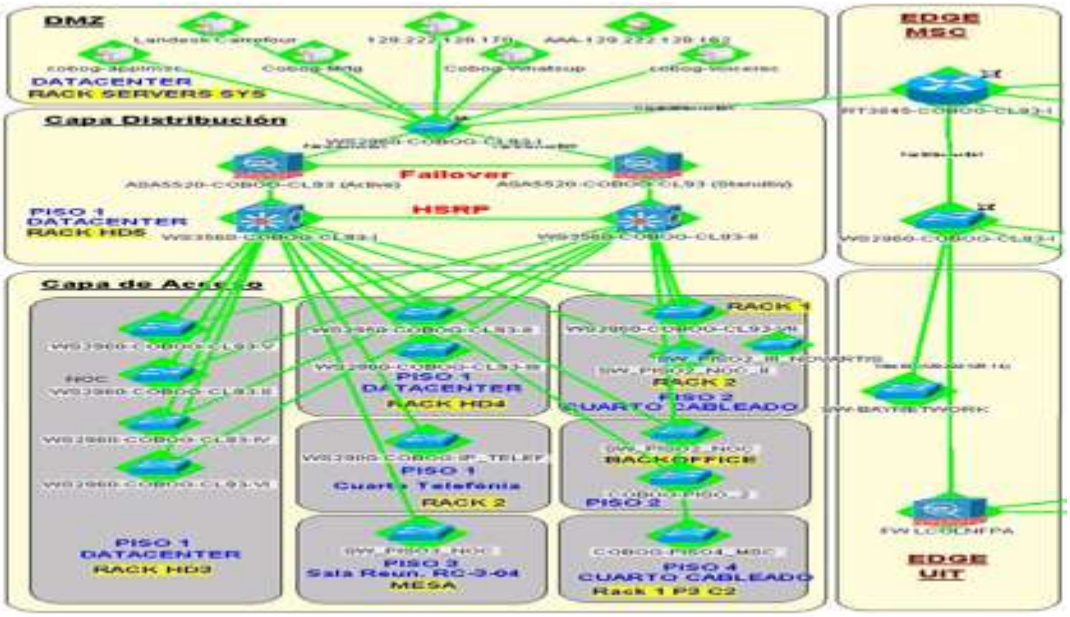
Fuente: Los autores

7. IMPLEMENTACIÓN DEL SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS EN LA RED OPERATIVA DE UNISYS DE COLOMBIA Y LA EFECTIVIDAD DE LOS CONTROLES PROPUESTOS

7.1 IMPLEMENTACIÓN DE LA TOPOLOGÍA Y CONFIGURACIÓN DE LA RED LAN

La implementación se realizó en el Ambiente Online Operativo de red LAN y WLAN de UNISYS de Colombia.

Figura 17. Esquema red operativa UNISYS de Colombia

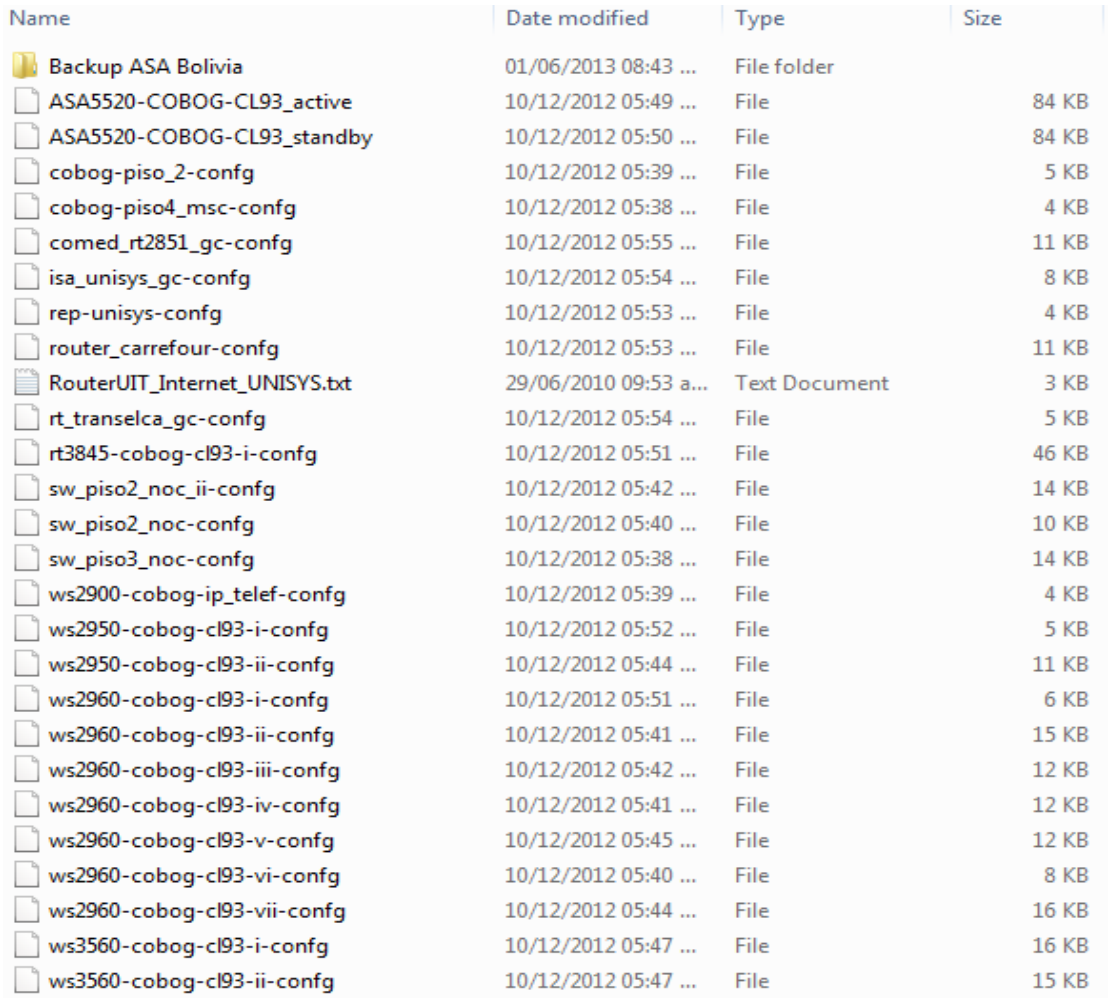


Fuente: Los autores

Por temas netamente de seguridad, no se dan a conocer las configuraciones de los equipos de comunicación de UNISYS de Colombia.

La ruta donde se tienen las respectivas configuraciones es: J:\Info_RSandoval\Solo Unisys\Informacion MSC Unisys\Informacion PC Walid\1. LACR INTERNAL\1. MSC Bogota\2. Documentacion Red MSC Bogota\Documentacion Red MSC Bogota v1.0 (Diciembre 2012)\3. Backups Equipos\Backups-10_12_2012

Figura 18. Red Operativa UNISYS de Colombia



Name	Date modified	Type	Size
Backup ASA Bolivia	01/06/2013 08:43 ...	File folder	
ASA5520-COBOG-CL93_active	10/12/2012 05:49 ...	File	84 KB
ASA5520-COBOG-CL93_standby	10/12/2012 05:50 ...	File	84 KB
cobog-piso_2-confg	10/12/2012 05:39 ...	File	5 KB
cobog-piso4_msc-confg	10/12/2012 05:38 ...	File	4 KB
comed_rt2851_gc-confg	10/12/2012 05:55 ...	File	11 KB
isa_unisys_gc-confg	10/12/2012 05:54 ...	File	8 KB
rep-unisys-confg	10/12/2012 05:53 ...	File	4 KB
router_carrefour-confg	10/12/2012 05:53 ...	File	11 KB
RouterUIT_Internet_UNISYS.txt	29/06/2010 09:53 a...	Text Document	3 KB
rt_transelca_gc-confg	10/12/2012 05:54 ...	File	5 KB
rt3845-cobog-cl93-i-confg	10/12/2012 05:51 ...	File	46 KB
sw_piso2_noc_ii-confg	10/12/2012 05:42 ...	File	14 KB
sw_piso2_noc-confg	10/12/2012 05:40 ...	File	10 KB
sw_piso3_noc-confg	10/12/2012 05:38 ...	File	14 KB
ws2900-cobog-ip_telef-confg	10/12/2012 05:39 ...	File	4 KB
ws2950-cobog-cl93-i-confg	10/12/2012 05:52 ...	File	5 KB
ws2950-cobog-cl93-ii-confg	10/12/2012 05:44 ...	File	11 KB
ws2960-cobog-cl93-i-confg	10/12/2012 05:51 ...	File	6 KB
ws2960-cobog-cl93-ii-confg	10/12/2012 05:41 ...	File	15 KB
ws2960-cobog-cl93-iii-confg	10/12/2012 05:42 ...	File	12 KB
ws2960-cobog-cl93-iv-confg	10/12/2012 05:41 ...	File	12 KB
ws2960-cobog-cl93-v-confg	10/12/2012 05:45 ...	File	12 KB
ws2960-cobog-cl93-vi-confg	10/12/2012 05:40 ...	File	8 KB
ws2960-cobog-cl93-vii-confg	10/12/2012 05:44 ...	File	16 KB
ws3560-cobog-cl93-i-confg	10/12/2012 05:47 ...	File	16 KB
ws3560-cobog-cl93-ii-confg	10/12/2012 05:47 ...	File	15 KB

Fuente: Los autores

La implementación se realizó en el ambiente operativo de redes de UNISYS de Colombia; donde se usaron 16 switches, 2 switches Core, 2 Firewall ASA Cisco, routers y 15 PCs para realizar las pruebas de interconexión y comunicación intra e inter VLAN. Se implementó la topología propuesta en el capítulo 3 en la FIGURA 3-1, con todos los protocolos propuestos sin ningún limitante: RSTP, Etherchannel, GLBP.

Cada switch se conectó por 2 enlaces GigaFastEthernet configurados en full duplex a una velocidad de 1000 BaseSX SFP, con lo que se consiguió un ancho de banda entre switches sea de 2 Gbps. Cada switch se conectó a todos los restantes de manera directa para tener redundancia y la caída de uno no afecte la comunicación entre los demás.

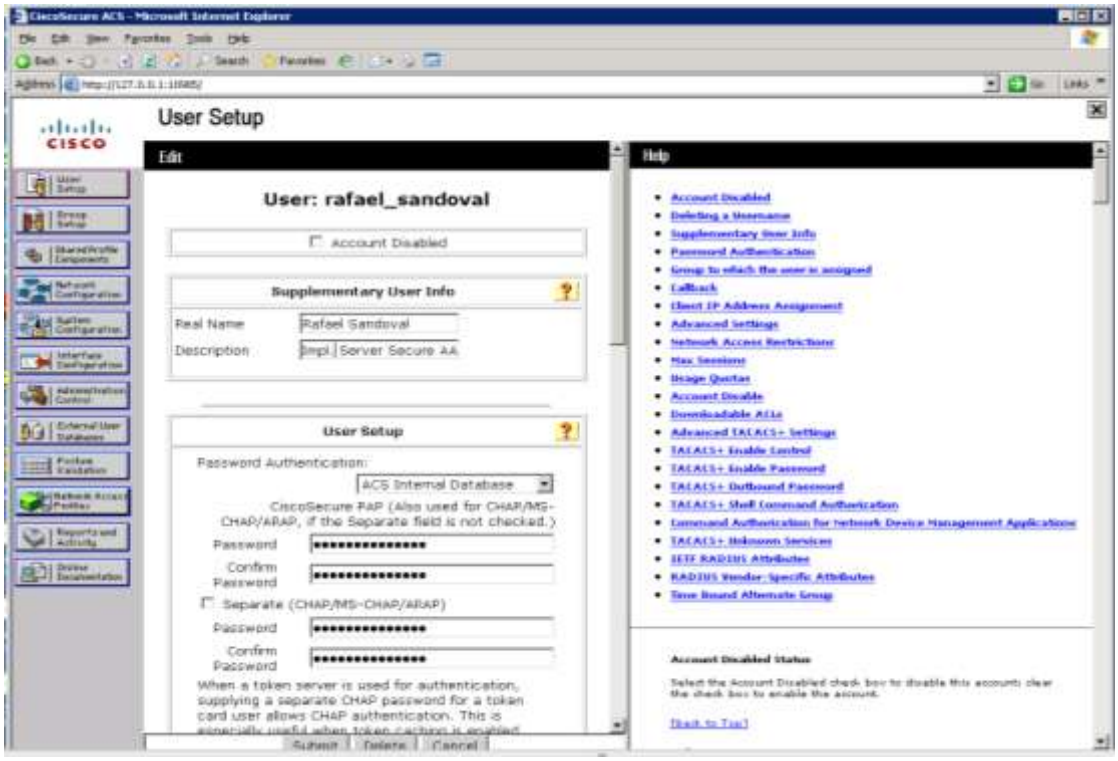
Los puertos han sido configurados como troncales pero diferenciando las VLAN necesarias la cual depende de las áreas de los usuarios para que se comunicarse entre ellas y alcanzar el destino requerido.

Debido al número de usuarios y la cantidad de subredes, se decidió implementar servidores DHCP en los Switches CORE de salida y Entrada, con esto se evitará un conflicto de direcciones. Gracias a la redundancia y balanceo de carga, si uno de ellos presenta problemas de funcionamiento se contará con un servidor de backup. Se reservan las 4 primeras direcciones IPs de cada subred para configuraciones de las puertas de enlace, IP virtual de ambos SWCORE y una para uso del administrador de red.

7.2 IMPLEMENTACIÓN DEL SERVIDOR AAA DE AUTENTICACIÓN TACACS+

Una vez afinada la red LAN operativa del NOC de UNISYS de Colombia, se debe implementar el servidor AAA de Autenticación TACACS+ encargado de autenticar a los usuarios que accedan a equipos de la red. A continuación, se muestra la configuración realizada:

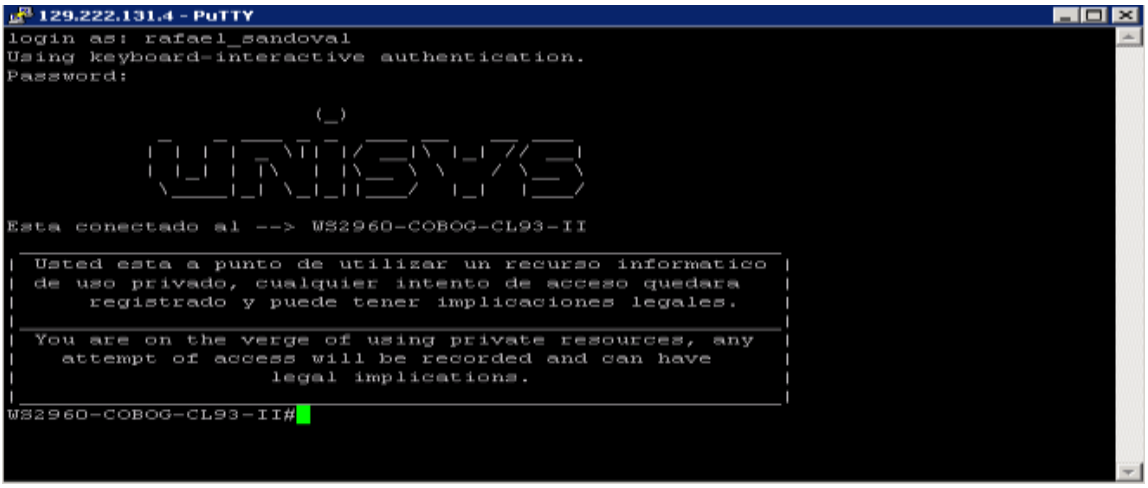
Figura 19**.** Servidor AAA TACACS+ operativo



Fuente: Los autores

Una vez implementado el servidor AAA TACACS+ en la maquina física robusta entregada por la corporación para tales fines, se agregó este nuevo elemento a la red y se ingresó a los equipos de la red mediante la autenticación y autorización que permite el Servidor AAA de TACACS+ configurado.

Figura 20. Conexión switches y autenticación servidor AAA TACACS+



Fuente: Los autores

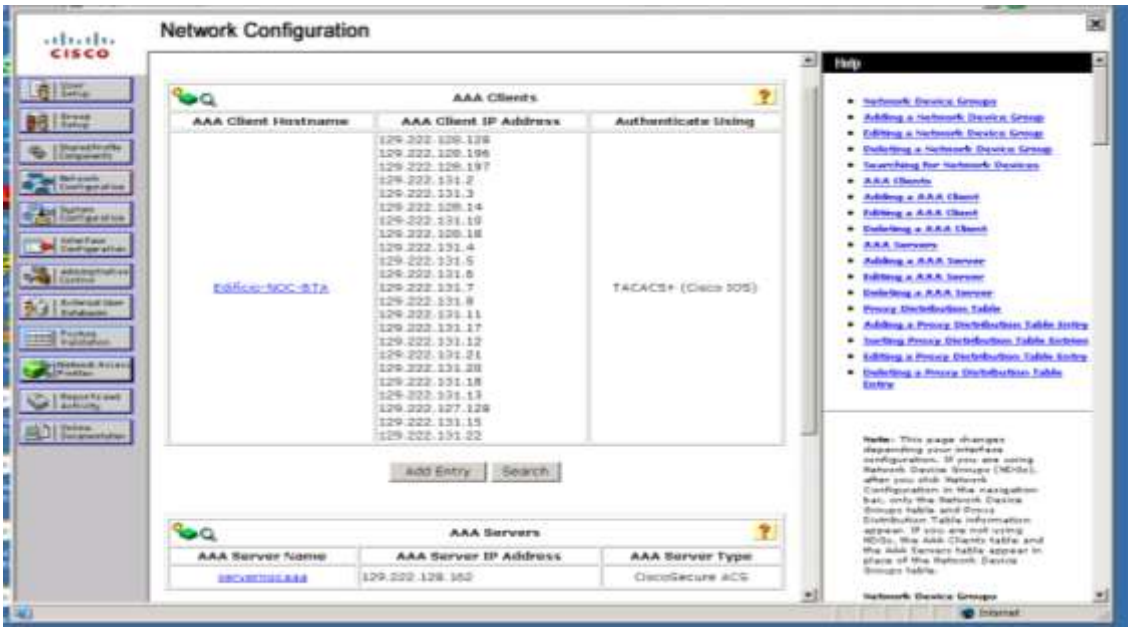
Para implementar el servidor AAA TACACS+ escogimos el Servidor Físico entregado por la corporación de Unisys de Colombia, el cual cuenta con las siguientes características: Procesador: Intel® Xeon® CPU E5504 @ 2.00 GHz, Memoria RAM: 4 GB, RAID 5, con Discos Duros de 500 Gb.

Primero se conectó el servidor en la VLAN NET_MANAGER y se instaló la versión licenciada del software Cisco TACACS+ descargado de la página web de CISCO, luego se creó un administrador del servidor AAA de Autenticación.

Ahora ingresamos los clientes TACACS+ que tiene la red: SW1… SW16, SWCORE y R2 con sus respectivas direcciones IPs (pertenecientes a la VLAN NET_MANAGER).

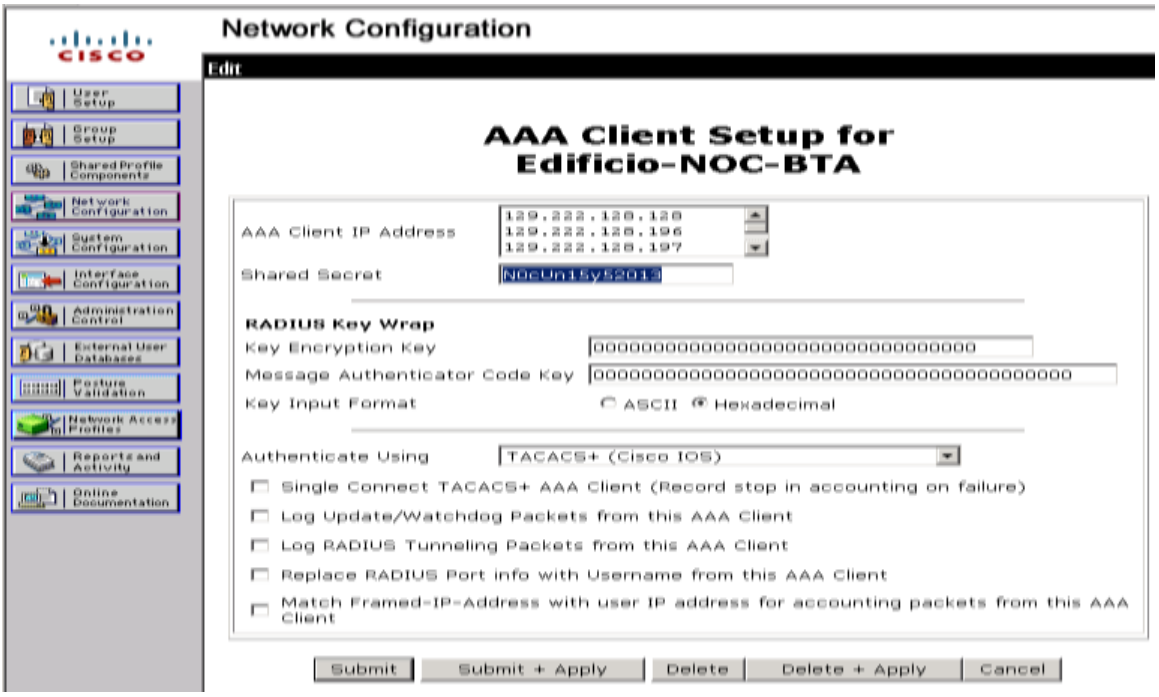
Además se ingresa la llave de seguridad que debe ser la misma en la configuración del cliente.

Figura 21. Lista de clientes TACACS+ en el servidor AAA de Autenticación



Fuente: Los autores

Figura 22. Registro de Cliente TACACS+ en el servidor AAA de Autenticación



Fuente: Los autores

Cuando los Clientes TACACS+ ya se encuentran registrados, creamos los grupos de usuarios que van a poder ingresar a los equipos de la red. Cada grupo tendrá un nivel de autorización diferente ya que como se indicó en el capítulo 2 los Networking Administrator y los System Administrator (Monitoreo) tendrán diferentes niveles de privilegios dentro de los equipos.

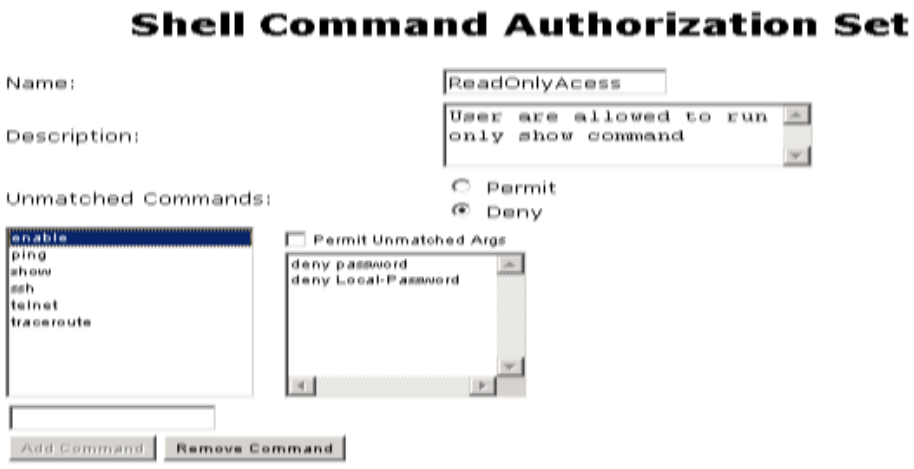
Los administradores van a tener nivel de privilegio 15 que es el nivel máximo, ellos podrán ver y realizar cambios en la configuración, a diferencia de System Administrator que solo podrán ver detalles de la red mas no la configuración del equipo ni realizar algún cambio en ella.

Figura 23. Grupos creados en el servidor AAA de Autenticación

Fuente: Los autores

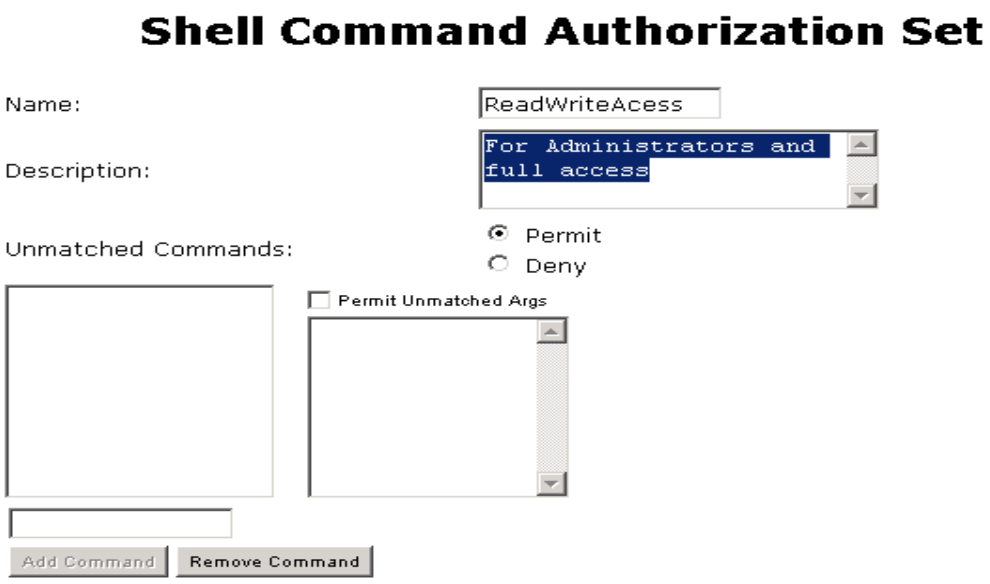
Como se muestra en la Figura 23, existen dos grupos creados de acuerdo a los procesos del NOC de UNISYS, a continuación se mostrará a detalle cada.

Figura 24. Detalle grupo ReadOnlyAccess



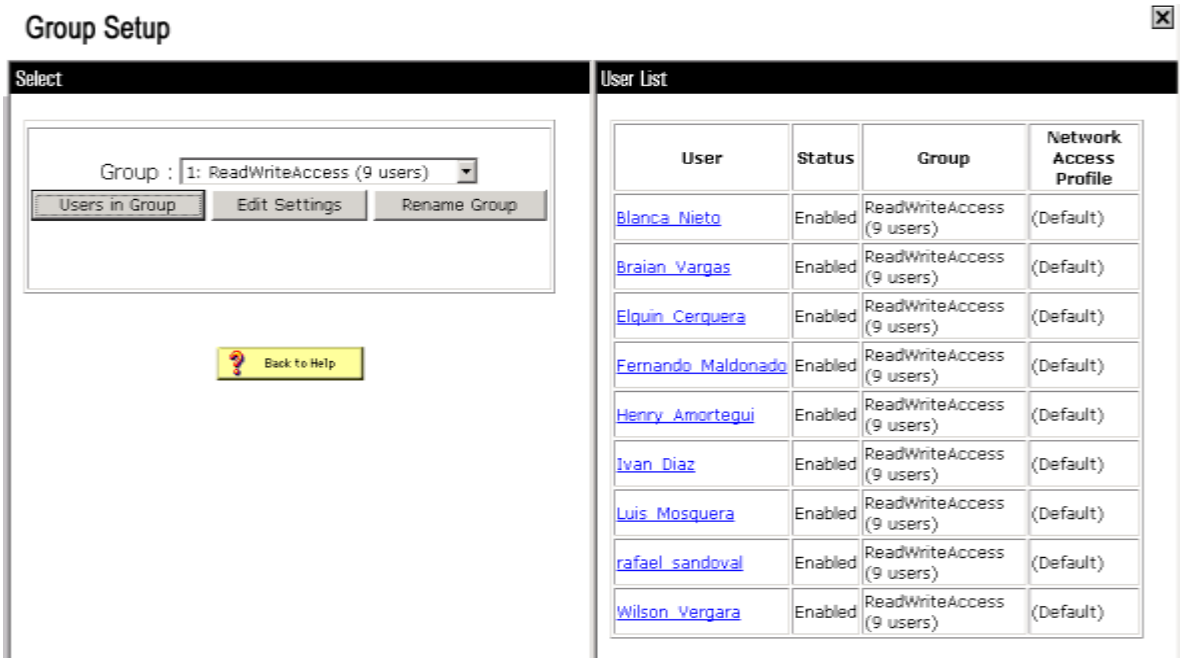
Fuente: Los autores

Figura 25. Detalle grupo ReadWriteAccess



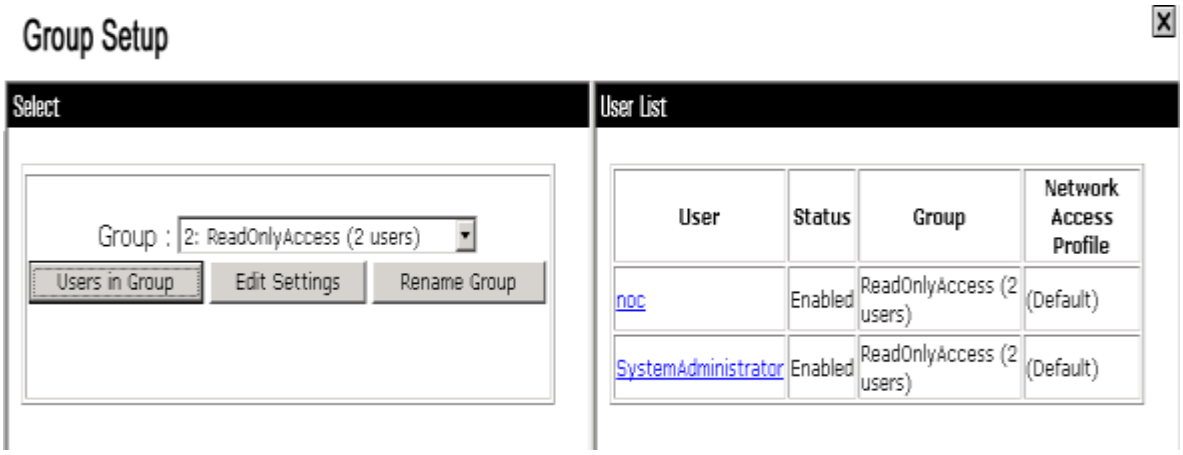
Fuente: Los autores

Figura 26. Grupos de administradores en el servidor AAA de Autenticación



Fuente: Los autores

Figura 27. Grupos de lectura en el servidor AAA de Autenticación



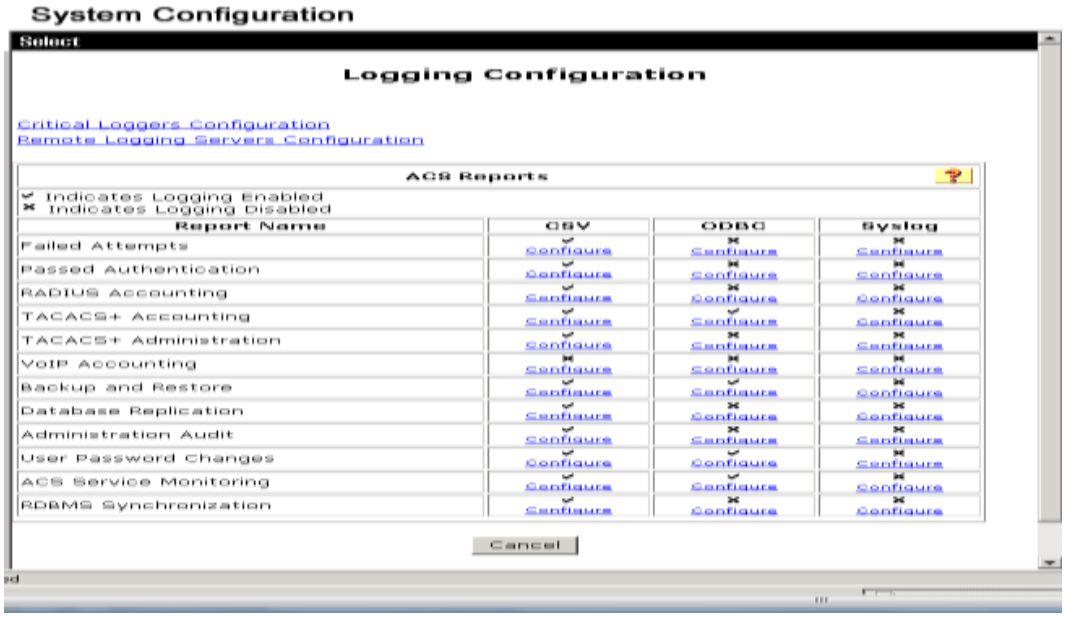
Fuente: Los autores

Los registros de eventos son archivos especiales que registran los eventos importantes que tienen lugar en el servidor AAA de Autenticación de Unisys de Colombia, como por ejemplo, cuando un usuario inicia una sesión en el equipo, que efectúe algún cambios sobre los equipos de comunicación, cuando se produce un error de autenticación, cuando se registran cada uno de los usuarios eliminados, o cual algún acceso no autorizado es registrado. Siempre que se producen estos tipos de eventos, El servidor AAA de autenticación de Unisys de Colombia, tiene incluido estás mejoras en un registro de eventos que se puede leer mediante el Visor de eventos.

Todos y cada uno de los estos reportes de logs de eventos, se pueden descargar para una mayor certificación de los mismos.

Los anteriores eventos, son el apoyo y la fiabilidad que se obtiene para demostrar en cualquier auditoria que efectivamente todas las amenazas y controles, son mitigadas. A continuación, se podrá observar los distintos log event implementados:

Figura 28. Configuración de los Logs Eventos del Servidor AAA de Autenticación TACACS+



Fuente: Los autores

Figura 29. Tipos de Reportes de Log Eventos Servidor AAA de Autenticación TACACS+

Fuente: Los autores

Figura 30. Reportes de Log Eventos Cuentas TACACS+

Fuente: Los autores

Figura 31. Reportes de Log Eventos Gestión del servidor AAA autenticación TACACS+

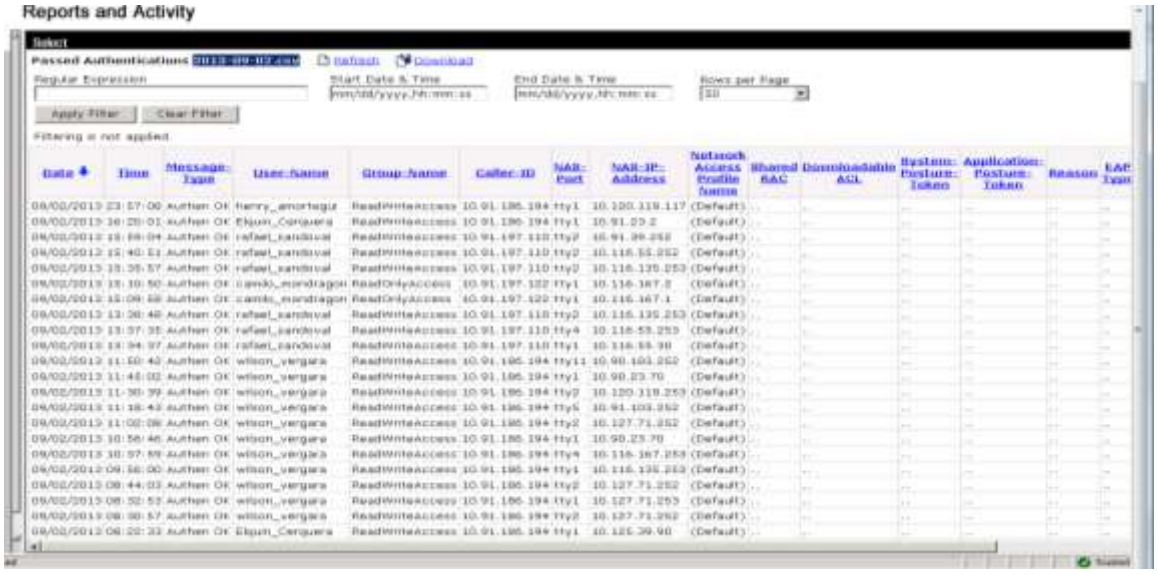
Fuente: Los autores

Figura 32. Reportes de Log Eventos Gestión del servidor AAA autenticación TACACS+

Fuente: Los autores

A continuación podemos observar al interior de alguno de estos archivos de logs, información más detallada:

Figura 33. Detalles de Reportes de Log Eventos de los usuarios Logueados al Servidor AAA autenticación TACACS+



Fuente: Los autores

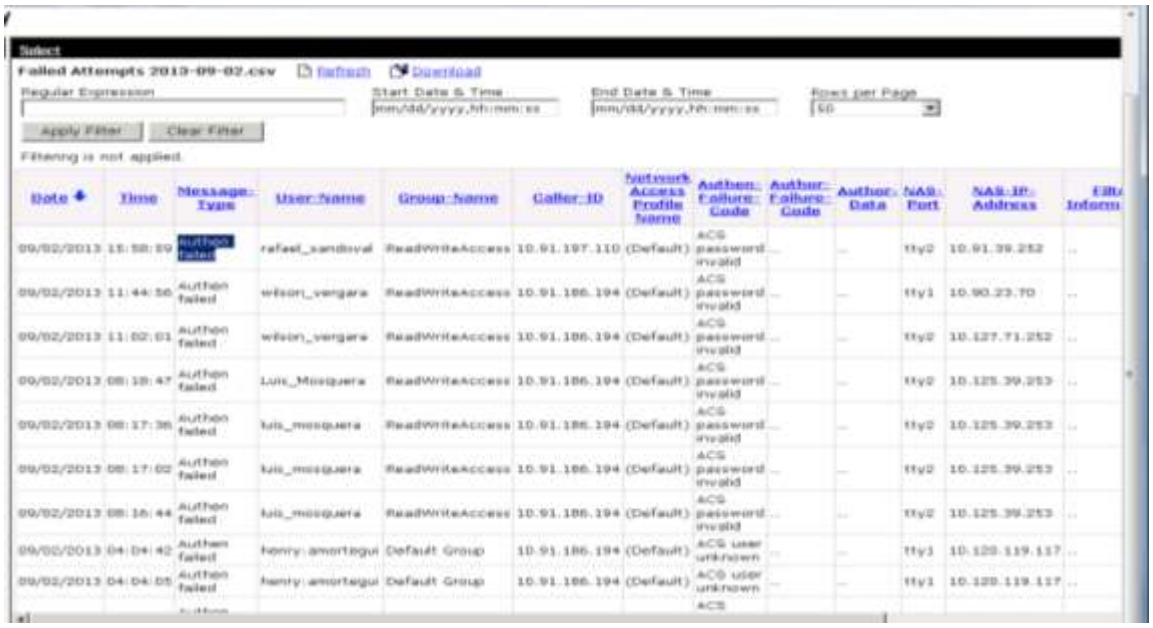
Figura 34. Detalles de Reportes de Log Eventos de los usuarios Sin permisos que desean Acceder a los equipos de Comunicación por medio del Servidor AAA autenticación TACACS+

Fuente: Los autores

Figura 35**.** Detalles de Reportes de Log Eventos de los usuarios Sin permisos que desean Acceder a los equipos de Comunicación por medio del Servidor AAA autenticación TACACS+

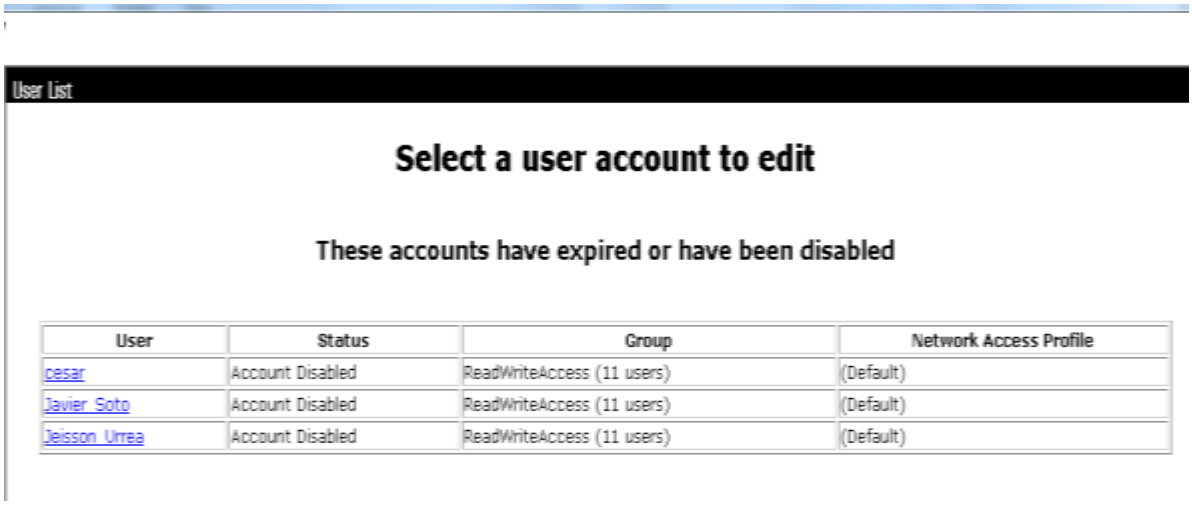
Fuente: Los autores

Figura 36**.** Detalles de Reportes de Log Eventos de los usuarios Sin permisos que desean Acceder a los equipos de Comunicación por medio del Servidor AAA autenticación TACACS+



Fuente: Los autores

Figura 37. Log Eventos de los usuarios Deshabilitados para acceder a los equipos de comunicación por medio del Servidor AAA autenticación TACACS+



Fuente: Los autores

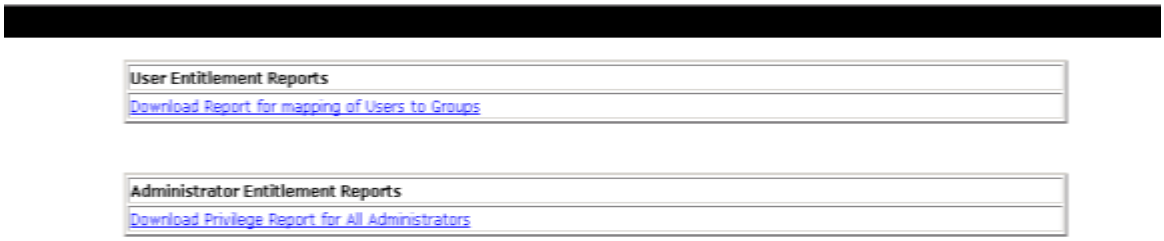
Figura 38. Log Eventos Backup de la base de datos diaria del Servidor AAA autenticación TACACS+

Fuente: Los autores

Figura 39. Log Eventos usuarios que han cambiado la contraseña por medio del Administrador del Servidor AAA autenticación TACACS+

Fuente: Los autores

Figura 40. Log Eventos por reportes consolidados del Servidor AAA autenticación TACACS+



Fuente: Los autores

7.3 CONFIGURACIÓN DE CLIENTES TACACS+

Una vez implementado el servidor AAA de TACACS+ se procede a configurar clientes AAA en todos los equipos de la red, esta configuración se realiza de manera similar. A continuación se muestra y se explica cuál es la configuración que debe tener cada equipo para que se convierta en un cliente TACACS+:

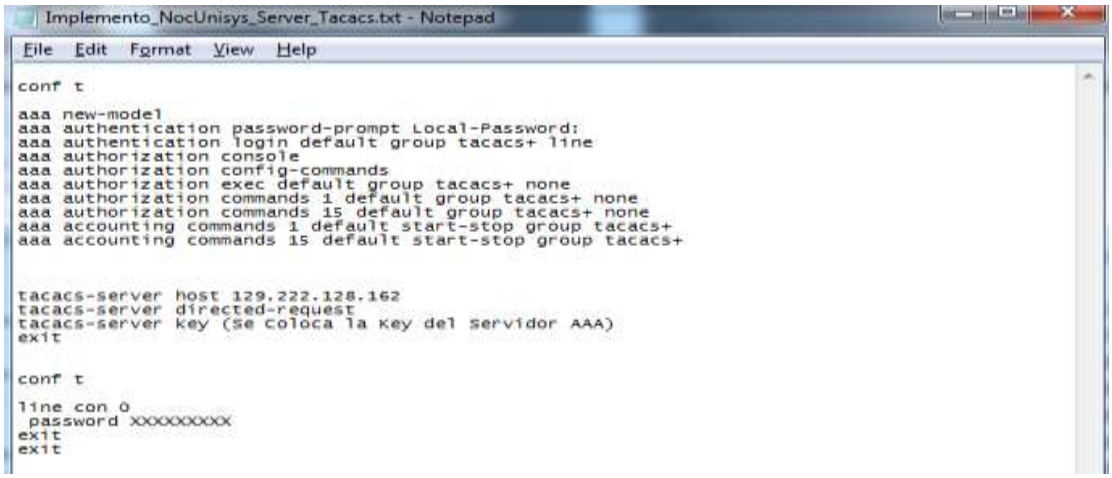
Primero se creó un usuario para el acceso desde consola, para que este pueda ser habilitado cuando el equipo no se encuentre conectado al servidor. Luego se definieron dos usuarios uno con nivel de privilegio 15 y otro con nivel de privilegio 1, esto se configura porque si bien ambos niveles están por defecto en los equipos de red, para que el servidor AAA TACACS+ pueda ingresar con cualquier nivel este debe estar definido, por esta misma razón se debe definir ambos niveles para la conexión remota VTY.
Después se comienza a configurar al equipo como cliente TACACS+ creando un modelo AAA y se indica cual es el servidor y cuál es la llave que debe coincidir con la configurada en el servidor. También se define que el servidor soportará 5 intentos fallidos antes de expulsarlo.

Para configurar la autenticación se usa el comando: authentication login, además se define que todas las interfaces y líneas van a ser autenticadas por el protocolo TACACS+ con los usuarios registrados en el servidor (usuarios locales del autenticador). Con el tercer comando se define que cuando la autenticación con el servidor este deshabilitada se pueda acceder por medio de la contraseña enable del equipo. También debemos definir que el servidor no acepte más de 5 intentos de autenticación.

Para configurar autorización primero definimos que va ser por comandos (modo commands). Luego definiremos que en cuanto la autorización se permitirá el uso de los comandos de acuerdo al nivel con que se ingrese, para esta implementación solo hemos definido los niveles: 1 (Solo Lectura) y 15 (Administradores).

A continuación se observa claramente el script que se debe correr a todos los switches de Unisys de Colombia:

Figura 41**.** Script TACACS+



Fuente: Los autores

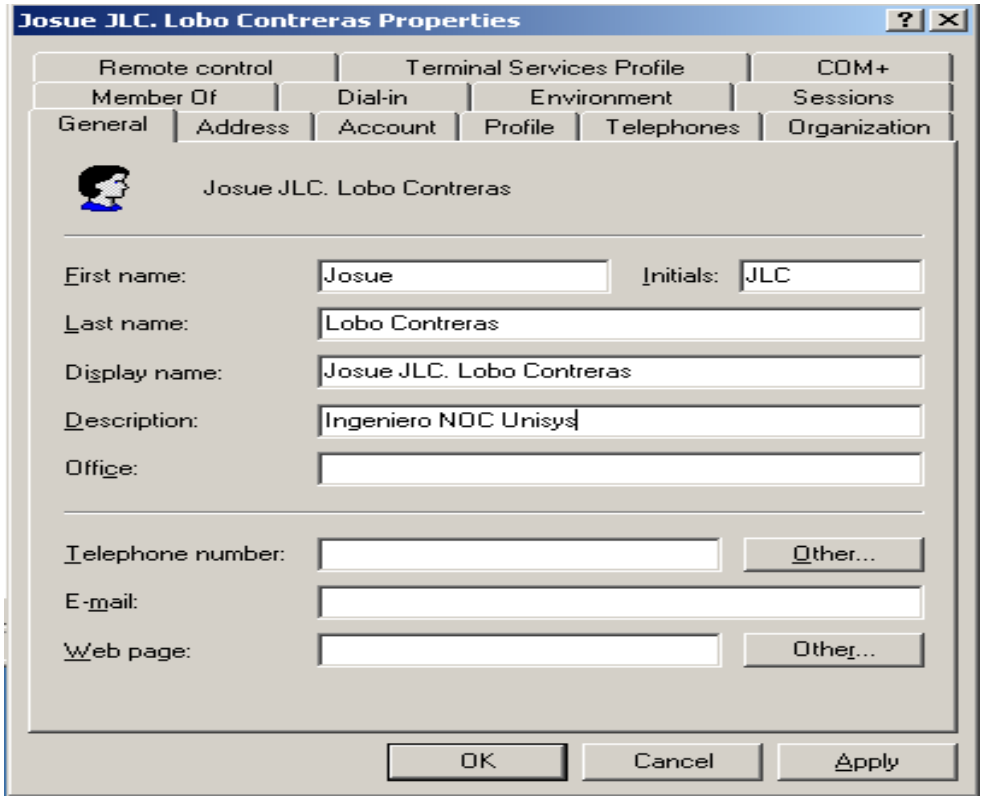
El proceso de accounting se iniciará cuando se intente o se inicie una sesión en el modo exec y se detendrá cuando se salga de este modo. De la misma manera cuando se ejecuten comandos de nivel 1 y 15 se iniciara el proceso y se tendrá cuando se salga del nivel. Todas las peticiones de servicio de red también serán contabilizadas (como las peticiones de ARP, SLIP o PPP), además cada vez que se inicie una sesión remota como SSH también se realizara el proceso de accounting.

7.4 IMPLEMENTACIÓN DEL SERVIDOR AAA DE AUTENTICACIÓN RADIUS PARA LOS USUARIOS CORPORATIVOS

Una vez afinada el servidor AAA de Autenticación TACACS+ de Unisys de Colombia debemos implementar el servidor AAA de Autenticación RADIUS encargado de autenticar a los usuarios que accedan a los recursos compartidos de la red Corporativa. A continuación se muestra la configuración realizada:

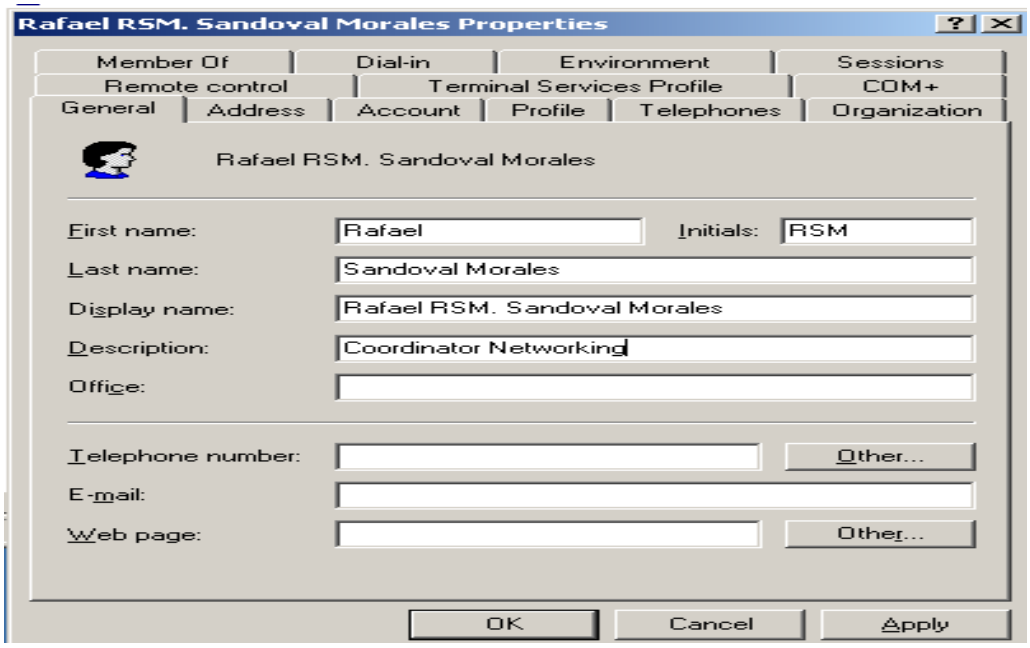
7.4.1 Creación de usuarios en el dominio

Figura 42. Creación de usuario Josue en el dominio unisys.com.co



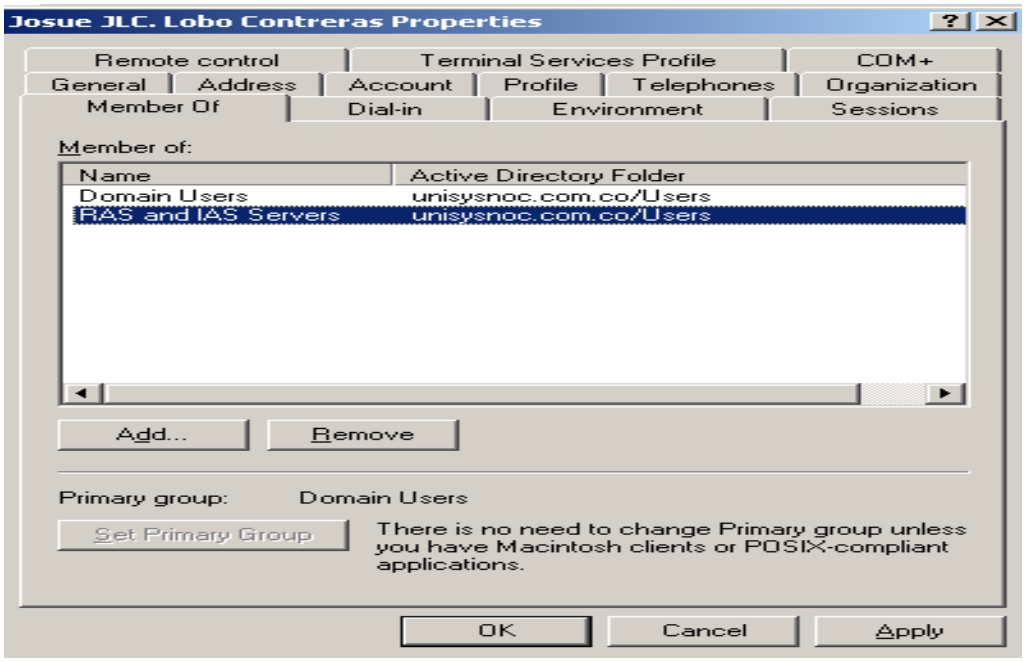
Fuente: Los autores

Figura 43. Creación de usuario Rafael en el dominio unisys.com.co



Fuente: Los autores

Figura 44. Añadir los usuarios del dominio al grupo RAS and IAS Servers

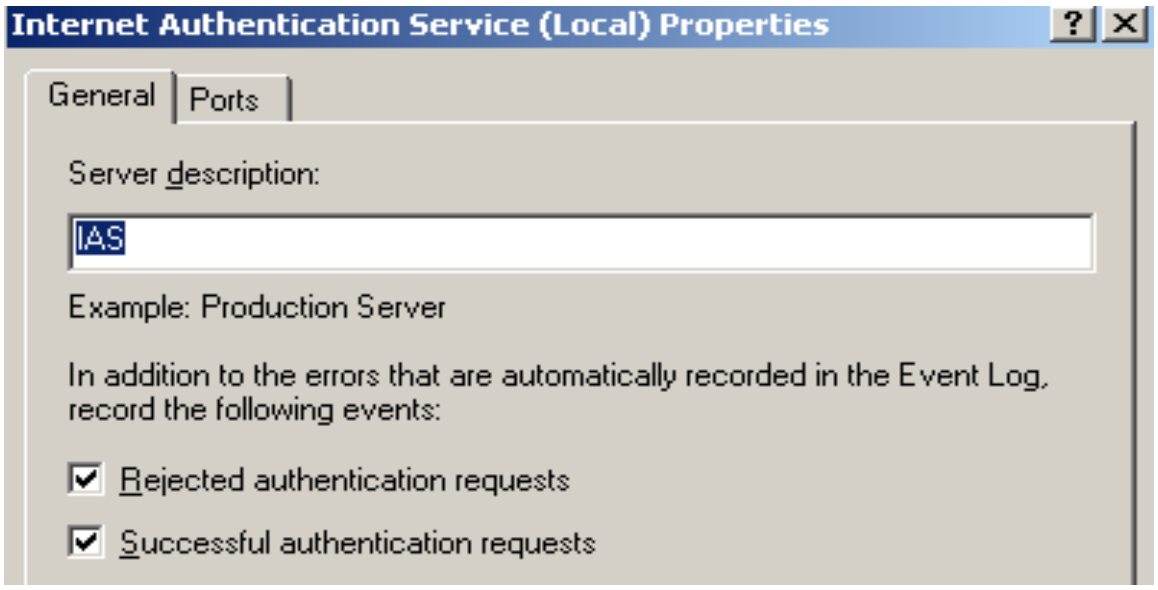


Fuente: Los autores

7.4.2 Configuración del Internet Authentication Service (IAS). IAS es un servicio que tiene integrado el sistema operativo Microsoft Windows 2003 R2, mediante el cual se proporcionan la funcionalidad de Autenticación, Autorización y Trazabilidad (AAA), la cual se puede configurar mediante el estándar RADIUS.

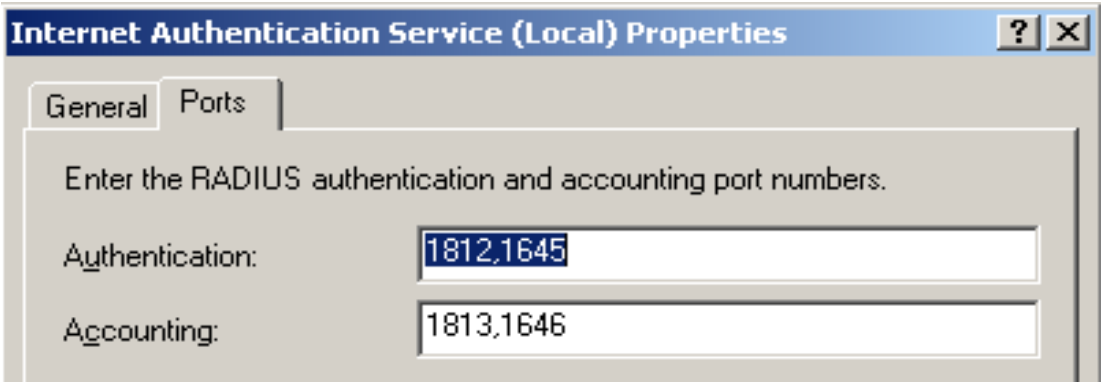
7.4.2.1 Configuración clientes RADIUS

Figura 45. Registrar en el archivo de eventos las conexiones exitosas y rechazadas



Fuente: Los autores

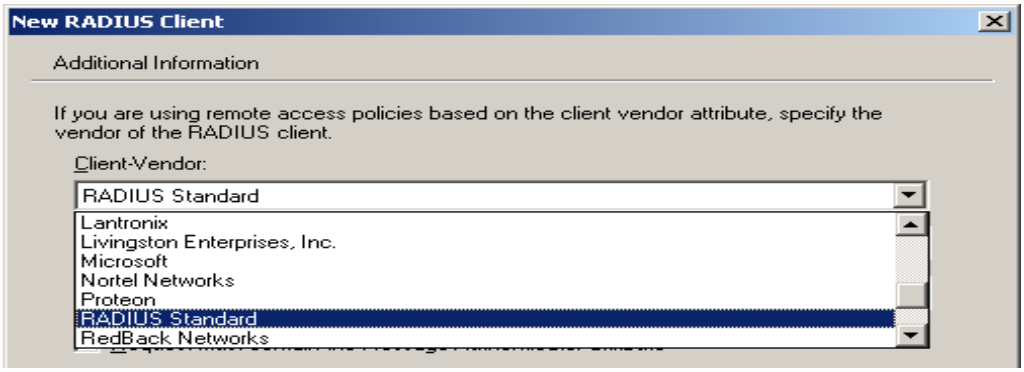
Figura 46**.** Establecer los puertos de autenticación y trazabilidad



Fuente: Los autores

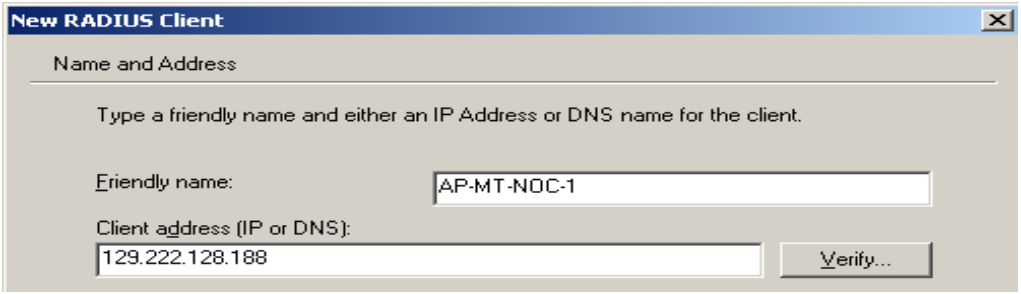
7.4.2.2 Agregar clientes RADIUS al servidor IAS

Figura 47. Establecer que el servidor AAA va a funcionar mediante el estándar RADIUS



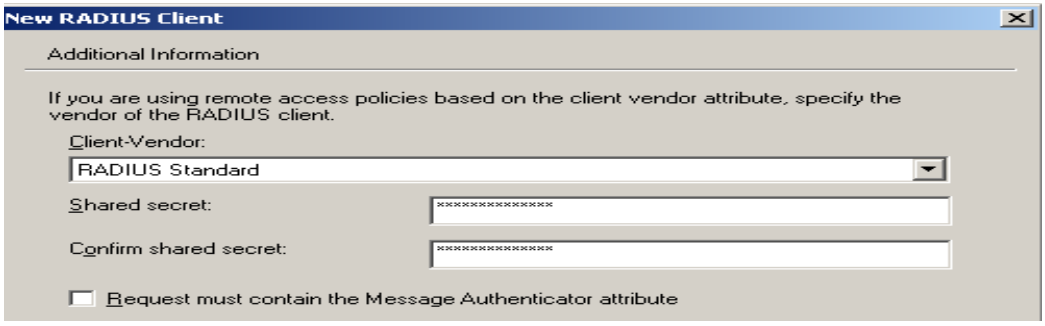
Fuente: Los autores

Figura 48. Registro de la dirección IP del Access Point para autenticación en la WLAN



Fuente: Los autores

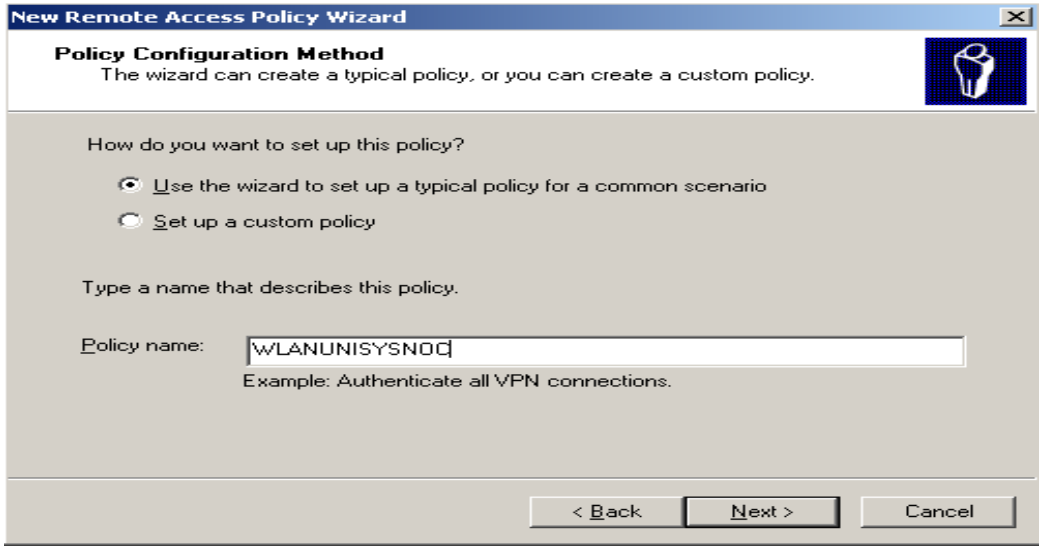
Figura 49. Clave compartida para integrar RADIUS con Active Directory



Fuente: Los autores

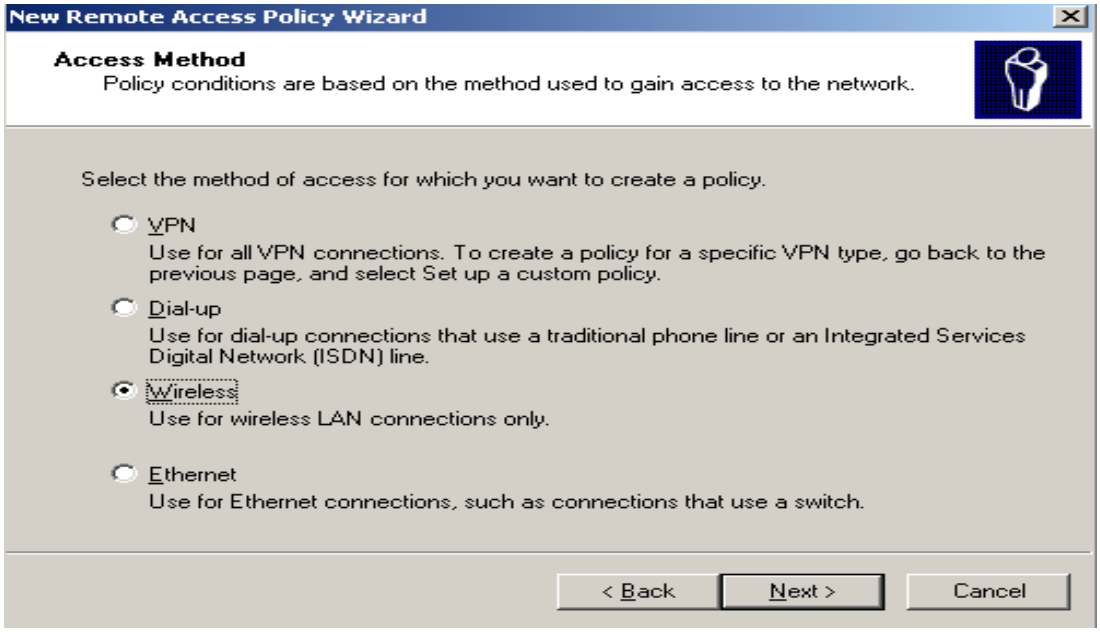
7.4.3 Creación de políticas de acceso remoto

Figura 50. Nombre de la política de acceso remoto



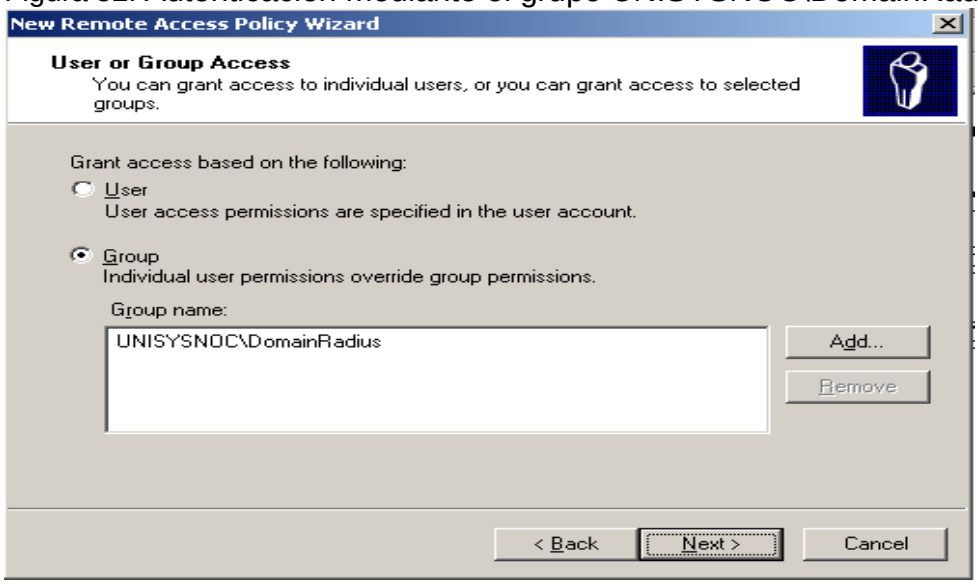
Fuente: Los autores

Figura 51. Método de acceso remoto inhalámbrico



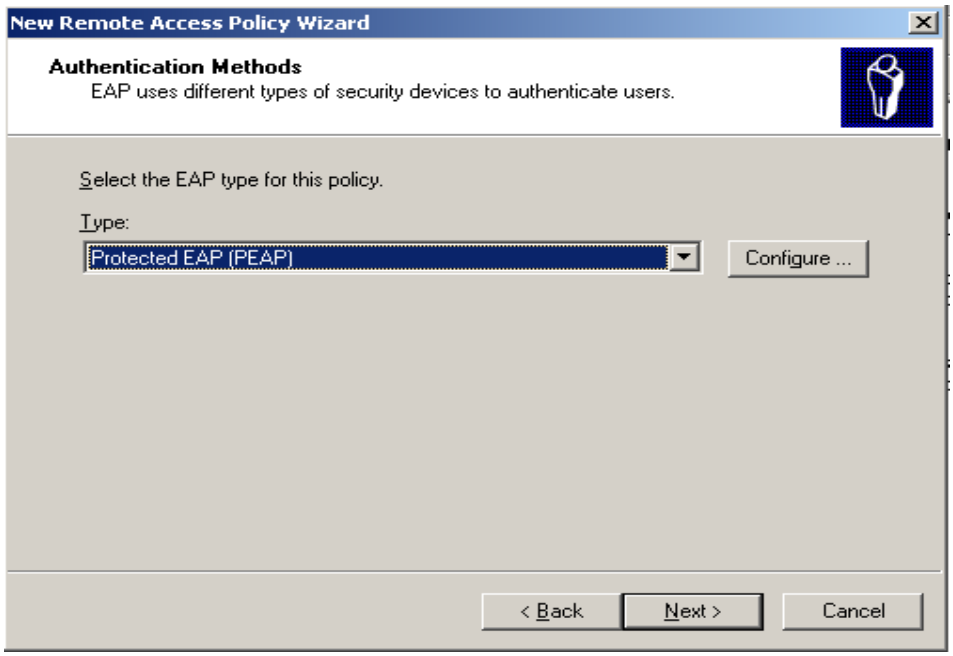
Fuente: Los autores

Figura 52. Autenticación mediante el grupo UNISYSNOC\DomainRadius



Fuente: Los autores

Figura 53. Tipo de método de autenticación Protected EAP (PEAP)

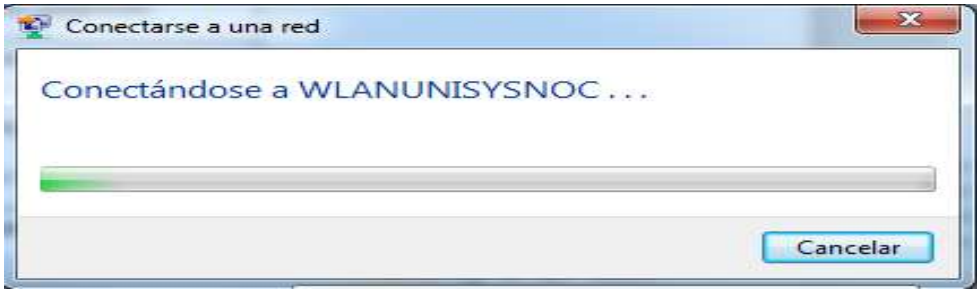


Fuente: Los autores

7.5 RESULTADO DE CONEXIÓN RED WLAN “INALÁMBRICA”

A continuación se puede observar la forma de configuración de la Red WLAN con el Servidor AAA de TACACS+/RADIUS.

Figura 54. Petición de conexión a la red con SSID WLANUNISYSNOC



Fuente: Los autores

Figura 55. Autenticación de red a nivel de usuario

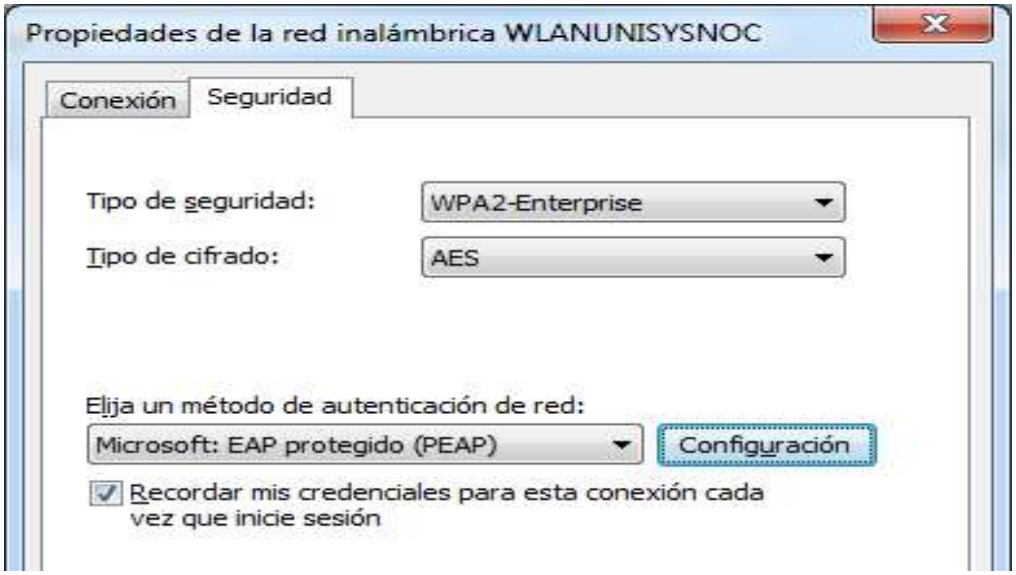
Fuente: Los autores

Figura 56. Solicitud de conexión rechazada por falta de parámetros de configuración

Fuente: Los autores

Para que la conexión sea exitosa, se debe configurar los parámetros de conexión correctos.

Figura 57**.** Seleccionar Microsoft: EAP protegido (PEAP) en propiedades de la red inalámbrica



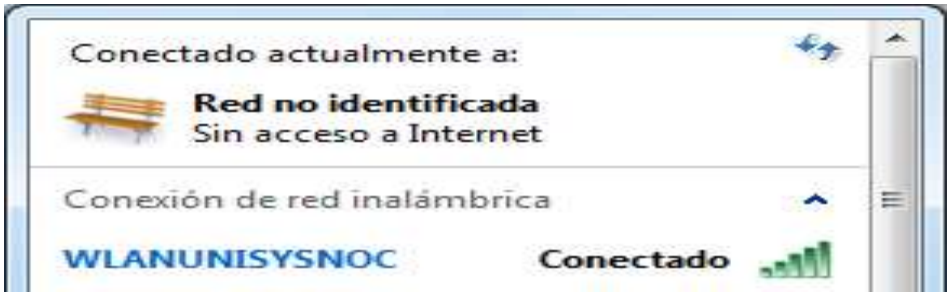
Fuente: Los autores

Posteriormente, intentamos nuevamente ingresar a la red del NOC de UNISYS

Figura 58. Intento de conexión a la red WLANUNSYSNOC

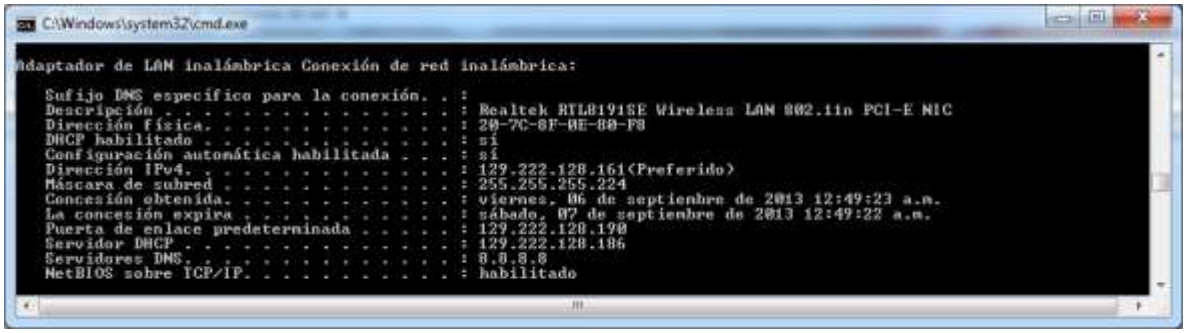
Fuente: Los autores

Figura 59. Autenticación y conexión permitida a la red del NOC de UNISYS de Colombia



Fuente: Los autores

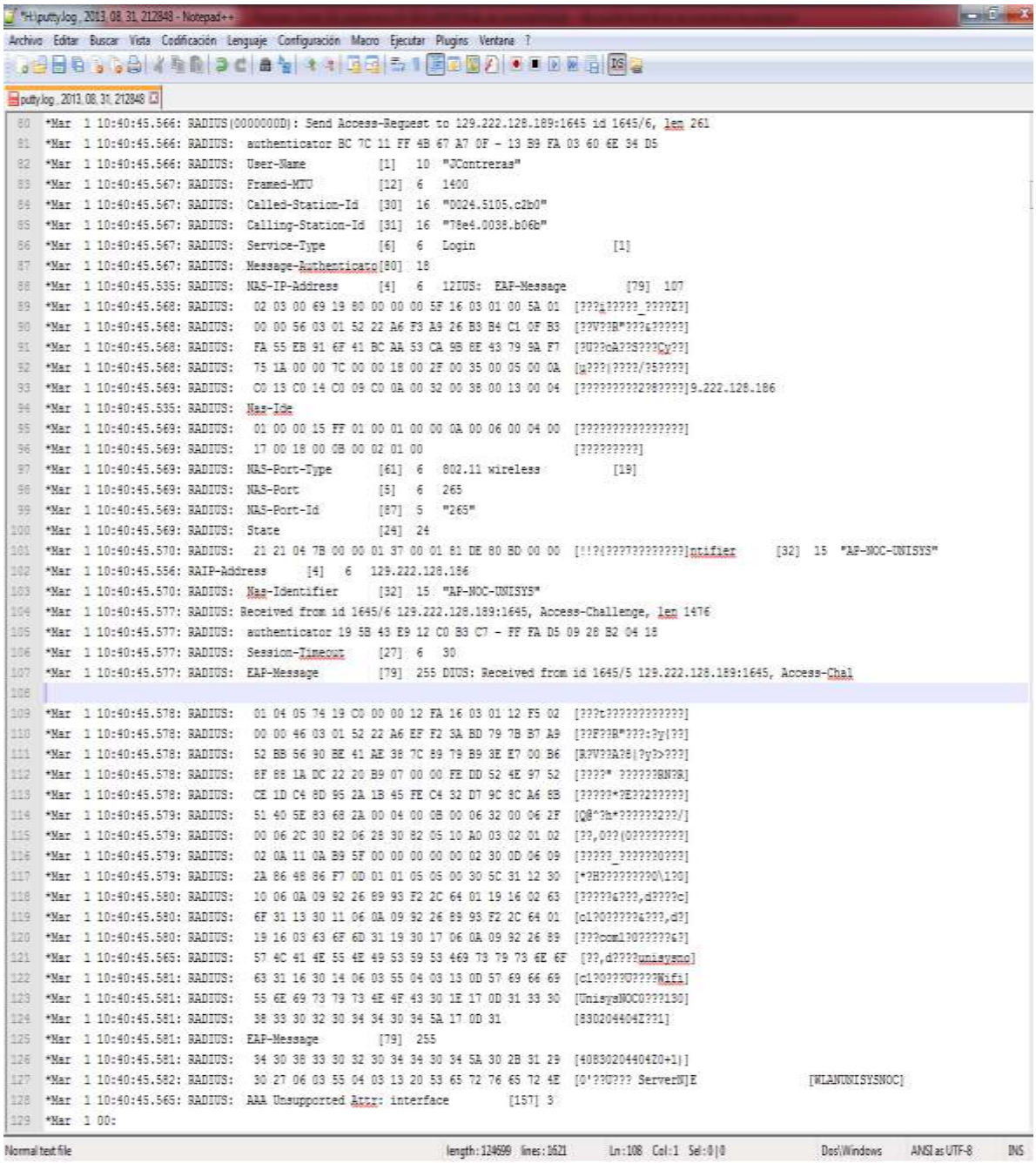
Figura 60. Configuración IP de Windows asignada por la red WLANUNISYSNOC



Fuente: Los autores

Si todo se realizó correctamente, en la ventana de conexiones de red podrá ver los diferentes estados del proceso de autenticación contra el servidor AAA de Tacacs+/Radius.

Figura 61. Autenticación del usuario JContreras cifrada mediante el protocolo EAP



Fuente: Los autores

Luego en la parte inferior derecha del escritorio verá un mensaje sobre que indica que el proceso de autenticación fue exitoso, esto significa que la máquina ya tomo una dirección IP mediante el servicio DHCP y puede acceder a la red corporativa de UNISYS de Colombia.

7.6 EFECTIVIDAD CONTROLES IMPLEMENTADOS

Tabla 17. Efectividad controles implementados

No.	Nombre del Riesgo	PROBABILIDAD		IMPACTO		VALORACIÓN RIESGO RESIDUAL
		Criterio cualitativo	Factor cuantitativo	Criterio cualitativo	Factor cuantitativo	
1	Inadecuado control de acceso lógico	MB	1	M	3	3
		B	2	A	4	8
		MB	1	A	4	4
2	Niveles de acceso no establecidos	MB	1	M	3	3
		MB	1	A	4	4
		MB	1	A	4	4
		MB	1	M	3	3
3	Asignación inadecuada de perfiles de usuarios	MB	1	M	3	3
		MB	1	MA	5	5
		MB	1	MA	5	5
4	Gestión deficiente de password	MB	1	M	3	3
		MB	1	A	4	4
5	Suplantación IP	MB	1	MA	5	5
		MB	1	M	3	3
		MB	1	A	4	4
		MB	1	MA	5	5
		MB	1	MA	5	5
6	Información sin clasificación	MB	1	M	3	3
		MB	1	M	3	3
7	Instalación por defecto de sistemas y aplicaciones	MB	1	A	4	4
		MB	1	A	4	4
8	Recursos compartidos	MB	1	M	3	3
		MB	1	A	4	4

	en red no protegidos	MB	1	MA	5	5
9	Uso de recursos sin monitoreo	MB	1	A	4	4
10	Intercambio de información sin cifrar	MB	1	M	3	3
		MB	1	A	4	4
11	No registro de Logs de acceso	MA	5	MA	5	25
		MB	1	A	4	4
		A	4	M	3	12
		MB	1	A	4	4
12	No registro de logs del sistema	MB	1	M	3	3
		MB	1	MA	5	5
		MB	1	MA	5	5
		MB	1	MA	5	5
13	Conexiones externas sin autenticación	MB	1	M	3	3
14	Grupos no establecidos para roles de usuarios	MB	1	M	5	5
15	Multiples conexionnes por usuario	MB	1	M	3	3
16	No verificar la complejidad de contraseñas	MB	1	M	3	3
		MB	1	M	4	4
		MB	1	M	4	4
17	No restringuir horarios de conexión	MB	1	MA	5	5
		MB	1	M	4	4
		MB	1	B	2	2
18	Uso de controles criptográficos deficiente	MB	1	M	3	3
		MB	1	A	4	4
		MB	1	M	3	3
		MB	1	M	3	3
19	Crecimiento del negocio	MB	1	M	3	3
		MB	1	M	3	3

		MB	1	MA	5	5
		MB	1	A	4	4
20	Instalación no controlada de software	MB	1	M	3	3
		B	2	F	4	8
		MB	1	M	3	3
		MB	1	M	3	3
		MB	1	M	3	3
21	Administración deficiente	MB	1	MA	5	5
		MB	1	MA	5	5
		MB	1	MA	5	5
		MB	1	MA	5	5
		MB	1	A	4	4
		MB	1	A	4	4

Fuente: Los autores

7.7 VALORACIÓN DEL RIESGO VS RIESGO RESIDUAL

Tabla 18. Valoración del riesgo vs Riesgo residual

No.	Nombre del Riesgo	VALORACIÓN DEL RIESGO	VALORACIÓN RIESGO RESIDUAL
1	Inadecuado control de acceso lógico	20	3
		20	8
		20	4
2	Niveles de acceso no establecidos	20	3
		25	4
		15	4
		15	3
3	Asignación inadecuada de perfiles de usuarios	20	3

		25	5
		25	5
4	Gestión deficiente de password	15	3
		16	4
5	Suplantación IP	25	5
		15	3
		20	4
		25	5
		25	5
6	Información sin clasificación	15	3
		20	3
7	Instalación por defecto de sistemas y aplicaciones	16	4
		16	4
8	Recursos compartidos en red no protegidos	15	3
		20	4
		25	5
9	Uso de recursos sin monitoreo	20	4
10	Intercambio de información sin cifrar	15	3
		20	4
11	No registro de Logs de acceso	25	25
		20	4
		12	12
		16	4

12	No registro de logs del sistema	15	3
		25	5
		25	5
		25	5
13	Conexiones externas sin autenticación	15	3
14	Grupos no establecidos para roles de usuarios	20	5
15	Multiples conexionnes por usuario	15	3
16	No verificar la complejidad de contraseñas	15	3
		20	4
		20	4
17	No restringuir horarios de conexión	25	5
		20	4
		10	2
18	Uso de controles criptográficos deficiente	15	3
		20	4
		15	3
		15	3
19	Crecimiento del negocio	12	3
		15	3
		25	5
		4	4

20	Instalación no controlada de software	15	3
		20	8
		12	3
		15	3
		15	3
21	Administración deficiente	20	5
		20	5
		20	5
		20	5
		20	4
		20	4

Fuente: Los autores

8. ANÁLISIS ECONÓMICO DEL PROYECTO

8.1 ANÁLISIS ECONÓMICO

En el análisis económico del proyecto se consideró los costos de implementación y operación, con estos resultados se generó el flujo de caja y se midió la rentabilidad del proyecto con los métodos financieros TIR.

8.1.1 Gastos

Los gastos que se generaron en la inversión inicial del proyecto y se dividieron así:

Diseño: Realizado por un equipos de ingenieros.

Tabla 19. Pago total a ingenieros por diseño

Duración en días	Horas	Numero de Ingenieros	Valor hora	Costo total
3	24	2	55.000	2.640.000

Fuente: Los autores

Implementación: Realizado por un equipos de ingenieros.

Tabla 20. Pago total a ingenieros por implementación

Duración en días	Horas	Numero de Ingenieros	Valor hora	Costo total
5	40	2	75.000	6.000.000

Fuente: Los autores

8.1.2 Inversión en Hardware

Los gastos en hardware empleados en el proyecto se detallan en la siguiente tabla

Tabla 21. Inversión en hardware para la implementación

Producto	Descripción	Cantidad	Costo por unidad	Costo total
Access Point	Cisco Aironet 1240AG Series 802.11A/B/G Access Poin	5	0	0
Switch	Cisco Catalyst 2960 24-Ports	16	0	0
Switch Core	Cisco Catalyst 3750	2	0	0
Firewall	Cisco ASA 5520 firewall	2	0	0
Computadores	Dell Core 2 Duo 2.8 GHz, 4GB DDR3 RAM y Disco Duro de 500GB	15	0	0
Servidores	Dell, Intel Xeon E5504 2.00Ghz, 4GB RAM, RAID 5, 500GB DD SCSI	2	0	0

Fuente: Los autores

8.1.3 Inversión Software

Tabla 22**.** Inversión en software para la implementación

Producto	Descripción	Cantidad	Costo por unidad	Costo total
Cisco ACS	**Cisco ACS** (**Access Control Server**)	2	0	0
Microsoft Windows Server 2003	Windows Server 2003 Professional	2	0	0
TACACS+	Terminal Access Controller Access-Control System	2	0	0

Fuente: Los autores

Para este proyecto se consideró un margen de ganancia del 10% en equipos, software y servicios profesionales de implementación.

Tabla 23. Proyección de ganancia del 10%

	Gastos	Margen de ganancia	Precio
Equipos	0	10%	0
Software	0	10%	0
Servicios de implementación	1.320.000	10%	2.640.000
Servicios de diseño	3.000.000	10%	6.000.000

Fuente: Los autores

8.1.4 OPEX. Los costos de operación y mantenimiento están ligados a los servicios que se ofrecen: Mantenimiento Preventivo (Babysitting) se pondrá un ingeniero junior en horario de oficina que estará en la sede del cliente los días laborables del mes.

Tabla 24. Pago mantenimiento preventivo

Duración en días	Horas	Numero de Practicantes	Valor hora	Costo total
30	160	1	4000	640.000

Fuente: Los autores

Mantenimiento Correctivo (Bolsa de Horas) el cliente cuenta con una bolsa de horas que podrá utilizar cuando surjan emergencias a cualquier hora, el cliente requirió una bola de 40 horas al mes.

Tabla 25. Pago mantenimiento correctivo

Duración en días	Horas	Numero de Practicantes	Valor hora	Costo total
30	160	1	4000	640.000

Fuente: Los autores

Soporte de Emergencia (24x7) el cliente cuenta con soporte remoto las 24 horas del día los 7 días de la semana.

Tabla 26. Pago por soporte de emergencia

Duración en días	Horas	Numero de Ingenieros	Valor hora	Costo total
30	720	1	8000	5.760.000

Fuente: Los autores

Tabla 27. Pago total gastos de mantenimiento y soporte

	Gastos	Margen de ganancia	Precio
Mantenimiento Preventivo	640.000	10%	704.000
Mantenimiento Correctivo	640.000	10%	704.000
Soporte de Emergencia	5.760.000	10%	6.336.000

Fuente: Los autores

8.1.5 Flujo de Caja. El flujo de caja de cada año se obtuvo de acuerdo a los precios fijados con el cliente y la inversión se recuperó en el primer año.

Tabla 28. Flujo de caja

	Año 0	Año 1	Año 2	Año3	Año 4	Año 5
Ingresos por HW y SW	0	0	0	0	0	0
Ingresos por Diseño e implementación	0	$3.520.000	$3.872.000	$4.259.200	$4.685.120	$5.153.632
Ingresos por Operación y Mantenimiento	0	$7.744.000	$ 8.518.400	$ 9.370.240	$ 10.307.264	$ 11.337.990
Egresos por HW y SW	0	0	0	0	0	0
Egresos por Diseño e Implementación	-$3.200.000	0	0	0	0	0
Egresos por Operación y Mantenimiento	-$7.040.000	- $7.040.000	- $7.040.000	- $7.040.000	-$ 7.040.000	- $7.040.000
Flujo de Caja	**- $10.240.000**	**$4.224.000**	**$5.350.400**	**$6.589.440**	**$7.952.384**	**$9.451.622**

Fuente: Los autores

INVERSION: **10.240.000**

Valor presente Neto (VPN):

$$VPN: \frac{f}{(1+ti)^n}$$

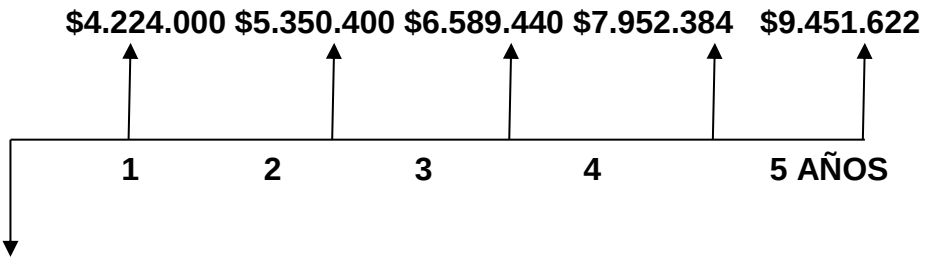
$$VPN: \frac{\$4.224.000}{(1+0.10)^1} + \frac{\$5.350.400}{(1+0.10)^2} + \frac{\$6.589.440}{(1+0.10)^3} + \frac{\$7.952.384}{(1+0.10)^4} + \frac{\$9.451.622}{(1+0.10)^5}$$

VPN: $3.840.000 + $4.421.819 + $4.950.744 + $5.431.585 + $5.868.714

VPN: $24.512.862

VPN: VP- INVERSION

$**(24.512.862) – (10.240.000): $14.272.862**



10.240.000

8.1.6 Inversión. Análisis: el proyecto es viable ya que tiene una tasa de rendimiento puesto que la tasa supera el costo de capital de la empresa por lo tanto genera un valor agregado para la empresa.

9. CONCLUSIONES

Mediante el análisis de riesgos realizado bajo la Metodología de Análisis y Gestión Riesgos de los Sistemas de Información – **MAGERIT**, se lograron identificar los puntos críticos en los cuales un evento inusual puede afectar considerablemente los procesos de negocio del NOC de UNISYS Colombia. Luego, se determinaron los impactos que estos sucesos pueden generar a la compañía en términos de negocio y posteriormente, se estudiaron procedimientos que permitieran mitigar los efectos anteriormente calculados.

La implementación del servidor AAA basado en el protocolo TACACS en la red del NOC de UNISYS Colombia, se constituye en una solución de seguridad informática para garantizar la Confidencialidad, Integridad y Disponibilidad de la información gestionada mediante los activos tecnológicos de la compañía. Por lo tanto, la temática del presente trabajo de grado puede ser aplicada en la infraestructura de red de cualquier organización que gestiones sus comunicaciones mediante dispositivos ***Cisco*** y que además, desee proteger sus elementos tecnológicos para prevenir eventos indeseados que puede obstaculizar lograr los objetivos de negocio.

Al culminar con la implementación del presente proyecto de grado se pudo concluir que, gracias al servidor AAA de RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor AAA TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos.

Se diseñó e implemento en un ambiente operativo de red, una solución teniendo en cuenta las características más valoradas por los usuarios finales: continuidad de servicio, rapidez en el intercambio de datos y seguridad de la información.

Por lo tanto, las organizaciones a nivel mundial deben ser conscientes de la gran importancia que constituye un adecuado manejo y uso de la información, por lo que deben establecer niveles de información para controlar el acceso a la misma y garantizar que los empleados, dependiendo del rol definido por la compañía, tengan acceso solo a la información necesaria para ejercer sus funciones.

La seguridad informática es un campo de estudio crítico de las redes de comunicación, lo que conlleva a pensar que esta disciplina debería contemplarse como una capa transversal de los modelos de comunicaciones TCP/IP y OSI.

Los profesionales de seguridad informática deben ser consientes de la gran importancia de constituye un adecuado manejo y uso de la información de las organizaciones.

10. RECOMENDACIONES

Que todos los dispositivos y equipo inalámbrico sean almacenados en un lugar filtrado y también es recomendable contar con una red tradicional (cableada), ya que los ataques de interceptación o interferencia del medio inalámbrico (radio-frecuencia), así como los ataques de bajo nivel de operación (burla del estándar 802.11, de-asociación falsa, etc.) siguen siendo una amenaza latente para las redes inalámbricas de área local.

Obtener un método de conexión a la red de Unisys de Colombia con autenticación de usuario y contraseña.

La infraestructura inicial de la empresa ya cuenta con cableado horizontal y vertical implementados, es por ello que la tesis no contempla dicho despliegue.

Las redes Wi-Fi funcionan en una frecuencia determinada (2,4 Ghz), y poseen canales de funcionamiento (un total de 11, del 1 al 11). Al igual que las radiofrecuencias de radio, existen interferencias entre frecuencias cercanas. De la misma forma, cuando se instalen más de un Access Point, se recomienda cambiar los canales de funcionamiento, de manera que queden lo más lejanos posibles. Generalmente los Access Point vienen configurados en el canal 1 ó 6.

Encriptar datos a nivel de capa de enlace (cifrados WEP, WPA y WPA2) ha sido utilizada como una medida de seguridad común. Lamentablemente esta práctica no asegura la confidencialidad punto a punto. Si se requiere seguridad a nivel de capa de enlace, además de evitarse el uso de WEP, debería implementarse el uso de IEEE 802.11i (WPA2).

Implementar grupos de diferentes usuarios, los cuales nos permitan separarlos dependiendo del uso o tipo de usuario que sean.

BIBLIOGRAFÍA

ARIEL, Maiorano. CRIPTOGRAFÍA. Técnicas de desarrollo para profesionales. Alfaomega, 2009

BEHROUZ A., Forouzan. Transmisión de datos y redes de comunicaciones, segunda edición. McGraw-Hill, 2002

_____. Transmisión de datos y redes de comunicaciones. Cuarta edición. McGraw-Hill, 2007

LOCKHART, Andre. Seguridad de Redes Los mejores trucos. ANAYA: Multimedia, 2007

PICOUTO RAMOS, Fernando; LORENTE PÉREZ, Iñaki; GARCIA MORAN, Jean Paul y RAMOS VARÓN; Antonio Ángel. Hacking y Seguridad en Internet. Alfaomega RA-MA, 2008

WILLIAM, Stallings. Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Segunda Edición. Prentice Hall, 2004

REFERENTES BIBLIOGRÁFICOS

ANONIMO, (s.f.). “Sincables,”. [Online]. Available: http://www.sincables.cl/. Consulted: Nov. 2010.

ASADOORIAN SANS, Paul. SysAdmin Audit, Networking and Security Institute. Implementing secure access to cisco devices using TACACS+ and SSH. [En línea]. Disponible en http://www.sans.org/reading-room/whitepapers/networkdevs/implementing-secure-access-cisco-devices-tacacs-plus-ssh-1041?show=implementing-secure-access-cisco-devices-tacacs-plus-ssh-1041&cat=networkdevs. Extraído el 11 Junio de 2013.

C. de Joomla en Colombia, “F.A.Q - joomla! en colombia”. [En línea]. Recuperado de <http://www.joomlaencolombia.net/zona-newbie/faq>. Extraído 5 Junio de 2013

CISCO SYSTEMS TECHNICAL SUPPORT AND DOCUMENTATION, Cisco IOS security configuration guide, 2008.

CISCO SYSTEMS TECHNICAL SUPPORT AND DOCUMENTATION, TACACS+ and RADIUS comparison, Document ID: 13838, Jan 2008.

CISCO SYSTEMS, Inc. CISCO AAA Implementation Case Study. [En línea]. Disponible en http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/aaasub/C262.pdf. Extraído el 15 Junio de 2013.

Clasificación y tipos de ataques contra sistemas de información. (Febrero 2009). Disponible en http://www.delitosinformaticos.com/seguridad/clasificacion.shtml.

EDER, Diego, Alejo, and Daniel. (2003). Colombia sin Cables<—->Medellinwireless. [Online]. Available: http://co.lab.cohete.net/wifi/MiTiN_2.html. Consulted: Nov. 2010.

EDNEY John; ARBAUGH, William. Real 802.11 Security Wi-Fi Protected Access and 802.11i. Addison Wesley Ed., 2004.

FORD, M., Lew, K., SPANIER, S. y Stevenson, T. Internetworking Technologies Handbook. Indianapolis: Cisco Press, 1997.

GULLAUME Lehembre. “Seguridad WI-FI WEP, WPA y WPA2. En: Revista Hackin9 Magazine. No. 1-2006. 2006.

I. telecommunicationsUnion, “X.170 : Arquitectura de la gestion de red a red para redes de datos.” vol. 1, no. 1, p. 17, Jun. 1999. [En línea]. Recuperado de <http://www.itu.int/rec/T-REC-X.170-199906-I>

INGRAM SANS, Steve. SysAdmin Audit, Networking and Security Institute. . Case study in implementing AAA Servers Using TACACS+. [En línea]. Disponible en http://cyber-defense.sans.org/resources/papers/gsec/case-study-implementing-aaa-servers-tacacs-plus-105774. Extraído el 11 Junio de 2013.

LAZO GARACIA, Nuttsy Aurora. Diseño E Implementación de una Red LAN y Wlan con Sistema de Control de Acceso Mediante Servidores AAA. [En línea]. Disponible en http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1445/LAZO_GARCIA_NUTTSY_SERVIDORES_AAA.pdf?sequence=1. Extraído el 3 Mayo de 2013]

MALDONADO TAPIA, Angél Vinicio. Implementación de un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del colegio san Luis Gonzaga a través de una autenticación de los usuarios mediante un servicio AAA implementado en un servidor que trabaje con protocolos Radius. [En línea]. Disponible en http://dspace.ups.edu.ec/bitstream/123456789/4167/1/UPS-ST000959.pdf. Extraído el 6 Mayo de 2013.

MEMORIAS IV FORO. (Nov. 2010. Día 3). Las TIC mejorando la calidad de vida. [Online]. Available: http://www.udtecnovirtual.org/index.php?option=com_content&view=article&id=573%3Aivforo-dia3&catid=1%3Alatest-news&Itemid=1. Consulted: Nov. 2010.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Gobierno de España. “MAGERIT – versión 3.0. En: *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro I - Método.

_____. Libro II – Catálogo de Elementos.

_____. Libro III - Guía de Técnicas.

PLASENCIA BEDÓN, Luis Carlos. Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de Networking de un ente del Ministerio de Defensa Nacional. [En línea]. Disponible en http://repositorio.utn.edu.ec/bitstream/123456789/994/1/04%20RED%20009%20TESIS_SERVIDOR_AAA.pdf. Extraído el 7 Mayo de 2013.

R.T. MORRIS. A Weakness in the 4.2BSD Unix TCP/IP Software. Computing Science Technical Report (No. 117), AT&T Bell Laboratories. New Jersey: Murray Hill, 1985

SIMPSON, W. PPP Challenge Handshake Authentication Protocol (CHAP). Agosto 1996.

The Internet Engineering Task Force (IETF), Internet Society. RFC Index Search engine. Available. Recuperado de http://www.ietf.org

Y. REKHTER, R. MOSKOWITZ, D. KARRENBERG, G. de Groot. Address Allocation for Private Internets, RFC 1918. September 2006.

WEBGRAFIA

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/EtherChannel.html

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml

http://windows.microsoft.com/es-co/windows-vista/enable-802-1x-authentication

www.aircrack-ng.org

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED SEGURA CON UN SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS

Lobo, Josue y Sandoval, Rafael.
josueloboc@gmail.com, Rafael_sandoval1983@hotmail.com
Universidad Piloto de Colombia
Especialización en Seguridad informática

Resumen

Este artículo muestra como el diseño e implementación de un servidor de autenticación AAA basado en el protocolo TACACS, puede proporcionar un nivel aceptable de seguridad en las infraestructuras de red Cisco y así mismo, garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de las compañías.

Índice de Términos— AAA, TACACS

I. Introducción

El presente proyecto se fundamenta en el diseño e implementación de una infraestructura red segura LAN (Local Area Network) y WLAN (Wireless Local Area Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting). El primer paso fue analizar y determinar que la red LAN actual de Unisys de Colombia una red LAN utiliza el servicio de PortChannel[1] y Hot Stand-by Redundancy Protocol[2] (HSRP) también conocido como Protocolo de Redundancia para equipos de Comunicación para optimizar el uso de recursos de la red. Luego se implementó el servidor ACS (Access Control Server) que utiliza el protocolo TACACS+ para centralizar todo el acceso de los administradores y usuarios de lectura a los equipos de la red. En lo que compete a las redes WLAN, se instaló e implementó el servidor de Microsoft IAS en plataforma Windows 2003 Server, luego se verificó que el punto de acceso inalámbrico (Access Point - AP) cumpla con el estándar de autenticación IEEE 802.1x[3] que se usó como intermediario entre la capa de acceso (L2) y el algoritmo de autenticación, finalmente se configuró con el mecanismo de autenticación WPA-Enterprise y WPA2-Enterprise.

II. Objetivos

A. General

- Diseñar e implementar una infraestructura de red segura con un servidor de autenticación AAA basado en el protocolo TACACS, para mejorar el control de acceso a los recursos tecnológicos y aumentar los niveles de seguridad en la red corporativa.

B. Objetivos específicos

- Documentar y recopilar información acerca del estado del arte sobre servidores de autenticación AAA basados en el protocolo TACACS.
- Estudiar los protocolos de autenticación TACACS y AAA enfocados hacía las herramientas de criptográficas empleadas por los mismos.
- Realizar un análisis de riesgos de la red del NOC de UNISYS
- Implementar y configurar el servidor de autenticación AAA basado en el protocolo TACACS en el NOC de UNISYS para el control de acceso de los usuarios.
- Evaluar la efectividad de los controles implementados para mitigar los riesgos identificados en la red del NOC de UNISYS.
- Realizar un análisis financiero para medir la rentabilidad del proyecto

[1] Cisco System . http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/EtherChannel.html
[2] Cisco System http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml
[3] Microsoft Corporation http://windows.microsoft.com/es-co/windows-vista/enable-802-1x-authentication

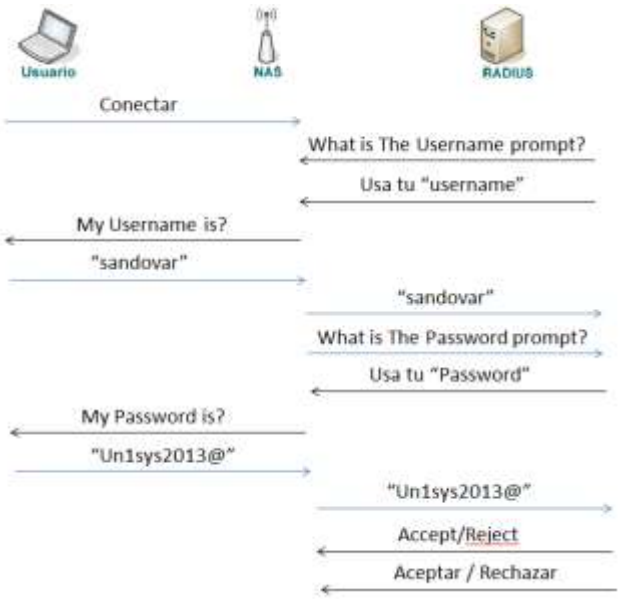
II. TACACS

A. Autenticación

Todo este proceso es únicamente establecido por el servidor de TACACS+, este se efectúa por medio de una comunicación parcial que recopila suficiente información del usuario para poderse autenticar. Eventualmente la información solicitada son las credenciales del usuario.

En la siguiente figura se muestra todo la secuencia del mensaje TACACS+ cuando son intercambiados entre el usuario, el equipo de comunicación (NAS) y el servidor AAA cuando se produce la autenticación de un usuario.

Figura 1. Proceso Autenticación TACACS+



Fuente: Los autores

B. Autorización

Si el proceso de autenticación se realizó de manera correcta y el cliente tiene habilitada la fase de autorización, el usuario no tendría problema en conectarse con su sesión.

Para ello el cliente se contacta nuevamente con el servidor, para recibir una respuesta que puede ser de la siguiente manera:

- ACCEPT: Acepta la autorización, y contiene información en forma de atributos que determinaran a que servicios puede acceder el usuario.

- REJECT: Autorización denegada

Entre los atributos contenidos en el mensaje ACCEPT están: parámetros de conexión, nombre del host o dirección IP, ACL, Timeouts para el usuario, en otras palabras toda la información del perfil del usuario.

Este control de acceso a los servicios de la red representa una gran medida de seguridad. Además el contar con un control de acceso a comandos de configuración restringe de manera significativa los ataques internos. El proceso de autorización de comandos se realizara cada vez que el usuario ingrese un comando, para que el servidor pueda determinar si es aceptado o rechazado de acuerdo al perfil del usuario.

En la siguiente figura se muestra el proceso de autorización para comandos ingresaron en los equipos de comunicación:

Figura 2. Proceso Autorización para las líneas de comando Mediante el Servidor TACACS+

Fuente: Los autores

C. Trazabilidad

El servidor AAA se encarga de registrar todos los diversos eventos, para de esa manera poder realizar un seguimiento detallado a cada sesión que se establece o rechaza a través de este servicio, dado que este log son almacenados en archivos .log o en una base de datos dependiendo de la configuración establecida. Los archivos log son fácilmente exportables a a diferentes tipos de bases de datos, archivos de hoja de cálculo o texto plano. La anterior información es muy útil para la administración y gestión de la red, para tener respaldo en las auditorias de las cuentas, los sistemas billing y generación de reportes que se requieran.

III. Sistemas de Control de Acceso (ACS)

El sistema de control de acceso es una solución óptima en cada una de las empresas, por qué provee un servidor AAA altamente escalable y robusto, su optimo control de acceso opera como servidor centralizado RADIUS o TACACS+, para su implementación se requiere el sistema operativo WINDOWS 2003 Server en cualquiera de sus versiones, además de las características solicitadas por el protocolo AAA con que decida trabajar, además cuenta con las siguientes características:

- Maneja diferentes niveles de acceso por usuario o por grupo, una vez que la autenticación se ha dado de manera correcta, ACS envía un profile del usuario al cliente, conteniendo políticas que indicaran a que servicios de la red puede acceder dicho usuario.
- Los accesos pueden ser diferenciados por: servicios, tiempo de acceso, y niveles de seguridad. Además puede aplicar políticas de control acceso ACL, restringiendo el acceso a determinadas áreas.
- Puede deshabilitar cuentas cuando se producen reintentos fallidos de ingreso o por vencimiento en la fecha.
- Los usuarios no podrá realizar el cambio de sus contraseña individualmente, el administrador de la gestión de la red es el único que podrá realizar este cambio.
- Componentes Internos del Sistema de Control de Acceso (ACS):
- El Sistema de Control de Acceso está desarrollado por 7 capas las cuales son instaladas como servicios en Windows al momento de instalar el programa:
- **CSAdmin:** Provee la interfaz web para la administración, soporta múltiples procesos que permiten múltiples sesiones, por defecto usa el protocolo HTTP en el puerto 2002.
- **CSAuth:** Provee el servicio de autenticación, permitiendo o negando el acceso, maneja la base de datos local ACS.
- **CSDBSync:** Maneja la sincronización y replicación de la base de datos hacia otros servidores AAA ACS.
- **CSLog:** Provee el servicio de logging, para la contabilidad y actividad del sistema. Para ello monitorea y registra: actividades de los usuarios y administradores, backups y restauraciones, replicación de bases de datos, sincronización, servicios centrales de ACS, contabilidad TACACS+, contabilidad VoIP.
- **CSTacacs:** Provee comunicación entre clientes TACACS+ y el servicio CSAuth.
- **CSRadius:** Provee comunicación entre clientes RADIUS y el servicio CSAuth.
- **CSMon:** Monitorea el estado de los servicios ACS y los recursos, registra y reporta todos los errores críticos, envía alertas vía e-mail al administrador, realiza test de login.

IV. Comparación TACACS y RADIUS

Una de las diferencias entre TACACS+ y RADIUS, es que TACACS+ utiliza TCP como protocolo de transporte mientras que RADIUS utiliza UDP. Debido a esto el protocolo TACACS+ es más confiable que el protocolo RADIUS porque tendrá retransmisión de mensajes en caso se produzca una pérdida.

Otras diferencias importante entre RADIUS y TACACS+ está en que RADIUS sólo cifra la contraseña en la petición de acceso hasta un máximo de 16 bytes TACACS +, por otra parte, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Por ello podemos decir que el cifrado que maneja el protocolo TACACS+ es más robusta que el cifrado usado por el protocolo RADIUS.

RADIUS combina la autenticación y la autorización como un solo servicio, mientras TACACS+ los ofrece como servicios independientes. Esto hace que TACACS+ pueda ser utilizado en implementaciones donde no solo se requiera autenticarse sino que se requiera definir diversos niveles de autorización.

Tabla 1. Comparación Servidor TACACS+ y RADIUS

Nombre	Protocolo de Transporte	Datos Cifrados	Autenticación y Autorización
TACACS+	TCP	Cuerpo del Paquete TACACS+	Servicios Independientes
RADIUS	UDP	La Contraseña	Se combina como un solo servicio

Fuente: Los Autores

Conclusiones

Mediante el análisis de riesgos realizado bajo la Metodología de Análisis y Gestión Riesgos de los Sistemas de Información – **MAGERIT**, se lograron identificar los puntos críticos en los cuales un evento inusual puede afectar considerablemente los procesos de negocio del NOC de UNISYS Colombia. Luego, se determinaron los impactos que estos sucesos pueden generar a la compañía en términos de negocio y posteriormente, se estudiaron procedimientos que permitieran mitigar los efectos anteriormente calculados.

La implementación del servidor AAA basado en el protocolo TACACS en la red del NOC de UNISYS Colombia, se constituye en una solución de seguridad informática para garantizar la Confidencialidad, Integridad y Disponibilidad de la información gestionada mediante los activos tecnológicos de la compañía. Por lo tanto, la temática del presente trabajo de grado puede ser aplicada en la infraestructura de red de cualquier organización que gestiones sus comunicaciones mediante dispositivos ***Cisco*** y que además, desee proteger sus elementos tecnológicos para prevenir eventos indeseados que puede obstaculizar lograr los objetivos de negocio.

Al culminar con la implementación del presente proyecto de grado se pudo concluir que, gracias al servidor AAA de RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor AAA TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos.

Se diseñó e implemento en un ambiente operativo de red, una solución teniendo en cuenta las características más valoradas por los usuarios finales: continuidad de servicio, rapidez en el intercambio de datos y seguridad de la información.

Por lo tanto, las organizaciones a nivel mundial deben ser conscientes de la gran importancia que constituye un adecuado manejo y uso de la información, por lo que deben establecer niveles de información para controlar el acceso a la misma y garantizar que los empleados, dependiendo del rol definido por la compañía, tengan acceso solo a la información necesaria para ejercer sus funciones.

La seguridad informática es un campo de estudio crítico de las redes de comunicación, lo que conlleva a pensar que esta disciplina debería contemplarse como una capa transversal de los modelos de comunicaciones TCP/IP y OSI.

Los profesionales de seguridad informática deben ser consientes de la gran importancia de constituye un adecuado manejo y uso de la información de las organizaciones.

Bibliografía

Ariel, Maiorano. (2009). Criptografía Técnicas de desarrollo para profesionales. Alfaomega.

Behrouz A. Forouzan. (2002). Transmisión de datos y redes de comunicaciones. Segunda edición. McGraw-Hill

Behrouz A. Forouzan. (2007). Transmisión de datos y redes de comunicaciones. Cuarta edición. McGraw-Hill

Lockhart, Andrew. (2007). Seguridad de Redes Los mejores trucos. ANAYA Multimedia.

Picouto Ramos, Fernando; Lorente Pérez, Iñaki et al. (2008). Hacking y Seguridad en Internet. Alfaomega: RA-MA.

William, Stallings. (2004). Fundamentos de Seguridad en Redes Aplicaciones y Estándares. Segunda Edición. Prentice Hall.

Referencias Bibliográficas

Anonimo, (s.f.). "Sincables,". [Online]. Available: http://www.sincables.cl/. Consulted: Nov. 2010.

Asadoorian Sans, Paul. SysAdmin Audit, Networking and Security Institute. Implementing secure access to cisco devices using TACACS+ and SSH. [En línea]. Disponible en http://www.sans.org/reading-room/whitepapers/networkdevs/implementing-secure-access-cisco-devices-tacacs-plus-ssh-1041?show=implementing-secure-access-cisco-devices-tacacs-plus-ssh-1041&cat=networkdevs. Extraído el 11 Junio de 2013.

C. de Joomla en Colombia, "F.A.Q - joomla! en colombia". [En línea]. Recuperado de <http://www.joomlaencolombia.net/zona-newbie/faq>. Extraído 5 Junio de 2013

Cisco Systems Technical Support And Documentation, Cisco IOS security configuration guide, 2008.

Cisco Systems Technical Support And Documentation, TACACS+ and RADIUS comparison, Document ID: 13838, Jan 2008.

Cisco Systems, Inc. Cisco AAA Implementation Case Study. [En línea]. Disponible en http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/aaasub/C262.pdf. Extraído el 15 Junio de 2013.

Clasificación y tipos de ataques contra sistemas de información. (Febrero 2009). Disponible en http://www.delitosinformaticos.com/seguridad/clasificacion.shtml.

Eder, Diego, Alejo, and Daniel. (2003). Colombia sin Cables<—->Medellinwireless. [Online]. Available: http://co.lab.cohete.net/wifi/MiTiN_2.html. Consulted: Nov. 2010.

Edney John; Arbaugh, William. Real 802.11 Security Wi-Fi Protected Access and 802.11i. Addison Wesley Ed., 2004.

Ford, M., Lew, K., Spanier, S. y Stevenson, T. Internetworking Technologies Handbook. Indianapolis: Cisco Press, 1997.

Gullaume Lehembre. "Seguridad WI-FI WEP, WPA y WPA2. En: Revista Hackin9 Magazine. No. 1-2006. 2006.

I. telecommunication sunion, "X.170 : Arquitectura de la gestion de red a red para redes de datos." vol. 1, no. 1, p. 17, Jun. 1999. [En línea]. Recuperado de <http://www.itu.int/rec/T-REC-X.170-199906-I>

Ingram Sans, Steve. SysAdmin Audit, Networking and Security Institute. . Case study in implementing AAA Servers Using TACACS+. [En línea]. Disponible en http://cyber-defense.sans.org/resources/papers/gsec/case-study-implementing-aaa-servers-tacacs-plus-105774. Extraído el 11 Junio de 2013.

Lazo García, Nuttsy Aurora. Diseño E Implementación de una Red LAN y Wlan con Sistema de Control de Acceso Mediante Servidores AAA. [En línea]. Disponible en http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1445/LAZO_GARCIA_NUTTSY_SERVIDORES_AAA.pdf?sequence=1. Extraído el 3 Mayo de 2013]

Maldonado Tapia, Ángel Vinicio. Implementación de un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del colegio san Luis Gonzaga a través de una autenticación de los usuarios mediante un servicio AAA implementado en un servidor que trabaje con protocolos Radius. [En línea]. Disponible en http://dspace.ups.edu.ec/bitstream/123456789/4167/1/UPS-ST000959.pdf. Extraído el 6 Mayo de 2013.

Memorias IV Foro. (Nov. 2010. Día 3). Las TIC mejorando la calidad de vida. [Online]. Available: http://www.udtecnovirtual.org/index.php?option=com_content&view=article&id=573%3Aivforo-dia3&catid=1%3Alatest-news&Itemid=1. Consulted: Nov. 2010.

Ministerio de Hacienda y Administraciones Públicas. Gobierno de España. "MAGERIT – versión 3.0. En: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I, I, III. Método.

Plasencia Bedón, Luis Carlos. Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de Networking de un ente del Ministerio de Defensa Nacional. [En línea]. Disponible en http://repositorio.utn.edu.ec/bitstream/123456789/994/1/04%20RED%20009%20TESIS_SERVIDOR_AAA.pdf. Extraído el 7 Mayo de 2013.

R.T. Morris. A Weakness in the 4.2BSD Unix TCP/IP Software. Computing Science Technical Report (No. 117), AT&T Bell Laboratories. New Jersey: Murray Hill, 1985

Simpson, W. PPP Challenge Handshake Authentication Protocol (CHAP). Agosto 1996.

The Internet Engineering Task Force (IETF), Internet Society. RFC Index Search engine. Available. Recuperado de http://www.ietf.org

Y. Rekhter, R. Moskowitz, D. Karrenberg, G. de Groot. Address Allocation for Private Internets, RFC 1918. September 2006.