ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE ELECTRÓNICA EN TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"ANÁLISIS Y DISEÑO DE UNA SOLUCIÓN DE SEGURIDAD PARA EL CONTROL DE ACCESOS ENFOCADOS EN LA IBNS SOBRE LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA FINANCIERA Y DE SERVICIOS"

DANIEL MARTÍN LESCANO RODRÍGUEZ

SANGOLQUI – ECUADOR

2012

CERTIFICACIÓN

Por parte del Ing. Darwin Aguilar e Ing. Carlos Romero certifican que la elaboración del proyecto ANÁLISIS Y DISEÑO DE UNA SOLUCIÓN DE SEGURIDAD PARA EL CONTROL DE ACCESOS ENFOCADOS EN LA IBNS SOBRE LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA FINANCIERA Y DE SERVICIOS fue realizado bajo su dirección.

Ing. Darwin Aguilar
DIRECTOR

Ing. Carlos Romero
CODIRECTOR

RESUMEN

El proyecto desarrollado tiene como objetivo fundamental forjar un mecanismo de seguridad en la infraestructura tecnológica de una empresa financiera y de servicios; dado que en este tipo de instituciones se maneja gran cantidad de dinero, es necesario contar con un mayor control de acceso a la red, ya sea esto en caso de fuga de información o de personal no autorizado que quiera ingresar a la red de la entidad.

Para esto se optó por la Identidad Basada en Servicios de Red (IBNS), la cual utiliza un servidor AAA, el mismo que se encarga de la autenticación, autorización y *accounting* (registro), para que los funcionarios de la institución financiera, puedan ingresar a la red y desarrollar su desempeño laboral con sus respectivos roles y perfiles sin tener ningún inconveniente.

El servidor AAA, se enlazará con una base de datos, ya sea esta externa o interna, y el equipamiento requerido para que esto se encuentre acorde a la configuración y funcionamiento apropiado.

En el resultado de este proyecto, se obtuvo un mayor control en el acceso a la red de la institución ya que exclusivamente los usuarios que pertenezcan a la institución, van a poder ingresar a la infraestructura tecnológica de la misma.

AGRADECIMIENTO

A Dios y a la Virgen María por guiarme cada día en el camino del bien, a mis padres por su apoyo incondicional en todo el transcurso de mi carrera, a mis tíos que me han ayudado y llevado hasta donde estoy ahora, al Ing. Darwin Aguilar Director de tesis, por su paciencia y colaboración en todo momento para la realización de este trabajo, a mis profesores a quienes les debo gran parte de mis conocimientos y finalmente un eterno agradecimiento a la ESCUELA POLITECNICA DEL EJERCITO, la cual me abrió sus puertas para prepararme en un futuro competitivo y formación en mi vida profesional.

DEDICATORIA

Dedico este proyecto de tesis a Dios ya que siempre ha estado conmigo en cada momento de mi vida, a mis padres quienes han velado por mi bienestar y educación, a mi familia por su entera confianza en cada reto que se me presentaba.

PRÓLOGO

En la actualidad, la importancia de la seguridad de la información y acceso a la misma resulta incuestionable. En este contexto, la relevancia de la autenticación fiable dentro de instituciones es importante, por motivos de se pueden encontrar gran cantidad de información trascendental que puede afectar a las instituciones en el caso de su uso indebido. Por sus cualidades y ventajas, el servidor AAA ha desarrollado un papel fundamental en la autenticación, autorización y *accounting* (registro) de usuarios. Esta tesis estudia el proceso de estos tres procedimientos para que un funcionario pueda ingresar al sistema de la institución en la que se encuentre desempeñando sus labores de trabajo, y que de esta manera pueda cumplir con sus funciones cotidianas, sin la necesidad de requerir mayor número de roles del que tiene asignado. Actualmente los roles y perfiles de cada funcionario se tienen por medio de los usuarios responsables de los aplicativos y de acuerdo al cargo de los funcionarios. Por esta razón, se determinan los roles de cada servidor de acuerdo al cargo que estos tengan para que puedan acceder al sistema de la institución y de esta manera se puedan realizar sus funciones sin ningún inconveniente. El presente trabajo trata dicha integración desde la perspectiva de los mecanismos de autenticación involucrados. Pero, ¿hacia dónde va dirigido este proceso?. Una solución de seguridad para el ingreso al sistema de la institución y por medio de este se pueda establecer mecanismos de control sobre los roles, perfiles y aplicativos de cada uno de los funcionarios. ¿En qué medida han sido diseñados para ser adaptados a estas nuevas circunstancias?. Esta tesis aborda la problemática de una forma conjunta, atendiendo al esquema de autenticación extremo a extremo y plantea un nuevo marco de autenticación para el ingreso de a la red de la institución por parte de los funcionarios, con la utilización de su respectivo usuario y contraseña.

ÍNDICE DE CONTENIDO

CAPÍTULO 1

ANÁLISIS Y DEFINICIONES DEL SERVIDOR AAA

1.1 Introducción a IBNS

La IBNS o Identidad Basada en Servicios de Red, es una solución unificada de Cisco que incluye varios dispositivos para permitir la autenticación, control de acceso y aplicación de políticas de usuarios basados en identidad para acceder de forma segura la conectividad a la red y sus recursos.

IBNS permite a las empresas el manejo seguro de la movilidad de sus empleados (acceso remoto seguro basado en identidad), además la asignación de los usuarios a su correspondiente segmento de red basados en su identidad.

El Framework empresarial IBNS ofrece movilidad y la reducción de costos de sobrecarga asociados a permitir y manejar el acceso seguro a los recursos.

Además la IBNS utiliza métodos de autenticación flexible en concordancia con el protocolo de la IEEE 802.1x, para el control de acceso a la red basada en puerto, esto permite la autenticación de los clientes conectados a los puertos LAN de switch permitiendo o no el acceso a la red (habilitando o no el puerto) en base al estado de la autenticación.

El protocolo 802.1x[1] autentica a los clientes usando información única para cada cliente y con credenciales conocidos únicamente por el cliente.

Este servicio es llamado "*port-level authentication*" ya que por razones de seguridad, es configurado en cada uno de los puertos de cada punto de acceso, además consta de varios beneficios como es el soporte de autenticación 802.1x, autenticación basada en dirección MAC, políticas de autorización por defecto y contenedores múltiples de información IP.

El proceso del estándar 802.1x se establece mediante el punto de acceso en búsqueda de acceso utilizando el "*supplicant*", el dispositivo al cual el punto de acceso pide autorización, se procede a dar el acceso, y este es conocido como el autenticador, el mismo que actúa como puerta de enlace para el servidor de autenticación y es responsable por las credenciales del dispositivo de acceso.

El control de admisión de redes (NAC) es un conjunto de tecnologías y soluciones basadas en una iniciativa de la industria elaborada por Cisco, utiliza la infraestructura de la red para hacer cumplir la política de seguridad en todos los dispositivos que pretenden acceder a los recursos informáticos de la red, limitando así el daño causado por amenazas emergentes en contra de la seguridad.

Los clientes que usan NAC tienen la capacidad de permitir que accedan a la red sólo dispositivos confiables de punto terminal como computadoras, servidores y agendas PDA, que cumplan con políticas de seguridad y puedan limitar el acceso de los dispositivos que no las cumplen.

[1] http://www.cisco.com/go/ibns, Identidad Basada en Servicios de Red

Este protocolo es utilizado también para la autenticación de clientes *wireless*, a través de esto, se permite o no el acceso autorizado a la red a nivel de enlace de datos es basado en EAP o *Extensible Authentication Protocol* que es un *framework* de autenticación utilizada en redes WLAN como LAN cableadas, además es una estructura de soporte que no define un único mecanismo de autenticación, sin embargo provee un conjunto de funcionalidades comunes para el o los mecanismos de autenticación escogidos; estos mecanismos se los conoce como métodos EAP.

El EAP[2] (*Extensible Authentication Protocol*) es una extensión del Protocolo punto a punto (PPP) que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias.

Con el EAP se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado.

EAP proporciona una arquitectura estándar para aceptar métodos de autenticación adicionales junto con PPP.

Mediante EAP, se pueden admitir esquemas de autenticación adicionales, conocidos como tipos EAP. Entre estos esquemas se incluyen las tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados. EAP, junto con los tipos de EAP seguros, es un componente tecnológico crítico para las conexiones de red privada virtual (VPN) seguras.

[2] http://technet.microsoft.com/es-es/library/cc782159%28WS.10%29.aspx

Los tipos EAP seguros, como los basados en certificados, ofrecen mayor seguridad frente a ataques físicos o de diccionario, y de investigación de contraseñas, que otros métodos de autenticación basados en contraseña, como CHAP o MS-CHAP.

La familia Windows Server 2003 admite dos tipos de EAP:

- EAP-MD5 CHAP (equivalente al protocolo de autenticación CHAP)
- EAP-TLS (utilizado para autenticación basada en certificados de usuario).

EAP-TLS es un método de autenticación mutua, lo que significa que tanto el cliente como el servidor deben demostrar sus identidades uno a otro. Durante el proceso de autenticación, el cliente de acceso remoto envía su certificado de usuario y el servidor de acceso remoto envía su certificado de equipo. Si el certificado no se envía o no es válido, se termina la conexión.

Dado que el EAP es un mecanismo de autenticación arbitrario, autentica las conexiones de acceso remoto, el cliente de acceso remoto y el autenticador (el servidor de acceso remoto o el servidor del servicio de usuario de acceso telefónico de autenticación remota [RADIUS]) negocian el esquema de autenticación exacto que se va a utilizar. El enrutamiento y acceso remoto admite de forma predeterminada al EAP-TLS y desafío-MD5, también se pueden conectar otros módulos EAP al servidor que ejecuta enrutamiento y acceso remoto para ofrecer otros métodos EAP.

EAP permite que se establezcan conversaciones abiertas entre el cliente de acceso remoto y el autenticador. Esta conversación se compone de las solicitudes de información de autenticación realizadas por el autenticador y las respuestas del cliente de acceso remoto. Por ejemplo, si se utiliza EAP con tarjetas testigos de seguridad, el autenticador puede consultar al cliente de acceso remoto el nombre, el PIN y el valor del testigo de la tarjeta por separado.

Con cada consulta realizada y respondida, el cliente de acceso remoto atraviesa otro nivel de autenticación. Una vez se ha respondido correctamente a todas las preguntas, se autentica al cliente de acceso remoto.

El cliente de acceso remoto y el autenticador deben admitir el mismo tipo de EAP para que la autenticación se lleve a cabo correctamente.

El protocolo EAP es un conjunto de componentes internos que proporciona la compatibilidad de arquitecturas con cualquier tipo de EAP en forma de módulo de complemento. Para que la autenticación se realice correctamente, el cliente de acceso remoto y el autenticador deben tener instalado el mismo módulo de autenticación EAP. La familia Windows Server 2003 proporciona dos tipos de EAP: Desafío-MD5 y EAP-TLS.

EAP-TLS sólo está disponible para los miembros de un dominio. También es posible instalar otros tipos de EAP adicionales. Los componentes del tipo de EAP deben estar instalados en todos los autenticadores y clientes de acceso remoto.

El desafío de síntesis de mensaje 5 (Desafío-MD5) es un tipo de EAP requerido que utiliza el mismo protocolo de desafío mutuo que CHAP basado en PPP, con la diferencia de que los desafíos y las respuestas se envían como mensajes EAP.

Desafío-MD5 suele utilizarse para autenticar las credenciales de los clientes de acceso remoto mediante sistemas de seguridad que usan nombres de usuario y contraseñas.

EAP-TLS

El tipo de EAP Seguridad del nivel de transporte EAP (EAP-TLS, EAP-*Transport Level Security*) se utiliza en entornos de seguridad basados en certificados. Si está utilizando tarjetas inteligentes para la autenticación de acceso remoto, debe utilizar el método de autenticación

EAP-TLS. El intercambio de mensajes EAP-TLS permite la autenticación mutua, la negociación del método de cifrado y la determinación de claves cifradas entre el cliente de acceso remoto y el autenticador. El EAP-TLS proporciona el método de determinación de claves y autenticación más eficaz.

El EAP-TLS sólo se admite en servidores que ejecutan enrutamiento y acceso remoto, que están configurados para utilizar la autenticación de Windows o RADIUS, y que son miembros de un dominio. Los servidores de acceso remoto que se ejecutan como servidores independientes o miembros de un grupo de trabajo no admiten EAP-TLS.

EAP-RADIUS

El EAP-RADIUS[3] no es un tipo de EAP, sino el paso de mensajes EAP de cualquier tipo de EAP a un servidor RADIUS por parte de un autenticador para su autenticación. Por ejemplo, si se configura un servidor de acceso remoto para la autenticación RADIUS, los mensajes EAP enviados entre el cliente y el servidor de acceso remoto se encapsulan y formatean como mensajes RADIUS entre el servidor de acceso remoto y el servidor RADIUS.

Además el EAP-RADIUS se utiliza en entornos en los que RADIUS se usa como proveedor de autenticación. La ventaja de utilizar EAP-RADIUS es que no es necesario instalar los tipos de EAP en todos los servidores de acceso remoto, sino sólo en el servidor RADIUS. En el caso de los servidores IAS (*Internet Authentication Service*), sólo debe instalar tipos de EAP en el servidor IAS.

[3] Cisco Systems, Inc, *User Guide for the Cisco Secure Access Control System 5.1*, Americas Headquarters, 1ª ed., West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 618

Por lo general, al utilizar EAP-RADIUS, el servidor que ejecuta enrutamiento y acceso remoto se configura para utilizar EAP y un servidor IAS para la autenticación.

Cuando se establece una conexión, el cliente de acceso remoto negocia el uso de EAP con el servidor de acceso remoto. Si el cliente envía un mensaje EAP al servidor de acceso remoto, éste encapsula el mensaje EAP como un mensaje RADIUS y lo envía al servidor IAS configurado. El servidor IAS procesa el mensaje EAP y devuelve un mensaje EAP encapsulado como RADIUS al servidor de acceso remoto. A continuación, el servidor de acceso remoto reenvía el mensaje EAP al cliente de acceso remoto.

En esta configuración, el servidor de acceso remoto sólo funciona como dispositivo de paso a través de todo el este proceso. Todo el procesamiento de los mensajes EAP se lleva a cabo en el cliente de acceso remoto y en el servidor IAS.

Se puede configurar enrutamiento y acceso remoto para realizar la autenticación localmente o en un servidor RADIUS. Si se configura enrutamiento y acceso remoto para realizar la autenticación localmente, todos los métodos de EAP se autenticarán localmente. Si se configura enrutamiento y acceso remoto para autenticar un servidor RADIUS, todos los mensajes EAP se reenviarán al servidor RADIUS con EAP-RADIUS.

Para habilitar EAP en una directiva de acceso remoto de un servidor, hay que asegurarse que el servidor de acceso a la red (NAS, Network Access Server) admite dicho protocolo.

En el marco del protocolo TACACS+[4], el ACS permite y simplifica la administración (basado en identidad) tanto de equipos Cisco (Switches, Routers, *Acess Points*, otros).

[4] Cisco Systems, Inc, *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*, 12 ª ed., Americas Headquarters, 170 West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 1410

El ACS es el dispositivo en la red que identifica a los usuarios y dispositivos que intentan conectarse a la red.

La validación de la identidad del los clientes que intentan ingresar a la red lo puede realizar directamente a través de su repositorio de identidad interna (base de datos de cliente sin terno, credencial eso mac-address“sin802.1x”) como autenticación local, o bien, mediante el uso de repositorios externos de identidad (Directorio Activo o LDAP).

El ACS provee funciones avanzadas para el monitorio, reporte así como herramientas de *troubleshooting* que ayudan a administrar y manejar el control de acceso a la red. Tanto el monitoreo como el reporte se lo puede configurar y administra mediante la consola de administración gráfica.

El *Protected Extensible Authentication Protocol* (PEAP) utiliza TLS (*Transport Layer Security*) para formar un túnel cifrado entre el intermediador (switch) y un servidor de autenticación (ACS). PEAP no define un método de autenticación sino que provee encapsulación segura (túnel cifrado) para transporte del método EAP escogido.

1.2 Definición del Servidor AAA

El servidor AAA es un servidor de Autenticación[5] (AAA/ACS), el mismo que realiza la autenticación, autorización y *accounting* para la validación de identidad del usuario (sea en la base de datos interna o en una base de datos externa como el Directorio Activo o LDAP) y notifica al Switch/WLC si el cliente está autorizado para acceder a la LAN y a los servicios del intermediador, siendo el intermediador un cliente RADIUS del ACS.

[5] http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html

El protocolo RADIUS lleva a la autenticación, autorización e información de configuración entre un NAS y un servidor RADIUS de autenticación. Las solicitudes y respuestas realizadas por el protocolo RADIUS se llaman atributos de RADIUS. Estos atributos pueden ser nombre de usuario, tipo de servicio, y así sucesivamente, además proporcionan la información necesaria para un servidor RADIUS para autenticar a los usuarios y para establecer el servicio de red autorizado por ellos. El protocolo RADIUS también lleva la información contable entre un NAS y un servidor RADIUS de contabilidad.

El *Remote Authentication Dial-In User Server*[6] (RADIUS) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer conexiones.

El UDP o *User Datagram Protocol* es un protocolo del nivel de transporte basado en el intercambio de paquetes de datos (datagramas), que permite el envío de los mismos a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El UDP, no tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; dado esto, no se sabe si han llegado correctamente, ya que no hay confirmación de entrega o recepción.

Entre las características importantes del protocolo RADIUS, es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión; así que al usuario se le podrá determinar su consumo y facturar su sesión. Los datos pueden ser utilizados con propósitos estadísticos.

[6] http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html

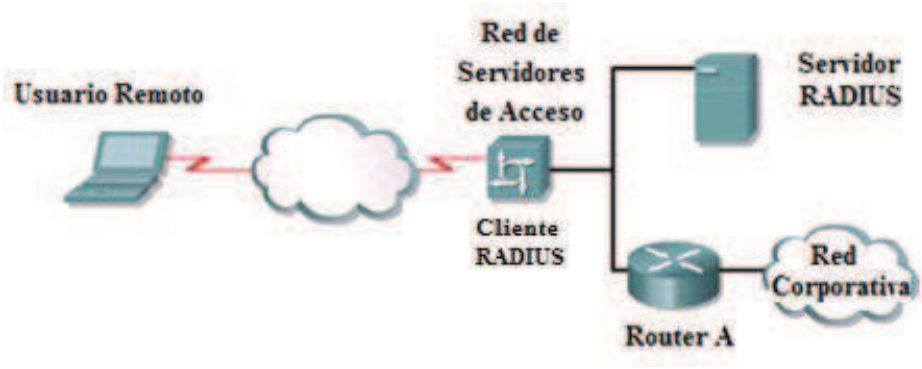

Figura. 1.1. Servidor central con RADIUS (Tomado de http://www.cisco.com/go/ibns)

Network Attached Storage (NAS)[7] es el nombre dado a la tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con computadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red TCP/IP. Además los protocolos de comunicaciones NAS se encuentran basados en ficheros, por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, por esta razón, son orientados a información almacenada en ficheros de pequeño tamaño y gran cantidad.

Terminal *Access Controller Access Control System* (TACACS+) es un sistema de control que envía información con usurario y *password* a un servidor de seguridad centralizada. Dependiendo del tamaño de la red y la cantidad de recursos, el AAA puede ser implementado en un dispositivo de forma local o puede ser gestionado por medio de un servidor central corriendo los protocolos RADIUS o TACACS+.

[7] http://es.wikipedia.org/wiki/Network-attached_storage

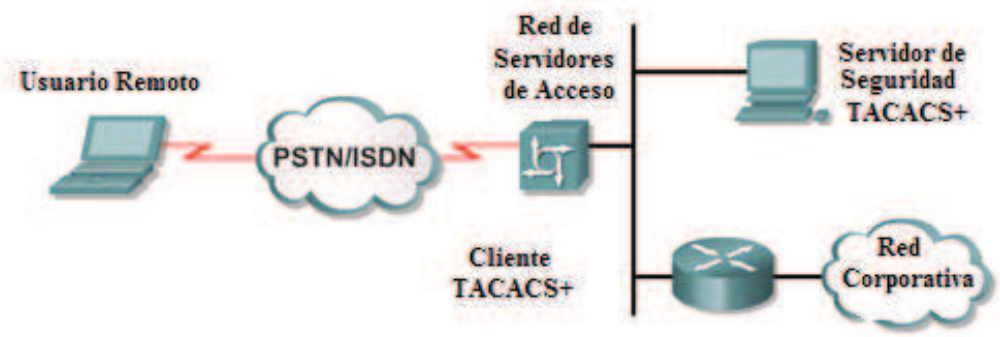

Figura. 1.2. Servidor central con TACACS+ (http://www.cisco.com/go/ibns)

La comparación entre estos servidores RADIUS Y TACACS+[8], se la puede determinar en la funcionalidad, protocolo de transporte y soporte, dirección, confidencialidad y registro.

A continuación se muestra las principales diferencias de estos servidores.

Tabla. 1.1. Comparativa de las características de los servidores TACACS+ y RADIUS

CARACTERÍSTICAS	TACACS+	RADIUS
Funcionalidad	AAA Separado	Autenticación y Autorización Combinado
Protocolo de Transporte	TCP	UDP
CHAP	Bidireccional	Unidireccional
Protocolo de Soporte	Multi-protocolo de Soporte	No ARA, no NetBEUI
Confidencialidad	Encriptación de paquetes	Encriptación de contraseña
Accounting	Limitado	Extenso

[8] http://es.scribd.com/doc/57741341/T3-AAA

1.3 Funcionamiento del Servidor AAA

La IBNS es una solución de seguridad de acceso a la red que incluye varios componentes para permitir la autenticación, autorización y aplicación de políticas de usuarios basados en identidad para acceder de forma segura la conectividad a la red y sus recursos. Además permite a las instituciones el manejo e ingreso seguro a la red de sus funcionarios con sus correspondientes segmentos de roles, perfiles y aplicativos basados en su identidad.

Figura. 1.3. Ingreso basado en IBNS de Cisco (http://www.cisco.com/go/ibns)

El funcionamiento de este servidor AAA, se establece con los parámetros de autenticación, autorización y *accounting*, los cuales se detallan a continuación:

Autenticación: los funcionarios deben probar que son ellos mediante usuario y contraseña, cuestiones desafío - respuesta, *tokens.* Hace referencia a quien es permitido el acceso a la red.

Autorización: determina a que recursos puede acceder un usuario después de haberse autenticado.

Que puede hacer un usuario y que no puede hacer un usuario una vez autenticado, es implementada utilizando un servidor AAA, la autorización es automática y no requiere actualización por parte del usuario.

Accounting (registro): que acciones han realizado los usuarios mientras se encontraban en la red.

Mediante el *accounting* se recogen datos que pueden ser utilizados en auditorias o para la elaboración de facturas, estos datos incluyen horas de comienzo y fin.

Para el control de acceso a la red, se establece con el protocolo de la IEEE 802.1x. Este tipo de protocolo, permite la autenticación de los clientes conectados a los puertos LAN al switch, permitiendo o no el acceso a la red (habilitando o no el puerto en base al estado de la autenticación).

También es utilizado para la autenticación de clientes *Wireless*.

A través de la autenticación se permite o no el acceso autorizado a la red a nivel de enlace de datos. La autenticación 802.1X se encuentra basada en EAP.

Los componentes que constituyen la solución de seguridad en el acceso a la red de la institución en relación con INBS son:

- Clientes (PC, Laptop periféricos con agentes 802.1x)
- Intermediador (Switches, Access Point)
- AAA (ACS Access Control)

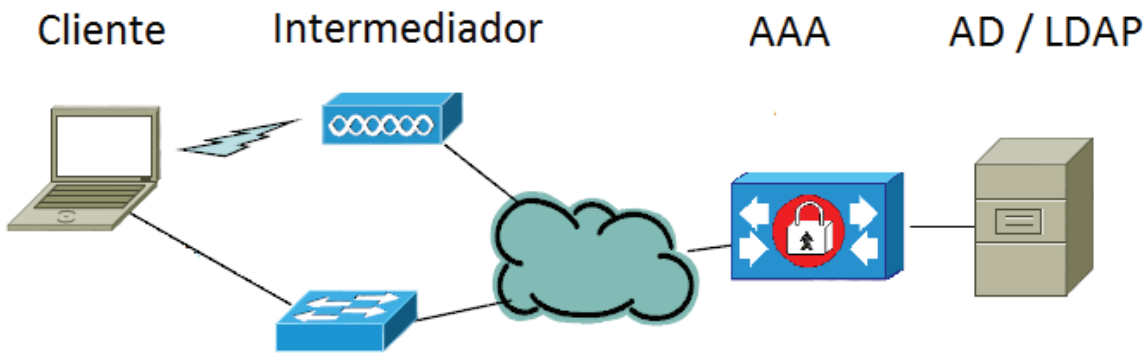

Figura. 1.4. Componentes de IBNS de Cisco (http://www.cisco.com/go/ibns)

Cuando se establecen las conexiones normales a la red de la institución, sin la utilización del protocolo 802.1x[9], se puede ingresar al sistema sin ninguna restricción dado que no se encuentra con seguridades específicas para el acceso al mismo.

Cuando el protocolo 802.1x *Port-Based Authentication*es[10] habilitado en el puerto de switch, antes de que un cliente sea autenticado, dicho puerto solo permite tráfico del tipo EAPoL (*Extensible Authentication Protocol over LAN*) y en el caso de Cisco CDP (*Cisco Discovery Protocol*) y STP (*Spanning Tree Protocol*), una vez autenticado el cliente, todo tráfico es permitido.

[9] http://technet.microsoft.com/es-es/library/cc732681(WS.10).aspx
[10] http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491729.html&ei=KNY2TuTFFrK50AH30ImiDA&sa=X&oi=translate&ct=result&resnum=3&ved=0CEAQ7gEwAg&prev=/search%3Fq%3DCisco%2BHCAP%26hl%3Des%26rlz%3D1R2RNTN_enEC381%26biw%3D1280%26bih%3D600%26prmd%3Divns

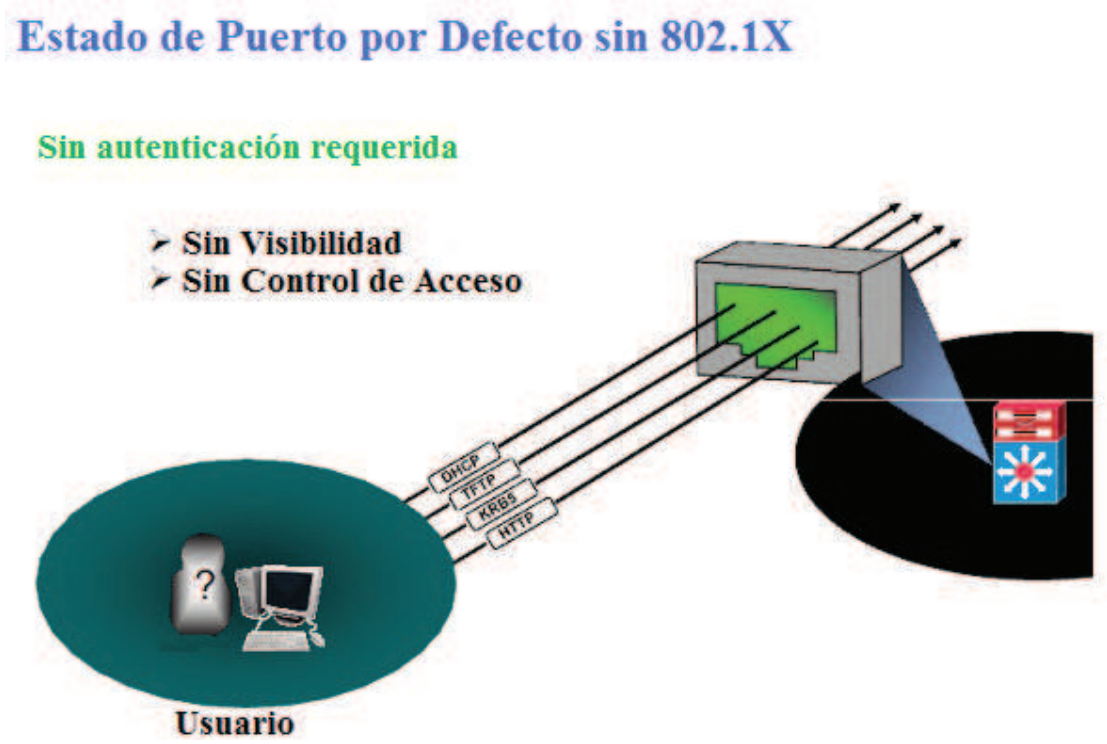

Figura. 1.5. Operación de un Puerto sin 802.1x (operación por defecto) (http://www.cisco.com/go/ibns)

El puerto habilitado con el protocolo 802.1x, impide el trasporte de DHCP, TFTP, KRBS, HTTP[11], y solamente tiene acceso al protocolo de autenticación extensiva bajo LAN (EAPoL) para el puerto de autocontrol de autenticación.

[11] http://technet.microsoft.com/es-es/library/cc732681(WS.10).aspx

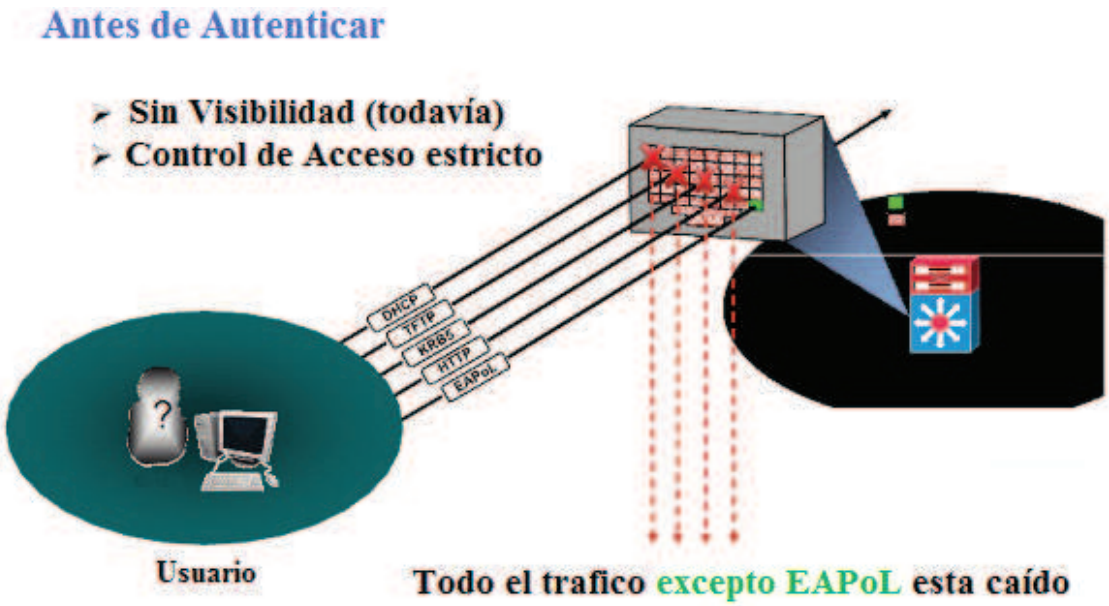

Figura. 1.6. Operación de un Puerto con 802.1x (http://www.cisco.com/go/ibns)

Para la aplicación de la contraseña con una mayor seguridad, existe un mecanismo con el uso de MD4 o *Message Digest 4*, el cual se utiliza para la creación de *password* para una sola utilización.

Un certificado digital o una firma es un código hash encriptado basado en una combinación de una llave pública y el algoritmo hash de un vía que se agrega al documento.

El algoritmo hash[12] son funciones que actúan como proyecciones de un conjunto dominio, generalmente con un número elevado de elementos (incluso infinitos), sobre un conjunto de tamaño fijo y mucho más pequeño que el anterior. De esta forma decimos que estas funciones resumen datos del conjunto dominio. La idea básica de un valor hash es que sirva como una representación compacta de la cadena de entrada.

[12] http://es.wikipedia.org/wiki/Hash

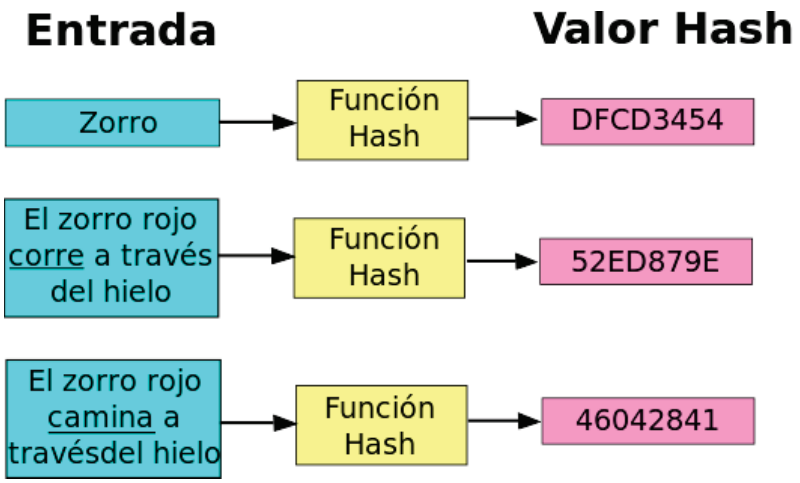

Figura. 1.7. Función Hash en funcionamiento (http://es.wikipedia.org/wiki/Funci%C3%B3n_Hash)

La validación de este certificado digital se lo realiza mediante un CA (*Certificate Authority*), el cual puede ser de terceros y es un ente confiable tanto para el que envía y el que recibe la información. Para validar la firma el receptor debe primero saber la llave publica, la cual es distribuida en otro momento o durante la instalación.

Figura. 1.8. Certificado Digital (http://www.cisco.com/go/ibns)

1.4 Compatibilidad y Definición de Equipos con el Servidor AAA

Para la compatibilidad de equipamiento con el servidor AAA, es fundamental establecer las topologías con las cuales se puede contar en la institución financiera, ya que de esto dependerán los equipos con los que se vaya a trabajar y el mejor desempeño que estos tengan referente a la misma.

En la obtención de la información de la red, debemos enfocarnos en el concepto de una topología de red la misma, que se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

Las redes de computadoras surgieron como una necesidad de interconectar los diferentes host de una institución para poder así compartir recursos y equipos específicos, pero los diferentes componentes que van a formar una red se pueden interconectar de diferentes maneras, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red[13] se conoce con el nombre de topología de la red y la topología idónea de una red concreta va a depender de los diferentes factores, como el número de máquinas a interconectar el tipo de acceso al medio físico que deseemos, etc.

La topología de red de forma lógica de red[14], se define como la cadena de comunicación de los nodos que conforman una red que usan para comunicarse. Además se debe conocer que la topología de red la determina únicamente la configuración de las conexiones entre nodos, esta configuración recoge tres campos que son físicos, eléctricos y lógicos.

[13] http://www.slideshare.net/guest7bb5a1/redes-topologia-de-red
[14] http://tesis-redes.blogspot.com

El campo físico es la disposición real de las máquinas, dispositivos de red y cableado en la red.

Tanto el nivel físico como eléctrico, se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación.

La topología lógica es la forma en la que las máquinas se comunican a través de un medio físico. Los dos tipos más comunes de topologías lógicas son *broadcast* y la transmisión de *tokens.*

La topología *broadcast,* simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar red para transmitir datos en el momento en que lo necesita.

En la transmisión de datos, el *tokens* controla el acceso a la red al transmitir un *token* eléctrico de forma secuencial a cada host. Cuando un host recibe el *token,* significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el *token* hacia el siguiente host y el proceso se vuelve a repetir.

Existen varios tipos de topologías de red como en estrella, árbol, bus, anillo, etc., los mismos que se pueden realizar de acuerdo a los requerimientos de la institución financiera y de los departamentos con los que cuente para un mejor funcionamiento y desempeño de la red.

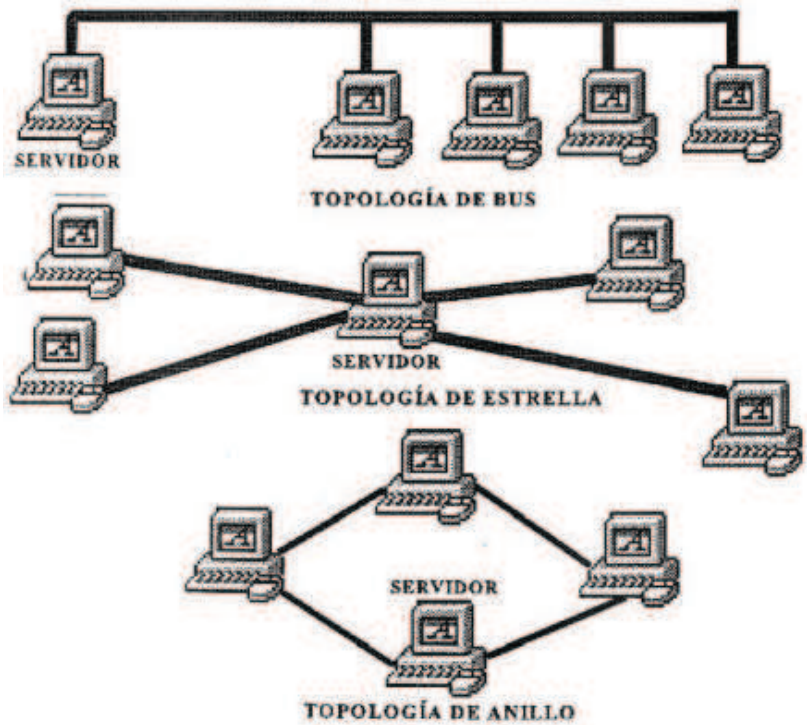

Figura. 1.9. Topologías de Red (http://vivianatelematicas.blogspot.com/2012/04/topologias-de-red.html)

Un claro ejemplo de la topología de árbol[15], la cual es llamada así por su apariencia estética, por la cual puede comenzar con la inserción del servicio de internet desde el proveedor, pasando por el router, luego por un switch y este deriva a otro switch u otro router o sencillamente a los hosts (estaciones de trabajo), el resultado de esto es una red con apariencia de árbol porque desde el primer router que se tiene se ramifica la distribución de internet dando lugar a la creación de nuevas redes o subredes tanto internas como externas.

La topología de bus tiene todos sus nodos (computadores) conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente. La ruptura de un cable hace que los host queden desconectados.

[15] http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

En esta topología, los elementos que constituyen la red se linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzando a los demás nodos.

Además de la topología estética, se puede dar una topología lógica a la red y eso dependerá de los parámetros que se necesite. En algunos casos se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de como el protocolo considera dicho cableado.

Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para que de esta manera logre determinar cuál es la que le corresponde.

También la topología de bus, permite que todos los dispositivos de la red puedan ver todas las señales que todos los demás dispositivos obtengan esta información. Pero esta metodología presenta una desventaja, ya que es común que presenten problemas de tráfico y colisiones, que se pueden disminuir segmentando la red de varias partes. Es una de las topologías más comunes en pequeñas redes LAN, con HUB o switch final de uno de los extremos.

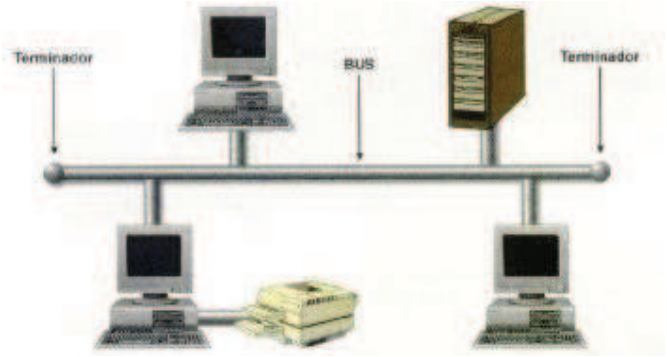

Figura. 1.10. Topología de Red tipo Bus (http://www.nicklabs.com.ar/?p=1687)

La topología en anillo y anillo doble es una diferente topología que se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes. Los dispositivos se conectan directamente entre sí por medio de cables en la que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

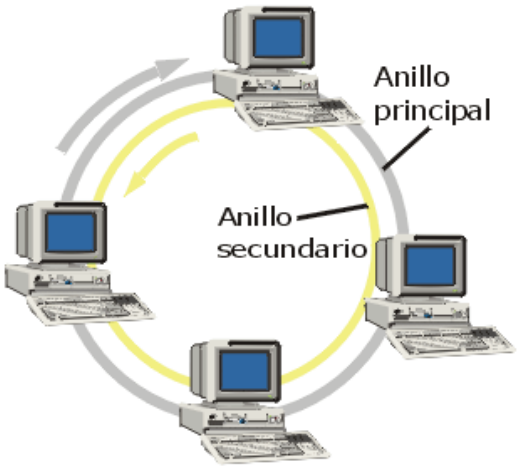

Figura. 1.11. Topología de Red tipo Anillo (http://albertosantamariacabanes.blogspot.com/)

La topología de anillo doble[16] consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia, es decir, que cuando un anillo falla, los datos pueden transmitirse por el otro anillo.

[16] http://porta-tlacuachasunidas.blogspot.com/2011/05/topologia-de-doble-anillo.html

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este.

Se utiliza sobre todo para redes locales. La mayoría de redes de área local que tienen un router, un switch o un HUB, siguen esta topología. El nodo central en estas sería el enrutador (router), el conmutador (switch) o el concentrador (HUB), ya que por este pasan todos los paquetes.

La topología en estrella[17] extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella.

Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs; la ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local.

[17] http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Figura. 1.12. Topología de Red tipo Estrella (http://www.nicklabs.com.ar/?p=1687)

La topología en árbol es un tipo de topología en la cual los nodos están colocados en forma de un árbol. Desde una visión topología, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un switch o hub, desde q se ramifican los demás nodos.

Es una variación de la topología de bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la topología de árbol como la de estrella, son similares a la de bus cuando el nodo de interconexión trabaja en nodo de difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

Figura. 1.13. Topología de Red tipo Árbol (http://emoxionezloqas10.blogspot.com/p/topologias-de-red.html)

La topología en malla es la topología de red en la que cada nodo está conectado a todos los nodos. De esta forma, es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

Esta topología a diferencia de otras, no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento, es decir, si se cae la red no es importante porque no implica la caída de toda la red, como la topología de árbol o estrella.

La desventaja física principal es que solo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna molesta.

Existe otro tipo de topología en la cual no existe un patrón de enlace de nodos. El cableado no sigue ningún modelo determinado, de los nodos salen cantidades variables de cables. Las redes se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas.

En las topologías mixtas como anillo, se establece una forma lógica únicamente, ya que de manera física se utiliza una topología en estrella.

El concentrador utilizando cuando se está utilizando esta topología se denomina Unidad de Acceso Multiestación (MAU), que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos, además contiene un anillo interno que se extiende a uno externo.

Las topologías de mixtas basadas en bus – estrella, es en realidad una topología en estrella que funciona como si fuese bus. Como punto central tiene un HUB pasivo que implementa internamente el bus, y al que están conectados todos los computadores.

La única diferencia que existe entre esta topología mixta y en estrella con HUB pasivo, es el acceso al medio utilizado.

Figura. 1.14. Topología de Red tipo Bus-Estrella (http://redes-angela.blogspot.com/2010/12/en-una-topologia-en-estrella-bus-varias.html)

La topología de red la determina únicamente la configuración de las conexiones entre nodos, es decir, depende de cada institución financiera la topología que utilice.

La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Dado que el servidor AAA es un servidor Cisco, los diferentes routers y switches se recomienda que los equipos también deben ser de esta marca para que exista una mejor y mayor compatibilidad entre estos, y de esta manera no tener ningún problema en caso de implementar este proyecto. En estudios anteriores, se ha podido determinar que existen conflictos entre switches que son de otras marcas, las cuales no le reconoce el servidor de autenticación.

Uno de los routers con los vamos a desarrollar este análisis es un router Cisco de la serie 1700 proporcionan un rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad. La serie 1700 ofrece una extensa familia de características de seguridad integradas como protección por "firewall", túneles VPN y detección de intrusos o "IDS". También proporcionan una vía de acceso a servicios como la Voz por IP o "Voice-over-IP" y telefónica IP a través de la convergencia de las redes de voz y datos que ofrecen servicios de procesamiento de llamada y calidad de servicio o "QoS".

Para los switches, vamos a tomar de diferentes series y marcas, de las cuales se va a obtener, gracias al estudio y análisis, una mayor y mejor perspectiva del equipamiento óptimo para la compatibilidad con el servidor AAA.

Uno de los más influyentes es el switch Cisco de la familia Catalyst 2960, que soporta las comunicaciones de datos, voz y tecnología inalámbrica, por lo que en caso de

implementación, estos servicios disponga de una red que admita todas sus necesidades de negocio. Además establece prioridad al tráfico de voz o al intercambio de datos para alinear la entrega de información a sus requisitos de negocio.

Posee una alta seguridad en la que protege la información importante y mantiene a los usuarios no autorizados alejados de la red y consiga un funcionamiento ininterrumpido.

Tiene una ventaja en aprovechamientos de los métodos basados en normas para conseguir una mayor fiabilidad y una rápida recuperación de errores, también puede agregar un suministro de energía redundante para obtener una fiabilidad adicional.

Este switch Cisco, utiliza *Cisco Network Assistant* ya que es un software para simplificar la configuración, las actualizaciones y la solución de problemas en caso su existencia.

Otro switch Cisco Catalyst que nos va a servir en nuestro estudio es el de la serie 2950, ya que es un conmutador de configuración fija, apilable interruptor independiente que ofrece velocidad de cable de FastEthernet y Gigabit Ethernet. Este conmutador ofrece dos conjuntos de funciones de software y una amplia gama de configuraciones para permitir que las sucursales pequeñas, medianas y grandes empresas y en entornos industriales para seleccionar la combinación correcta para el borde de la red.

Ofrece de imagen estándar Cisco IOS Software para las funciones básicas de datos, voz y video. Además en caso de redes con requisitos de seguridad adicionales, brinda calidad de servicio (QoS). Este IOS de imágenes mejoradas ofrece servicios inteligentes, tales como la limitación de velocidad y el filtrado de seguridad para el despliegue en el borde de la red.

Para uso industrial a nivel de redes, el nuevo switch Cisco Catalyst de la serie 2955 es un interruptor ideal para implementaciones de Ethernet industriales, con sistemas de transporte inteligentes (STI), y soluciones de red de transporte.

Es adecuado para uso militar ya que puede soportar condiciones ambientales extrema que superan las especificaciones de otros productos de conmutación comercial.

Este switch también ofrece Cisco *Network Assistant* que permite un fácil uso de la interfaz gráfica para su configuración, solución de problemas y facilitar en supervisión de la red. Además simplifica la tarea de administración de conmutadores de Cisco routers y puntos de acceso inalámbricos.

El conmutador Cisco Catalyst de la serie 3550, es un switch apilable, de múltiples capas que proporciona alta disponibilidad, QoS y seguridad para mejorar las operaciones de red. Con una gama de configuraciones tanto de FastEthernet como de gigabit Ethernet.

Los clientes pueden desplegar varios servicios de carácter inteligente como QoS avanzado, limitación de velocidad, seguridad en el control de acceso, gestión de multidifusión, IP de alto rendimiento de enrutamiento y mantener la simplicidad de la conmutación LAN tradicionales.

El switch Catalyst 3550, posee una aplicación de administración centralizada gratuita llamada Cisco *Network Assistant* la cual simplifica la tarea de administración de conmutadores de routers Cisco y su punto de acceso inalámbrico. También ofrece facilidad de usar interfaz gráfica para configurar, solucionar problemas y facilitar la supervisión de la red, al igual que el resto de equipos que tienen esta aplicación.

La característica común de los diferentes equipos es la que poseen el protocolo 802.1x, en el cual se desarrollará el análisis en base al ACS.

Otra de las marcas establecidas para nuestro análisis es SMC Networks que tiene equipos switch de la familia Tiger 6152L2, este switch 10/100 se encuentra enfocado a SMB (*Server Message Block*). El switch tiene 48 puertos 10/100 más 4 puertos gigabit con capacidad suplementaria de *uplinks*. También lleva instalado el software *clustering* que permite la agrupación con otros productos SMC6100 o SMC8100. Este switch para grupos de trabajo 10/100 está diseñado para gestionar la arquitectura de *clustering*. Es capaz de alcanzar hasta 12.8Gbps con arquitectura *non-blocking* incluyendo los 4 puertos gigabit. Ofrece así un switch Ethernet con calidad-precio inmejorable para redes de banda ancha que requieren características de seguridad avanzada para la transmisión de datos críticos. Las especificaciones de seguridad incluyen RADIUS, IEEE802.1x, SSH, SSL, TACACS+, y ACL. Puerto de alta densidad y 1U *high*, este switch es ideal para instalaciones en la pequeña y mediana empresa.

La serie 7200-48P de la marca D-Link, es una tarjeta de línea para los switches de chasis DES-7200. Ofrece 44 interfaces Gigabit eléctricas 10/100/1000Base-T y 4 interfaces Gigabit combo ópticas/eléctricas, que proporcionan conmutación L2/L3 a velocidad de cable (10/100/1000Base-T o SFP). El 7200-48 es cambiable en funcionamiento.

El switch V1905-48 de la marca HP/3Com se lo puede administrar vía Web de Capa 2, además esta administración es compatible con SNMP. Dispone de 48 puertos 10/100Mbps y 2 puertos Gigabit de uso dual (cobre o fibra basada en SFP) y un puerto de Consola RJ-45. Puede trabajar de forma *plug and play* sin necesidad de configurar solamente con los valores por defecto. Si se desea más control, la interfaz del conmutador permite incluso a los usuarios principiantes configurar el conmutador de forma rápida y segura. Las VLANs permiten segmentar la red, reagrupando los usuarios en función de sus necesidades de intercambio de datos o tráfico para un uso óptimo del ancho de banda disponible. El tráfico VoIP (voz sobre

IP) puede asignarse automáticamente a una VLAN de voz dedicada, optimizando así este tráfico sensible al retardo. La agregación de enlaces manual permite agrupar puertos para crear una conexión troncal con ancho de banda ultra grande con la red troncal, y ayuda a prevenir los cuellos de botella de tráfico. El control de acceso a la red IEEE 802.1X proporciona seguridad basada en estándares, combinada con autenticación local. El soporte del protocolo *Rapid Spanning Tree* (RSTP) permite mejorar la compatibilidad, escalabilidad y disponibilidad de la red. El IGMP *snooping* y *query* y el filtrado *multicast* permiten optimizar el rendimiento de la red. Estándar IEEE 802.3, 802.3u, 802.3ab. Puertos MDIX automáticos, dúplex medio o completo. Procesador ARM 88E6218 a 150 MHz, 8 MB de SDRAM, y 4 MB de Flash. Capacidad de conmutación 13.6 Gbps. Capacidad de envío 10,1 mpps.

1.5 Nivel Seguridad Actual en la Institución Financiera

Las fuentes de vulnerabilidad de una institución financiera, están intrínsecamente relacionadas con sus principales funciones. Cada una de las responsabilidades limitadas de los funcionarios y la información asimétrica, tienden a incrementar el nivel de seguridad de para el acceso a la red de la institución financiera.

Actualmente podemos indicar que cualquier institución financiera cuente con un área de seguridad informática recientemente constituida o un sistema de seguridad baja; los roles y perfiles en responsabilidades del área ya se encuentran formalizados y las tareas desempeñadas por cada área y una base de datos conjunta y se limitan por ahora al control de accesos de la mayoría de sistemas de la entidad.

Algunas tareas correspondientes a la administración de seguridad son realizadas por el área de sistemas como la administración de red, firewalls y bases de datos, otras tareas son desarrolladas directamente por las áreas usuarias, y finalmente otras responsabilidades como la elaboración de las políticas y normas de seguridad, concientización de los usuarios, monitoreo

de incidentes de seguridad, etc. En este sentido, en el presente trabajo detallamos los roles y responsabilidades de cada funcionario y la administración de seguridad de la información que involucra no solamente a miembros de las áreas de seguridad informática y sistemas como administradores de seguridad de información y custodios de información, sino a los gerentes y jefes de las unidades de negocio como propietarios de información, y a los usuarios en general.

1.6 Descripción de Cargos de Funcionarios y Personas Pertenecientes a la Institución Financiera

La descripción de los cargos, dependen de los tipos de tareas que ejecute cada funcionario, no existe un formato estándar de descripciones de puestos, su apariencia y contenido varían de acuerdo de una empresa a otra; no obstante, la mayor parte de las descripciones de puestos tendrán por lo menos tres características:

Título del Puesto - le da importancia psicológica y de estatus al empleado, también debe indicar el nivel relativo que ocupa quien lo tiene en la jerarquía de la empresa.

Sección de Identificación del Cargo - incluye argumentos como la ubicación departamental del puesto, la persona con la que reporta quien lo ocupa y la fecha en que se revisó por última vez su descripción.

Sección de los Deberes del Cargo - estos aparecen en orden de importancia, además estas declaraciones deben indicar el peso o valor de cada tarea; por lo general, se indican las herramientas y equipo que utiliza el empleado para desempeñar su trabajo.

Existen varios Departamentos como Auditoría, Tecnología, Cobranzas, Servicios, Recursos Humanos entre otros, dentro de los cuales se obtienen diferentes cargos. Los más

específicos dentro de una entidad financiera son Gerente General, Directores, Jefes de Áreas y Departamentos, Expertos, Especialistas, Auditor, Asistentes.

Las funciones básicas de los cargos de los funcionarios se detallan a continuación:

El Gerente General tiene a su cargo la planificación y dirección de todas las actividades y operaciones en toda la institución, necesarias para atender las necesidades y servicios que experimentan los clientes, además es responsable de la buena marcha de la entidad, con utilidades dentro del marco de políticas, objetivos y presupuestos establecidos por la administración superior.

El Director General supervisa todas las áreas para saber las necesidades de la institución y tomar decisiones inteligentes que mejoren la situación de ésta, además informa al consejo administrativo de la situación actual de la entidad financiera, establece buenas relaciones a todos los niveles internos y externos para establecer el correcto uso de los recursos de la empresa.

Los Jefes de Áreas son los responsables de investigar, proveer y comunicar a su respectivo equipo, los descubrimientos, las tendencias y los avances que se estén dando en el área de su responsabilidad., dirige, coordina y controla las actividades de enseñanza y aprendizaje en su respetiva área y en su entorno institucional.

Los Especialistas tienen a su cargo la atención de consultas de usuarios internos y proveedores, colaboración con los análisis y control de documentación, seguimiento de trámites, elaboración de informes y brindar colaboración a los integrantes del área.

La función del Auditor interno es la prevención y detección de los fraudes lleguen a concretarse, es decir, que cuando ocurre el fraude, se debe analizar el caso, ver los costos que

tuvo para la empresa y generar un plan de acción que lo remedie y evitar que ese fraude genere un mayor perjuicio para la entidad financiera.

Asistente Administrativo tiene a su cuenta la recepción y registro de toda la documentación de ingreso y salida emitida por la institución financiera, apoya la generación de comunicados y otros documentos de información que emita su departamento, brinda apoyo y colaboración a los integrantes de su área y apoyo en la generación de informes.

Este tipo de esquema se lo realiza mediante una base de datos que se encuentra vinculada con el Directorio Activo, es decir, los roles, perfiles y aplicativos perteneciente a cada cargo de los diferentes funcionarios, se los establece mediante este programa, con esto podemos determinar el usuario para que con el registro del mismo y su respectiva contraseña, logremos el ingreso a dichos cargos.

El *Active Directory* (AD) es el término que utiliza Microsoft refiriéndose a la implementación de servicio de directorio en una red distribuida de computadores. Utiliza diferentes protocolos, principalmente LDAP, DNS, DHCP, etc.

La estructura jerárquica del Directorio Activo permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

El AD permite que los administradores establezcan políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Además almacena información de una organización en una base de datos central que sea organizada y accesible.

La estructura del Directorio Activo está basado en dominios y subdominios que se identifican utilizando la misma notación de las zonas DNS, razón por la cual el AD requiere uno o más servidores DNS que permitan el direccionamiento de los equipos pertenecientes a la red, como el listado de equipos conectados, los componentes lógicos de la red y el listado de usuarios.

El funcionamiento del Directorio Activo es similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. La ventaja que presenta esto es la sincronización presente entre los distintos servidores de autenticación de todo el dominio.

A su vez, cada uno de estos objetos en la base de datos, tendrá atributos que permiten identificarlos en modo unívoco como los campos nombre, email, etc; las impresoras de red tendrán sus propios campos como nombre, fabricante, modelo, usuarios que pueden acceder, etc. Toda esta información queda almacenada en el AD replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

De esta forma, es posible crear recursos como carpetas compartidas, impresoras de red, etc. y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en AD, siendo esta lista de objetos replicada a todo el dominio de administración con eventuales cambios puedan ser visibles en todo el contexto institucional, es decir, el Directorio Activo es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red como pueden ser usuarios, equipos y recursos.

CAPÍTULO 2

ANÁLISIS Y DEFINICIÓN DE REQUERIMIENTOS

2.1 Levantamiento de Información de la Topología Física y Lógica de Conexión a la Red

El término topología se refiere a la forma en que está diseñada la red, bien físicamente (rigiéndose de algunas características en su hardware) o bien lógicamente (basándose en las características internas de su software).

La topología de red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (denominados nodos).

Una de las topologías más utilizadas para este tipo de infraestructuras institucionales son las topologías de árbol, en la cual se destaca la combinación en características de la topología de estrella con la de bus, este tipo de topología consiste en un conjunto de subredes estrella conectadas a un bus, es decir, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

Además, facilita el crecimiento de la red, por este motivo es adecuada para este tipo de conexiones de red.

Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

El controlador central del árbol es un concentrador activo, el mismo que contiene un repetidor, es decir, un dispositivo hardware que regenera los patrones de bits recibidos antes de retransmitidos.

Un concentrador es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples hosts y regenerar la señal. El concentrador es una entidad que cuenta con determinada cantidad de puertos (posee tantos puertos como equipos a conectar entre sí, generalmente 4, 8, 16 ó 32).

Su único objetivo es recuperar los datos binarios que ingresan a un puerto y enviarlos a los demás puertos. Al igual que un repetidor, el concentrador funciona en el nivel 1 del modelo OSI.

Los concentradores activos están conectados a una fuente de alimentación eléctrica y permiten regenerar la señal que se envía a los diferentes puertos, y los pasivos simplemente envían la señal a todos los hosts conectados, sin amplificarla.

La retransmisión de las señales de esta forma, amplifica su potencia e incrementa la distancia a la que puede viajar la señal.

Los concentradores secundarios pueden ser activos o pasivos. Un concentrador pasivo proporciona solamente una conexión física entre los dispositivos conectados.

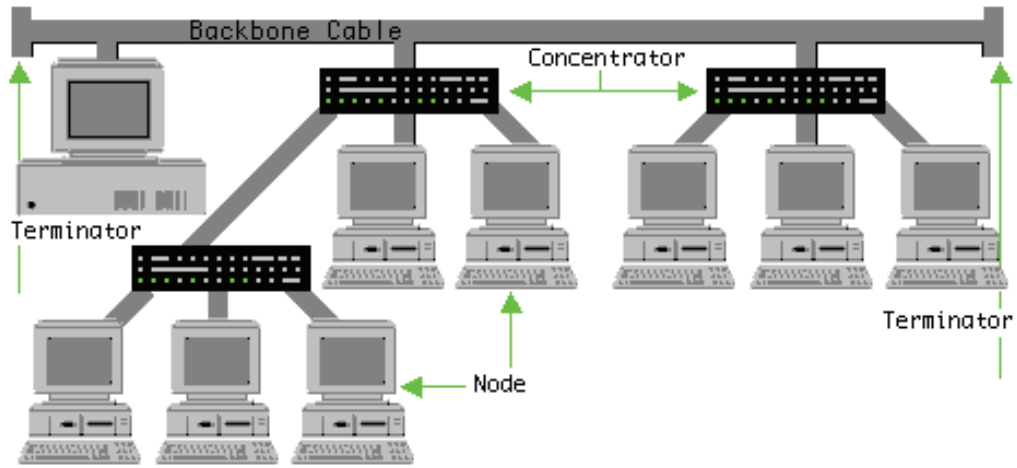

Figura. 2.1. Topología de Red en Árbol (http://abelperaza.tripod.com/arbol.htm)

Ventajas:

- El Hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.
- Permite conectar más dispositivos.
- Permite priorizar las comunicaciones de distintas computadoras.
- Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
- Permite priorizar y aislar las comunicaciones de distintas computadoras.
- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Desventajas:

- Se requiere mucho cable.
- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.
- Es más difícil su configuración.

Para los equipos switch con los que se va a realizar el análisis y diseño, va a ser de las marcas D-Link, HP/3Com, SMC y Cisco, los mismos que se van a encontrar en la infraestructura de red de la institución financiera.

2.2 Análisis de equipamiento compatible con el servidor AAA

Con un análisis muy detallado de las ventajas y desventajas del equipamiento con el cual se podría llevar a cabo este proyecto, se investigaron varias marcas como son D-Link, HP/3Com, SMC y Cisco.

Para las características de cada marca del equipamiento compatible con el servidor AAA, iniciaremos con el detalle de la marca SMC y la mejor opción con el switch SMC 6152l2 tiger switch 10/100.

Tabla. 2.1. Características del Switch SMC 6152l2

Características		Detalles
Transmisión de datos	Tasa de transferencia (máx)	1 Gbit/s
	Tasa de transferencia de datos(min/max)	10/100/1000 Mbit/s
	Capacidad de conmutación	17.6 Gbit/s
	Velocidad de transferencia	13 Mpps

	(paquete)	
Red	Estándar de red	IEEE802.3; IEEE802.3u/D/p/Q/ac/ad/w/v/x; IEC8802.3
	Tipo de interruptor	Administrado
	Plataforma de gestión	Telnet, SLIP, SNMP
	MIB, soporte	MIB II (RFC 1213), *Bridging MIB* (RFC 1493), *Ethernet-Like MIB* (RFC 2665), *Bridge MIB Extensions* (RFC 2764), RMON MIB (RFC 1757), RFC 2737, RFC 2742, RFC 2021, RFC MIB II (RFC 1213), MIB (RFC 1493), MIB (RFC 2665), MIB (RFC 2764), RMON MIB (RFC1757), R
	Calidad de servicio (QoS) soporte	SI
Características de manejo	Administración de *Web-based*	SI
Protocolos	Protocolos de red admitidos	(802.1D, .1w); 802.1Q/v
	Cantidad de puertos	48
	Copper ethernet cabling technology	10/100/1000 BASE-T
	Gigabit Ethernet (cobre), cantidad de puertos	4
	Ethernet LAN (RJ-45) cantidad de puertos	48
Conectividad	Puerto - RS-232	1
Memoria	Memoria temporal	0.5 MB
	Algoritmo de seguridad	TACACS+; HTTPS & SSL; SSH (Telnet); JFS; DFI; MCF
	MAC, filtro de direcciones	SI
Seguridad	Acceso a lista de control (ACL)	SI
	Dimensiones (Ancho x Profundidad x Altura)	440 x 171 x 230 mm
Peso y dimensiones	Peso	3150 g
	Energía sobre Ethernet (PoE), soporte	NO
	Consumo energético	30 W
Control de energía	Tipo de fuente de	AC

	alimentación	
	Requisitos de energía	100-240 V, 50-60 Hz, 1A
Resistencia	Tiempo medio entre fallos	70080 horas
Aprobaciones reguladoras	Seguridad	UL / CUL (UL 60950-1, CSA 22.2 NO60950-1); TUV/GS (EN60950-1); CB (IEC60950-1)
	Certificados	CE Mark
	Emisiones electromagnéticas	FCC *Class* A; *Industry Canada Class* A; EN55022 (CISPR 22) *Class* A; EN 61000-3-2/3; VCCI *Class* A; EN 61000-4-2/3/4/5/6/8/11
Condiciones ambientales	Humedad relativa	10 - 90 %
	Alcance de temperatura operativa	0 - 40 °C
	Temperatura	-40 - 70 °C
Detalles técnicos	Tecnología de conectividad	Con cables
	Características técnicas	(max.) 0.25A @ 115VAC
		(max.) 0.12A @ 230VAC
		out: 44-57 VDC
		(max.) PPP: 15.4 W
		(max.) CPP: 350 mA
Iluminación/Alarmas	Energía LED	SI
	Indicadores LED	SI

Para el switch 7200-48P de la marca D-Link podemos detallar las siguientes características:

Tabla 2.2. Características del Switch D-Link 7200-48P

Especificaciones técnicas	
Características	**Detalles**
Puerto	48 puertos RJ-45 10/100 de detección automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX), tipo de soporte: MDIX automático, dúplex: medio o completo; 2 puertos RJ-45 10/100/1000 de doble personalidad (IEEE 802.3 tipo 10BASE-T,

	IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T); 1 puerto de consola de serie RJ-45
Memoria y procesador	Procesador: ARM 88E6218 a 150 MHz, 8 MB de SDRAM, tamaño de búfer de paquetes: 384 MB, 4 MB de memoria Flash
Latencia	Latencia de 100 Mb: < 5 µs; Latencia de 1000 Mb: < 5 µs
Velocidad	10,1 millones de pps
Capacidad de encaminamiento/conmutación	13,6 Gbps
Funciones de gestión	Interfaz de línea de comandos limitada; Navegador Web; Administrador de SNMP; MIB Ethernet IEEE 802.3
Requisitos de energía y operación	
Características	**Detalles**
Voltaje de entrada	De 100 a 240 V CA
Frecuencia de entrada	50 / 60 Hz
Seguridad	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03
Compatibilidad electromagnética	FCC parte 15 Clase A; VCCI Clase A; EN 55022 Clase A; CISPR 22 Clase A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Clase A
Margen de temperaturas operativas	De 0 a 45°C
Intervalo de humedad en funcionamiento	del 10 al 90% (sin condensación)
Dimensiones y peso	
Características	**Detalles**
Dimensiones (Ancho x Fondo x Alto)	23,88 x 44,2 x 4,32 cm
Peso	2,9 kg
Protocolos Generales	IEEE 802.1w *Rapid Reconfiguration of Spanning*
	Tree
	IEEE 802.3ab 1000BASE-T
	IEEE 802.3ac (VLAN Tagging Extension)
	IEEE 802.3ad Link Aggregation Control Protocol
	(LACP)
	IEEE 802.3i 10BASE-T

	IEEE 802.3u 100BASE-X
	IEEE 802.3x Flow Control
	IEEE 802.3z 1000BASE-X

El switch V1905-48 de la marca HP/3COM, posee varias características importantes, las mismas que detallamos a continuación.

Tabla. 2.3. Características del Switch HP/3COM V1905-48

Características		**Detalles**
Iluminación/Alarmas	Conectividad LEDs	SI
	Energía LED	SI
Detalles técnicos	Tecnología de conectividad	Cableado
Condiciones ambientales	Temperatura	-40 - 70 °C
	Alcance de temperatura operativa	0 - 45 °C
	Humedad relativa	10 - 90 %
Control de energía	Requisitos de energía	100/240V
	Tipo de fuente de alimentación	AC
	Consumo energético	- W
	Energía sobre Ethernet (PoE), soporte	SI
Peso y dimensiones	Apilable	SI
	Peso	2900 g
	Dimensiones (Ancho x Profundidad x Altura)	442 x 238.8 x 43.2 mm
	Montaje en bastidor	1U
Seguridad	SSH/SSL *support*	SI
	MAC, filtro de direcciones	SI
	Acceso a lista de control (ACL)	SI
Anchura de banda	Velocidad	6600000 pps
Memoria	Memoria Flash	4 MB
	Memoria temporal	0.384 MB
	Memoria RAM	8 MB
Procesador	Procesador	150 MHz
	Built-in processor	ARM 88E6218
Conectividad	DC-*in jack*	SI

	Ethernet LAN (RJ-45) cantidad de puertos	48
	Gigabit Ethernet (cobre), cantidad de puertos	2
	Copper ethernet cabling technology	10/100/1000Base-T(X)
	Cantidad de puertos	48
Características de manejo	Administración de *Web-based*	SI
	Multidifusión, soporte	SI
	Calidad de servicio (QoS) soporte	SI
	Switch capa	L2
	MIB, soporte	SI
	Plataforma de gestión	CLI
	Tipo de interruptor	Administrado
Red	Auto MDI/MDI-X	SI
	Estándar de red	IEEE 802.3, 802.3u, 802.3ab
	IGMP *snooping*	SI
	Spanning tree protocol	SI
	IP *routing*	SI
	Alcance limitado	SI
	Puerto espejo	SI
	Adición de vínculos	SI
	Soporte de control flow	SI
	Características de red	Gigabit Ethernet
	Tamaño de la tabla de direcciones MAC	- entradas
Transmisión de datos	10G *support*	NO
	Tasa de transferencia (máx)	1 Gbit/s
	Tasa de transferencia de datos(min/max)	10/100/1000Mbps
	Capacidad de conmutación	13.6 Gbit/s

El router Cisco 2811 el mismo que se la utiliza por naturaleza de las comunicaciones corporativas en las oficinas. Hoy en día, las redes IP corporativas necesitan llevar a cabo muchas tareas, más aun las organizaciones necesitan no solo comunicaciones rápidas, sino

también comunicaciones seguras. Además, las infraestructuras IP pueden ahora llevar señales de voz y video, una excelente manera de mejorar la productividad y disminuir costos.

Este router ofrece soporte sin precedente para estas funciones. El paquete de seguridad Cisco 2811 con los servicios avanzados de IP Cisco IOS incluye 64 MB Flash/256 MB DRAM, AIM-VPN-EPII-PLUS *Enhanced-performance* DES, 3DES, AES y la compresión VPN y el cifrado (AIM).

El router Cisco 2811 de servicios integrados, proporciona las siguientes herramientas:

- La velocidad de cable de rendimiento para los servicios concurrentes, tales como seguridad y voz, y servicios avanzados para múltiples tipos de WAN T1/E1/xDSL.
- Protección de la inversión mejorada a través de un mayor rendimiento y modularidad.
- Aumento de la densidad a través de las ranuras de alta velocidad Tarjeta de interfaz WAN (cuatro).
- Red mejorada de ranura del módulo.
- Soporte para más de 90 módulos existentes y nuevos.
- Soporte para la mayoría de AIMS, los mecanismos nacionales, WIC, VWIC y VIC.
- Dos integrada 10/100 Fast Ethernet.
- Capa 2 opcional soporte de cambio con *Power over Ethernet* (PoE) (como opción).
- Memoria RAM: 256 MB (instalados) / 768 MB (máx.) - DDR SDRAM, 256 MB (instalados) / 760 MB (máx.) - DDR SDRAM.
- Seguridad:
    - A bordo de cifrado.
    - Soporte de hasta 1500 túneles VPN con el módulo AIM-EPII-PLUS.
    - Defensa antivirus apoyo a través de Network Admission Control (NAC).

- De prevención de intrusiones, así como de estado de Cisco IOS Firewall de apoyo y las características esenciales de muchos más seguridad.

- Voz

  - De voz analógicas y digitales apoyo llamada.
  - Soporte opcional de correo de voz.
  - Soporte opcional para Cisco *Call Manager Express* (CME de Cisco) para el procesamiento de llamadas locales de negocio independiente de hasta to36 teléfonos IP.
  - Soporte opcional para capacidad de supervivencia de apoyo *Remote Site Telephony* para el procesamiento de llamadas locales en pequeñas sucursales de empresas de hasta 36 teléfonos IP.

Los switches de Cisco Catalyst 2960-48TT-L soportan voz, datos, vídeo y acceso seguro, además ofrecen una gestión escalable conforme cambian las necesidades de la empresa o institución en cual se vaya a necesitar.

Una descripción breve de la serie 2960-48TT-L de switches es la siguiente:

- **Comunicaciones todas en uno:** Soporte de datos, voz y tecnología inalámbrica, por lo que cuando esté listo para implementar estos servicios disponga de una red que admita todas sus necesidades de negocio.

- **Inteligencia:** Dé prioridad al tráfico de voz o al intercambio de datos para alinear la entrega de información a sus requisitos de negocio.

- **Seguridad mejorada:** Proteja la información importante, mantenga a los usuarios no autorizados alejados de la red y consiga un funcionamiento ininterrumpido.

- **Fiabilidad:** Aprovéchese de las ventajas de los métodos basados en normas para conseguir una mayor fiabilidad y una rápida recuperación de errores. También puede agregar un suministro de energía redundante para obtener una fiabilidad adicional.

- **Fácil configuración:** Utiliza Cisco *Network Assistant* para simplificar la configuración, las actualizaciones y la solución de problemas.

Los switches de Cisco Catalyst Serie 2960-48TT-L ofrecen una amplia gama de características, que incluye:

- Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.
- Capacidad de *Power over Ethernet* para que puedan implementar nuevas funcionalidades como voz y tecnología inalámbrica sin tener que realizar un nuevo cableado.
- Opción de Fast Ethernet (transferencia de datos de 100 Mbps) o Gigabit Ethernet (transferencia de datos de 1000 Mbps), dependiendo del precio y las necesidades de rendimiento.
- Múltiples modelos de configuración, con la habilidad para conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
- Capacidad de configurar LANs virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
- Seguridad integrada.

- Funciones de monitorización de red y solución de problemas de conectividad mejoradas.
- Actualizaciones de software sin gastos adicionales.
- Garantía limitada de hardware de por vida.

Otro de los equipos con los que podemos realizar la configuración con el servidor AAA es el switch 3560G-48TS perteneciente a la familia Catalyst de Cisco es una completísima línea de switches de alto rendimiento, diseñados para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas.

Los switches Catalyst de Cisco ofrecen un amplio espectro para aplicaciones de usuarios, desde switches para pequeños grupos de trabajo hasta switches multicapa para aplicaciones empresariales escalables en el centro de datos o en el *backbone*. Los switches Catalyst ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos Ethernet, Fast Ethernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio.

Algunos de los detalles de la familia de switches 3560 Catalyst de Cisco, son los siguientes:

Tabla. 2.4. Características del Switch Catalyst 3560G-48TS

Características		**Detalle**
Iluminación/Alarmas	Energía LED	SI
	Conectividad LEDs	SI
Emisión de sonidos	Emisiones de presión acústica	48 Db

Aprobaciones reguladoras	Emisiones electromagnéticas	FCC Part 15 Class A, EN 55022: 1998 (CISPR22), EN 55024: 1998 (CISPR24), VCCI Class A, AS/NZS 3548 Class A, CE, CNS 13438 Class A, MIC
	Seguridad	UL to UL 60950, C-UL to CAN/CSA C22.2, TUV/GS to EN 60950:2000, CB to IEC 60950, NOM-019-SCFI, CE
Detalles técnicos	Tecnología de conectividad	*Wired*
Condiciones ambientales	Alcance de temperatura operativa	0 - 45 °C
	Temperatura	-25 - 70 °C
	Humedad relativa	10 - 85 %
	Altitud operacional	3049 m
Resistencia	Tiempo medio entre fallos	173400 MB/s
Control de energía	Consumo energético	160 W
	Requisitos de energía	100-240 VAC, 3.0-1.5A, 50-60Hz
	Energía sobre Ethernet (PoE), soporte	NO
Peso y dimensiones	*Apilabre*	NO
	Peso	6400 g
	Dimensiones (Ancho x Profundidad x Altura)	445 x 409 x 44 mm
	Montaje en bastidor	1U
Memoria	Memoria Flash	32 MB
	Memoria interna	128 MB
Conectividad	DC-*in jack*	SI
	Cantidad de puertos SFP	4
	Gigabit Ethernet (cobre), cantidad de puertos	48
	Copper ethernet cabling technology	10Base-T, 100Base-TX, 1000Base-T
	Cantidad de puertos	52
Protocolos	Protocolo de conmutación	EIGRP, IPv6, DTP, PAgP, DHCP,HSRP, TCP, UDP

	Protocolo de trasmisión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
	Protocolos de gestión	IGMP, RMON, SNMP, Telnet
Características de manejo	Administración de *Web-based*	SI
	Multidifusión, soporte	SI
	Calidad de servicio (QoS) soporte	SI
	Plataforma de gestión	Cisco IOS CLI, Cisco *Network Assistant*, SAA
	Tipo de interruptor	*Managed*
Red	Auto MDI/MDI-X	SI
	IGMP snooping	SI
	Spanning tree protocol	SI
	IP *routing*	SI
	DHCP, servidor	SI
	Control de Tormentas de *Broadcast*	SI
	Guardar y remitir	SI
	Jumbo *Frames*, soporte	SI
	Adición de vínculos	SI
	Características de red	Ethernet, Fast Ethernet, Gigabit Ethernet
	Soporte de control *flow*	SI
	Estándar de red	IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q VLAN, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab,IEEE 802.3z
Tamaño de la tabla de direcciones MAC		12000 entradas
Transmisión de datos	Velocidad de transferencia (paquete)	38.7 Mpps
	Capacidad de conmutación	32 Gbit/s
	Full dúplex	SI
	Tasa de transferencia de datos(min/max)	10/100/1000 Mbps
	Tasa de transferencia (máx)	1 Gbit/s

De acuerdo al análisis de cada uno de los equipos y marcas detalladas anteriormente, se puede establecer las características principales para las cuales detallamos a continuación, las mismas que servirán para nuestros requerimientos del proyecto:

Tabla. 2.5. Diferencias Principales entre las marcas de Switch

Características	D-Link (7200-48P)	HP/3Com (V1905-48)	SMC (6152l2)	Cisco (Catalyst 3560G-48TS)
Puertos	48 puertos 10/100/1000MDIX automático	48 x 10/100/1000Base-T(X)	48 x 10/100/1000 BASE-T	48 x 10/100/1000 + 4 x Gigabit SFP
Capacidad de encaminamiento/conmutación	13,6 Gbps	13.6 Gbit/s	17.6 Gbit/s	32 Gbit/s
Estándar de red	IEEE 802.1w Rapid Reconfiguration of Spanning, IEEE 802.3ab 1000BASE-T, IEEE 802.3x Flow Control, IEEE 802.3z 1000BASE-X	IEEE 802.3, 802.3u, 802.3ab	IEEE802.3; IEEE802.3 u/D/p/Q/ac/ ad/w/v/x; IEC8802.3	IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q VLAN, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab,IEEE 802.3z
Velocidad de transferencia (paquete)	10,1 Mpps	6.6 Mpps	13 Mpps	38.7 Mpps
Tasa de transferencia (máx)	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s
Tasa de transferencia de datos(min/max)	10/100/1000Mbps	10/100/1000 Mbps	10/100/1000 Mbit/s	10/100/1000 Mbps

Seguridad	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03	SSH/SSL *support,* MAC, filtro de direcciones, Acceso a lista de control (ACL)	Algoritmo de seguridad, MAC, filtro de direcciones , Acceso a lista de control (ACL)	SSH/SSL *support*, MAC, filtro de direcciones, Acceso a lista de control (ACL)
Memoria Flash	4 MB	4 MB	4 MB	32 MB
Memoria RAM	8 MB	8 MB	8 MB	128 MB
Protocolo de conmutación	EIGRP, IPv6, DTP, PAgP, DHCP,HSRP, TCP, UDP	IP *routing* (BGP, *Border Gateway Protocol*; IS-IS, *Intermediate System* - Sistema Intermedio; OSPF, Open Shortest Path First; RIP, Protocolo de Información de Enrutamiento)	EIGRP, IPv6, DTP, PAgP, DHCP,HSRP, TCP, UDP	EIGRP, IPv6, DTP, PAgP, DHCP,HSRP, TCP, UDP
Protocolo de trasmisión de datos	Gigabit Ethernet	Gigabit Ethernet	Ethernet, Gigabit Ethernet	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolos de gestión	Telnet, SLIP, SNMP	Telnet, SLIP, SNMP	Telnet, SLIP, SNMP	IGMP, RMON, SNMP, Telnet

En la tabla 2.5, podemos observar las diferencias principales entre marcas del equipamiento, por lo que el equipo de la marca Cisco Catalyst, es uno de los más completos que existe en el mercado. Esta es una de las razones por las cuales es recomendable trabajar con esta unidad.

Además, la ventaja principal para el equipamiento compatible con el Servidor AAA, se constituye en routers y switches, de marca Cisco, ya que de acuerdo a experiencias realizadas con este servidor, lo más apropiado es que la conexión realizada entre estos equipos de seguridad sea del mismo fabricante.

2.3 Levantamiento de información relacionada al acceso a los servicios tecnológicos e información institucional

En una red es muy común el robo o manejo indebido de la información y es conocida la facilidad de uso y capacidad de almacenamiento de las memorias USB. La cantidad de virus que se transmite a través de estos dispositivos son un dolor de cabeza para cualquier administrador de red.

GiliSoft USB Lock es una herramienta de prevención de fugas de datos que evita las fugas y la copia de sus datos en unidades USB, discos externos, CDs / DVDs u otros dispositivos portátiles.

Una vez instalado, USB *Lock*[18] le permite bloquear todas las unidades o dispositivos que no pertenecen a usted. Con USB *Lock*, usted puede compartir su PC con cualquier persona sin temor a los datos sean robados. Este es un sencillo y potente DLP (Procesamiento Digital de Luz) que le ayuda a bloquear el puerto USB, hacer DVD / CD *Burner* sólo lectura, bloquear algunos sitios web, prohibir algunos programas y desactivar varios dispositivos.

[18] http://www.gilisoft.com/product-usb-lock.htm

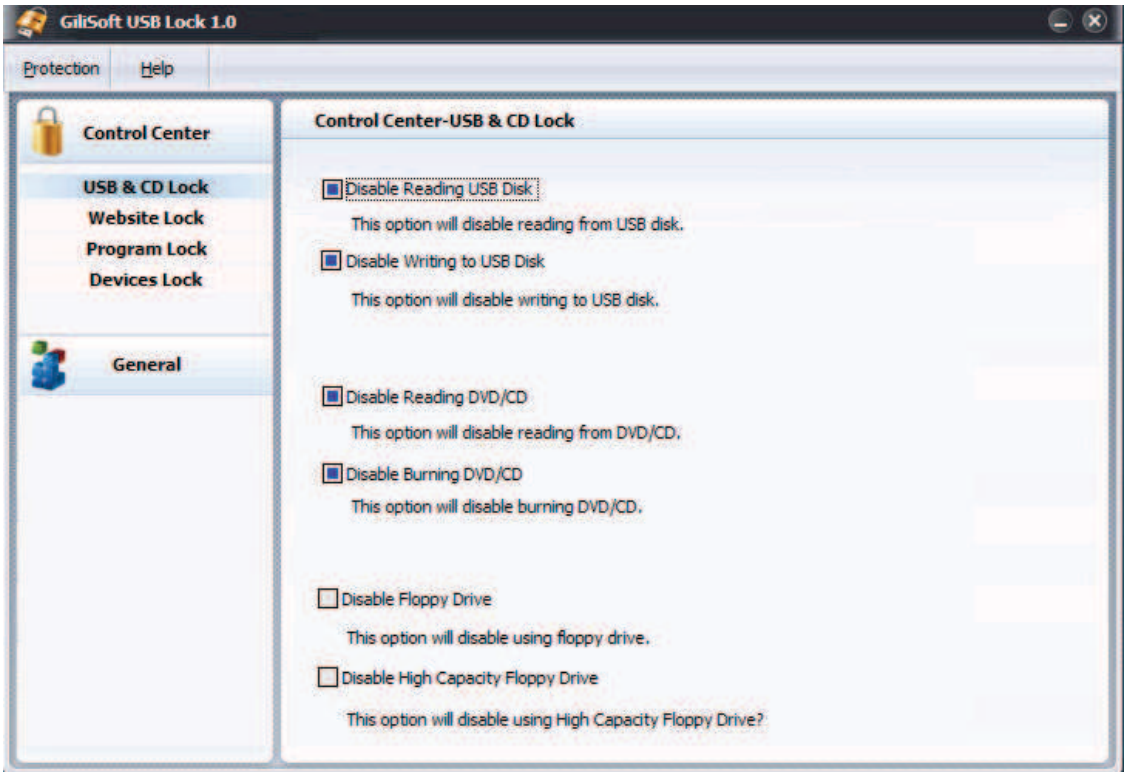

Figura. 2.2. Software Gilisoft USB Lock 1.0 (http://www.gilisoft.com/product-usb-lock.htm)

Las características y beneficios de este software son las siguientes:

• **Bloquear USB Drives:**

Desactivar la lectura de los discos USB o deshabilitar la escritura USB disks.USB bloqueo no permite ningún tipo de dispositivo USB para acceder a su equipo a menos que usted lo autorice. Por defecto, todos los tipos de unidades USB se bloquea incluyendo discos duros externos, *FireWire*, Mejorada mini-USB, *Host Controller Interface* (HCI), HP-IL, COM, LPT, IrDA, USB sobre la marcha, U3, EHCI, RAID controlador, el adaptador de host, cable serie (con el uso de transferencia de datos), Serial ATA ACCESS.bus, y cualquier dispositivo de almacenamiento que está conectado al puerto USB que muestra una unidad en el sistema.

• **CD de bloqueo, el Media Block y discos *Blu-ray*:**

Desactivar la lectura de DVD / CD discos o hacer DVD / CD *Burner* solo lectura. La aplicación también bloquea cualquier tipo de disco que utiliza el centro del disco, la bahía, o combo de CD / DVD y asigna una letra de unidad, por ejemplo, CD-R, CD-RW, CD-RAM, DVD-R, DVD-RW, DVD-RAM, HD-R,-RW de alta definición, HD-RAM, *Blu-Ray-R, Blu-Ray* RW, *Blu-Ray* de RAM, disquetera A, *Floppy* B de discos y unidades Zip.

• **Sitio Web de bloqueo:**

Bloquear el acceso a algunos sitios web. Esta utilidad te permite bloquear sitios web no deseados desde la pantalla de Internet Explorer. Si un sitio web está bloqueado el usuario es enviado a una página en blanco o una "página bloqueada" y el contenido de la página original no se cargan en tu PC. Detener la carga de banners y anuncios, deje a sus hijos de pasar horas en las salas de chat o sitios web no deseados quitar de su vista. Evitar que sus hijos tengan acceso a ciertos sitios web de contenido tales como los sitios para adultos y juegos de azar.

• **Programas de bloqueo:**

Bloquear ejecutando ningún programa, incluyendo Internet Explorer, Outlook, AOL, AIM, y mucho más. Usted puede incluso bloquear el panel de control con un clic del botón. Otras características incluyen la capacidad de elegir su propio mensaje para mostrar que si alguien intenta ejecutar uno de sus programas bloqueados, y también incluye la protección con contraseña para que sólo usted pueda abrir el programa cuando esté listo para usarlo. Permite que todo el equipo para mantenerse activo y en funcionamiento, y que quede solo e impide el acceso a los programas que usted especifique. Interfaz fácil de usar que muestra el estado

actual de todos los programas bloqueados, y te permite hacer clic con facilidad y liberar a su gusto.

• **Dispositivos de bloqueo:**

El programa se puede utilizar para restringir el acceso de lectura o escritura a dispositivos de medios extraíbles como CD, DVD, disquetes, flash y USB drives. Esto también se puede utilizar para desactivar la impresora, Moderna, con puertos LPT, infrarrojos, *bluetooth*, puertos 1394.

• **Notificación de alarmas:**

Si el usuario ingresa una contraseña incorrecta más de 5 veces, enviará notificaciones de alarma a su dirección de e-mail.

• **Protección contra la copia:**

El programa utiliza un nivel avanzado de la tecnología de prevención de fugas de datos que no permite la duplicación de los archivos importantes y el material de derechos de autor de cualquier unidad USB u otros dispositivos de almacenamiento, sin su permiso.

El programa funciona mediante el bloqueo de todos los tipos de dispositivos de almacenamiento no autorizados, como memorias USB, discos duros externos, CDs, DVDs, etc, de esta manera se evita el plagio, la piratería, la distribución y la copia ilegal de sus datos.

• **Fuga de Información:**

USB *Lock* es una fuga de datos de software de prevención. Impide que los datos de conseguir filtrado a unidades USB y otros dispositivos de almacenamiento como por lo que le permite controlar qué dispositivo puede acceder a su ordenador, mientras que el bloqueo de todos los otros dispositivos no autorizados que no pertenecen a usted. Con USB Lock instalado en su computadora, usted puede sentirse seguro de que sus datos se mantendrán en su PC seguro.

• **Compatibilidad del Sistema:**

Ventanas 2000/2003/XP/Vista/Windows 7 (32 y 64)

El software *NetWrix USB blocker* es una buena solución para realizar el trabajo de proteger los puertos USB desde un punto centralizado. Al ser compatible con el Directorio Activo se necesita obviamente tener una red con dominio bien configurada y políticas establecidas.

Una vez descargado podremos configurarlo y activarlo rápidamente, pudiendo incluso definir una lista de ordenadores en los que no se aplicarán esas políticas. De este modo, evitaremos que se puedan conectar dispositivos USB de almacenamiento, haciendo más difícil el robo de información o la entrada de malware.

El uso de USB *Blocker* es gratuito, aunque también ofrecen una versión comercial con algunas mejoras, como definir que dispositivos concretos están permitidos y prohibidos o la posibilidad de ofrecer códigos de acceso temporales para cuando haya necesidad de conectar algo a un ordenador.

Además, a diferencias de otros programas similares, el USB *Blocker* permite que no sea necesario instalar nada en los ordenadores clientes de una red, gracias al uso de Políticas de Grupo de Windows.

Una de las características más interesantes de esta herramienta es su simplicidad, tan sólo hay que realizar un par de *clicks* para tenerla en funcionamiento.

La descarga e instalación del software es muy sencilla, además de los pasos y su configuración para las diferentes funcionalidades que tiene este software.

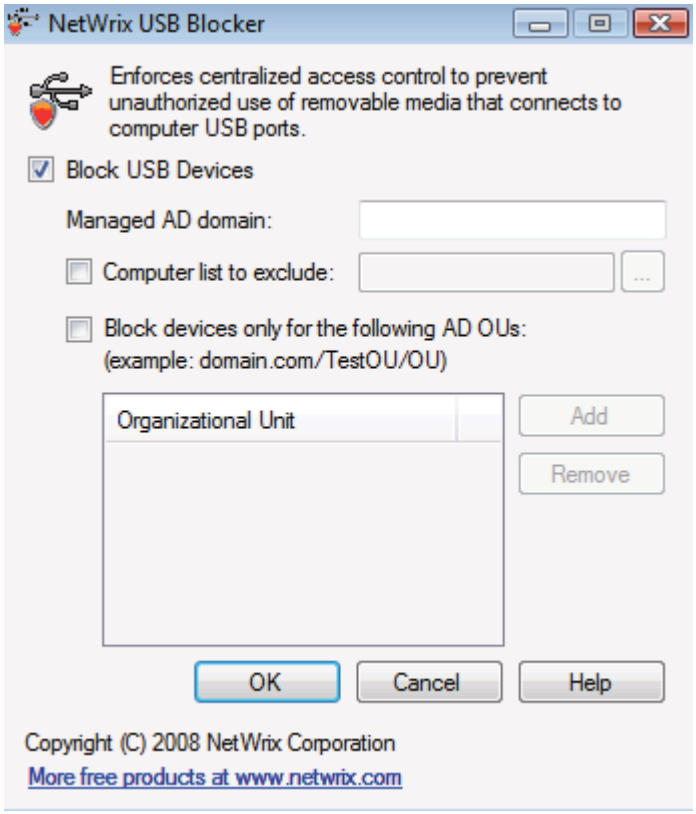

Figura. 2.3. Programa NetWrix USB Blocker. (http://www.gilisoft.com/product-usb-lock.htm)

Para el uso práctico de este software, detallamos a continuación los pasos que se debe seguir de acuerdo a la configuración que sea necesaria.

1) Instale el programa en cualquier ordenador en el dominio administrado (no necesariamente un controlador de dominio).
2) Activa o desactiva los dispositivos USB, seleccionando la opción deseada.
3) Indique el nombre del dominio (por ejemplo, ACME, o ACME.com).
4) Opcionalmente, puede seleccionar la opción por el bloqueo de unidad organizativa y especificar una lista de bloques de anuncios de la organización. Las unidades organizativas deben estar en el formato de nombre *canonincal*: FQDN / padre / hijo, por ejemplo, "example.com / *Acme* / Contabilidad". Puede copiar nombres OU del complemento ADUC (ver ficha Objeto de la hoja de propiedades OU).
5) Haga clic en Aceptar. Esto crea una configuración de Directiva de grupo que se aplica a todos los equipos en el dominio administrado durante el siguiente reinicio.

Todos los servicios tecnológicos de la entidad financiera, se deben solicitar bajo previa autorización de su respectivo jefe inmediato, detallando su funcionalidad y el tiempo en el cual va a permanecer habilitado el acceso al puerto USB, grabador de CD e internet.

2.4 Análisis de requerimientos de conexión física a la red institucional

En base al análisis de requerimientos, nos enfocaremos con los funcionarios de la institución y personas que no pertenecen a la misma, por tal motivo, debemos ver las necesidades que estos tengan para permitir el ingreso a la red de la entidad.

Por esto se determinó que los funcionarios, por ser servidores de la institución tienen su enfoque en el trabajo propiamente de los mismos, ya que al ser adaptados en función a los

roles, perfiles y aplicativos, no deberían tener más permisos adicionales en los que les permita realizar actividades que perjudiquen a la institución como en el desempeño de su trabajo.

Por este motivo se determinó que el acceso a la red por parte de los funcionarios de la institución, debe ser solamente para el desempeño óptimo de trabajo y no para tener permisos a ciertos roles o aplicativos que no pertenezcan a su perfil y que puedan interrumpir su capacidad laboral.

En el uso de computadores personales ya sea de funcionarios o de servidores externos que se deseen conectarse a la red, esto se va a poder realizar sin ningún problema, ya que no existe un control en el acceso a la misma, en lo que sería perjudicial para la entidad en caso de substracción de información trascendental.

En caso de que los funcionarios lleven su propio computador personal a la institución, y se conecte a la red de la misma, el servidor AAA les va a configurar sus accesos a los roles, perfiles y aplicativos que estos tengan en base a sus funciones, es decir, el nivel de seguridad que se establece con este servidor serán el más óptimo y apropiado para el ingreso a la red.

Para el personal pasante o terceras personas que se encuentran dentro de la institución, este control debería ser más exhaustivo, dado que como son personas que no pertenecen directamente a la misma, la seguridad de la información y los permisos a los accesos de la red poseen un enfoque más relevante.

Para este tipo de servidores, se deben considerar los accesos y permisos a la red que estos puedan tener, es decir, si en caso que utilicen un computador de la institución, este computador debe tener los accesos restringidos a la red, o a su vez, se deben configurarlos para que no posean accesos que involucren el mal uso del ordenador y puedan tener demasiados permisos.

Pueden existir casos en los cuales el personal externo de la institución lleve su computador personal y se conecte a la red de la misma, esta le pedirá clave y contraseña, para poder tener acceso, es decir, el servidor AAA determinará si es funcionario de la entidad en el caso que lo sea o tenga permisos relevantes que le permitan ingresar a la red. Con esto se realizará una validación del personal que se encuentra laborando dentro de la organización y a su vez los accesos que estos tengan.

Podríamos definir a una red informática como un sistema formado por dos o más ordenadores interconectados entre sí, a través de tarjetas con transmisión por cable o de forma inalámbrica para compartir ficheros, recursos, aplicaciones, conexión a internet, etc.

Uno de los requerimientos para la conexión física son las estaciones de trabajo ya que son dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información. Estos permiten que los usuarios intercambien rápidamente información y en algunos casos, compartan una carga de trabajo.

En cualquier red informática, siempre encontraremos que dicha red consta de dos partes fundamentales esenciales e indispensables.

1. La parte física o hardware, y
2. La parte lógica o software.

El hardware o parte física de la red local es la parte tangible y se encuentra constituida por:

- Las tarjetas de red
- El medio de transmisión (cable trenzado, coaxial o microondas electromagnéticas)

- Los periféricos compartidos.

El software de la red es la parte inmaterial pero tan indispensable como la física y está constituida por:

1. El sistema operativo de red
2. Controladores de red
3. Programas de aplicación

Generalmente nos enfocamos en los ordenadores más costosos ya que posee la última tecnología, pero para el diseño de una red de área local solamente necesitamos unas estaciones que cumpla con los requerimientos exigidos, tengamos cuidado de no equivocarnos ya que si damos fallo a un ordenador que no cumpla los requerimientos perderemos tiempo y dinero.

A continuación, detallaremos los hardwares y software de red.

El switch o (HUB) es el dispositivo encargado de gestionar la distribución de la información del servidor (HOST), a las estaciones de trabajo y/o viceversa. Las computadoras de red envían la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor. Tengamos cuidado cuando elegimos un tipo de concentrador (HUB), esto lo decimos ya que se clasifican en 3 categorías. Solo se usaran concentradores dependiendo de las estaciones de trabajo que así lo requieran.

Existen también switches para grupos de trabajo que se conectan en varios equipos, dependiendo su entorno inmediato.

Switches intermedios, que se encuentra típicamente en el closet de comunicaciones de cada planta. Y los switch corporativos representa el punto de conexión central para los sistemas finales conectados los concentradores intermedios (Concentradores de Tercera Generación).

El modem es un equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora.

Los periféricos compartidos de una red pueden ser de dos tipos:

- Los periféricos directos son los que se conectan a la red directamente a través de su propia tarjeta de red.
- Los periféricos indirectos son los que se conectan a la red a través de un equipo servidor.

La tarjeta de red Ethernet es aquella que se encarga de interconecta las estaciones de trabajo con el concentrador y a su vez con el Servidor (HOST), es decir, permite la conexión del hardware al medio de transmisión y puede ser PCI, USB o integrada; generalmente a las tarjetas de red se las conoce con las siglas NIC (*Network Interface Card*).

El cableado es el medio empleado para trasmitir la información en la red, es decir el medio de interconexión entre y las estaciones de trabajo. Los principales medios de transmisión son los cables trenzados con terminal RJ-45, cable coaxial de tipo RG-58, fibra óptica y conexión inalámbrica o conexión aérea por ondas.

El Sistema Operativo de red administra y gestiona las comunicaciones y recursos, así como los datos, programas y aplicaciones.

Los Controladores de red, así como cualquier dispositivo de un computador necesita tener instalado sus correspondientes controladores o drivers, el hardware de red también tiene sus propios controladores.

Los programas de aplicación en red pueden ser de todo tipo, desde programas de aplicación general hasta programas de comunicación tales como correo electrónico, navegador de páginas web, etc. Hasta programas de terminal tal como telnet, etc.

Cuando se establezca la conexión de un computador a la red de la institución financiera, inmediatamente va a solicitar usuario y contraseña, esto se lo realizará mediante el servidor IBNS, y el AAA, ya que existe una configuración adecuada enviada desde el servidor a la dirección IP detectada en ese momento.

Una vez ingresados correctamente el usuario y contraseña, el funcionario podrá ingresar a la red de la institución y desarrollar sus respectivas operaciones sin ningún problema.

2.5 Roles y perfiles de accesos a la información institucional

El Rol es el nombre que se le confiere al conjunto de perfiles[19] que le son asignados al usuario para el ejercicio de sus funciones, mientras que un perfil es la descripción detallada de las posibles transacciones que puede realizar un usuario en el sistema.

[19] http://agile.inntegra.eu/metodologia/dimension-proyecto/a8-personas-roles-y-perfiles

Los roles y perfiles dependen de cada entidad financiera, ya que existen roles que permiten el acceso a ciertos parámetros que sirven para el desempeño laboral de los funcionarios.

Determinados roles permiten el ingreso a cierta información trascendental de la institución, por tal motivo el acceso al mismo debe ser restringido y poseer alta seguridad, ya que si se tiene este tipo de roles, pueden tener acceso a información confidencial de la entidad financiera.

Cada uno de los roles van de acuerdo a las funcionalidades de los servidores, es decir, a los cargos profesionales de los mismo. Estos se los establece con un análisis de cargos y van de acuerdo a la institución financiera como la desarrolle según sus requerimientos.

Los cargos anteriormente detallados en el primer capítulo, poseen roles, los mismos se pueden basar en accesos a cierta información de la institución que necesite para el desarrollo de su campo laboral.

Los diferentes roles implicados en la institución financiera podrán ser:

a) Dinamizador de Equipo:

Persona responsable de asegurar el cumplimiento de las pautas de trabajo establecidas en el modelo de gestión de proyectos. Se trata de un miembro de equipo más cuya responsabilidad y poder de decisión abarca la sistemática de funcionamiento.

b) Enlace Cliente:

Miembro del equipo que posee relación y contacto directo con el cliente. Preferiblemente será una persona de perfil técnico que participará en la ejecución del proyecto.

c) Responsable de Producto:

Persona interna y/o cliente, que representa la voz del cliente así como sus necesidades. La participación del cliente es fundamental sobre todo en determinadas labores o actividades clave del proyecto como:

- Identificación y priorización de entregables.
- Planificación y seguimiento de entregas.

2.6 Elaboración de requerimientos de seguridad para la conexión física de computadores de escritorio y/o portátiles a la red institucional

Para los requerimientos de seguridad en la conexión física de los computadores[20], ya sean estos de escritorio o portátiles, se establecer políticas y normas que se deben de implantar y seguir.

Las políticas[21] proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas y la manera que deberían actuar los empleados de una organización en circunstancias normales y la forma que deberían reaccionar si se presentan circunstancias inusuales, esto a su vez define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

[20] http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml#mejores
[21] AREITO, Javier, *Seguridad de la Información, Redes, Informática y Sistemas de Información*, 1ª ed., PARANINFO, Magallanes, 25;28015 Madrid - España, 2008, 561

Toda política debe de tener un propósito y procedimiento bien específico que articule claramente de la razón por la cual fueron creados tales políticas o procedimientos y qué beneficios se espera la organización derivada de las mismas.

Cada política y procedimiento debe tener una sección que defina su aplicabilidad, por este motivo se deberá desarrollar una política de seguridad que se aplique a todos los sistemas de cómputo y redes, además una política de información debe aplicarse a todos los empleados.

La sección de responsabilidad de una política o procedimiento, define quién se hará responsable por la implementación apropiada del documento. Quien quiera que sea designado como el responsable de aplicar una política o procedimiento de ser capacitado de manera adecuada y estar consciente de los requerimientos del documento. Las políticas de información definen qué información es confidencial y cual es de dominio público dentro de la organización, y cómo debe estar protegida esta misma. Esta política está construida para cubrir toda la información de la organización.

Las políticas de seguridad definen los requerimientos técnicos para la seguridad en un sistema de cómputo y de redes. Define la manera en que un administrador de redes o sistema debe de configurar un sistema respecto a la seguridad que requiere la empresa o el momento. Esta configuración también afecta a los usuarios y alguno de los requerimiento establecidos en la política y debe de comunicarse a la comunidad de usuarios en general de una forma pronta, oportuna y explícita.

Las políticas de uso de las computadoras extienden la ley en lo que respecta a quién puede utilizar los sistemas de cómputo y cómo pueden ser utilizados. Gran parte de la información en esta política parece de simple sentido común, pero si las organizaciones no las establecen específicamente, toda la organización queda expuesta a demandas legales por parte de los empleados.

Las políticas de uso de Internet y correo electrónico se incluyen con frecuencia en la política más general del uso de las computadoras. Sin embargo, en ocasiones se plantea en una política aparte, debido a la naturaleza específica del uso de Internet. Las organizaciones conceden conectividad a Internet a sus empleados para que éstos puedan realizar sus labores con mayor eficacia y de este modo beneficia a las organizaciones. Desgraciadamente, Internet proporciona un mecanismo para que los empleados hagan uso de los recursos de cómputo.

Las políticas de respaldo y normalización de actividades después de un desastre tienen que ser muy bien especificadas para que en un lapso muy corto de tiempo, la empresa u organización regrese a sus actividades y las pérdidas económicas sean mínimas o nulas.

Para la seguridad lógica, la empresa debe de desarrollar un procedimiento para identificar la vulnerabilidad en sus sistemas de cómputo; normalmente las exploraciones son realizadas por el departamento de seguridad y los ajustes son realizados por los administradores del sistema canalizándolos a los programadores y/o proveedores del sistema.

Existen algunas herramientas para realizar estas pruebas, también se puede recurrir a pruebas de desempeño y análisis de código, pero también se puede recurrir a la experiencia de uso de los usuarios.

Las medidas técnicas de seguridad se ocupan de la implementación de los controles de seguridad sobre los sistemas de cómputo y de red. Estos controles son manifestaciones de las políticas y los procedimientos de la organización.

En las empresas como en las casas ya se cuenta con conexiones permanentes a las redes o a Internet y estas deben de estar protegidas mediante muros de fuego que actúan de manera que su homónimo arquitectónico entre dos habitaciones de un edificio. Puede ser físico (equipo) ó lógico (software).

Las conexiones de acceso remoto pueden ser intervenidas para obtener acceso no autorizado hacia las organizaciones y, por consiguiente, deben de estar protegidas. Este tipo de conexiones pueden ser por marcación telefónica o atreves de Internet.

Puesto que estas conexiones entran a la red de la empresa o a la computadora tiene que tener un sistema de autentificación como los módems de retroalimentación (que contienen en si mecanismos de autentificación); las contraseñas dinámicas son apropiadas para utilizarse como un mecanismo de autentificación mientras las contraseña dinámica sea combinada con algo conocido por el usuario; también existen programas y dispositivos de encriptación para asegurar que la información no es altera desde su creación hasta su lectura por el receptor.

El monitoreo en redes debe de llevarse a cabo para detectar diversos tipos de actividades inesperadas de virus, códigos maliciosos o uso inapropiado de esta, existen programas como los *sniffers* para ver el tráfico o todo aquello que pasa por la red, también existen equipos como los IDS´s (*Intrusion Detection System*) que cuentan con mecanismos para hacer análisis de paquetes y errores en las redes.

La seguridad física debe ser empleada junto con la seguridad administrativa y técnica para brindar una protección completa. Ninguna cantidad de seguridad técnica puede proteger la información confidencial si no se controla el acceso físico a los servidores, equipos y computadoras. Igualmente, las condiciones climáticas y de suministro de energía pueden afectar la disponibilidad de los sistemas de información.

El acceso físico es importante[21], ya que todos los equipos delicados deben de estar protegidos del acceso no autorizado; normalmente esto se consigue concentrando los sistemas en un centro de datos.

Para el acceso al sistema de la institución financiera, se la puede controlar de diferentes maneras, como limitando el acceso con dispositivos, o instalar cerraduras de combinación para restringir los accesos a empleados y personas ajenas a las instalaciones.

Es importante tener una temperatura ambiente estable[22], ya que los sistemas de cómputo son sensibles a las altas temperaturas. Los equipos de cómputo también generan cantidades significativas de calor. Las unidades de control de clima para los centros de cómputo o de datos deben de ser capaces de mantener una temperatura y humedad constante.

Para evitar pérdidas y daños físicos a equipos y computadoras[23] hay que contar con una instalación eléctrica adecuada, no hay que saturar la toma de corriente y se recomienda utilizar fuentes reguladas como reguladores para la protección de equipos. Si existen instalaciones específicas para los equipos y computadoras se recomienda utilizar fuentes redundantes y una planta de energía auxiliar.

[22] http://platea.pntic.mec.es/~lmarti2/cableado.htm
[23] http://www.monografias.com/trabajos28/manual-redes/manual-redes.shtml#determin

CAPÍTULO 3

RECOMENDACIONES DE SEGURIDAD

3.1 Definición de los requerimientos mínimos de seguridad que los computadores de escritorio y/o portátiles deben cumplir previo a la conexión física a la red institucional

Para un nivel de seguridad óptimo en la conexión a la red de la institución, se debe establecer bajo previos puntos a nivel de computador, con esto se elaborará un mejor control en el sistema, libre de software malicioso o aplicaciones que a la larga puedan afectar el desempeño de nuestro servidor AAA y al resto de ordenadores.

Uno de los primero puntos a cubrir para la seguridad en un equipo, nodo o computadora son las claves de acceso, las mismas que en su constitución no sean muy comunes, como es el caso de las iniciales del nombre propio y la fecha de nacimiento, apodos o sobrenombres que todo mundo conoce, o constituirlas de solo letras o solo números; estos tipos de claves son en las que los intrusos, Hackers y ladrones buscan de primera mano; hay que hacer combinaciones de letras mayúsculas, minúsculas y números alternadamente.

Para la determinación de las contraseñas, se lo realiza mediante la integración de Directorio Activo, en el mismo que se integran los usuarios y contraseñas de los funcionarios de la institución financiera.

En base al funcionamiento del servidor AAA y como una normativa de seguridad, no se debe compartir claves con ninguna persona, ya que en el caso de otorgar el usuario y contraseña de un funcionario de la institución, este puede ingresar al sistema de la entidad desde cualquier computador de la entidad y tener acceso a los roles y perfiles del otro funcionario.

Previo a la conexión física de un computador a la red de la institución es necesario el uso de un antivirus actualizado, ya sea este propio del equipo o a su vez de un servidor antivirus de la institución, en base a una cuenta de administrador para que este pueda configurarlo y adaptarlo al propio servidor.

Si los equipos, computadoras o servidores tienen niveles de permisos de uso de archivos y de recursos, se debe configurarlos en el mismo servidor AAA, ya que este va a ser quien autentique los accesos a los requerimientos que tiene cada funcionario para la realización propia de su trabajo dentro de la entidad.

Las actualizaciones periódicas de los computadores de la institución, se las realizará en base a la conexión que estos tengan a internet y los requerimientos de los funcionarios para su uso, es decir, si los usuarios tienen acceso a internet de acuerdo a su cargo u obligación para el desempeño de su trabajo, podrán ser actualizados sin ningún inconveniente. De acuerdo a los cargo de los funcionarios, el servidor AAA, va a ser el que otorgue los accesos a estos servicios.

En el caso que existiera reubicación de un puesto de trabajo de un funcionario, ya sea esto como un cambio administrativo o departamental, no será necesario el cambio de equipo otorgado a ese funcionario, ya que el servidor AAA, establece que el usuario pueda conectarse a la red de la institución desde cualquier otro computador con los roles y perfiles propios del usuario. Esto se lo realiza solamente con el usuario y contraseña de este funcionario.

3.2 Definición de las recomendaciones de seguridad a implementar en herramienta para control de accesos físicos a la red y o dispositivos relacionados

En la seguridad a implementar en la herramienta para el control de accesos físicos a la red de la institución, debemos relacionarnos con la conexión de los computadores, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar, ya que es ajustable al sitio de trabajo en donde los usuarios vayan a desarrollar sus funciones.

Para esto iniciaremos con el diseño y estructura del Directorio Activo en la institución financiera, ya que el Directorio Activo es un proceso que hace un equipo especializado, divido en grupos que cubren tres fases más importantes que son el diseño, planificación e implementación.

Las características del Directorio Activo que se desarrollará de acuerdo a nuestros requerimientos, será la elaboración de una base de datos dentro del sistema en la cual se encuentran los usuarios y contraseñas de cada funcionario de la entidad financiera, para que los mismos datos sean utilizados en el servidor AAA.

Para el dominio con el que se vaya a desarrollar en el Directorio Activo, lo realizaremos con un único nombre de domino, el cual nos va a servir para el diseño en el servidor AAA.

Además, el tener un único nombre de dominio permitirá centralizar más fácilmente la administración, y la configuración.

El nombre del dominio debe ser pensado no sólo en base a la situación actual, además conviene tener en cuenta la evolución que se puede esperar de la empresa.

Con el dominio, sólo es necesario crear las identidades de usuario una vez. Es posible hacer referencia a estas identidades desde cualquier equipo unido al bosque donde reside el dominio. Los controladores de dominio que forman un dominio se utilizan para almacenar cuentas y credenciales de usuario (como contraseñas y certificados) de una manera segura.

Los controladores de dominio proporcionan servicios de autenticación para usuarios y ofrecen datos adicionales de autorización, por ejemplo, relacionados con las pertenencias a grupos de usuarios.

Antes de implementar Directorio Activo, lo realizaremos desde el Windows Server 2003, para esto se debe planear y diseñar la estructura lógica del Directorio Activo de acuerdo al entorno. La estructura lógica de Directorio Activo determina la organización de los objetos de directorio y proporciona un método eficaz para la administración de cuentas de red y recursos compartidos.

El diseño de la estructura lógica del Directorio Activo conlleva la definición de una parte considerable de la infraestructura de red de la organización.

Para el diseño de la topología de red en la institución financiera, debemos iniciar desde la topología estudiada anteriormente, ya que para nuestro análisis es la una de las más recomendables en este tipo de entidades.

Con esto podemos establecer una topología básica para nuestro diseño, ya que en el caso de incrementarse un mayor número de equipos, sean estos router, switch o computadores, no se debe tener problema con la configuración y escalabilidad de los mismos.

Con el fin de garantizar el rendimiento eficaz de Directorio Activo, deberá determinar el número adecuado de controladores de dominio para cada sitio y comprobar que cumplen los requisitos de hardware de Windows Server 2003. La planeación meticulosa de capacidades con referencia a los controladores de dominio evitará que se subestimen los requisitos de hardware, lo que podría influir de forma negativa en el rendimiento de los controladores de dominio y el tiempo de respuesta de las aplicaciones.

Las características específicas en el Directorio Activo que servirá en la conexión con el servidor AAA son las siguientes:

Administración simplificada de usuarios y recursos de red

Puede utilizar para crear estructuras de información jerárquicas, que simplifican el control de las credenciales administrativas y otras opciones de seguridad, y permiten a los usuarios localizar recursos de red, como archivos e impresoras, con mayor facilidad.

Consolidación de directorios

Es posible organizar y simplificar la administración de usuarios, equipos, aplicaciones y dispositivos, y facilitar a los usuarios la búsqueda de la información que necesitan. Podrá aprovechar la compatibilidad con la sincronización mediante las interfaces basadas en el Protocolo ligero de acceso a directorios y trabajar con los diversos requisitos de consolidación de directorios específicos de las aplicaciones.

Infraestructura y aplicaciones habilitadas para el uso de directorios

Las características del Directorio Activo, facilitan la configuración y administración de las aplicaciones y otros componentes de red habilitados para el uso de directorios.

Escalabilidad sin complejidad

El Directorio Activo puede escalarse hasta llegar a tener millones de objetos por cada dominio y utiliza tecnología de indización y técnicas de replicación avanzadas para aumentar el rendimiento.

Uso de los estándares de Internet

El Directorio Activo proporciona acceso mediante LDAP y utiliza un espacio de nombres basado en el sistema de nombres de dominio (DNS).

Un entorno de desarrollo eficaz

Ofrece un entorno de desarrollo eficaz mediante las interfaces de servicio de Directorio Activo (ADSI), que le proporciona una interfaz orientada a objetos. ADSI facilita a los programadores y administradores la creación de programas de directorio mediante herramientas de alto nivel como Microsoft Visual Basic, Java, C o Visual C++, sin necesidad de preocuparse de las diferencias subyacentes entre los diversos espacios de nombres.

En el caso de la existencia de equipos atendidos por terceros, el Departamento de Soporte deberán normar al respecto, es decir, los usuarios encargados de la configuración de los equipos (*Help Desk*) van a ingresar a los mismos por medio de un usuario administrador, el

cual les permite que tengan mayores privilegios y que a su vez quede registrado como un agente de *Help Desk* quien realizó la configuración de dicho equipo. Además la configuración o cambios que se van a realizar en los computadores de la institución, deben quedar registrados en el Directorio Activo por medio de un dominio específico, este dominio se basa de acuerdo a la entidad financiera.

Con la configuración de los equipos que se realizará por parte del Departamento de Soporte hacia el servidor AAA, nos ayudará para que un usuario al momento de ingresar a la red, el servidor AAA pueda detectarlo como un computador registrado en la red de la institución y el usuario tengan accesos de acuerdo al perfil del funcionario que ingrese a la red.

Los funcionarios responsables de las áreas de cómputo de un Departamento pueden otorgar detalles preventivos y correctivos, esto en el caso de que un computador se encuentre con inconvenientes en el momento del ingreso a la red de la institución.

El Departamento de Tecnología será responsable de proporcionar a los funcionarios el acceso a los recursos informáticos, es decir, proporcionar la distribución de los equipos necesarios que sean utilizados dentro de la institución para que los usuarios puedan desarrollar su trabajo con normalidad, a pesar de que los mismos no se encuentren en su puesto de trabajo, ya que con el servidor AAA los funcionarios pueden ingresar al sistema desde cualquier computador que se conecte a la red de la entidad financiera..

Por medio del servidor AAA, el acceso lógico al equipo especializado de cómputo como servidores, enrutadores, bases de datos, etc., conectado a la red, va a ser administrado por el Departamento de Tecnología. Por tanto, todos los ordenadores que se encuentren conectados a la red de la institución o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, deben de sujetarse a la configuración previa para la conexión a la red de la institución.

Finalmente, el servidor AAA, podrá autenticar el ingreso de un computador a la red de la institución, por medio de su usuario y contraseña que se encuentre registrado a un dominio en el Directorio Activo, autorizar sus accesos a los perfiles que el usuario tenga asignado, es decir, lo que puede realizar este usuario mientras está conectado a la red y registrar su desempeño laboral y los accesos en los cuales ha ingresado cuando se encontraba conectado a la infraestructura de red.

3.3 Definición del mecanismo para la implementación de procedimientos técnicos necesarios para el control de conexiones físicas a la red institucional

Para los mecanismos de implementación se debe proceder con la obtención de una base técnica de los equipos y el número de estos para la conexión a la red de la institución, es decir, que todos los equipos de computo o estaciones de trabajo se encuentren registrados como propias de la entidad financiera y que deban sujetarse a controles previos a la conexión de estos ordenadores con la infraestructura de red y por ende al servidor AAA.

Además se deberá sustentar la información de los equipos a utilizarse con un registro que especifique los detalles de los equipos de trabajo, los cuales van a estar conectados a la red de la institución financiera, por tanto un reconocimiento que las unidades de desempeño laboral son de propiedad de la institución financiera.

Esta información detallada de todo el equipamiento perteneciente a la institución, nos servirá para el momento de la conexión de los mismos con el servidor AAA, y tener un cronograma de actividades para la configuración de cada equipo, de acuerdo a las necesidades que la entidad financiera lo requiera.

Además de los equipos nuevos que lleguen a la institución, estos deberán ser ya configurados por el Departamento de Soporte o *Help Desk* para que en el momento de su funcionamiento, no tengan problemas en la conexión con el servidor AAA.

Los equipos de la institución deben ser de propósito específico y tenga una misión crítica asignada, además convendrá estar ubicado en un área que cumpla con los requerimientos de seguridad física, las condiciones ambientales, la alimentación eléctrica.

En el caso de algún cambio por parte de los funcionarios a otra área de trabajo, no va a ser necesario el traslado también del equipo, ya que con el servidor AAA podrá desempeñar sus labores sin ningún problema, ya que el funcionario podrá ingresar a la red de la institución con su usuario y contraseña sin perder sus roles y perfiles que el usuario tiene asignado.

Relacionado con el control de acceso a la red, todos los ordenadores ya sean estos computadoras personales, estaciones de trabajo y demás relacionados, que sean propiedad de la institución financiera, deberán ser configurados el ingreso a la red, ya que sin previa configuración no podrán acceder a la misma, ya que el servidor AAA no identificará a ese nuevo equipo como parte de la infraestructura tecnológica de la entidad.

Dado que el servidor AAA, permitirá establecer un control minucioso al acceso a la red de la institución, el sitio más apropiado para la ubicación de dicho servidor, debe ser con el resto de equipos switch, routers, servidores, etc., con los que cuenten con una seguridad inviolable y que a su vez garantice el buen funcionamiento del servidor con el resto de los equipos.

En la conexión del servidor AAA con el resto de equipos como switch, routers o servidores, deben ser controlados periódicamente para su buen funcionamiento y verificación de conexiones físicas que se realice por parte de los funcionarios de la entidad financiera.

Con estas conexiones a la red y sus controles establecidos con el equipamiento y los accesos por parte de los usuarios, podemos determinar un registro en el cual nos indique el desempeño laboral de cada uno de los funcionarios que ha ingresado a la red y el tiempo que ellos se encontraron dentro de la misma.

CAPÍTULO 4

DISEÑO DE LA SOLUCIÓN

4.1 Diseño y planteamiento de las recomendaciones de seguridad en la topología de conexión física de computadores de escritorio y/o portátiles a la red institucional

Con el servidor AAA optaremos una solución para el ingreso a la red de la institución con previa autorización y los accesos que un usuario tiene en base al perfil que este tenga.

El servidor AAA, basado en la autenticación, se basa en la pregunta ¿quién es?, es decir, si el funcionario que pretende ingresar a la red de la institución es un usuario validado por el servidor AAA o es un usuario desconocido; con la autorización se refiere a lo que puede hacer el usuario una vez ingresado a la red, esto se lo transmite mediante el perfil con el cual el funcionario se desempeña laboralmente y los roles que este tiene para la ejecución de su trabajo; y el registro es lo que el usuario está haciendo mientras se encuentra conectado, es decir, existe un control a nivel del servidor AAA para que este lleve un reporte de lo que el funcionario a realizado en el tiempo en que este se encuentra conectado a la red.

En base a su perfil, además de un control constante en el desempeño del usuario al momento de encontrarse dentro de la red de la institución, podemos tener un registro de los accesos en los cuales le está permitido tener solamente para el desempeño de su trabajo dentro

de la institución y que a su vez no sea mal utilizado para fines que no sean los apropiados y que perjudiquen a la institución.

En el enfoque a los requerimientos, vamos a utilizar los siguientes comandos que nos sirven para la configuración de acuerdo a los equipos switch, o por medio de las VLAN, MAC.

Para los planteamientos en base a la seguridad, se detallan los siguientes procedimientos para los switches con los que se establecería la conexión en un computador, con los diferentes comandos básicos para su configuración de acuerdo a lo requerido.

En base al uso de los siguientes comandos, detallaremos la configuración que se optará en los equipos para su correcto enlace con el servidor AAA y el funcionamiento óptimo de los mismos.

En la institución financiera podemos establecer las VLAN de acuerdo a nuestro diseño, para esto se debe conocer que el rango normal de VLANs son de 1 a 1005 y si el switch con el que vamos a desarrollar nuestro esquema se lo realizará en modo trasparente VTP, es decir, en este modo se puede adicionar, modificar o remover configuraciones con las VLANs en la base de datos de las mismas.

El uso del protocolo VTP, se lo puede establecer como una configuración consistente en la cual se puede adicionar, modificar o borrar las VLANs sobre una red. Además VTP minimiza las configuraciones inconsistentes que pueden causar severos problemas como nombres duplicados de VLANs, especificaciones incorrectas y violaciones de seguridad.

Las configuraciones en modo de VTP se van a realizar de la siguiente manera:

Primero se debe poner el conmutador en modo VTP, este es un protocolo propietario de Cisco.

Switch (config)# vtp mode transparent
(Protocolo propietario de Cisco)

A continuación creamos las VLANs con sus nombres, como ejemplo tomares vlan10 y vlan20, y revisaremos si ya se encuentran creadas con los siguientes comandos.

switch (config)# vlan 10	(Crea una VLAN con un nombre (vlan 10))
switch (config)# vlan 20	(Crea una VLAN con un nombre (vlan 20))
switch (config)# show vlan	(Permite revisar las vlans creadas en un switch)
switch (config)# show vlan 10	(Permite revisar una vlan en particular con su número)

Para configurar un puerto del conmutador en una de las VLANs se debe establecer el modo de configuración de la interfaz.

switch (config)# interface FastEthernet 0/1

switch (config-if)# switchport access vlan 10
(Este comando se ejecuta en modo de configuración de la interfaz correspondiente)

De acuerdo a los pasos anteriores, se realizan los mismos para la vlan20.

switch (config)# interface FastEthernet 0/1

switch (config-if)# switchport access vlan 20

Para revisar la asignación de puerto de las VLANs, ponemos la siguiente configuración:

switch (config)# show vlan-membership
(Permite revisar la asignación de puertos de VLANs)

Una vez creadas las VLANs, la configuración con las direcciones MAC de los computadores en los switch, se realiza los siguientes puntos:

switch(config-if)# mac-address-table static interface FastEthernet vlan10

Para la limitación de la cantidad de host por puerto o asegurar puertos en la configuración del switch se puede establecer:

swicth(config)#interface FastEthernet 0/1
switch(config-if)#switchport port-security maximum 1

El siguiente tipo de configuración establece la con conexión con un switch global y 802.1x:

switch# configure terminal (Modo de configuración global)

switch(config)# aaa-new model (Habilitar AAA)

switch(config)# aaa authentication auten

(Creación de un método de autenticación 802.1x. Para la creación de un listado *auten* se utiliza cuando el nombre de la lista no se encuentre especificado en el comando de autenticación)

switch(config)# auten system-auth-control

(Habilitación de la autenticación global 802.1x sobre el switch)

switch(config)# aaa autorization autori group radius

((Recomendable) Configuración del switch para usar la autorización RADIUS para todas las redes o solicitud de servicios relacionados tal como la asignación de ACL o VLAN)

switch(config)# radius-server host 192.168.10.10

(Para el uso de ACL y el modo de un host)

switch(config)# radius-server key CISCO

((Recomendable) Se especifica la llave de autenticación y encriptación usado entre el switch y el RADIUS server)

switch(config)# interface FastEthernet 0/1

(Especifica el puerto conectado al cliente para habilitar la autenticación con 802.1x, e ingresar al modo de configuración de la interface)

switch(config-if)# switchport mode access auten 100

((Recomendable) Configuración al puerto para el modo acceso solo si es configuración del servidor RADIUS)

switch(config-if)# authentication port-control auto or auten port control auto

(Habilitación de la autenticación 802.1x sobre el puerto)

switch(config-if)# end (Regreso al modo de privilegio)

switch# show authentication or show auten 100

(Verificación de las entradas)

switch# copy running-config startup-config

(Guarda las entradas en la carpeta de configuración)

Para el procedimiento de la configuración en base a la habilitación de los switch con *Guest* VLAN se procede de la siguiente manera:

switch# configure terminal (Modo de configuración global)

switch(config)# interface FastEthernet 0/1

(Especifica el puerto a ser configurado e ingresa a la interfaz en modo de configuración)

switch(config-if)# switchport mode access or switchport mode private-vlan host

(Conjunto de puertos en modo de acceso)

switch(config-if)# authentication port-control auto or auten port-control auto

(Habilitación de autenticación 802.1x sobre el puerto)

switch(config-if)# auten guest-vlan vlan10

(Especifica una VLAN activa como una VLAN 802.1x invitada, el rango es de 1 a 4094)

switch(config-if)# end (Regreso al modo de privilegio)

switch(config)# show authentication FastEthernet 0/1 or show auten FastEthernet 0/1

(Verifica las entradas)

switch(config)# copy running-config startup-config

((Recomendable) Guarda las entradas en la carpeta de configuración)

En el procedimiento siguiente, se detallan los comandos que se configuran en el switch para las VLAN que se encuentran registradas.

switch# configure terminal (Modo de configuración global)

switch(config)# interface FastEthernet 0/1

(Especifico el puerto a ser configurado e ingreso a la interfaz en modo de configuración)

switch(config-if)# switchport mode access or switchport mode private-vlan host

(Conjunto de puertos en modo de acceso)

switch(config-vlan)# authentication port-control auto or auten port-control auto

(Habilitación de autenticación 802.1x sobre el puerto)

switch(config-vlan)# auten auth-fail vlan 10

(Especifica una VLAN activa como una VLAN 802.1x restringida, el rango es de 1 a 4094)

switch(config-vlan)# end (Regreso al modo de privilegio)

switch# show authentication FastEthernet 0/1 or show auten FastEthernet 0/1

(Verifica las entradas)

switch# copy running-config startup-config

((Recomendable) Guarde sus entradas en la carpeta de configuración)

Para la configuración en el switch habilitando la dirección MAC de los computadores, se lo realizará con los siguientes comandos de configuración y el procedimiento posteriormente descrito:

switch# configure terminal (Modo de configuración global)

switch(config)# interface FastEthernet 0/1
(Especifica el puerto a ser configurado e ingresa a la interfaz en modo de configuración)

switch(config-if)# authetication port-control auto or auten port-control auto
(Habilitación de autenticación 802.1x sobre el puerto)

switch(config-if)# auten mac-auth-bypass [esp | timeout activity 10]
(Habilitación de autenticación bypass MAC)

switch# end (Regreso al modo de privilegio)

switch# show authentication FastEthernet 0/1 or show auten FastEthernet 0/1
(Verifica las entradas)

switch# copy running-config startup-config
((Recomendable) Guarde sus entradas en la carpeta de configuración)

Para los comandos de configuración de 802.1x en los switch de configuración, debemos tomar en cuenta que se deberá necesitar la configuración de RADIUS; para esto se deberá llevar a cabo el siguiente procedimiento con la habilitación del servidor AAA como un nuevo modelo:

switch(config)# aaa new-model (Habilitación AAA)

switch(config)# aaa authentication auten default group radius

(Crea una base de puertos del método de autenticación 802.1x)

switch(config)# aaa authorization network default group radius

(Requerido para asignar VLAN/ACL)

switch(config)# aaa accounting auten default start-stop group radius

(Habilitación del 802.1x acconuting y MAB)

Se procede con la habilitación del RADIUS con los siguientes comandos de configuración:

switch(config)# radius-server host acs5.server.11.0.1.1 auth-port 1645 acct-port 1646

(Especifica la dirección IP del servidor RADIUS)

switch(config)# radius-server key user-defined-shared-key

(Especifica la llave pre-compartida)

Los tipos de mensajes RADIUS que se nos despliegan para la conexión a la red, son los siguientes:

Access-Request.- enviado por un cliente Radius para solicitar la autenticación y autorización en un intento de conexión.

Access-Accept.- enviado por un servidor Radius como respuesta a un mensaje *Access-Request*, en este se indica si es autenticado y autorizado el cliente.

Access-Reject.- enviado por el servidor Radius como respuesta a un mensaje *Acces-Request*, en el se informa de que se ha rechazado el intento de conexión. Se envía este mensaje si el servidor comprueba que las credenciales no son legítimas o si no se autorizado el intento de conexión.

Access-Challenge.- enviado por un servidor Radius como respuesta a un mensaje *Acces-Request*, siendo este mensaje un desafío al cliente Radius que exige respuesta.

Accounting-Request.- enviado por un cliente Radius para especificar información de administración de cuentas de una conexión que ha sido aceptada.

Accounting-Response.- enviado por el servidor Radius como respuesta a un mensaje de *Accounting-Request*, confirmándose la recepción y procesamiento correctos del mensaje del mismo.

Para la habilitación de la interfaz se lo realiza mediante los siguientes comandos de configuración de la esta manera:

switch(config)# auten system-auth-control

(Habilitación global del puerto basado en la autenticación 802.1x)

Procedimiento de identificación de la composición para ser añadido a los puertos de acceso:

switch(config)# interface range g2/1-16

(Rango para el puerto de configuración)

switch(config-if)# authentication open

(Habilitación de la pre-autenticación de acceso abierto no restringido)

switch(config-if)# authentication port-control auto

(Habilitación del puerto basado en la autenticación sobre la interfaz)

switch(config-if)# auten pae authenticator

(Habilitación 802.1x de la autenticación sobre la interfaz 802.1x)

switch(config-if)# mab (Habilitación de la autenticación bypass de la MAC)

switch(config-if)# authentication host-mode multi-auth

(Permite un solo teléfono IP o más datos de clientes independientemente autenticados sobre un puerto autorizado. Cada host o dirección MAC es autenticado individualmente)

switch(config-if)# end (Regreso al modo de privilegio)

Podemos tomar un modelo en el cual detallamos la habilitación de los switch con el servidor RADIUS y TACACS.

switch(config)# aaa new-model (Habilitación AAA)

switch(config)# aaa authentication login default group tacacs+ local

(Autenticación default de grupo de tacacs+ local)

switch(config)# aaa authentication auten default group radius

(Autenticación del grupo de Radius)

switch(config)# aaa authorization network default group radius

(Autorización a la red del grupo de Radius)

switch(config)# aaa accounting auten default start-stop group radius

(Registro de inicio y parada del grupo de Radius)

switch(config)# tacacs-server host10.1.0.10 timeout 10

(Servidor tacacs en host de ejemplo)

switch(config)# tacacs-server directed-request

(Servidor tacacs con solicitud dirigida)

switch(config)# tacacs-server key CISCO

(Servidor tacacs con la llave CISCO)

switch(config)# radius-server host10.1.0.10 auth-port 1645 acct-port 1646

(Especificación de la IP con el servidor Radius)

switch(config)# radius-server retransmit 5

(Retransmisión del servidor)

switch(config)# radius-server key CISCO

(Contraseña CISCO)

switch(config)# radius-server vsa send accounting

(Servidor Radius envía un registro)

switch(config)# radius-server vsa send authentication

(Servidor Radius envía la autenticación)

Tacacs+ establecido como un protocolo cliente servidor, normalmente es un proceso demonio que corre en UNIX o servidor Microsoft, la característica principal de Tacasc+ es la separación que hace de la autenticación, autorización y administración de cuentas.

La autenticación *Tacacs+* permite que el contenido del intercambio de autenticación sea de longitud variable por lo que puede utilizar cualquier mecanismo de autenticación como PPP, CHAP, EAP, etc., esta autenticación no es obligatoria.

En el proceso de autenticación existen los siguientes tipos de mensajes:

- *Start,* el cliente inicia la autenticación con el servidor.
- *Continue,* que es siempre enviado por el cliente.
- *Reply,* siempre enviado por el servidor.

El inicio de la autenticación se procede mediante el envió del mensaje *Start* por parte del cliente. El mensaje describe el tipo de autenticación a ser usado por ejemplo CHAP, PAP, etc., y puede contener el nombre de usuario y algún dato de autenticación.

El mensaje *Start* siempre tiene un número de secuencia igual a 1 y solo se envía en el primer mensaje de una sesión de autenticación o como paquete inmediatamente después de un reinicio.

El mensaje *Start,* se describe como el servidor enviando un mensaje *Reply,* este mensaje indica si la autenticación continúa o ha finalizado. Si el mensaje indica que continua, el mensaje también indica que el servidor necesita nueva información, el cliente obtiene la nueva información y responde con un mensaje *Continue.* Este proceso continua hasta que toda la información para la autenticación sea obtenida hasta concluir este proceso.

Cuando la autenticación ha finalizado, el cliente inicia el proceso de autorización el mismo que se realiza con el intercambio de un par de mensajes. *Request* seguido por un Response.

El *Request* de autorización contiene un número fijo de campos que describen y procesan la autenticidad del usuario, y un número no constante de argumentos que describen los servicios para la autorización que se pide.

La administración de cuentas graba lo que el usuario ha hecho, y sirve a dos propósitos; puede utilizarse para el pago de los servicios que utilizó es decir para facturación o como una herramienta de seguridad, para determinar el uso correcto o incorrecto de las normas impuestas por la política de seguridad.

Para realizar la contabilidad *Tacacs+* utiliza 3 clases de registros:

- El registro *Start* que indica que un servicio está a punto de iniciar.
- El registro *Stop* que indica la finalización de un servicio.
- Los registros *Update* que indican que el servicio se está realizando.

Los registros de contabilidad contienen información específica como tiempo de inicio y tiempo de parada y la información de uso del respectivo servicio.

Las transacciones cliente servidor se autentican a través de una contraseña secreta compartida que nunca se envía sobre la red, además de encriptar todo el tráfico entre los dos.

El proceso AAA de *tacacs+* es el siguiente:

a. El usuario inicia una autenticación sobre PPP al Cliente Tacas+.
b. El cliente *Tacacs+* le pide al usuario nombre y contraseña.
c. El usuario replica con su contraseña.
d. El cliente *Tacacs+* envía un paquete encriptado con la información de usuario al

servidor *Tacacs+*.

e. El servidor *Tacacs+* responde con la autenticación o negación.

f. El servidor *Tacacs+* y el cliente intercambian mensaje de autenticación, Si la autorización fue positiva el cliente *Tacacs+* deja entrar al usuario.

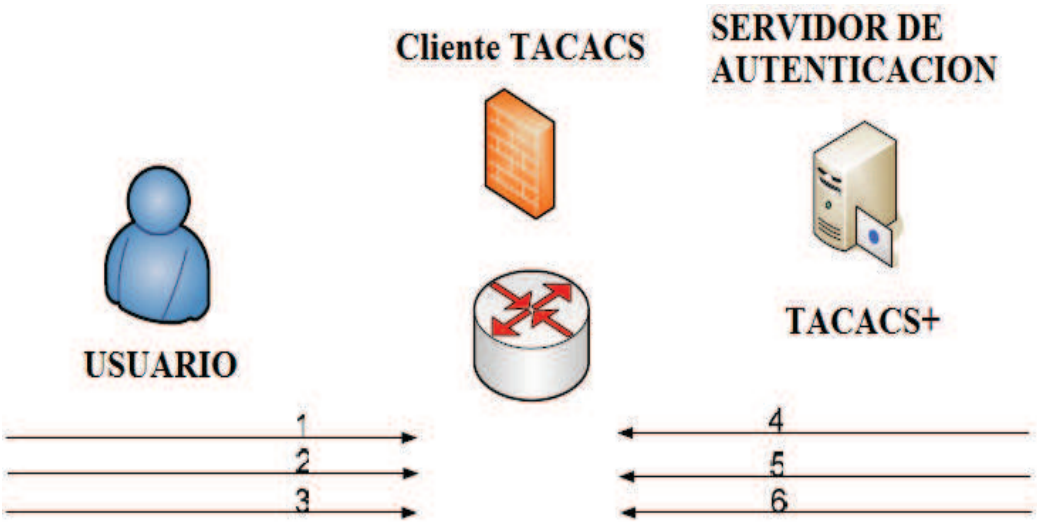

Figura. 4.1. Protocolo TACACS+ (http://www.cisco.com/go/ibns)

A continuación se detalla el procedimiento y la utilización de los comandos de configuración de 802.1x en el switch, habilitación de 802.1x en la interfaz:

switch(config)# interface FastEthernet0/1	(Habilitación intefaz FastEthernet 0/1)
switch(config-if)# switchport access vlan 100	(Puerto de acceso al switch por vlan 100)
switch(config-if)# switchport mode access	(Modo de acceso al puerto del switch)
switch(config-if)# auten port-control auto	(Sistema de control de autorización global)

switch(config)# spanning-tree portfast	(Habilitar el puerto rápido en un puerto de acceso conectado a una estación de trabajo o servidor)

4.2 Diseño de procedimientos técnicos para la implementación de la conexión física de computadores de escritorio y/o portátiles a la red institucional en base a roles y perfiles

Para la conexión a la red institucional y el enlace a la base de datos correspondientes a los roles, perfiles y aplicativos de cada usuario, se basan en el ACS el mismo que se enlaza con el servidor AAA para que el funcionamiento sea el apropiado.

Entre las principales características de seguridad en las que se basa el servidor AAA, son el bloqueo al acceso a la red de personas que no pertenecen a la institución y que no se encuentran previamente registradas, los cargos de los funcionarios con sus respectivos roles y perfiles a los que conlleva el no tener accesos más que los suficientes en el sistema de la institución, además de la conexión con la red de la institución en un acceso remoto.

Mediante los comandos de configuración para cada uno de los equipo switch con VLANs y direcciones MAC, se procede con la configuración del servidor AAA con el Directorio Activo, ya que la conexión entre estas dos herramientas, establecerá que el usuario y contraseña de los funcionarios sean los mismos, ya que la base de datos original se encuentra en el Directorio Activo y por medio de este se realizará la conexión con el servidor AAA.

En la fase de implementación y configuración del ACS procedemos de la siguiente manera:

Paso 1: encender el ACS, acceder a la consola de administración de línea de comandos a través de la interfaz serial del equipo. El acceso al puerto se lo realiza mediante un emulador del terminal (*Hyper Terminal*) configurando los siguientes parámetros:

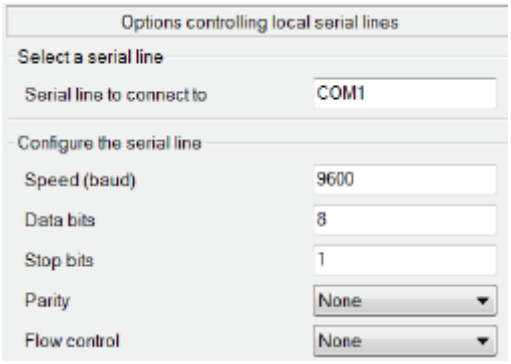

Figura. 4.2. Hyper Terminal (http://www.cisco.com/go/ibns)

Paso 2: Una vez que se ha ingresado a la consola de administración (CLI) aparecerá el siguiente mensaje:

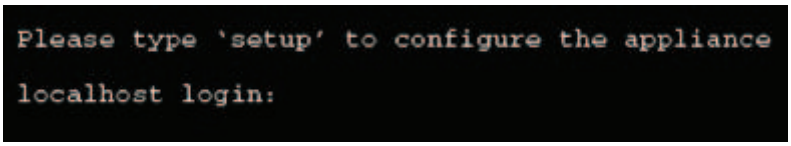

Figura. 4.3. Mensaje CLI (http://www.cisco.com/go/ibns)

En el campo "*localhost loging*" ingresamos "*setup*".

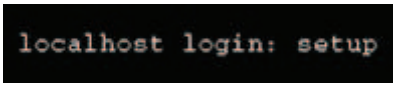

Figura. 4.4. Mensaje localhost login (http://www.cisco.com/go/ibns)

Paso 3: Ingresar cada uno de los datos requeridos en el proceso de instalación:

Figura. 4.5. Proceso de instalación ACS (http://www.cisco.com/go/ibns)

A continuación se observa el proceso de aplicación de la configuración inicial y el reinicio del equipo.

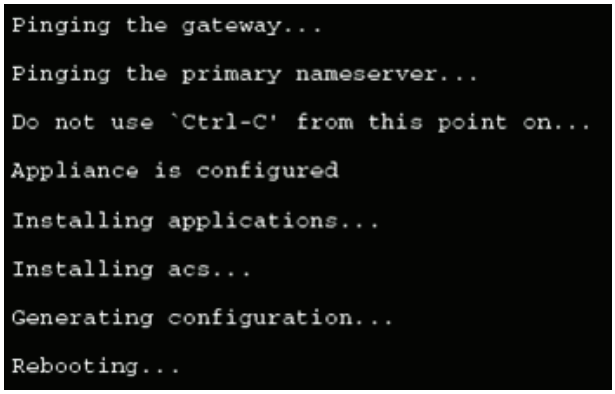

Figura. 4.6. Configuración interna (http://www.cisco.com/go/ibns)

Paso 4: Tras la aplicación de la configuración inicial y el reinicio del equipo, aparecerá el *prompt* de autenticación para el ingreso a la Consola de Administración CLI; se ingresan las credenciales previamente configuradas.

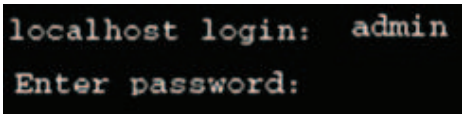

Figura. 4.7. Ingreso a las credenciales configuradas (http://www.cisco.com/go/ibns)

Paso 5: Una vez que se ha ingresado a la CLI, se puede ejecutar comandos de visualización y configuración del ACS.

Para los comandos de verificación del estado del ACS procedemos de la siguiente manera:

show application status acs **(**Permite visualizar el status de los servicios del ACS)

Figura. 4.8. Ingreso a las credenciales configuradas (http://www.cisco.com/go/ibns)

show application: Permite visualizar la instalación correcta del equipo.

```
<name>          <Description>
acs             Cisco Secure Access Control System 5.1
```

Figura. 4.9. Instalación correcta del equipo (http://www.cisco.com/go/ibns)

show application version acs (Permite visualizar el release y la versión instalada del ACS)

```
Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.1.0.44
Internal Build ID : B.2347
```

Figura. 4.10. Instalación correcta del equipo (http://www.cisco.com/go/ibns)

Adicionalmente a través de la CLI se puede cambiar los parámetros de configuración del ACS como la dirección IP y DNS.

Paso 6: Ingresar a la interfaz gráfica de administración mediante un web browser con la url:

https://<acs_host>/acsadmin, donde <acs_host> es la dirección IP del equipo.

Debido a que se ingresa a un sitio web seguro se debe aceptar las condiciones de seguridad.

Con la url https://<acs_host>/acsadmin, ingresamos por defecto las credenciales en la interfaz gráfica del ACS: Username: ACS Admin y Password: default.

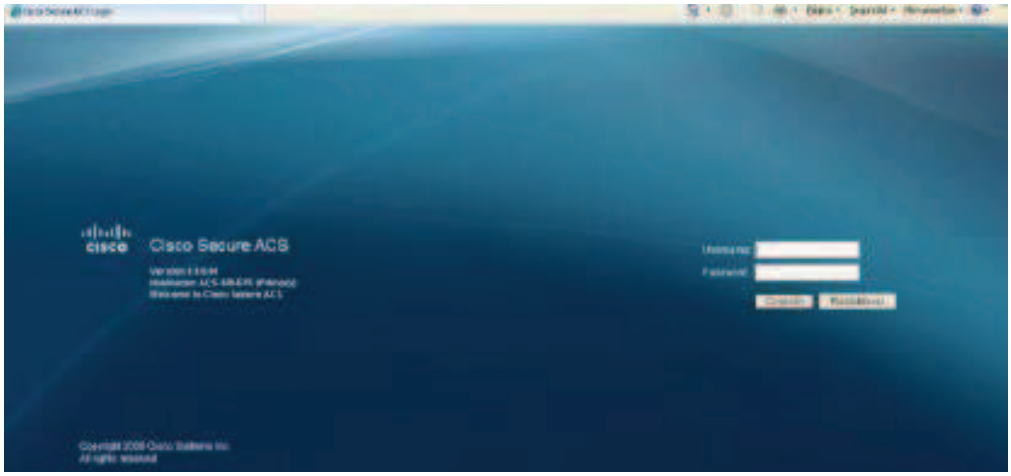

Figura. 4.11. Interfaz gráfica (http://www.cisco.com/go/ibns)

Paso 7: A continuación se solicitará el cambio de la contraseña (se recomienda no utilizar contraseñas por defecto).

Tras realizar el cambio de la contraseñas e ingresará a la página principal de la interfaz gráfica de administración y configuración.

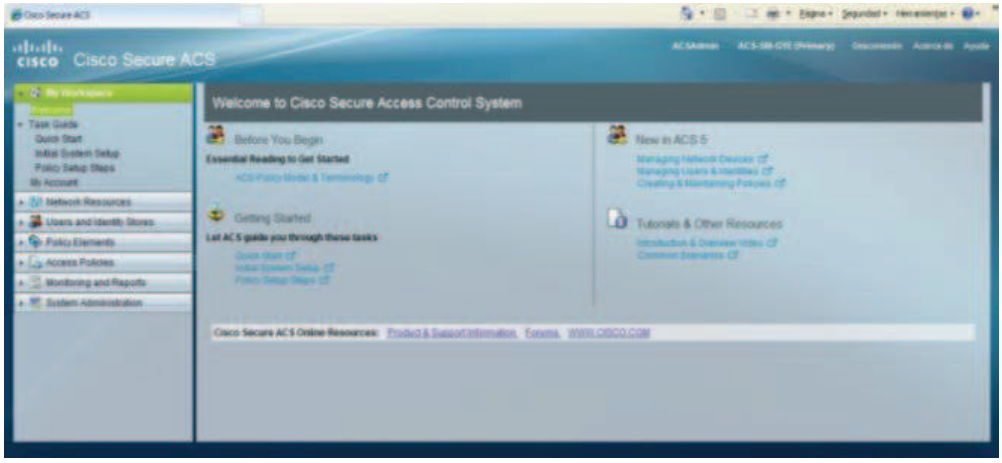

Figura. 4.12. Página principal ACS (http://www.cisco.com/go/ibns)

A continuación se procede con la creación e instalación del certificado digital para el acceso al Directorio Activo de la institución financiera.

Paso 1: Ingresar en la sección ACS *System Administration* > *Configuration* > *Local Server Certificates* > *Local Certificates* y seleccionar *Add*

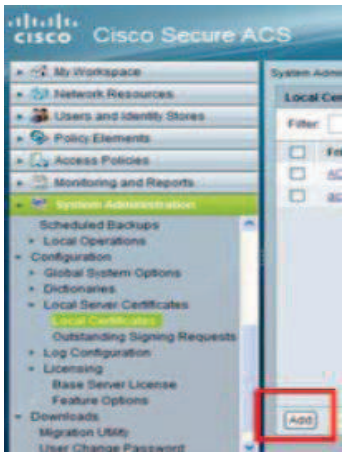

Figura. 4.13. Adicionamiento del certificado digital (http://www.cisco.com/go/ibns)

Paso 2: Seleccionar la opción *Generate Certificate Signing Request* y seleccionar Siguiente:

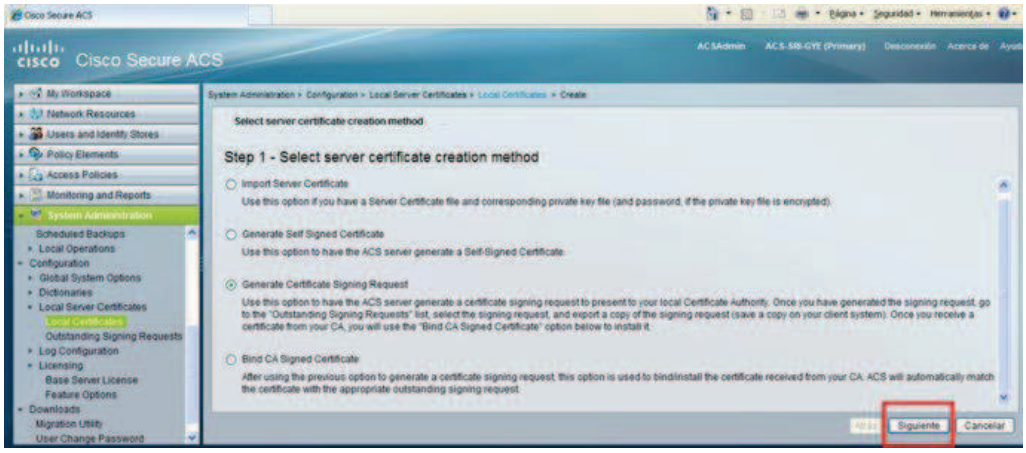

Figura. 4.14. Generación del certificado digital (http://www.cisco.com/go/ibns)

Paso 3: Ingresar el nombre completo del equipo incluyendo el nombre de dominio en el *Certificate Subject* y seleccionamos una longitud de llave *Key Lenght* de 4096 y seleccionamos Finalizar.

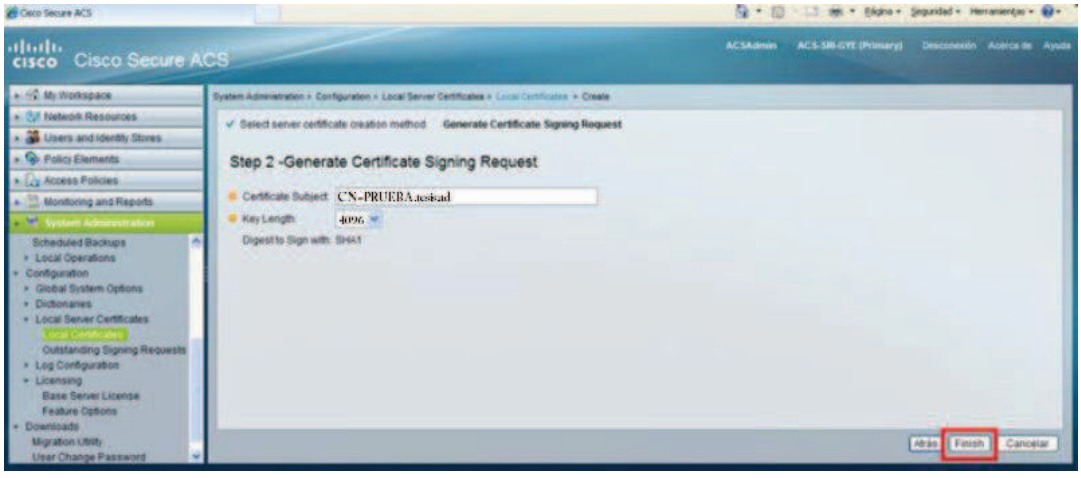

Figura. 4.15. Integración de datos sujetos al certificado digital (http://www.cisco.com/go/ibns)

Paso 4: Ingresar a la pestaña *System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests* y seleccionar la petición de firma de certificado creada anteriormente y descargarla mediante la opción "*Export*".

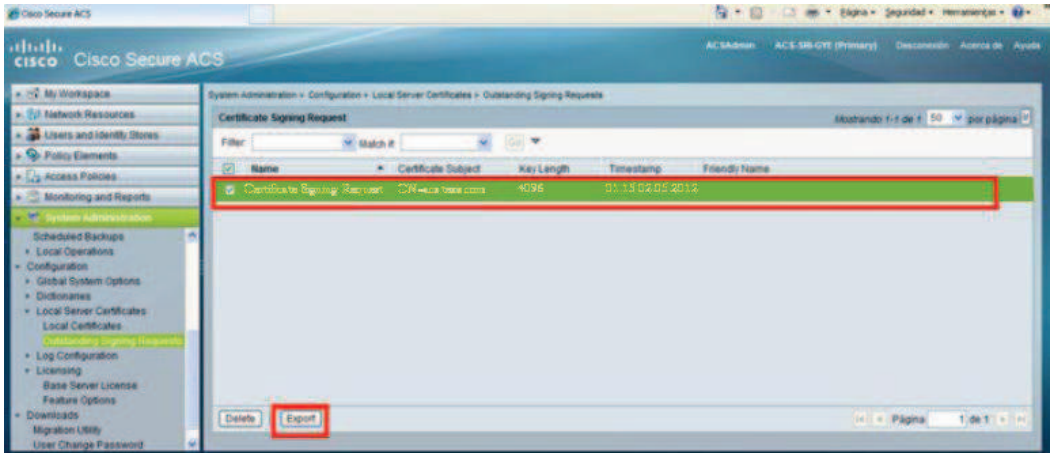

Figura. 4.16. Integración de firma del certificado digital (http://www.cisco.com/go/ibns)

Paso 5: Este requerimiento será entregado (cargado) a la CA que está generar y firme el certificado digital del ACS.

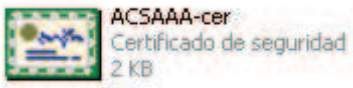

Figura. 4.17. Certificado Digital (http://www.cisco.com/go/ibns)

Paso 6: Se debe instalar el certificado digital generado por la CA en el ACS para esto ingresamos a la pestaña *System Administration > Configuration > Local Server Certificates > Local Certificates* y seleccionamos *Add.*

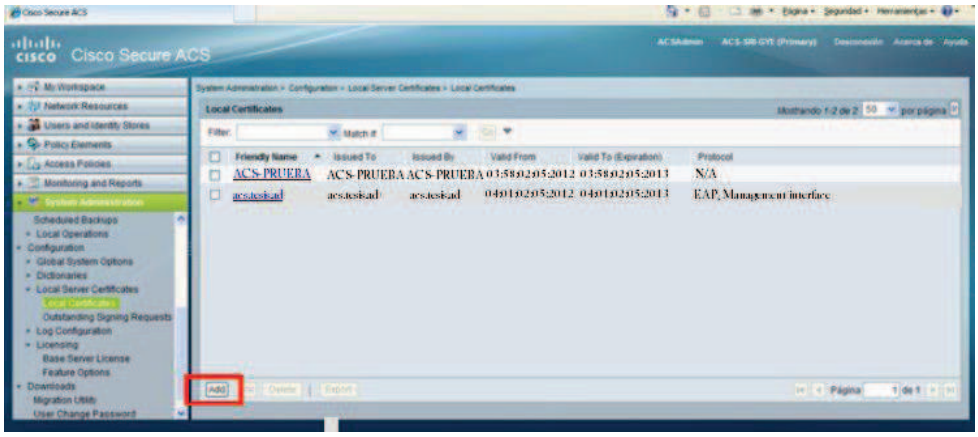

Figura. 4.18. Instalación del Certificado Digital (http://www.cisco.com/go/ibns)

En la siguiente pantalla mostrada a continuación se debe elegir la opción *Bind CA Signed Certificate* y damos Siguiente.

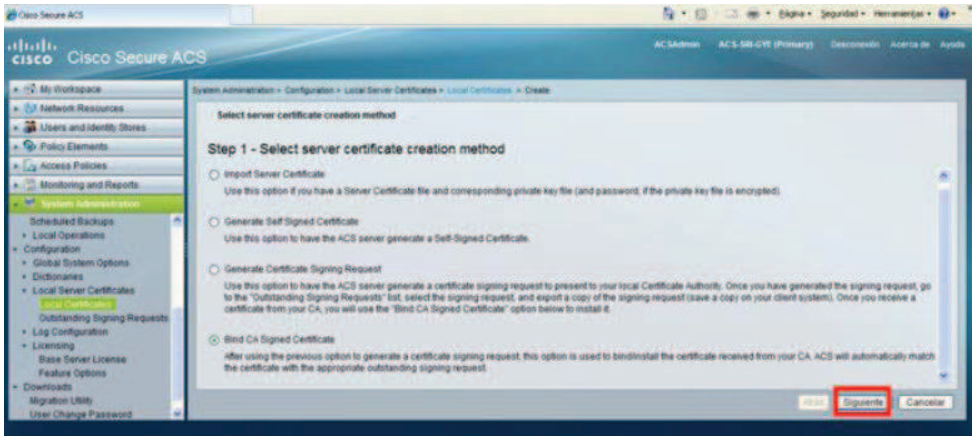

Figura. 4.19. Certifica digital firmado CA (http://www.cisco.com/go/ibns)

A continuación se cargará el certificado en el ACS a través de la opción examinar:

Figura. 4.20. Cargar el certificado digital (http://www.cisco.com/go/ibns)

Para verificar que el certificado ha sido instalado correctamente, se ingresa a la siguiente pestaña: *System Administration > Configuration> Local Server Certificates > Local Certificates*.

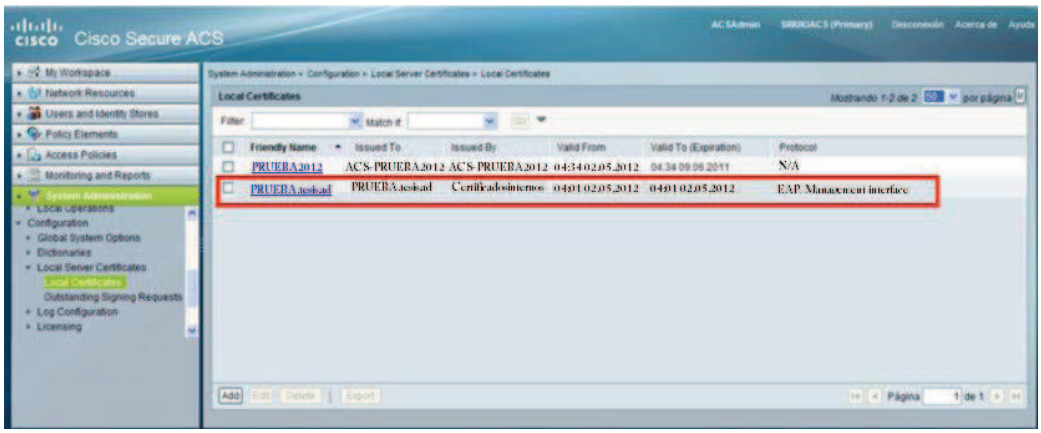

Figura. 4.21. Certificado Digital instalado (http://www.cisco.com/go/ibns)

4.3 Diseño de las recomendaciones de seguridad a implementar en herramienta y dispositivos para control de accesos físicos a la red (AAA)

Uno de los componentes más importantes de IBNS es el servidor de Autenticación es decir el ACS, ya que es el encargado de validar la identidad de los usuarios y host que intentan acceder a la red sea a través de una base de datos local o una base de datos eterna y permite o no el ingreso a la red en función de las políticas (políticas basadas en reglas) aplicadas al perfil de autorización.

Figura. 4.22. Modelo Basado en Normas Políticas (http://www.cisco.com/go/ibns)

Una Política es un conjunto de reglas que el ACS usa para evaluar el requerimiento de acceso de un usuario o host (tipo de cliente, con o sin agente 802.1x, otros) y en función de esto toma la decisión de permitir o no el acceso a la red y es asignado al perfil de autenticación.

El modelo de reglas basadas en las políticas de ACS 5.x se establecen en el caso de las características de los Switch Cisco Catalyst de nueva generación, ya que soportan la característica de IEEE 802.1X con multi-autenticación.

Para la secuencia de Autenticación flexible en el ACS 5.x, se procede con el funcionamiento del protocolo IEEE 802.1x y MAB, es decir, los accesos que tienen por medio de estos y los dominios de autenticación.

- IEEE 802.1X con acceso abierto
- IEEE 802.1X y MAB con ACL descargable (dACL)
- IEEE 802.1X y MAB con VLAN descargable.
- Multi-dominio de Autenticación (MDA)

El protocolo IEEE802.1X con Multi-Auth permite que más de un host sea autenticado en un puerto habilitado con 8021.x; en este caso cada cliente debe ser autenticado de forma individual antes de tener acceso a la red.

La secuencia de autenticación flexible proporciona un mecanismo flexible de espera para permitir que se ejecuten de manera secuencial los diferentes métodos de autenticación 802.1x, MAC Authentication Bypass (MAB) and Web authentication, (control de la secuencia de los métodos de autenticación). De esta manera se simplifica la configuración a nivel de los equipos de acceso (Switch) pudiendo conectar e identificar en los puertos habilitados con 802.1x cualquier tipo de usuario o host.

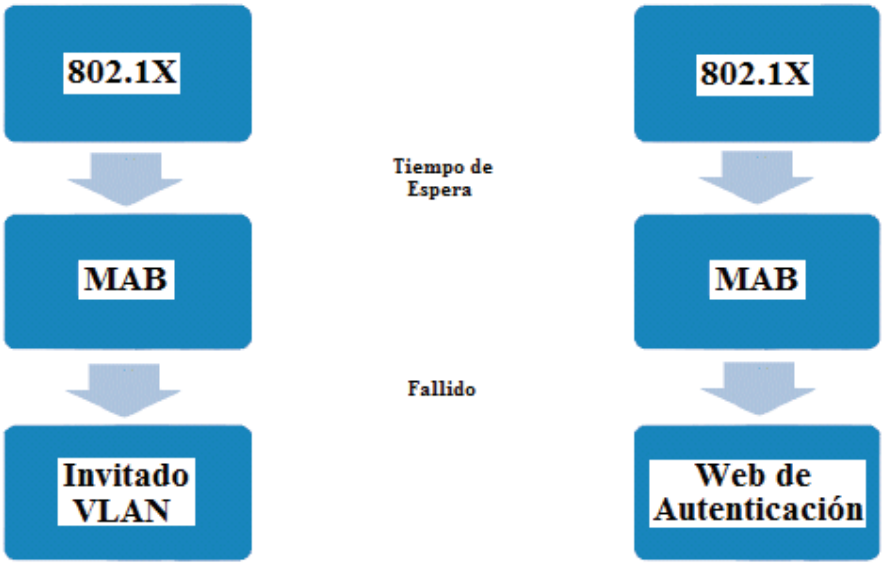

Figura. 4.23. Secuencia de autenticación flexible (http://www.cisco.com/go/ibns)

El protocolo IEEE802.1X con acceso abierto en modo de autenticación, permite a los usuarios tener acceso limitado a la red controlado por ACL o una VLAN.

Tomando en cuenta las configuraciones de los dispositivos de acceso a la red de la institución, iniciamos con clientes AAA (RADIUS y TACACS+), es decir, la configuración y clasificación a los clientes por ubicación y tipo de dispositivo.

Paso 1: Dentro del ACS, ingresamos a la pestaña *Network Resources*, seleccionamos *Network Device Groups* para definir los tipos de dispositivos y sus ubicaciones.

Figura. 4.24. Localización y creación de usuarios (http://www.cisco.com/go/ibns)

Paso 2. Ingresamos los datos solicitados para la ubicación *(Name, Description, Parent*).

Figura. 4.25. Datos de ingreso de ubicación (http://www.cisco.com/go/ibns)

Paso 3: Ingresamos a la pestaña *Network Resources*, seleccionamos *Network Device Groups* para definir los tipos de dispositivos.

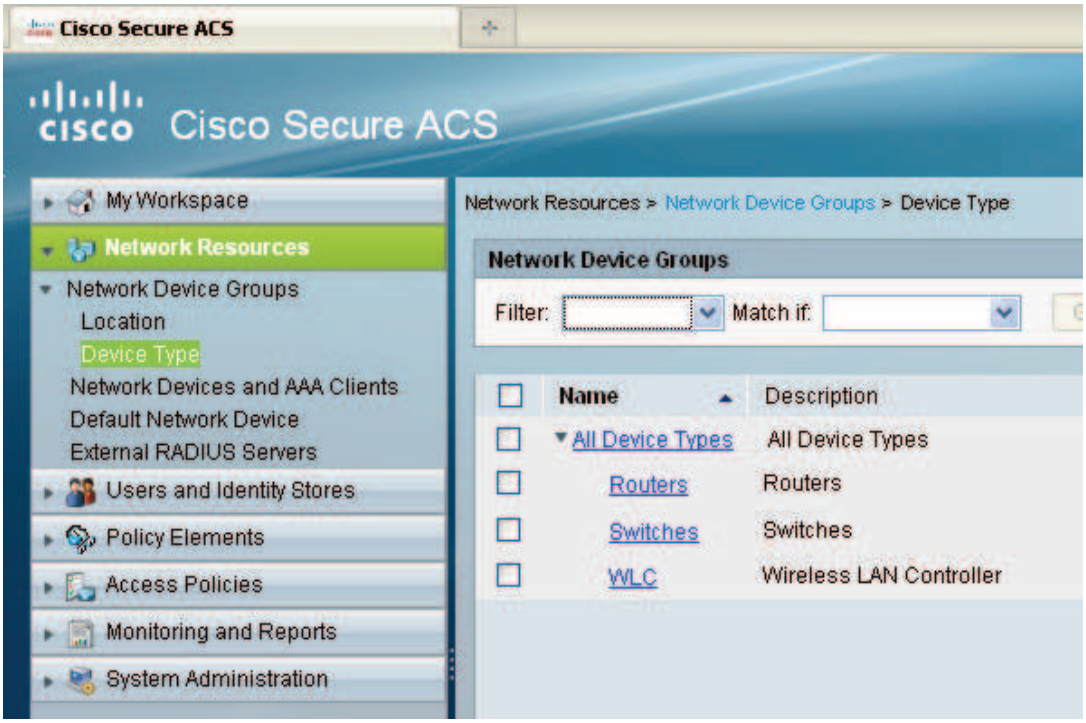

Figura. 4.26. Selección de dispositivos (http://www.cisco.com/go/ibns)

Tanto en el caso de la ubicación y en el tipo de dispositivos se los puede ingresar mediante archivos en formato CSV (en excel) mediante la opción *File Operation*.

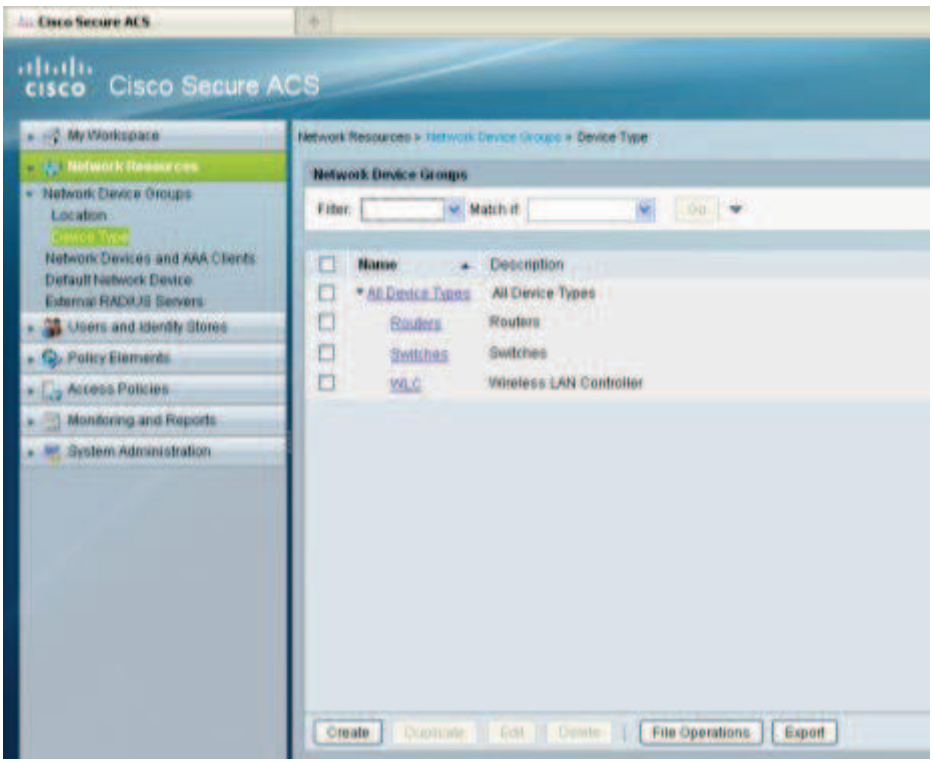

Figura. 4.27. Ingreso de archivos .csv (http://www.cisco.com/go/ibns)

Para la configuración de clientes AAA (RADIUS y TACACS+) procedemos de la siguiente manera.

Paso 1: Ingresamos a la sección *Network Resources/Network Devices and AAA Clients* y seleccionamos la opción "*Create*".

Figura. 4.28. Ingreso Network Resources/Network Devices and AAA Clients (http://www.cisco.com/go/ibns)

Paso 2: Ingresamos los datos Nombre, Descripción, IP de administración del Equipo, ubicación y tipo de dispositivo (estas últimas a través de la opción *Select*) como se muestra en la siguiente pantalla:

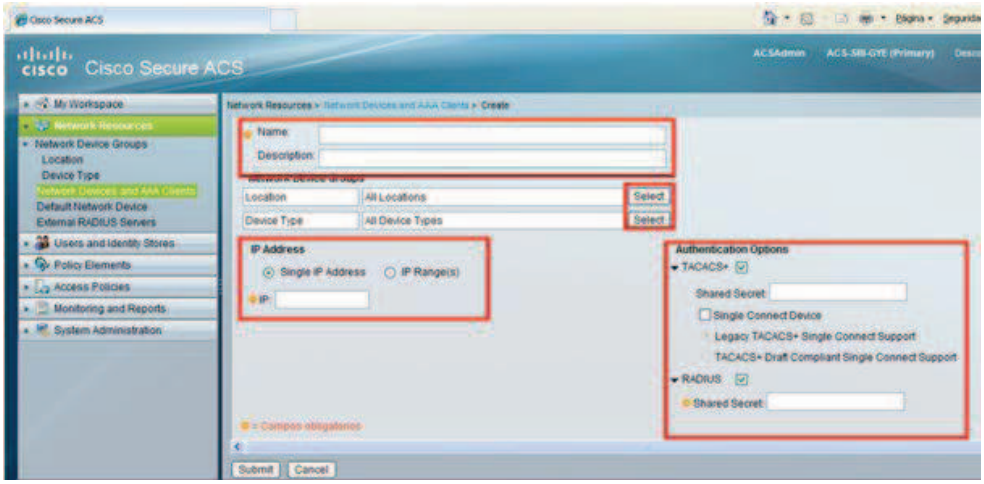

Figura. 4.29. Configuración RADIUS y TACAS+ (http://www.cisco.com/go/ibns)

Además activamos las opciones de Autenticación TACACS+ y RADIUS.

A través de la opción *User and Identity Stores*, el ACS puede administrar la base de datos (interna o externa) donde las credenciales (identidad) del cliente pueden ser validadas.

Cuando un cliente requiere acceso a la red sus credenciales son enviadas al ACS; para autenticar y autorizar al cliente el acceso; el ACS consulta las bases de datos (repositorios) creadas en *User and Identity Stores* pudiendo ser estas internas o externas.

Para realizar este procedimiento, realizamos los siguientes pasos:

Paso 1: Configuración de los "*Identity Groups*". Ingresamos a la sección "*User and Identity Stores/Identity Groups*" y seleccionamos "*Create*".

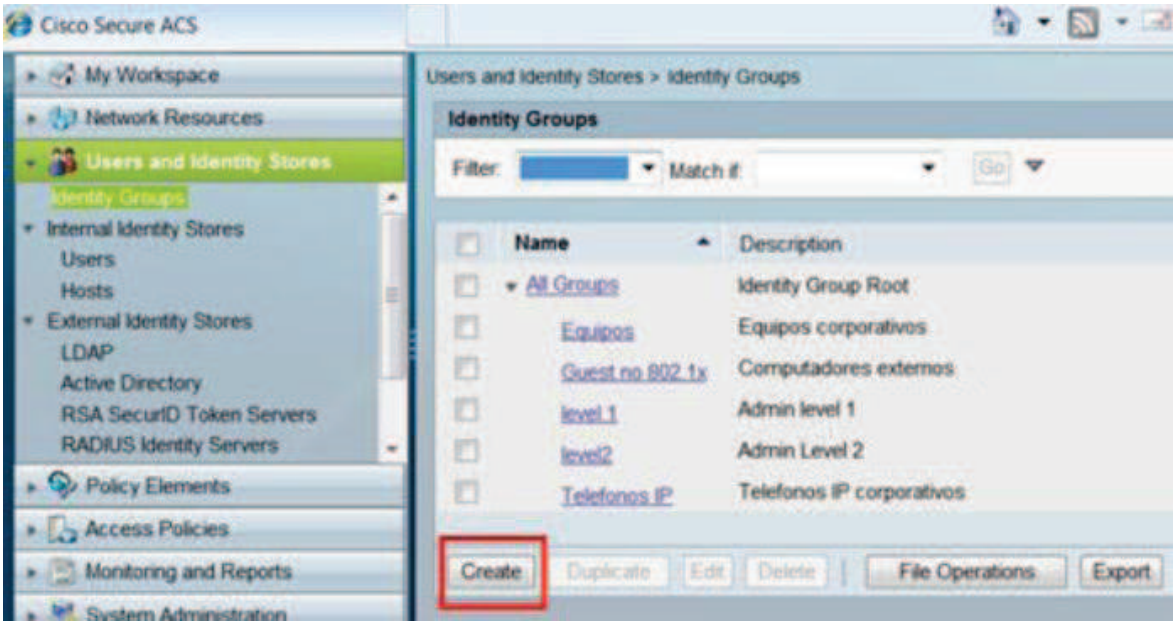

Figura. 4.30. Configuración de los grupos de identidad (http://www.cisco.com/go/ibns)

Los "*Identity Groups*" son nombres de grupos de usuarios internos que se los crean para que a su vez sean asociados con los usuarios o host que residen en el "*Internal Identity Stores*"

Paso 2: Ingresamos los datos solicitados (*Name, Description, Parent*).

En la sección *Parent*, se puede elegir la raíz de la estructura de "*Identity Groups*" para un manejo jerárquico.

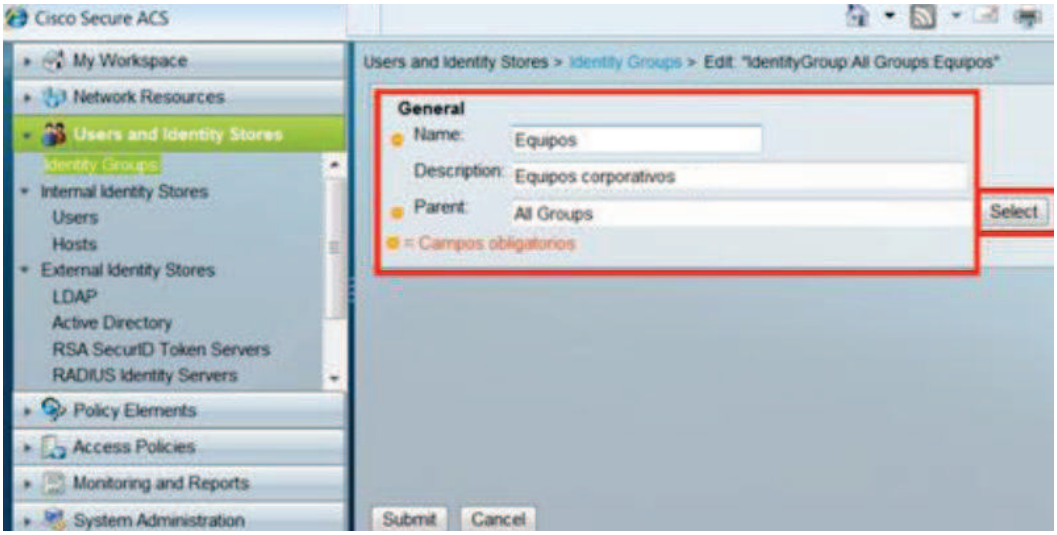

Figura. 4.31. Ingreso de datos (nombre, descripción y parent) (http://www.cisco.com/go/ibns)

Paso 3: Ingresamos a la sección "*User and Identity Stores/Internal Identity Store/User*" y seleccione "*Create*".

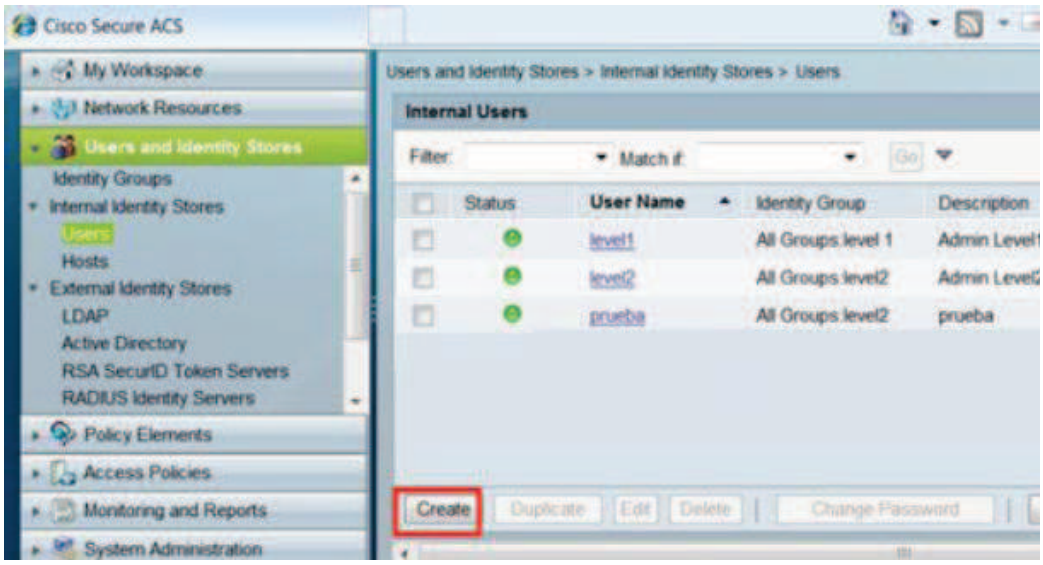

Figura. 4.32. Ingreso a User and Identity Stores (http://www.cisco.com/go/ibns)

Paso 4: Ingresamos los datos solicitados (*Name, Description, Identity Group*); para seleccionar el "*Identity Group*" al cual corresponde el usuario, utilice "*Select*".

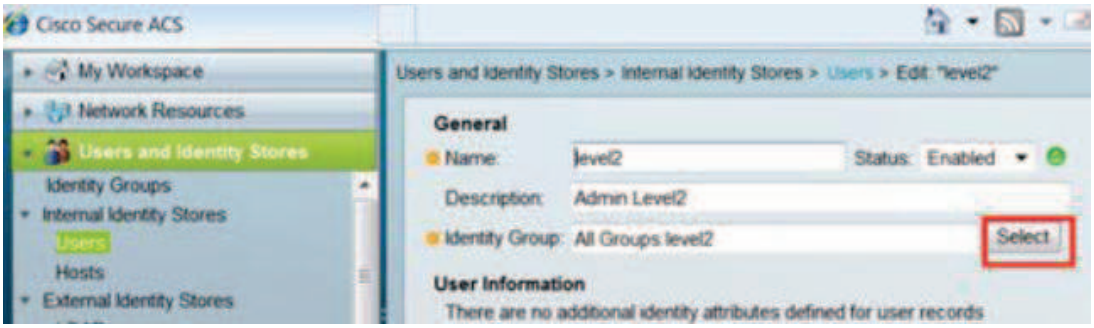

Figura. 4.33. Ingreso de datos (http://www.cisco.com/go/ibns)

Paso 5: Ingresamos a la sección "*User and Identity Stores/Internal Identity Store/host* y seleccione "*Create*".

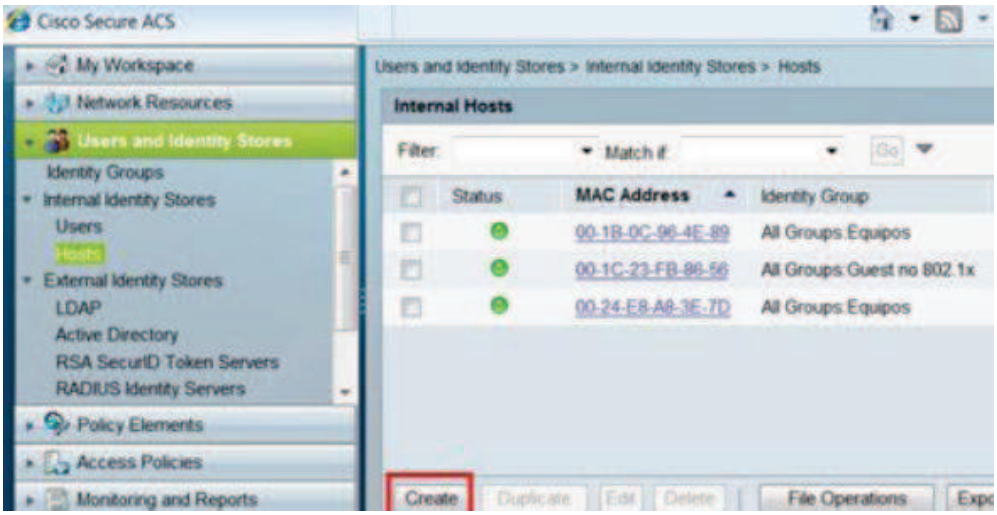

Figura. 4.34. Creación de host (http://www.cisco.com/go/ibns)

Paso 6: Ingresamos los datos solicitados (*Mac Address, Description, Identity Group*); para seleccionar el "*Identity Group*" al cual corresponde el usuario utilice "*Select*".

Para la configuración de la base de datos externa es necesario que entre el ACS y servidor de base de datos se establezca una previa conexión.

Para esta configuración optamos por los siguientes pasos:

Paso 1: Para la configuración del Directorio Activo como base de datos externa, ingresamos a la sección "*User and Identity Stores/External Identity Store/Active Directory*".

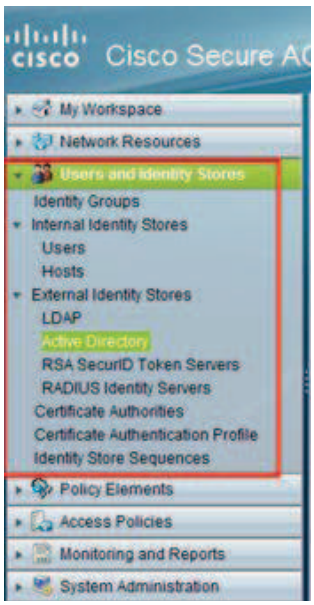

Figura. 4.35. Configuración con Directorio Activo (http://www.cisco.com/go/ibns)

Paso 2: Ingresamos los datos solicitados (nombre del dominio, usuario y *password* de la cuenta con la que accederemos al directorio) y realizamos un Test de Conexión.

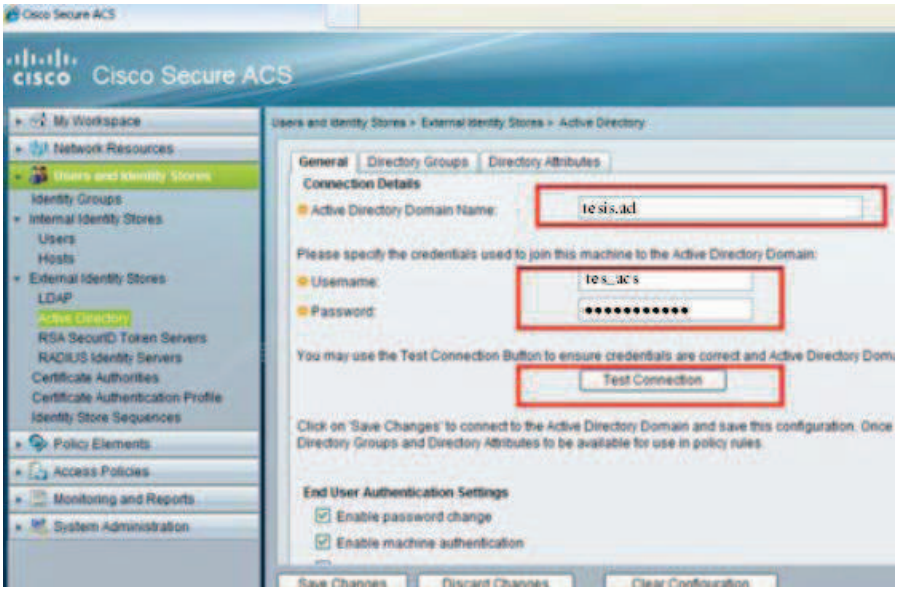

Figura. 4.36. Ingreso de datos (nombre de dominio, usuario y password) (http://www.cisco.com/go/ibns)

Paso 3: Ingresamos mediante consola CLI o monitor con las credenciales de acceso a consola.

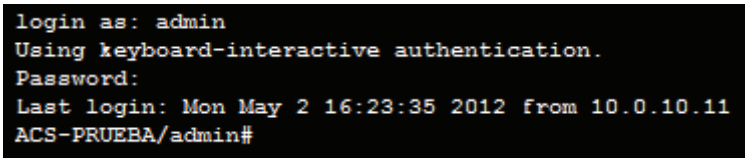

Figura. 4.37. Ingreso con las credenciales de acceso (http://www.cisco.com/go/ibns)

Paso 4: Ingresamos a modo de configuración global e ingresamos el comando "*clock time zone*".

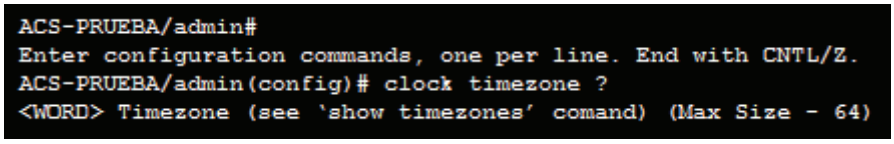

Figura. 4.38. Configuración de la zona horaria (http://www.cisco.com/go/ibns)

Como se mencionó anteriormente es necesario configurar la zona hora, para esto visualizamos las zonas horarias disponibles ingresamos el comando "Show time zone", que para el caso de Ecuador se utilizará la "*timezone*" America/Guayaquil.

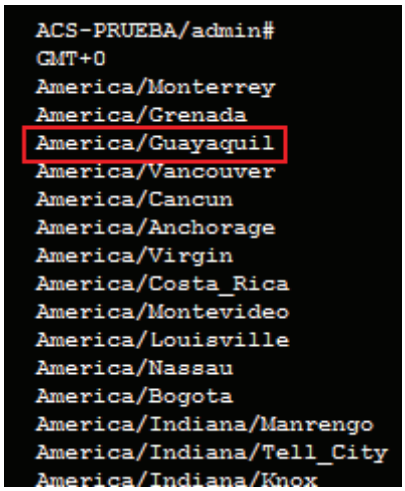

Figura. 4.39. Configuración de la zona horaria para Ecuador (http://www.cisco.com/go/ibns)

Tras realizar esta confirmación de de cambio en la zona horaria, se procede a reiniciar los servicios del ACS, para que se produzca el ajuste en dichos cambios.

Paso 5: Una vez sincronizada la fecha, hora y *timezone,* volvemos a realizar el test de conexión del Directorio Activo. Ingresamos a la sección "*Users and Identity Stores/External Identity Stores/Active Directory*" y seleccionamos "*Test Connection*"

Figura. 4.40. Test de conexión (http://www.cisco.com/go/ibns)

Paso 6: Una vez que el Test de conexión ha sido exitoso, ingresamos a la pestaña "*Directory Groups*".

Dentro del directorio de grupos, seleccionamos los grupos de dominio con los cuales se va a filtrar y aplicar políticas a los usuarios del Directorio Activo.

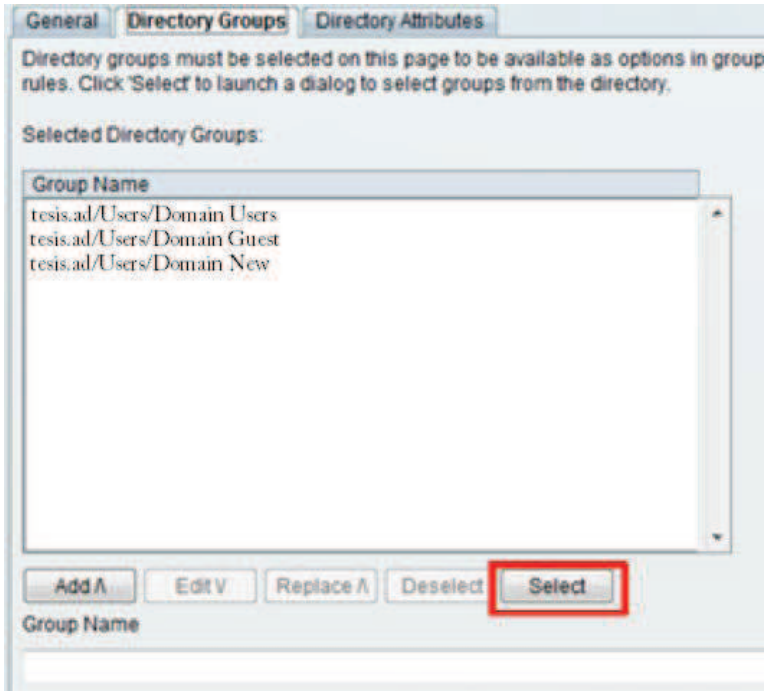

Figura. 4.41. Selección de grupos de dominio en el Directorio Activo (http://www.cisco.com/go/ibns)

Una vez terminada la configuración tanto de la base de datos interna del ACS como la base de datos externa (AD), es necesario definir la secuencia de búsqueda para lo cual procedemos de la siguiente manera:

Paso 1: Ingresamos a la sección **"***User and Identity Stores/Identity Stores Sequences*" y seleccione "*Create*".

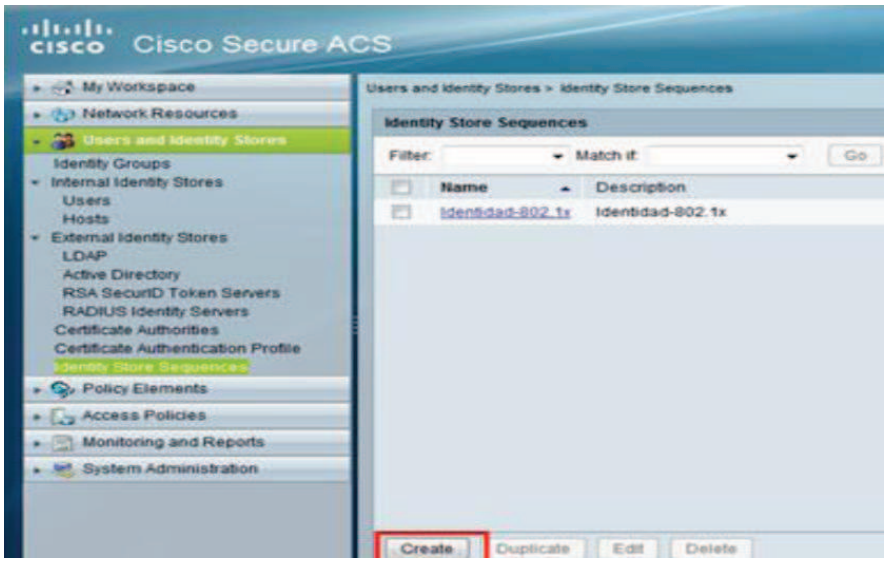

Figura. 4.42. Secuencia de búsqueda de base de datos (http://www.cisco.com/go/ibns)

Paso 2: Seleccionamos el orden de búsqueda de las credenciales de los usuarios.

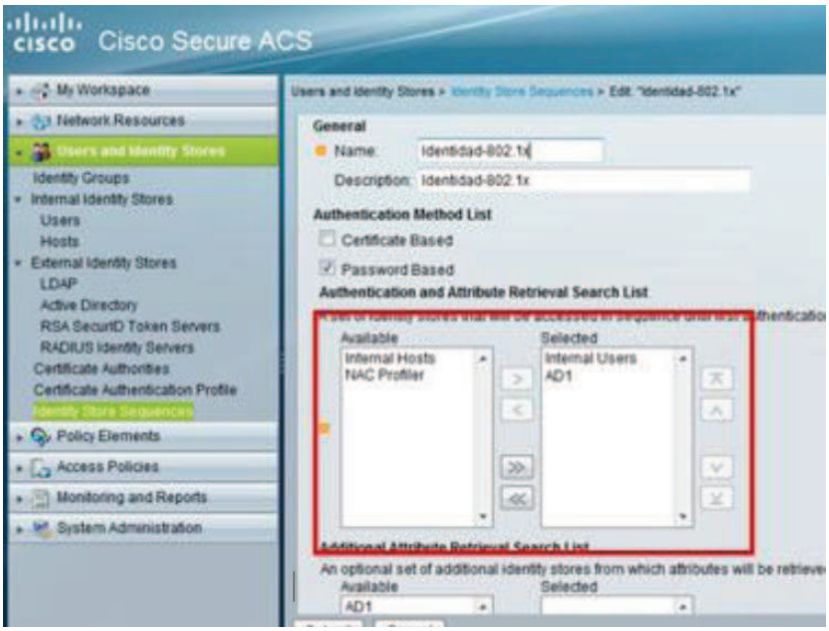

Figura. 4.43. Orden de búsqueda de las credenciales de usuario (http://www.cisco.com/go/ibns)

CAPÍTULO 5

ANÁLISIS DE COSTOS

5.1 Análisis de costos del servidor AAA

Para la estimación del costo del equipamiento enfocado en el servidor AAA de la red de la institución financiera, es importante contar con información de ofertas reales, las mismas que se van a encontrar en el mercado ecuatoriano, dado que si tomamos en cuenta los gastos por trasporte de otro país, este nos va a representar un valor adicional por los equipos; además debemos tener presente que la empresa con la que vamos a proceder con la adquisición de los equipos, va a tener trascendencia internacional. Los costos presentados en este capítulo, corresponden a datos económicos otorgados por una empresa de gran prestigio a nivel nacional como internacional que cuenta con estos equipos establecidos con la tecnología acorde al estudio.

El cálculo de costo se integra al sistema de informaciones imprescindibles para el servicio de la empresa.

El análisis de costos empresariales es sumamente importante, esencialmente desde el punto de vista práctico, puesto que si no se realiza un estudio adecuado, esto puede llevar a una pérdida de consumos económicos muy elevada.

El detalle de la valoración del ACS, se va a encontrar asignada la licencia, la misma que es propietaria de *Cisco System*, ya que sin esta no se logrará un óptimo funcionamiento de este equipo.

Tabla. 5.1. Costos ACS

Nombre	Desarrollador	Versión	Costos (Dólares)	Tipo de Licencia	Plataforma
Cisco Secure Access Control System (ACS)	Cisco System	5.1	14995	Propietaria	Linux y Windows

5.2 Análisis de costo de equipamiento compatible con el servidor de Autenticación (AAA)

El análisis de los costos estimados del equipamiento compatible con el servidor de autenticación, debe ser igual al ACS, ya que la empresa proveedora de estos equipos, deberá tener un ambiente de negocios nacional como internacional, esto servirá de referencia económica para estimar el presupuesto final del proyecto.

Además de este equipamiento, se debe considerar la infraestructura de enlaces entre equipos y demás materiales que pueden llegar a necesitarse para que la conexión entre equipos sea el más óptimo.

Todo esto se lo debe analizar y desarrollar en base a la infraestructura de la institución financiera.

A continuación se muestra el análisis en el cual se detallan el equipamiento compatible para el ACS v5.1.

Tabla. 5.2. Costos de equipamiento compatible

Nombre	Desarrollador	Cantidad	Precio Unitario	Valor
Switch WS-C2960-48TT-L	Cisco Catalyst	2	1048	2096
Switch WS-C3550G-48TS-S	Cisco Catalyst	2	3518	7036
Cisco Catalyst 2950G-48 Ethernet Switch	Cisco Catalyst	2	2150	4300
Cisco 1721 VPN Security Router Bundle	Cisco System	2	1798,74	3597,48
Servidor Windows	Windows	1	469,00	469,00
Materiales		500	0,75	375
Personal Capacitado		3	600	1800
			Sub-Total:	19673,48

El costo total, deberá ser fijado mediante el precio del ACS v5.1 y el equipamiento compatible con el mismo.

Tabla. 5.3. Costo total ACS y equipos

Descripción	Precio
Cisco Secure Access Control System (ACS)	14995
Sub-Total (Equipamiento Compatible)	19673,48
Total:	34668,48

Se puede detallar que el precio total del equipamiento y el servidor de autenticación ACS son de $ 34668,48 dólares; lo que hace referencia en relación costo, al control de recursos tecnológicos de la institución financiera y la seguridad en la información de la misma, ya que sin la utilización de esta herramienta, podría conllevar a una pérdida importante referente al factor económico de la empresa.

5.3 Análisis de costo/beneficio en relación a la seguridad del acceso a la red de la institución financiera

El costo/beneficio que se traería a la institución financiera se establece mediante el análisis de la seguridad que esta adoptará para que los funcionarios no pretendan extraer información susceptible que a la larga pueda afectar a dicha entidad.

Dado que el mecanismo de defensa contra fuga de información de la entidad financiera sea muy bajo, este método de seguridad podrá direccionar un control más riguroso al acceso de la red de la misma.

En el caso de pérdida de información de la institución financiera, se puede determinar un valor muy alto en relación de costos, ya que esta información puede ser mal utilizada por los funcionarios que acceden al sistema de la entidad para su beneficio personal y no a favor del lugar en donde estos se desempeñan, por este motivo se especifica que el beneficio de un nuevo sistema de seguridad basado en el servidor de autenticación, le de acceso solamente a las funciones que estos servidores requieran para desarrollar su trabajo y no para el mal uso de la información a la que estos puedan acceder.

Durante el período de levantamiento de información, una institución financiera maneja millones de dólares, por lo que la relación costo-beneficio es relevante comparado con la seguridad que se podría desarrollar en las entidades financieras.

Por este motivo, se puede establecer que el servidor de autenticación, autorización y registro, es una herramienta muy útil que servirá para que la información considerada como confidencial, no pueda ser sustraída por funcionarios que a futuro puedan manipularla con fines de lucro.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- El análisis y diseño de este proyecto, ayuda a tener una mejor proyección en los ambientes de control de acceso a la red de una institución financiera y a su vez establece una seguridad en el manejo de información.

- La seguridad que presta el servidor de autenticación es muy valiosa para instituciones que tienen información confidencial, ya que la mala utilización de la misma puede ser perjudicial para dicha entidad.

- El servidor AAA desempeña una barrera de seguridad mejor elaborada con un seguimiento exhaustivo del ingreso de los funcionarios a la red de la institución financiera. Además establece un óptimo sistema con el cual evita ataques y fraudes.

- El servidor AAA al ser un módulo centralizado, debe ser capaz de manejar todas las conexiones de la red de la institución financiera además de controlar el acceso a la red en todo momento.

- Al centralizarse todo el sistema con el servidor de autenticación, se logra obtener un manejo fácil del enlace, ya que se tiene todas las aplicaciones concentradas en un solo servicio y permite de esta manera una configuración más rápida y sencilla.

- La relación y enlace a cada rol y perfil de los funcionarios, se lo desarrolla mediante los roles y perfiles que cada institución los tengan, es decir, va a depender de la entidad en la que se desee desarrollar este sistema de autenticación ya que este análisis se lo realiza de manera general para cualquier organismo financiero sin importar la cantidad de roles y perfiles que tenga cada cargo.

- La integración del servidor RADIUS con el control de tráfico y la base de datos, se alcanzó con el objetivo del diseño de la aplicación para la administración en base a un nivel de privilegios basándose en un sistema de autentificación.

- El nivel de control de acceso a la infraestructura tecnológica, se lo determinó en base a los roles y perfiles de cada funcionario, ya que con esto se logró un mejor desempeño en las funciones de los mismos.

- Se logró establecer un mecanismo de seguridad en el cual se detalle la autenticación, control y registro de cada uno de los funcionarios que ingresen a la red de la institución financiera.

- Se analizó el equipamiento compatible con el servidor AAA, ya que si se utiliza router o switches de otras marcas, que no sean del mismo servidor de autenticación, pueden traer problemas en el momento de su conexión.

- La configuración con los roles y perfiles de los cargos de los funcionarios, va a depender del Directorio Activo, ya que si este no funciona, el servidor AAA no logrará establecer los aplicativos a los cuales pertenece cada usuario.

- Solamente los funcionarios que se encuentren autorizados, podrán manipular y configurar el servidor AAA.

6.2 Recomendaciones

- Se debe establecer una ruta crítica en caso de controversias en las actividades, dado que se pueden encontrar problemas, ya sean estos de índole administrativa, financiero o al momento de su ejecución.

- Debemos tomar muy en cuenta las direcciones Ip con las que se vaya a trabajar, dado que son direcciones privadas y de carácter confidencial.

- Establecer grupos de administradores para el servidor AAA con el fin de llevar a cabo la autenticación, autorización y administración de las cuentas de los funcionarios.

- Dado que los switch de borde, routers, servidor AAA, son de marca Cisco, es recomendable la utilización de equipos de la misma marca.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

IBNS.- Identidad Basada en Servicios de Red.

ACS.- Sistema de Seguridad para el Control de Acceso.

AAA.- autenticación, autorización y accounting (registro).

EAP.- Protocolo Extensible de Autenticación.

NAS.- Network-attached storage.

MAU.- Unidad de Acceso Multiestación.

REFERENCIAS BIBLIOGRÁFICAS

1. Cisco Systems, Inc, *User Guide for the Cisco Secure Access Control System 5.1*, Americas Headquarters, 1ª ed., West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 618

2. Cisco Systems, Inc, *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*, 12 ª ed., Americas Headquarters, 170 West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 1410

3. AREITO, Javier, *Seguridad de la Información, Redes, Informática y Sistemas de Información*, 1ª ed., PARANINFO, Magallanes, 25;28015 Madrid - España, 2008, 561

4. http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html, Authentication, Authorization, and Accounting (AAA)

5. http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html, Authentication, Authorization, and Accounting (AAA)

6. http://technet.microsoft.com/es-es/library/cc732681(WS.10).aspx, Protocolo de autorización de credenciales de host

7. http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491729.html&ei=KNY2TuTFFrK50AH30ImiDA&sa=X&oi=translate&ct=result&resnum=3&ved=0CEAQ7gEwAg&prev=/search%3Fq%3DCisco%2BHCAP%26hl%3De

s%26rlz%3D1R2RNTN_enEC381%26biw%3D1280%26bih%3D600%26prmd%3Divns, Guía de Implementación de Integración

8. http://es.scribd.com/doc/57741341/T3-AAA, AAA

9. http://www.cisco.com/go/ibns, Identidad Basada en Servicios de Red

10. http://es.wikipedia.org/wiki/RADIUS, Protocolo RADIUS

11. http://es.wikipedia.org/wiki/Network-attached_storage, Network-attached storage (NAS)

12. http://www.cisco.com/en/US/docs/routers/access/1700/1701/software/configuration/guide/1700swcg.html, Guía de Configuración de Router Cisco, antiguo

13. http://www.cisco.com/en/US/products/ps6406/index.html, Switch Cisco Catalyst 2960 Series

14. http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red, Topologías de red

15. http://tesis-redes.blogspot.com/, Tesis de redes

16. http://www.eclac.org/noticias/paginas/3/20623/SeparataM_R.pdf, Redes de Seguridad Financiera e Integración regional

17. http://platea.pntic.mec.es/~lmarti2/cableado.htm, Cableado estructurado

18. http://ddd.uab.cat/pub/redes/15790185v11/Vol11_9.htm, La vida social de los routers

19. http://porta-tlacuachasunidas.blogspot.com/2011/05/topologia-de-doble-anillo.html, Topologías de red

20. http://www.slideshare.net/guest7bb5a1/redes-topologia-de-red, Topología de red

21. http://www.cisco.com/en/US/products/ps5881/index.html, Router Integrado Cisco 2811

22. http://www.gilisoft.com/product-usb-lock.htm, Gilisoft Lock

23. http://www.monografias.com/trabajos28/manual-redes/manual-redes.shtml#determin, Manual para el Diseño de Redes LAN

24. http://agile.inntegra.eu/metodologia/dimension-proyecto/a8-personas-roles-y-perfiles, Roles y Perfiles

25. http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml#mejores, Seguridad en Redes en Computadoras

26. http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/catalyst_2960_series_switches/index.html#~overview, Switches CISCO Catalyst Series 2960

27. http://es.hardware.com/tienda/cisco/WS-C3560G-48TS-S/refurbished/, Switches Cisco Catalyst 3560-48TS-S

28. http://telematica.cicese.mx/seguridad/poli-segu.pdf, Política Oficial de Seguridad Informática del CICISE

29. http://networkeando.blogspot.com/2009/01/configurando-aaa-en-un-router.html, Configurando AAA en un Router

30. http://www.ciao.es/Cisco_Catalyst_3560G_48TS_48__637607, Cisco Catalyst 3560G-48TS 48

31. http://technet.microsoft.com/es-es/library/cc737807%28WS.10%29.aspx, Protocolo de autenticación de contraseña

32. http://technet.microsoft.com/es-es/library/cc785956%28WS.10%29.aspx, Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)

33. http://technet.microsoft.com/es-es/library/cc758984%28WS.10%29.aspx, Protocolo MS-CHAP

34. http://technet.microsoft.com/es-es/library/cc787927%28WS.10%29.aspx, Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (MS-CHAP v2)

35. http://technet.microsoft.com/es-es/library/cc739678(WS.10), Protocolo MS-CHAP versión 2

36. http://technet.microsoft.com/es-es/library/cc782159%28WS.10%29.aspx, Protocolo de autenticación extensible (EAP)

37. http://technet.microsoft.com/es-es/library/cc782851%28WS.10%29.aspx, Protocolo EAP

38. http://es.wikipedia.org/wiki/Hash, Función Hash

39. http://es.scribd.com/doc/40359306/A-a-A, Introducción AAA

40. http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones-node4.html, Seguridad en Nivel de Red

HOJA DE RECEPCIÓN

El presente Proyecto de Grado fue entregado en la fecha:

Sangolquí, 21 de Agosto del 2012

Daniel Martín Lescano Rodríguez
Autor

Sr. Ing. Edwin Chávez
Coordinador de la Carrera
Ingeniería en Electrónica, Telecomunicaciones.