ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

ESCUELA DE INGENIERIA ELECTRONICA EN TELECOMUNICACIONES Y REDES

"PROPUESTA DE SOLUCION AL ACCESO INSEGURO DE LOS RECURSOS DE LAS REDES LAN CORPORATIVAS MEDIANTE APLICACIONES NETWORK ACCESS CONTROL DE SOFTWARE LIBRE."

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN ELECTRONICA Y COMPUTACION

Presentado por:

Diego Armando Cujilema Yupa

RIOBAMBA – ECUADOR

2011

Dedicatoria

La culminación de la tesis solo representa la mínima parte de todo el esfuerzo realizado a lo largo de este tiempo en la Politécnica de Chimborazo

A mi Dios gracias a sus bendiciones nada de esto fuera realidad; a mi santa madre Herminia y madre Juanita, a quienes se los debo todo, a mi tío Jaimito, quién estuvo en los momentos de necesidad y a mis grandes amistades que uno ha sembrado en la camino de la vida.

Los llevo infinitamente en mi corazón y la gratitud por que han sido y serán el impulso más grande del ser humano.

Agradecimiento

“Yo Diego Armando Cujilema Yupa, soy el responsable de las ideas, doctrinas y resultados expuestos en esta: Tesis y el patrimonio intelectual de la misma pertenecen a la ‘Escuela Superior Politécnica de Chimborazo’”.

NOMBRE	FIRMA	FECHA
ING. IVAN MENES **DECANO FACULTAD** **INFORMATICA Y ELECTRONICA**	**.....**	**.....**
ING. PEDRO INFANTE **DIRECTOR ESCUELA** **INGENIERIA ELECRONICA** **EN TELECOMUNICACIONES Y REDES**	**.....**	**.....**
ING. ALBERTO ARELLANO **DIRECTOR DE TESIS**	**.....**	**.....**
ING. WILSON BALDEON **MIEMBRO DEL TRIBUNAL**	**.....**	**.....**
Lcdo. CARLOS RODRIGUEZ **DIRECTOR CENTRO DE** **DOCUMENTACION**	**.....**	**.....**
NOTA DE LA TESIS	**.....**	

"Yo Diego Cujilema soy responsables de las ideas, investigaciones y resultados expuestos en esta tesis y el patrimonio intelectual de la tesis de grado perteneciente a la ESCUELA DE INGENIERIA ELECTRONICA Y COMPUTACION de la ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO".

_____

Sr. Diego Cujilema

INDICE GENERAL

Contenido

BIBLIOGRAFÍA

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

1 GENERALIDADES

1. 1. ANTECEDENTES

Una de las tareas más demandantes para los administradores de sistemas es asegurar que cualquier dispositivo que se conecte a la red corporativa en cualquiera de sus formas y a través de cualquier medio de acceso, cumplan con el modelo de seguridad definido para la organización.

La conectividad está tomando mayor importancia para los Profesionales de empresas y organizaciones, ya que los usuarios requieren conexión desde diferentes puntos, lo cual aumenta los riesgos de seguridad y al mismo tiempo, exige la puesta a punto de los sistemas para poder ofrecer un servicio de igual calidad en cualquier dispositivo.

Las estaciones de trabajo se han convertido en el enlace más débil en relación con la seguridad. Las organizaciones necesitan asegurarse de que todos los ordenadores que

se conectan a la red están protegidos y cumplen con las políticas de uso aceptable de la empresa y las políticas establecidas por la organización.

Teniendo en cuenta esta necesidad, en los últimos años emergieron tecnologías de control de acceso como NAC, NAP (Network Access Protection) de Microsoft y TNC (Trusted Network Connect) de Trusted Computing Group, a alto nivel estas tecnologías tienen por objetivo verificar que los dispositivos cumplan con el modelo de seguridad definido para la organización antes de que estos tengan acceso a la red corporativa.

El concepto de control de acceso a red abarca cualquier tecnología que permita a las empresas garantizar la imposición de las políticas de seguridad corporativas a los puntos finales conectados a sus redes. Estas políticas de seguridad para puntos finales, también pueden haber sido definidas para prevenir la utilización de determinadas aplicaciones, como la compartición de ficheros peer-to-peer (P2P) o la mensajería instantánea. Es decir, determinan el estado y el comportamiento permitido por la empresa a los puntos finales conectados a sus redes.

El creciente riesgo de las amenazas y la movilidad en aumento del personal constituyen una preocupación para muchos equipos dentro de una organización.

Sin embargo, la explosión de las LAN, de las bases de datos online y del mundo conectado en general fue creando una enorme y urgente demanda de acceso a cualquier cosa, en cualquier lugar, en cualquier momento y casi desde cualquier tipo de dispositivo. El control de acceso a red se convirtió en algo secundario porque los esfuerzos de seguridad fueron concentrándose en los puntos finales. Pero a medida que las vulnerabilidades de tales puntos han empezado a ser explotadas cada vez en

mayor medida y más rápidamente por los hackers y virus maliciosos, la idea de controlar el acceso a red es una necesidad inmediata.

1. 2. JUSTIFICACIÓN

En este proyecto se presenta una solución usando como alternativa una de las entidades autentificadas para el acceso a la red, evidenciando que este tipo de aplicación no se ha hecho todavía.

Para ello se basara en software libre en plataforma Linux el cual hace la función de administrador de esta tecnología, la cual se comparara con una tecnología comercial.

Se pretende con esto dar una solución al control de acceso no deseado a la red tanto interno como externo, Una solución NAC debe garantizar que todos los equipos cumplan con la política de uso aceptable y de seguridad definida.

Permitiendo establecer con el trabajo de investigación parámetros para su utilización.

Para obtener un resultado que ofrezca a las empresas una reducción significativa en el número de incidentes de seguridad, mejora el nivel de cumplimiento de las políticas de configuración y brindar además la confianza de que los mecanismos de seguridad de puntos finales están correctamente activados.

Brindará beneficios tangibles, tales como:

- Reducción en la propagación de código malicioso,
- Un nivel de riesgo inferior gracias a un mayor control de los puntos finales administrados y no administrados que acceden a la red corporativa.

- Mayor disponibilidad de la red y menos interrupciones de los servicios para los usuarios finales.

Hay tres enfoques principales de NAC basados en función del punto en el que se refuerza el control de accesos:

- Control de extremo.
- Control central.
- Control de cliente.

Se dispondrá de un escenario para las pruebas del acceso a la red, basándonos en las políticas y funcionalidades de la organización, como se observa en la figura 1.1

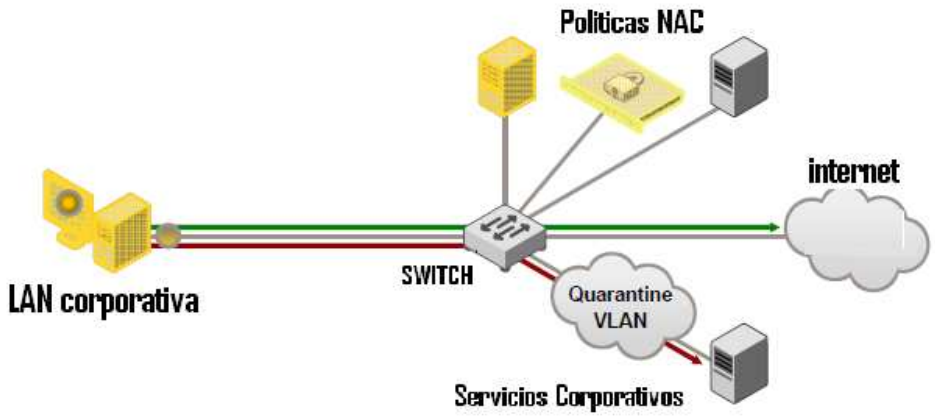

Figura I.01: Funcionalidad del NAC

1. 3. OBJETIVOS.

1. 3. 1 OBJETIVOS GENERALES

Proponer una solución al acceso inseguro a los recursos de las redes LAN mediante la aplicación de Network Access Control.

1. 3. 2 OBJETIVOS ESPECÍFICOS

- Investigar las vulnerabilidades más comunes en el acceso de los recursos a las redes LAN Corporativas.

- Estudiar la Arquitectura para soluciones de Network Access control.

- Evaluar una de las posibles soluciones de Network Access Control de Software Libre como:

    - FreeNAC (también llamado OpenNAC) prevé la asignación dinámica de VLAN, el inventario en vivo y control de acceso para LAN Switches y todo tipo de dispositivos de red.

    - PacketFence es totalmente compatible, confiable, libre y de código abierto de la red de control de acceso (NAC) del sistema.

- Definir una propuesta Metodológica de la solución NAC.

1. 4 HIPÓTESIS

Con la presente propuesta de solución a los recursos permitirá mejorar el control y acceso de los usuarios a la organización.

CAPITULO II

2 RED CORPORATIVA

2.1 Introducción

Una Red Corporativa debe ser vista como la infraestructura de información corporativa, y constituye la forma principal de comunicación entre los grupos de trabajo para obtener la información necesaria que les permita trabajar con sinergia para alcanzar los objetivos empresariales.

Puede soportar comunicación de arriba hacia abajo haciendo que las decisiones ejecutivas y las discusiones sobre estrategias sean fácilmente accesibles. Cuando un empleado de bajo nivel escribe un plan de producto o una propuesta de marketing construida en torno a una estrategia de alto nivel, éste podrá incluir un vínculo de

hipertexto a la versión del documento de estrategia, facilitando así a los demás participantes en el proyecto que se familiaricen. La intranet permite que todo el mundo se conecte directamente con la versión original de las declaraciones del director general de una forma más eficaz que cuando el director general hace una presentación a una serie de jefes de departamento, que a su vez notifican lo que ha sido dispuesto para cada dependencia, etc.

2.2 Concepto

Se entiende por una Red Corporativa, también denominada intranet corporativa, a aquella intranet o red privada perteneciente a una empresa o corporación. El principal motivo que está llevando cada vez más a un importante número de compañías a desarrollar su propia intranet es la concienciación por parte de los directivos de la importancia que tiene la gestión del conocimiento en el ámbito empresarial. De entre los posibles beneficios que puede traer una intranet corporativa suelen destacar para las empresas el aprendizaje y la evaluación de los procesos productivos en lo referente a calidad, productividad, eficacia y costes.

La estrategia de construcción de las redes corporativas podría ser considerada en un principio como la evolución de la informática de los grupos de trabajo en las grandes compañías, que tendían a la integración de todas las computadoras dentro de la red. Por tanto el ámbito de las redes corporativas incluye toda la serie de redes que componen la telaraña empresarial (LAN,s, WAN,s, MAN,s, etc.), también pretende integrar todos los sistemas de una organización, donde existen todo tipo de

computadoras (DOS, OS/2, Macintosh, UNIX Workstations, miniordenadores, mainframes, etc.).

Una red corporativa debería asemejarse a una plataforma de conexión y trabajo que ofreciera la conectividad necesaria a una organización que desea conectar cualquiera de sus recursos informáticos.

Por otra parte en la definición de lo que sería una "Intranet", debería tener presentes los mismos objetivos que una red corporativa, puesto que lo es, pero con la peculiaridad de utilizar los mismos protocolos de red que se utilizan en "Internet", en definitiva TCP/IP. En el caso de Intranets, estamos hablando de un único protocolo transparente para todos los sistemas a interconectar, y que al mismo tiempo nos va a permitir el acceso a Internet sin ningún tipo de problema, puesto que utilizamos sus propios estándares, dentro de los mismos podemos por ejemplo estar hablando de la utilización de navegadores para acceder a nuestras aplicaciones corporativas, podemos estar hablando de la utilización extensa del File Transfer Protocol, podemos estar hablando de conexiones rápidas vía Telnet (TN5250, TN3270, etc.), y al mismo tiempo permitir que personas ajenas a nuestra empresa puedan acceder a nuestras bases de datos de producto, en definitiva a nuestra Web.

Por tanto, la diferencia entre Red Corporativa e Intranet, se encuentra no tanto en los objetivos a conseguir como en las características técnicas que caracterizan a ambas. Podemos ver que en una red corporativa estamos hablando normalmente (no por propio concepto) de distintos protocolos de red, de transporte etc, mientras que una

Intranet cumple normalmente la simplificación a uno solo de ellos (no por propio concepto).

2.3 Características

Una red corporativa típica tiene las siguientes características:

- Muchos segmentos de LAN con una red troncal (por ejemplo, un segmento en cada piso o ala de varios edificios).
- Más de un protocolo de red.
- Áreas configuradas con Abrir la ruta de acceso más corta primero (OSPF, Open Shortest Path First).
- Conexiones de acceso telefónico para usuarios que establezcan una conexión desde su casa o mientras viajan.
- Conexiones de línea concedida con sucursales.
- Conexiones de marcado a petición con sucursales.
- Conexiones con Internet.

En la siguiente ilustración se muestra un ejemplo de red corporativa.

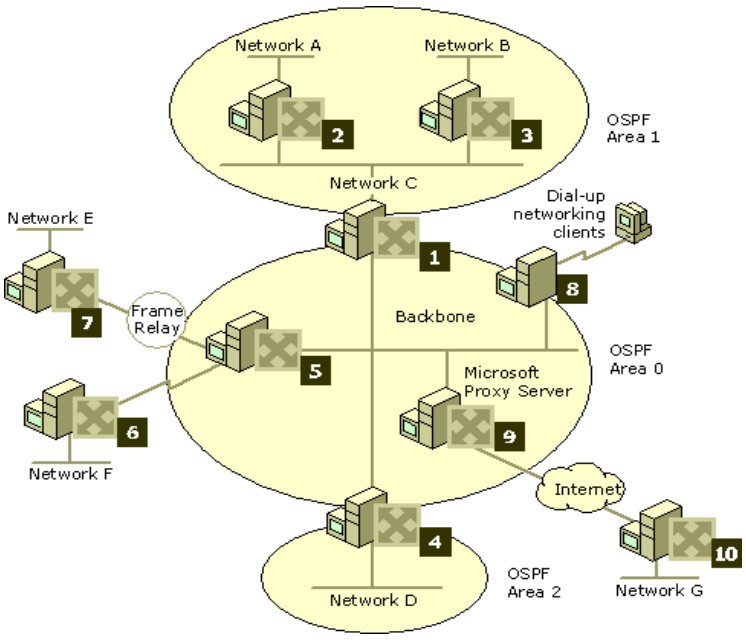

Figura II.02: Ejemplo Red Corporativa

Una red corporativa utiliza normalmente diferentes tipos de medios de red. Los diferentes segmentos de la oficina pueden utilizar redes Ethernet o Token Ring de 10 megabits por segundo (Mbps), pero la red troncal que se utiliza para conectar con las diferentes redes y servidores de host está formada normalmente por redes Ethernet de 100 Mbps o una Interfaz de datos distribuidos por fibra (FDDI, Fiber Distributed Data Interface). Las conexiones con redes externas (Internet) se establecen a través de líneas concedidas o de servicios de conmutación de paquetes como Frame Relay. Las conexiones con sucursales se establecen a través de medios conmutados (ISDN (RDSI) o módems analógicos), medios dedicados (líneas concedidas o Frame Relay) o Internet.

2.4 Beneficios y Ventajas

- Capacidad de compartir recursos (impresoras, escáner...) y posibilidad de conexión a Internet (acceso a la información de la red y a sus posibilidades comunicativas).
- Alojamiento de páginas web, tanto la del centro como de estudiantes o profesores, que pueden consultarse con los navegadores desde todos los ordenadores de la Intranet o desde cualquier ordenador externo que esté conectado a Internet.
- Servicios de almacenamiento de información. Espacios de disco virtual a los que se puede acceder para guardar y recuperar información desde los ordenadores del centro y también desde cualquier equipo externo conectado a Internet. Cada profesor y cada estudiante puede tener una agenda en el disco virtual.

- Servicio de correo electrónico, que puede incluir diversas funcionalidades (buzón de correo electrónico, servicio de webmail, servicio de mensajería instantánea...).
- Foros, canales bidireccionales de comunicación entre los miembros de la comunidad escolar, que permiten el intercambio de opiniones, experiencias... Algunos de estos foros pueden estar permanentemente en funcionamiento, y otros pueden abrirse temporalmente a petición de algún profesor, grupo de alumnos... Por ejemplo, tablones de anuncios y servicios de chat y videoconferencia.
- Instrumentos diversos que permiten, a las personas autorizadas a ello, la realización de diversos trabajos tales como gestiones de tutoría, plantillas que faciliten a profesores y alumnos la creación de fichas, test, periódicos; gestiones de secretaria y dirección; de biblioteca; y gestiones administrativas como petición de certificados, trámites de matrícula, notas de los estudiantes, etc.

2.5 Redes LAN

2.5.1 Introducción a las Redes LAN

Redes de comunicación, no son más que la posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información.

La generalización del ordenador o computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a

información en bases de datos remotas, cargar aplicaciones desde puntos de ultramar, enviar mensajes a otros países y compartir archivos, todo ello desde un ordenador personal.

Las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño e implantación de una red mundial de ordenadores es uno de los grandes 'milagros tecnológicos' de las últimas décadas.

2.5.2 Definición

LAN es la abreviatura de Network Area Local (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos para intercambiar recursos e información. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Todos los dispositivos pueden comunicarse con el resto aunque también pueden funcionar de forma independiente. Las velocidades de comunicación son elevadas estando en el orden de varios millones de bits por segundo dependiendo del tipo de red que se use. Es un sistema fiable ya que se dispone de sistemas de detección y corrección de errores de transmisión.

Dentro de una red local existen algunos ordenadores que sirven información, aplicaciones o recursos a los demás. Estos ordenadores se les conocen con el nombre de servidores.

Los servidores pueden ser dedicados o no dedicados:

Dedicados. Normalmente tienen un sistema operativo más potente que los demás y son usados por el administrador de la red.

No dedicados. Pueden ser cualquier puesto de la red que además de ser usado por un usuario, facilita el uso de ciertos recursos al resto de los equipos de la red, por ejemplo, comparte su impresora.

El creciente uso de las redes locales se debe al abaratamiento de sus componentes y a la generalización de sistemas operativos orientados al su uso en red. Con esto se facilita las operaciones de compartir y usar recursos de los demás ordenadores y periféricos.

2.5.3 Beneficios y Ventajas de una red local

Bien planificada e implementada, una red local aumenta la productividad de los PCs y periféricos implicados en ella. Si no se planifica y monta apropiadamente puede ser motivo de frustración y de pérdida de tiempo e información.

Algunas de las facilidades que nos abre el uso de una red local son:

- Compartir los recursos existentes: impresoras, módems, escáner, etc.
- Uso de un mismo software desde distintos puestos de la red.

- Acceder a servicios de información internos (Intranet) y externos (Internet).
- Intercambiar archivos.
- Uso del correo electrónico.
- Permite conexiones remotas a los distintos recursos.
- Copias de seguridad centralizadas.
- Simplifica el mantenimiento del parque de máquinas.

2.6 Seguridad Lógica

Nos referimos a seguridad lógica como los procedimientos existentes para controlar el acceso lógico no autorizado a la información, ya sea que se realice mientras ésta se encuentra almacenada o durante la transmisión.

Ejemplos de barreras de seguridad a nivel software (seguridad lógica):

- Cortafuegos.
- Antivirus.
- Antispam.
- Antispyware.
- Números de serie.
- Protección anti copia.

2.7 Mecanismos de Seguridad

Los mecanismos de seguridad son el tercer aspecto que se considera en la seguridad de la información.

Un mecanismo de seguridad es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o

recobrarse de un ataque de seguridad. Los servicios de seguridad especifican "qué" controles son requeridos y los mecanismos de seguridad especifican "cómo" deben ser ejecutados los controles.

Los mecanismos básicos pueden agruparse de varias formas. Conviene resaltar que los mecanismos poseen tres componentes principales:

1. Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
2. Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado y generación de números aleatorios.
3. Conjunto de procedimientos, que definen como se usaran los algoritmos, quien envía que a quien y cuando.

No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información. Los mecanismos pueden ser clasificados como preventivos, detectives, y recuperables.

2.7.1 Tipos de Mecanismos

2.7.1.1 Mecanismos de seguridad generalizados

Se relacionan directamente con los niveles de seguridad requeridos, es decir, a la administración de seguridad - y permiten determinar el grado de seguridad del sistema ya que se aplican a éste para cumplir la política general.

2.7.1.2 Etiquetas de seguridad

Se asocian a los recursos para indicar el nivel de sensibilidad, se trata de números que permiten graduar la sensibilidad de determinados datos clasificando la información por niveles de seguridad: secreta, confidencial, no clasificada, etc. Estas etiquetas pueden ser transmitidas con los datos o pueden estar implícitas. Ejemplos de etiquetas de seguridad implícitas son aquéllas implicadas en el uso de una clave específica para cifrar los datos.

2.7.1.2 Detección de eventos

Este mecanismo detecta movimientos peligrosos o normales dentro del sistema.

Seguimiento de auditorías de seguridad: El propósito de un seguimiento de auditoría de seguridad es probar qué tan adecuados son los controles del sistema para asegurar la complacencia de las políticas establecidas y los procedimientos operacionales.

2.7.1.3 Recuperación de seguridad

Realiza acciones de recuperación basadas en la aplicación de una serie de reglas. Las acciones de recuperación pueden ser inmediatas como la desconexión, temporales, invalidación temporal de una entidad o de largo plazo intercambio de clave.

2.7.1.4 Mecanismos de seguridad específicos

Los mecanismos de seguridad específicos definen la implementación de servicios concretos. Los más importantes son los siguientes:

2.7.1.4.1 Intercambio de Autentificación

El mecanismo de intercambio de autenticación se utiliza para verificar la supuesta identidad de quienes envían los mensajes y/o los datos, corroborando

así que una entidad, ya sea origen o destino de la información, es la deseada. Los mecanismos de este tipo pueden ser:

Fuertes: comúnmente llamados de autenticación fuerte porque emplean técnicas criptográficas propiedades de los sistemas criptográficos de clave pública para proteger los mensajes que se van a intercambiar. Un usuario se autentica mediante su identificador y su clave privada. Su interlocutor debe verificar que aquél, efectivamente, posee la clave privada, para lo cual debe obtener, de algún modo, la clave pública del primero. Para ello deberá obtener su certificado, un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el periodo de tiempo determinado, que asocia una clave pública a un usuario.

Débiles: generalmente llamados de autenticación simple ya que se basa en técnicas de control de acceso. El emisor envía su identificador y una contraseña al receptor, el cual los comprueba.

Este mecanismo funciona de la siguiente manera: se corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, la computadora A envía un número aleatorio cifrado con la clave pública de la computadora B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser.

2.7.1.4.2 Integridad de Datos

Los mecanismos de integridad de datos aseguran que los datos no sean alterados o destruidos. La manera en que funciona el mecanismo de integridad de datos implica el cifrado de una cadena (compactada) de datos a transmitir,

llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV).

Existen dos procesos para determinar la integridad de una unidad o campo de datos simples. El primer proceso genera un valor en la entidad emisora y lo adiciona a la unidad o campo de datos. Este valor es un código de verificación de datos o una cantidad criptográfica que se calcula en función de los datos y que se manda como información suplementaria. El segundo proceso genera el valor correspondiente de la unidad o campo de datos recibido en la entidad receptora, y lo compara con el valor recibido.

2.7.1.4.3 Firma Digital

La firma digital se puede definir como un conjunto de datos como códigos o claves criptográficas privadas que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello, se cifra la unidad de datos junto con alguna componente secreta del firmante, y se obtiene un valor de control ligado al resultado cifrado.

La manera en que funciona la firma digital se describe a continuación: para personalizar un mensaje, un determinado usuario A cifra un mensaje utilizando su clave secreta y lo envía al destinatario. Únicamente la clave pública de A (Alicia) permitirá descifrar el mensaje, por lo tanto, se comprueba que efectivamente A fue quien envió el mensaje. Un mensaje así puede ser descifrado por cualquiera que tenga la clave pública de A.

Una firma digital tiene las siguientes ventajas:

- La firma es auténtica: porque cuando un usuario usa una clave pública de A para descifrar un mensaje, él confirma que fue A y solamente A quien envió el mensaje.
- La firma no puede ser violada: porque solamente A conoce su clave secreta.
- El documento firmado no puede ser alterado: porque en caso de existir cualquier alteración en el mensaje cifrado, éste no podría ser restaurado (descifrado) con el uso de la clave pública de A.
- La firma no es reutilizable: debido a que la firma es una función del documento y no puede ser transferida para otro documento.

La firma digital, aunque tiene varias ventajas y cada usuario tenga un par de claves únicas, existe el riesgo de que se presente un ataque a la integridad de los datos. Para verificar que efectivamente el emisor envió el mensaje y utilizó su clave privada, existen las Autoridades de Certificación.

2.7.1.4.4 Control de Acceso

El mecanismo de control de acceso se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado, se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación. Este mecanismo soporta el servicio de control de acceso y está muy ligado a la autenticación y confianza.

Detrás de este mecanismo de seguridad es importante la “confianza”. En el mundo de la red, la “confianza” es la capacidad para autenticar a las compañías y a los individuos que intercambian información a través de la red.

2.7.1.4.5 Tráfico de Relleno

También conocido como mecanismo de relleno de tráfico - es un mecanismo que provee una generación de tráfico falso.

Se llaman rellenos porque consisten en generar eventos de comunicación, unidades de datos y datos falsos, en forma semi-aleatoria, con el fin de "confundir" a un analizador de tráfico. Lo que hace el tráfico de relleno es generar una salida de texto cifrado continuamente, incluso en ausencia de texto original, de este modo es imposible que un atacante distinga entre el flujo de datos verdadero y el ruido, con lo que resulta imposible deducir la cantidad de tráfico real.

El mecanismo de tráfico de relleno puede ser utilizado para proveer varios niveles de protección contra el análisis de tráfico.

2.7.1.4.6 Control de Encaminamiento

También es conocido como control de ruta, está destinado a seleccionar de manera física cada una de las rutas alternativas que pueden utilizarse según el nivel de seguridad y la información que se esté transmitiendo es decir, este mecanismo de seguridad cubre todos los aspectos de la ruta que siguen los datos en la red.

El control de encaminamiento, durante el proceso de conmutación, selecciona para una cierta comunicación determinados enlaces, redes o repetidores, buscando una mayor confidencialidad, para esto se lleva a cabo una recodificación de rutas y tablas del sistema para evitar líneas o máquinas comprometidas. Cualquier mecanismo de control de encaminamiento se usa para lograr la selección dinámica o pre-establecida de rutas específicas para la transmisión de datos, por esto, a los datos con determinadas etiquetas de seguridad se les prohíbe pasar por ciertas subredes o

líneas. Algunos mecanismos, más sofisticados, de este tipo incluso reaccionan ante la insistencia de ataques a una ruta determinada, dejando esta ruta fuera de las posibles selecciones.

2.8 Implementación de políticas de seguridad

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática

debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de

informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el administrador es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

2.9 Software Libre

El software libre es el software que no esconde su código, lo deja libre, permite su libre distribución. Esto permite que en los países no tan desarrollados, no se tenga que reinventar la rueda, ya que para crear software se ocupan algoritmos básicos, que pertenecen a toda la humanidad, por lo cual no deben ser patentados.

La generalización de la Informática en las actividades genéricas y corrientes del ser humano ha traído consigo una serie de limitaciones impuestas por los esquemas tradicionales de actuación que han planteado (y aún actualmente plantean) grandes problemas.

Por ejemplo, el esquema tradicional de patentes y otras restricciones se adecúan muy poco a cosas tan mentales o etéreas como el soporte lógico informático (también llamado software).

Evidentemente, el software, en tanto a mero soporte intelectual, tiene un componente radicalmente distinto a aquellas invenciones implementadas de forma 'física' (desde el soporte físico informático o hardware hasta un coche o una lavadora). Este es que, a diferencia de los nuevos diseños físicos, tiene una copia mucho más fácil, y, además, dada su naturaleza cognoscitiva o intelectiva, esta facilidad de copia es un atributo propio del propio 'invento lógico'. Además, la copia no altera en absoluto el original.

Precisamente, por la necesidad de superación de ciertas limitaciones, aparece el Software Libre, aquel que garantiza una reproducción y copia legal (tanto parcial como totalmente), al mismo tiempo que permite el acceso a su código fuente para poder mejorar ese soporte lógico. Grado de desarrollo: 00% (a fecha de 19:04 19 oct, 2005 (UTC))

2.9.1 Licencias en Software Libre

Estrictamente hablando, lo que diferencia al software libre del resto del software es un aspecto legal: la licencia. Se trata, en palabras de uso común, de un contrato entre el autor (o propietario de los derechos) y los usuarios, que estipula lo que los éstos pueden hacer con su obra: uso, redistribución, modificación, etc., y en qué condiciones.

Aunque en esencia software libre y software propietario se diferencien en la licencia con la que los autores publican sus programas, es importante hacer hincapié en que las diferencias entre las diferentes licencias, aunque puedan parecer nimias, suelen suponer condiciones de uso y redistribución totalmente diferentes y, como se ha podido demostrar a lo largo de los últimos años, han desembocado no sólo en métodos de desarrollo totalmente diferentes, sino incluso en una forma alternativa de entender la informática.

2.9.2 Tipos de software

- Software propietario: la copia y distribución es un delito.
- Shareware: tras un periodo de prueba es necesario pagar.
- Freeware: permiten la copia y distribución.
- Software libre: permiten la copia, distribución, modificación y posterior redistribución del software modificado.

2.9.2 Desarrollo de software libre GNU

- GNU: Acrónimo recursivo para "Gnu's Not Unix" (Software basado en el sistema informático Unix, pero no propietario).

- Soft desarrollado por una comunidad, sin ánimo de lucro. Estás invitad@ a participar en la lista de tareas GNU (Software necesario, aún por desarrollar).
- No se debe pagar por el permiso de usarlo.
- Distribuye el código fuente (el programa escrito, sin compilar) para que, el que sepa, pueda modificar el programa según sus necesidades.
- El software propietario sólo se distribuye en binarios, listo para usar en el ordenador. Mientras que WIN y MAC mantienen el código fuente de sus sistemas operativos en secreto (sino serían también libres), GNU/Linux lo hace público.
- GNU/Linux: En 1991 Linus Torvalds programa un núcleo compatible con Unix; la combinación con soft GNU crea en 1992 el primer sistema operativo libre completo.

2.9.3 Beneficios del Software Libre

En la ética

El Software Libre tiene sus bases en una ideología que dice el software no debe tener dueños, es un asunto de libertad: la gente debería ser libre de usarlo en todas las formas que sean socialmente útiles.

De esta forma, el movimiento del Software Libre pone lo que es beneficioso para la sociedad por encima de los intereses económicos o políticos.

Entre los beneficios que percibe la sociedad podemos mencionar:

- Tecnologías transparentes, confiables y seguras.
- Tecnologías como bien público.

- Promoción del espíritu cooperativo, en el que el principal objetivo es ayudar a su vecino.
- Precios justos.

En la práctica

El Software Libre ofrece a las personas la posibilidad de utilizar, estudiar, modificar, copiar y redistribuir el software. Para hacer efectivas estas libertades, el código fuente de los programas debe estar disponible.

Gracias a estas libertades obtenemos muchos beneficios prácticos:

- Podemos ejecutar el software cuando queramos y para lo que queramos.
- Podemos aprender de los programas existentes.
- Podemos mejorarlos.
- Podemos adaptarlos para que se ajusten a nuestras necesidades.
- Podemos basarnos en ellos, de forma que evitamos los costos adicionales de empezar un programa desde 0.
- Podemos formar negocios alrededor de la creación, distribución, soporte y capacitación de programas libres.

Y el efecto de todos estos beneficios es la formación de Comunidades enormes alrededor de proyectos de software libre, gracias a las cuales tenemos acceso a desarrolladores, documentadores y testers de todo el mundo.

Este estudio realizado sobre una distribución de Linux indica que el sistema para el 2001 contenía 30 millones de líneas de código fuente, y que su desarrollo hubiera

costado $1000 millones y 8000 años persona, siguiendo las etapas tradicionales del desarrollo de software propietario.

CAPITULO III

3 MARCO INVESTIGATIVO

Se ha realizado una visita técnica a la “Escuela Superior Militar Eloy Alfaro” y a la Super Intendencia de Telecomunicaciones, para poder obtener suficiente información de su red corporativa y su forma de administrarla, obteniendo así la siguiente información.

3.1 Entrevista al administrador de la red del ESMIL

Actualmente el ESMIL está constituido por la siguiente distribución:

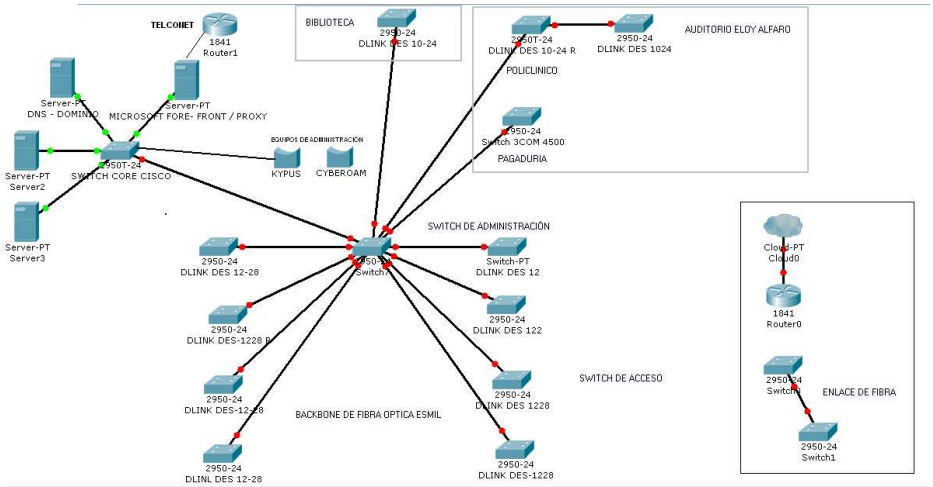

Figura III.03: Infraestructura de red del ESMIL

La administración de la red es realizada por el Departamento de Servicios Informáticos.

La administración y políticas de seguridad se verán en al ANEXO1.

3.2 Entrevista al departamento Administrativo y técnico de la SENATEL

La Secretaría Nacional de Telecomunicaciones actualmente está constituida por Departamentos, los cuales se encuentran distribuidos en cada piso de la infraestructura, para una administración más fácil de la red global se han dividido estos Departamentos dentro de VLANs por medio de la dirección física de cada uno de los equipos implementados en los puestos de trabajo.

La administración de la red es realizada por el Departamento de Servicios Informáticos de la SENATEL, en donde se encuentran todos los equipos como: Servidores, Routers, Switches, y las aplicaciones para distribuir los diferentes servicios a todos los funcionarios de la SENATEL.

Estas VLAN"s manejan un alto nivel de encriptación de seguridad por la importancia de datos que se maneja dentro de la Institución, para certificar la legitimidad de los documentos; los Directores de cada Departamento fueron provistos de llaves los cuales insertan una firma digital única de cada funcionario cuando se envían hacia distintas instituciones.

Dentro de la SENATEL se han elaborado de esta manera cada una de las VLANs de acuerdo a como se distribuyeron los departamentos y puestos de trabajo en cada uno de ellos.

A continuación se muestra la disposición de cada una de las VLANs que se han creado de acuerdo a los pisos y a los departamentos dentro de la Secretaría Nacional de Telecomunicaciones.

3.3 Investigación de una Red Corporativa

3.3.1 Arquitectura Jerárquica

Cuando se diseña una red, con el fin de evitar mayores problemas en recursos y administración se aplica un modelo de diseño jerárquico, esto implica en dividir en capas jerárquicas a la red para que el rendimiento y la escalabilidad.

A continuación se indica la manera de cómo dividir una red en tres capas.

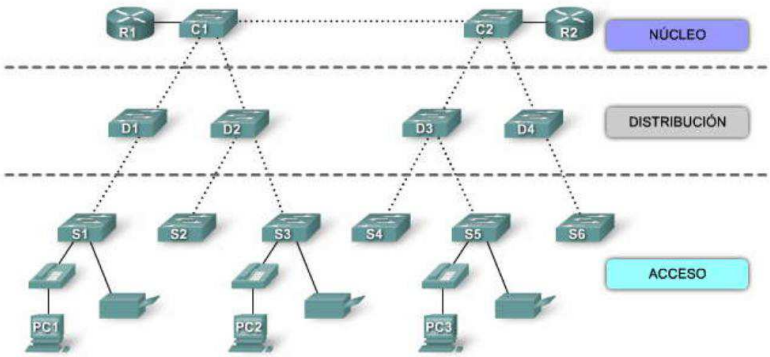

Figura III.04: Arquitectura Jerárquica

3.3.2 Capa de Acceso

Esta capa de acceso es la manera de cómo llegar hacia los dispositivos finales de la red y controlar los equipos que se pueden comunicar a la red.

Hace interfaz con los dispositivos finales como son impresoras, scanner, teléfonos IP y hosts para permitir el acceso al resto de la red.

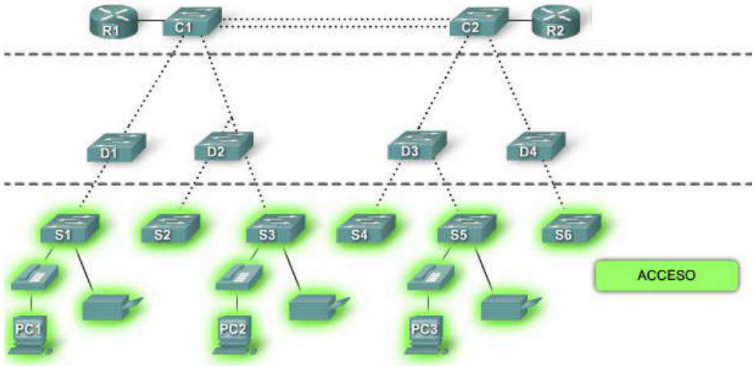

Figura III.05: Capa de Acceso

3.3.3 Capa de Acceso

La capa de distribución es aquella que controla el flujo de la información entre la capa de acceso y la capa de núcleo, este control se lo realiza por medio de políticas y dominios de broadcast en el enrutamiento de las funciones de las respectivas VLAN‟s que se hayan conformado en la red. En esta capa se agrega la información que entregan los switches de la capa de acceso que van a ser enrutados en la capa de núcleo para que lleguen hasta su destino final.

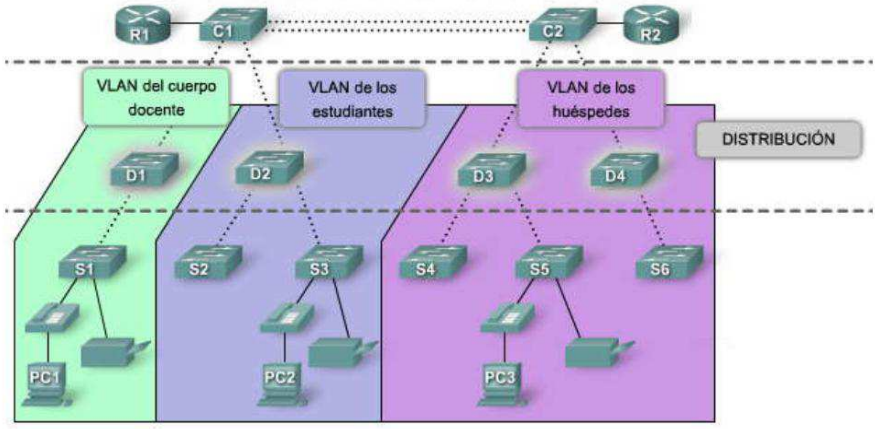

Figura III.06: Capa de Distribución

3.3.4 Diseño de redes Jerárquicas

Para poder diseñar redes jerárquicas hay que tomar en cuenta parámetros previos tales como el diámetro de la red, agregado de ancho de banda y redundancia

Diámetro de la red

El diámetro de la red es la cantidad de equipos que debe cruzar un paquete para llegar hacia el destino, si el diámetro de la red es bajo se puede asegurar una latencia baja entre los equipos interconectados.

3.3.5 Agregado de ancho de banda

Este parámetro puede ser aplicado en cualquiera de las capas jerárquicas, se deben conocer los valores necesarios de ancho de banda para poder implementar enlaces entre los switches previamente determinados para combinar los enlaces de puerto de múltiples switches para aumentar el rendimiento.

3.3.6 Redundancia

El buscar redundancia en una red indica que siempre debe estar disponible, para esto se pueden incrementar los enlaces entre los equipos o aumentar los equipos por lo que buscar mayor redundancia es más costoso de acuerdo al tamaño de la red.

3.3.10.1 Análisis del flujo de tráfico

Es el proceso de medición del ancho de banda que se utiliza así como de los datos para mejorar el rendimiento y tomar las mejores decisiones en la parte física.

En la actualidad no existe una definición concreta sobre el flujo de tráfico por lo que se lo define como la cantidad de paquetes en un determinado tiempo. Todos los paquetes son tomados en cuenta para este análisis sin importar el propósito que cumplan.

Para controlar el flujo de tráfico en la red se pueden manipular los puertos del Switch con el fin de gestionar el ancho de banda a los caminos por donde existe mayor cantidad de congestión de datos.

3.3.10.2 Análisis de comunidades de usuario

Este análisis es aquel para identificar los grupos establecidos y el uso que cada uno de ellos le da a la red. Esto conlleva a determinar la selección de equipos cuando se realiza el diseño de una red, ya que de acuerdo a las tareas que cada usuario realiza y el tráfico que lleva, se determinaran los dispositivos para conformar la red.

Siempre se debe analizar para un crecimiento a futuro de la red y que siga manteniendo las mismas prestaciones a todos los usuarios, para esto se debe observar en base a años anteriores ya que debe mantener una constante de crecimiento para seleccionar los switches necesarios.

3.3.10.3 Almacenamiento de datos y servidores de datos

Los medios de almacenamiento de datos pueden ser de varios tipos como servidores, redes SAN, almacenamiento adjunto a redes (NAS), o cualquier otro que tenga la capacidad de almacenar grandes cantidades de datos.

Aquí se debe tomar en cuenta el análisis de flujos de tráfico ya que varios equipos solicitan información de los servidores produciendo que haya congestiones en la red, por lo que el ancho de banda y tasas de reenvío son importantes para tratar de solucionar este problema.

El tráfico que se origina entre los dispositivos de almacenamiento pueden ocupar grandes volúmenes de tráfico y una manera de optimizar esto es que estos equipos se encuentren a distancias cortas para disminuir el tráfico entre ellos y no afectar al resto de la red.

3.3.11 Métodos de conmutación

En la conmutación de paquetes el switch establece un enlace de comunicación entre dos tramas durante el tiempo necesario para el envío de paquetes.

Existen 3 métodos para llevar a cabo el proceso de conmutación de paquetes:

- Store and forward (Almacenamiento y envío)
- Cut through (pasar a traves)
- Adaptative Cut through (cortar y enviar adaptativo)

3.3.11.1 Store and forward

En este modo los paquetes previo a ser enviados son guardados en un buffer, hasta que se revise si se tienen errores de redundancia cíclica denominados CRC, para lo que se recibe un flujo de datos de cualquier trama de entrada y devuelve una longitud fija de salida, si encuentra un error en la trama esta será descartada, caso contrario si no detecta errores verifica la dirección MAC de destino y envía el paquete.

Requiere de un mayor tiempo para poder verificar las tramas por lo que el delay será cada vez más grande.

3.3.11.2 Cut Through

Aquí se busco reducir el tiempo de verificación de las tramas, solamente se verifican los primeros 6 bytes de la trama e inmediatamente se procede a enviar el paquete hacia su destino.

Los switches que utilizan este método no pueden detectar si hay errores en las tramas ocasionados por colisiones de las tramas o CRC‟s, por tanto el ancho de banda será cada vez mayor para encaminar los paquetes que contienen errores.

3.3.11.3 Adaptative Cut Through

Este método soporta cualquiera de los dos métodos mencionados anteriormente. Esto puede ser configurado mediante el administrador o por el mismo switch si está en capacidad de hacerlo dependiendo de las tramas errores que pasan por los puertos.

Cuando se establece un cierto nivel de margen de paquetes errados se puede cambiar el modo de conmutación a store and forward y cuando el tráfico se normalice y disminuyan estos paquetes corruptos volver al modo de cut through.

3.3.12 VLANs

Las VLANs son redes locales que agrupan a ciertos equipos de manera lógica, está conformada por varios dispositivos como hubs, routers, switches para conformar una subred mediante software y además tiene su propio dominio de broadcast.

Es una agrupación lógica de puertos dentro de un switch para formar una red LAN independiente, que supera el inconveniente de la agrupación geográfica de los equipos y que se crea la segmentación de acuerdo a los criterios que el administrador necesite.

A continuación se puede observar la diferencia entre una LAN tradicional y una VLAN para el mismo propósito.

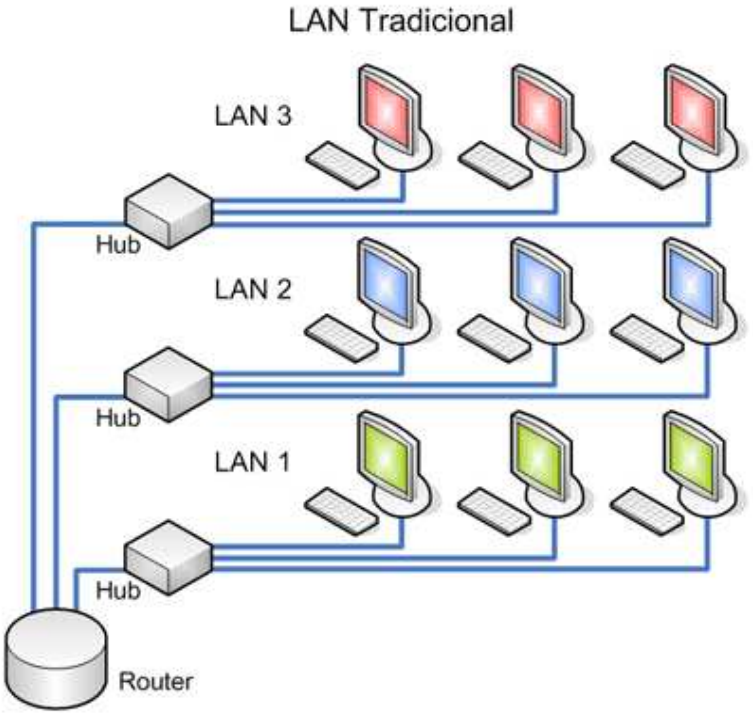

Figura II.07: Diseño de una Red LAN básica

La implementación de VLANs se la emplea mediante switches, esto permite un control más inteligente en lo que refiere a tráfico ya que puede aislarlo dando como resultado un incremento en la eficiencia de la red.

Cuando se distribuyen los diferentes usuarios a los respectivos grupos se lo hace mediante segmentación lo que ocasiona un incremento del ancho de banda en dichos grupos.

3.3.12.1 Segmentación

La segmentación es la creación de dominios para los grupos de trabajo mediante la conexión física de los equipos y servidores a los puertos del switch, teniendo una conexión dedicada hacia la red.

Esta es una ventaja considerable ya que reduce el tráfico dentro de la red, porque solo se transmiten los paquetes que están dentro del dominio de la VLAN, un mejor ancho de banda así como la confidencialidad de los datos, y una disminución de la latencia.

Para comunicar los switches que comunican las VLAN se utiliza el proceso denominado Trunking, el protocolo encargado de llevar esto acabo es el VTP (VLAN Trunking Protocol).

3.3.12.2 Clasificación de las VLANs

Existen diversos tipos de VLAN‟s, están pueden ser diseñadas de acuerdo a lo que el administrador así lo requiera, tales como:

- VLAN de puerto central
- VLAN estáticas
- Por puerto
- Por dirección MAC
- Por protocolo
- Por dirección IP
- Por nombre de usuario
- VLAN dinámicas (DVLAN)

VLANs de puerto central

Son aquellas que unen sus nodos en un puerto común del switch.

VLANs estáticas

Se encuentran previamente definidas por el administrador, los puertos del switch están asignados a una única estación de trabajo.

VLANs por puerto

Se definen de acuerdo a los puertos del switch para establecer los grupos de trabajo, a continuación se indica cómo se distribuye de acuerdo a los puertos las VLANs respectivas.

TABLA Nº I: Configuración VLAN mediante puerto

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3
7	1
8	2
9	3

VLANs por dirección MAC

Se establecen los grupos de trabajo de acuerdo a la dirección física de la estación de trabajo.

TABLA Nº II: Configuración VLAN mediante dirección MAC

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

VLANs por protocolo

En base a la forma de comunicación, el switch va agrupando los equipos para formar los grupos de trabajo.

TABLA Nº III: Configuración VLAN mediante protocolo

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

VLANs por dirección IP

Se basa en el encabezado de la capa 3 del modelo OSI, esto no quiere decir que actúe como router, sino que únicamente realiza una inspección de las direcciones autorizadas a ingresar a la red, conlleva un gran ahorro de tiempo debido a que no se debe configurar nuevamente el switch y la dirección IP de la estación siempre será la misma

CAPITULO IV

4 EVALUACION DE LAS SOLUCION NETWORK ACCESS CONTROL DE SOFTWARE.

4.1 SOLUCION DEL PROBLEMA

4.1.1 ALTERNATIVAS DE CODIGO ABIERTA

Las comunidades NAC de código abierto aportan dos ventajas clave comunes a todas las comunidades de software libre:

1. La capacidad para encontrar fallas de seguridad rápidamente gracias al espíritu de colaboración con el que trabajan
2. La ampliación progresiva de características y funcionalidades a medida que crece la demanda.

En la lista de proveedores de código abierto N.A.C. :

4.2 FreeNAC

Desarrollado por Swisscom, el operador dominante de Suiza. Su versión comercial incorpora algunas características no disponibles en la versión de código abierto que se pueden conseguir por una tasa de suscripción que incluye instalación y soporte. El servicio se dirigía inicialmente a empresas con infraestructuras heterogéneas sin actualizar, como switches sin soporte de autenticación de puerto 802.1x, una exigencia de muchos productos NAC convencionales. Sin embargo, FreeNAC, que, como otras herramientas de código libre, comenzó utilizando VMPS de Cisco para reforzar políticas, ahora también soporta 802.1X cubriendo así, además, entornos mixtos en proceso de actualización a soluciones comerciales.

Un switch detecta una nueva PC y pide la autorización de FreeNAC, que comprueba su base de datos y se niega o concede el acceso a la red basado en la dirección MAC. FreeNAC es una versión muy mejorada de "OpenVMPS" y directamente puede sustituir a otras soluciones VMPS con importantes mejoras en la facilidad de uso.

Se clasifican en dos grupos:

Clienless no necesita de ningún software instalado en los dispositivos

Client-based un componente de software es pre instalado en los dispositivos para poder asistir al proceso de NAC

Figura IV.08: Figura: Logo FreeNAC

Contiene numerosas funciones para ayudar al administrador con el manejo y puesta en marcha de redes virtuales, al mismo tiempo que proporciona control de acceso a redes.

Las características principales son:

- Asignación dinámica de redes virtuales
- Control de acceso a redes
- Flexibilidad en mecanismos de autentificación para redes: 802.1x, VMPS, Cisco Mac-Auth-Bypass
- Altamente automatizado
- Redundancia y repartición de carga de red para una mejor disponibilidad
- Inventario en tiempo real de los aparatos conectados a la red
- Documentación del cableado de la red
- Reportes flexibles

La edición comunitaria se puede descargar gratuitamente; la versión Empresarial provee características adicionales, como se detalla a continuación:

Tabla I: Tabla comparativa FreeNAC

Comparación de características	Comunitaria	Empresarial
Autentificación basada en dirección MAC (VMPS mac-auth-bypass)	✔	✔
Interfaz de usuario Windows	✔	✔
Interfaz de usuario basada en Web	✔	✔
Integración inteligente de hubs		✔
Comprobación de puertos abiertos e identificación del sistema operativo en los dispositivos		✔
Inventario automatizado de nombres de computadoras		✔
Soporte para el manejo de máquinas virtuales	✔	✔
Asignación de redes virtuales dependiendo de la localización del switch		✔
Scripts para ayudar en la importación inicial de sistemas desde un archivo CSV		✔
Alertas de eventos claves del sistema		✔
Detección automática de dispositivos no manejados activamente por NAC, para proporcionar un inventario completo de los dispositivos en la red		✔
Integración con servidores SMS de Microsoft (Software package/gestión del sistema)		✔
Herramienta web para ayudar en documentar la localización de cables/puertos de switches		✔
Herramienta de "paro" de emergencia la cual puede desactivar NAC y rápidamente configurar redes virtuales estáticas en los puertos del switch (recuperación en un desastre o en una situación extrema)		✔
Módulos personalizados para entornos de clientes específicos (por ejemplo, interfaces a sistemas corporativos "estáticos" de inventario)		✔
Soporte prioritario de parte del equipo FreeNAC		✔

La **edición comunitaria** se puede descargar gratuitamente; la **versión Empresarial** provee características adicionales, como se detalla a continuación:

Con FreeNAC, tan pronto como un nuevo dispositivo es conectado al puerto del switch, su dirección MAC se pasa al servidor, donde será almacenada y comprobada para determinar si este dispositivo tiene acceso a la red. Si el dispositivo está autorizado a tener acceso, el servidor le regresará al switch la red virtual a la que este dispositivo pertenece.

Si este dispositivo todavía no está registrado, su acceso es bloqueado o se coloca en una red virtual limitada, dependiendo de la política.

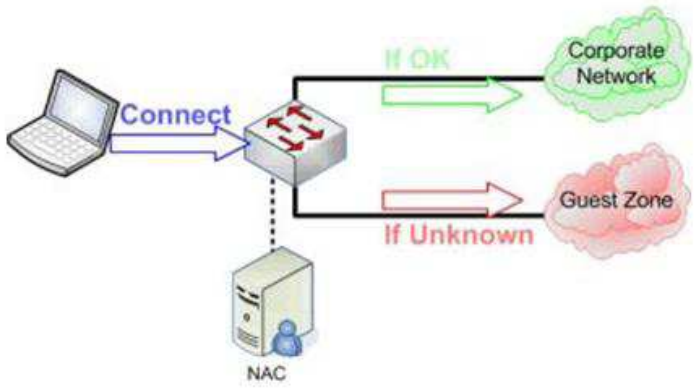

Figura IV.09: Direccionamiento de VLAN con FreeNAC

4.3 Conexión entre los sistemas operativos

FreeNAC por defecto viene configurado para utilizar el modo bridge el cual es necesario para estar corriendo activamente en la red y para recibir paquetes en una dirección IP dedicada.

Automáticamente el momento de instalar la aplicación de máquinas virtuales este asigna una dirección IP al adaptador de Ethernet de la red y en base a esta se procederá a configurar el adaptador Ethernet de la máquina virtual para que se encuentren dentro de la misma red y poder establecer la comunicación entre los dos sistemas operativos

A continuación se muestra la configuración de la interfaz de Windows para el dispositivo Ethernet y del cual se debe configurar el de la máquina virtual

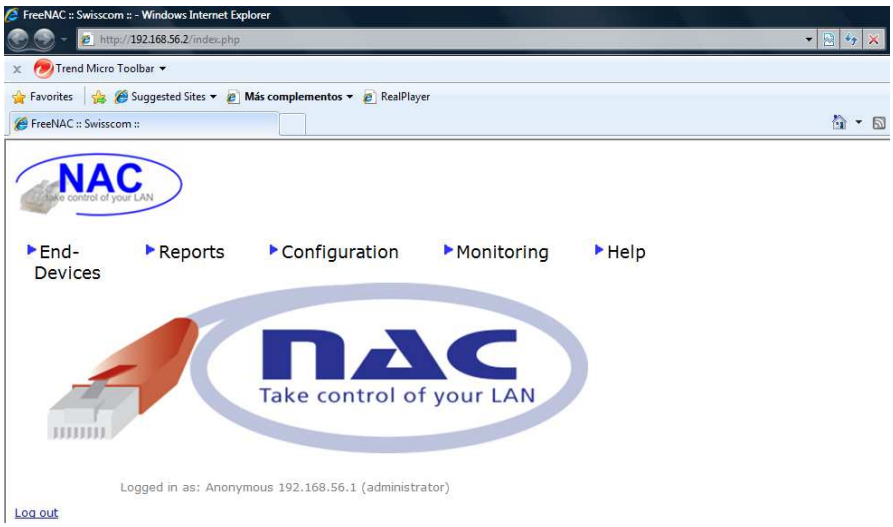

Figura 10: Interfaz WEB FreeNac

Aquí se podrá observar todos los parámetros con los cuales el servidor trabajará con la red, así como de varias opciones como dispositivos conectados, switches, routers, direcciones permitidas, rendimiento del sistema entre otros, lo primero será revisar la configuración global que abarca todos los parámetros principales.

Para poder modificar todos estos valores, se lo podrá hacer únicamente mediante la interfaz de Windows la cual se configurará más adelante.

4.4 Configuración de la base de datos (MySQL)

Inicialmente se deberá asegurar que mysql comience de forma automática cada vez que se inicia el servidor, en el sistema operativo con el que se está trabajando se lo hace mediante:

update-rc.d mysql defaults

Para acceder con mayor brevedad hacia el directorio de la base de datos mysql se establece un enlace simbólico que apunte hacia esta dirección, por ejemplo /var/lib/mysql, esto con el fin de agilitar el acceso hacia este directorio.

Archivo de configuración (my.cnf)

Este es el archivo encargado de iniciar la base de datos y contiene los datos de quienes pueden acceder a la base de datos, el nombre de la base de datos que va a ejecutar, el puerto por el cual va a escuchar entre otras.

En la máquina virtual existen dos archivos que se encuentran en dos rutas diferentes y que deben contener los mismos datos, ya que podrían existir conflictos el momento de la conexión y el servidor no trabajará.

Las direcciones donde se encuentra este archivo son:

/etc/mysql/my.cnf

/opt/nac/contrib/etc/my.cnf

Dentro de este archivo se deben revisar los siguientes parámetros:

```
log-bin = vmps1-bin
log-warnings
report-host = vmps1
server-id       = 10                    [10 for master, 20 for slave1, 20 for slave 2 etc..]
relay-log=vmps1-relay-bin
replicate-do-db= opennac
replicate-wild-ignore-table= opennac.vmpsauth%
```

Figura IV.11: Parámetros de configuración de archivo my.cnf

El parámetro server-id se indica a través de un número indicando cual es el servidor maestro y cuáles son los secundarios, en este caso 10 es para el servidor maestro y tiene el nombre de vmps1. Además se debe tener en cuenta el incremento de los

tiempos de espera para evitar una desconexión en redes de tráfico bajo, se agrega lo siguiente:

```
interactive_timeout = 604800
wait_timeout = 604800
```

Figura IV 12: Tiempos de espera

Incremento de tiempo de espera MySQL tiene que escuchar a la red a través del puerto 3306 (por defecto de MySQL), pero podría estar vinculado únicamente para localhost (parámetro por defecto de Ubuntu) por lo que dentro del archivo se deberá comentar este comando:

```
#bind-address = 127.0.0.1
```

Figura IV.13: Dirección local

Cada servidor puede insertar datos a nivel local, los cambios se replican en otros servidores y estos no entran en conflicto. Los conjuntos de datos deben ser configurados mediante las teclas de autoincremento y este valor deberá ser diferente en cada uno de los servidores, esto con el fin de evitar conflictos de replicación.

Si el valor fuera de 5 significa que permite un máximo de 5 servidores, cada servidor deberá tener un valor de auto incremento de desplazamiento diferente (1 para el principal, 2 para el segundo, etc).

4.5 Dirección IP

En nuestra virtualización asignamos la dirección Ip de nuestro servidor

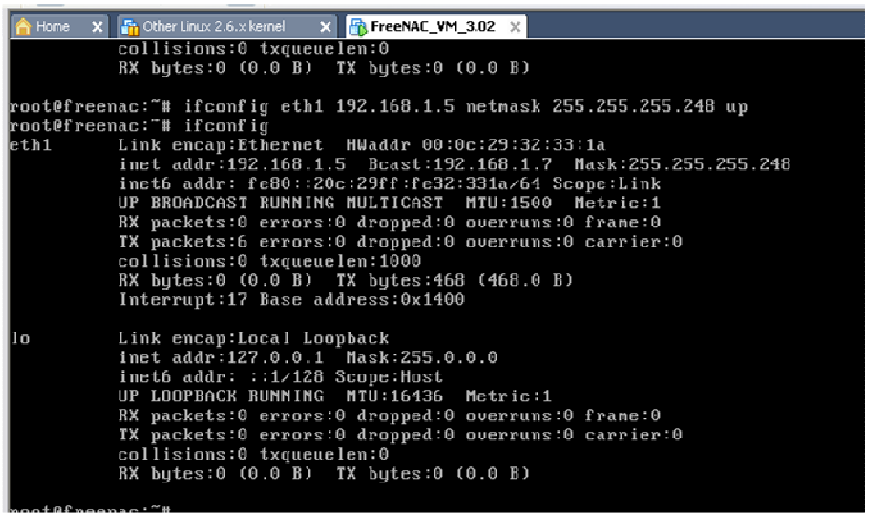

Figura IV.14: Asignación de IP

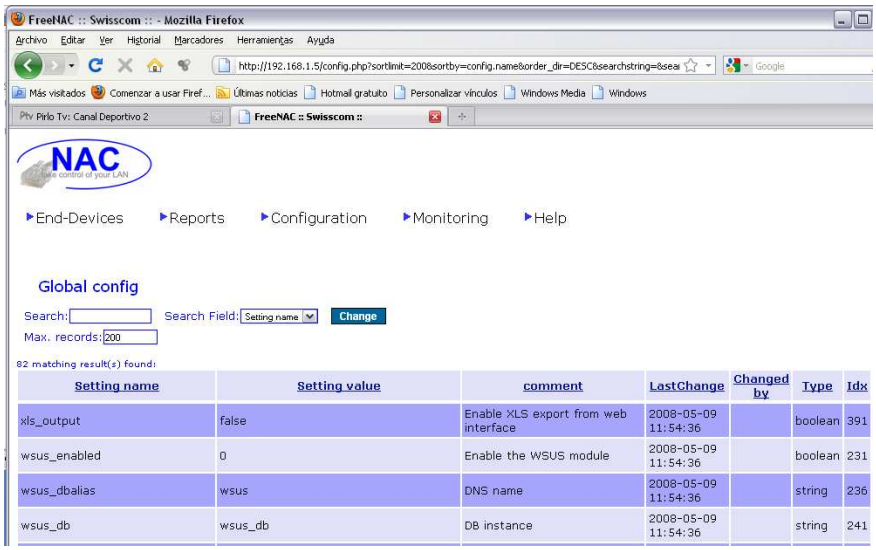

Figura IV.15: Portal WEB NAC

Un switch detecta una nueva PC y pide la autorización de FreeNAC, que comprueba su base de datos y se niega o concede el acceso a la red basado en la dirección MAC. FreeNAC es una versión muy mejorada de "OpenVMPS" y directamente puede sustituir a otras soluciones VMPS con importantes mejoras en la facilidad de uso.

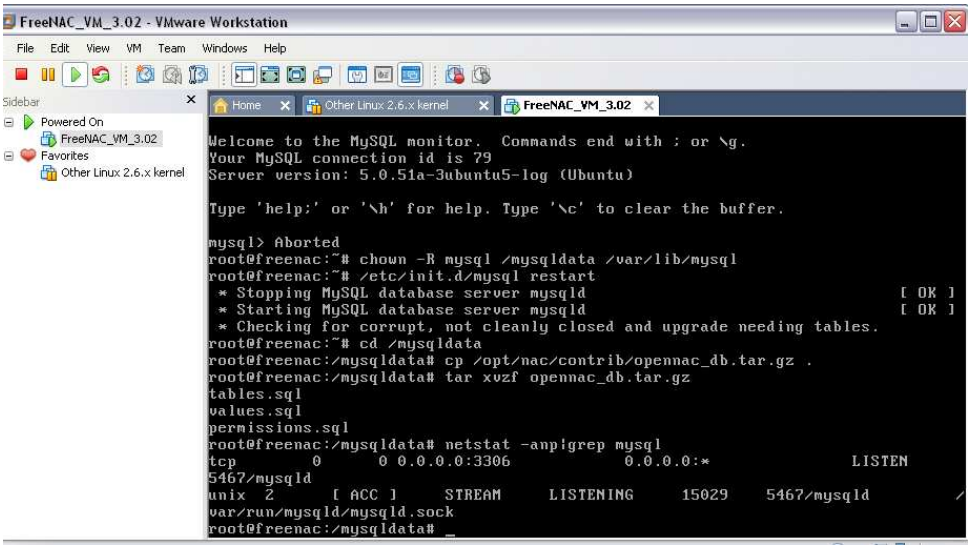

Figura IV.16: Ingreso a FreeNAC

4.6 Asignación de claves

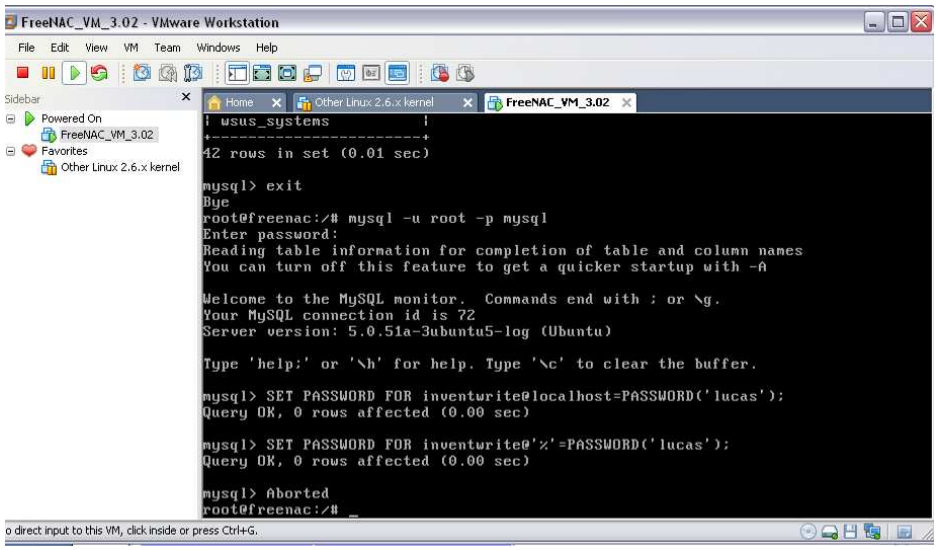

Figura IV.17: Claves FreeNAC

4.8 Edición del archivo config.inc

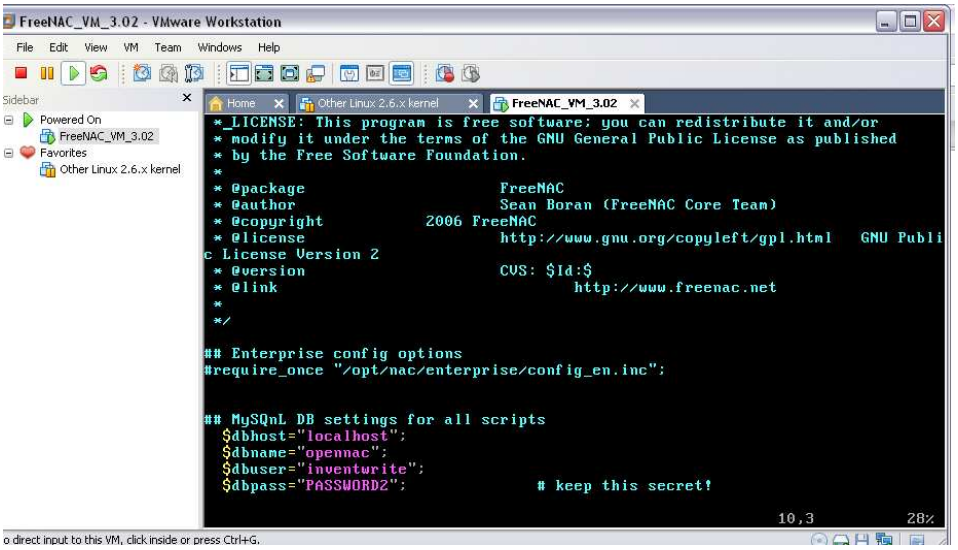

Figura IV.18: Archivo config.inc

4.9 Inicialización de la interfaz de usuario

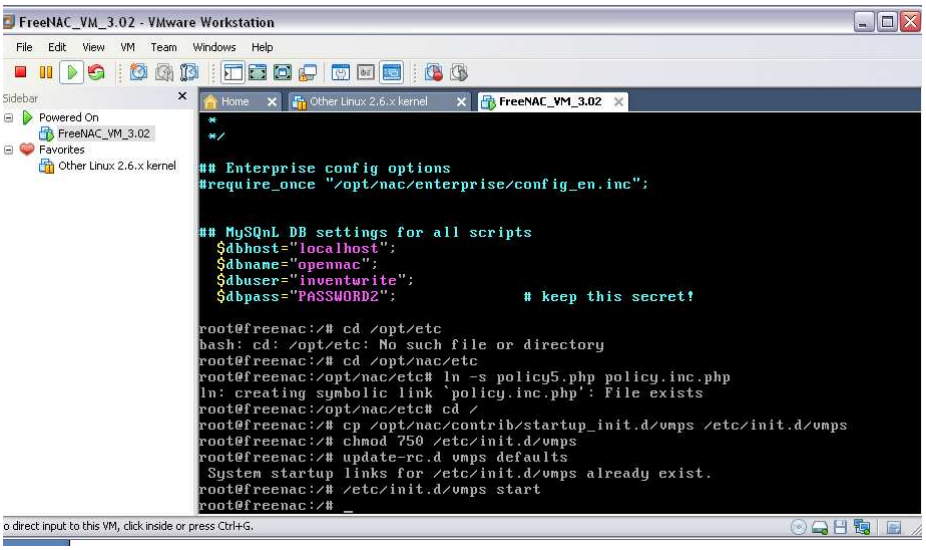

Figura IV.19: Interfaz de Usuario

4.10 Verificación del usuario invetwrite

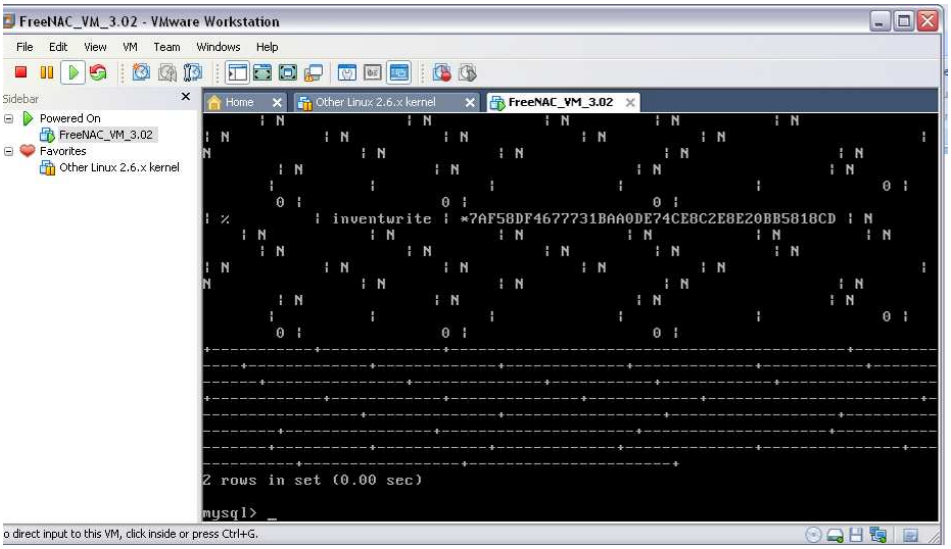

Figura IV.20: Usuario Inventwrite

4.11 Encriptacion de clave usuario root

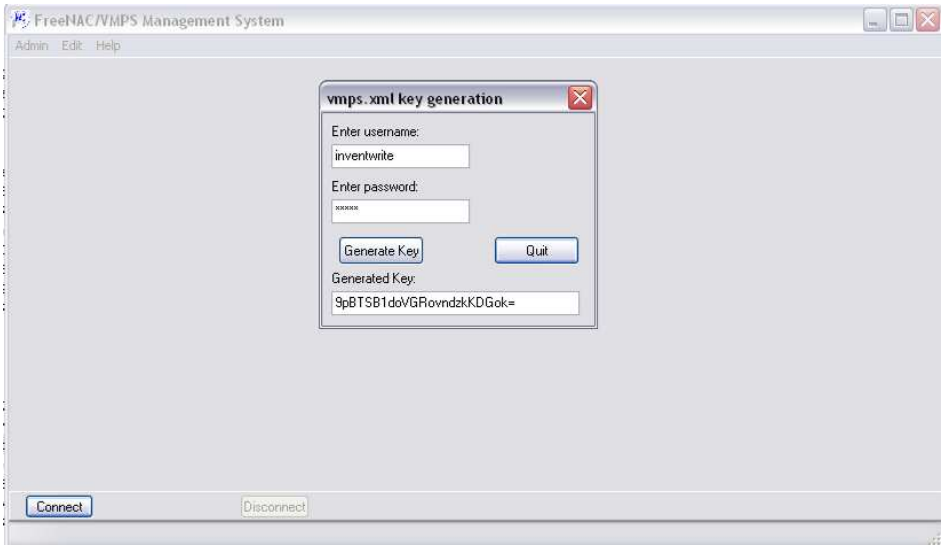

Figura IV.21: Usuario Root

4.12 Ingreso de la clave encriptada al archivo vmps.xml

Figura IV.22: Archivo vmps.xml

4.13 Creacion usuario opennac

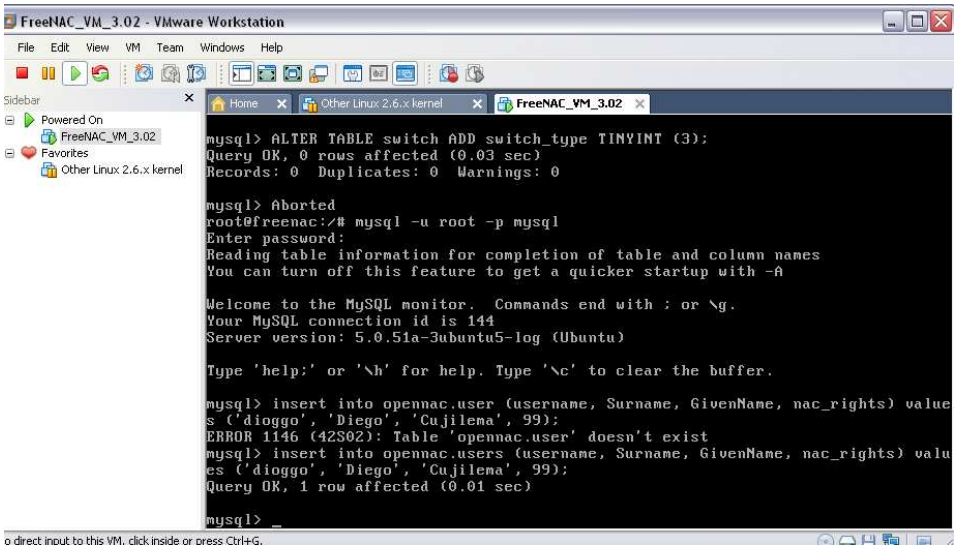

Figura IV.23: Usuario OpenNAC

4.14 Ingreso a la interfaz de usuario

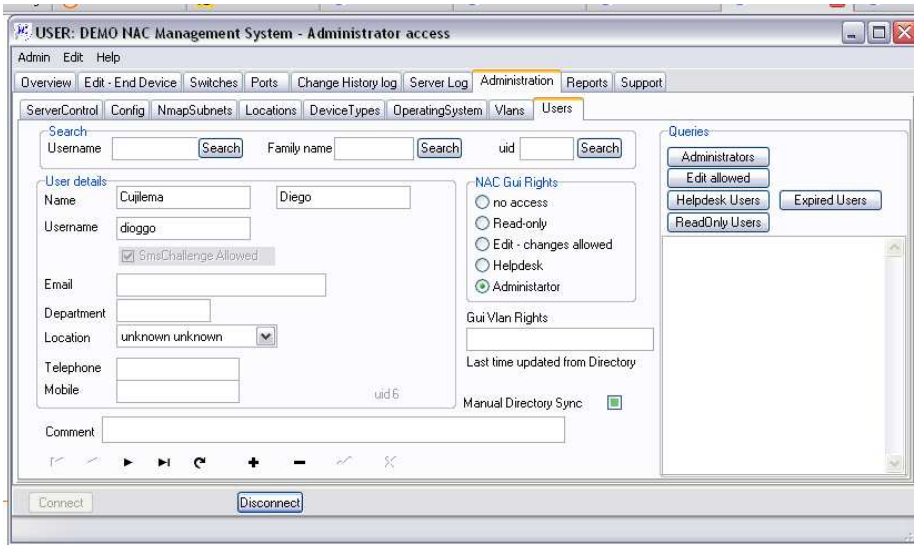

Figura IV.24: Interfaz de usuario

4.15 Error de conexión 1

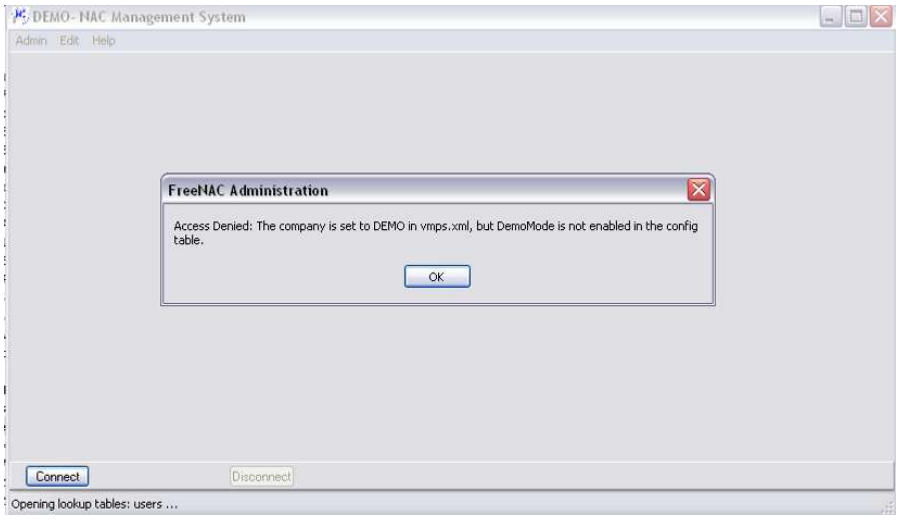

Figura IV.25: Error 1 de conexiòn

4.16 Error de conexión 2

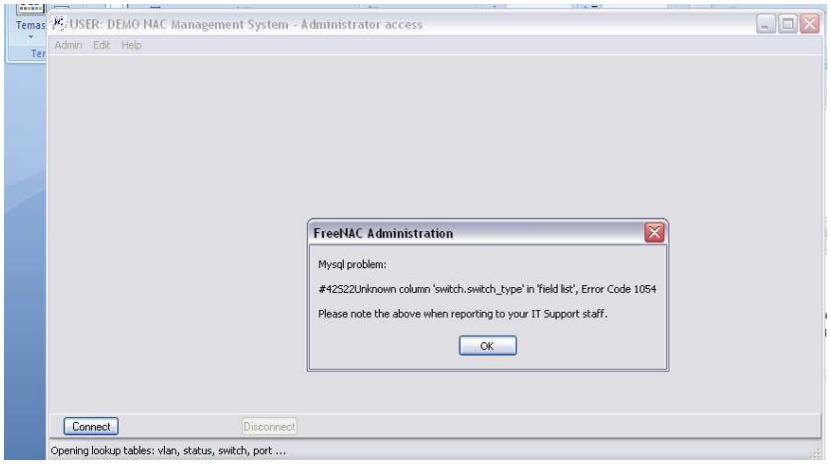

Figura IV.26: Error 2 de conexión

Existe bastante oferta de código abierto para NAC. Ciertamente, el software "libre", el software de código abierto en general es propenso a la falta de apoyo técnico del creador, la falta de actualizaciones y la grave falta de interoperabilidad. Cuando se solicita soporte de Microsoft para recibir asesoría y le dice que estaba en ejecución NAC de código abierto no obtendrá ningún tipo de garantía.

El potencial de la falta de apoyo técnico a su vez tiende a muchos usuarios de software de código abierto a invertir mucho tiempo tratando de solucionar temas de compatibilidad.

La elección de una alternativa de código abierto es una solución que en general no tiene buena aceptación por lo menos en las grandes empresas, ya que prefieren adoptar tecnologías provistas por sus proveedores tecnológicos y no tener que lidiar con soluciones en las que tengan que invertir horas de sus equipos de desarrollo. Además, la adopción de un código abierto es mucho más complicada, ya que de una u

otra manera forman parte o tiene estrechas relaciones con las grandes multinacionales y están atadas a seguir los lineamientos que dictan sus casas matrices.

El NAC de Symantec, antes NAC de Sygate, no ofrece el SNMP. Los IP estáticos son puente al DHCP, así que 802.1x e incluso las trampas del SNMP apuntan los IP estáticos de la subsistencia de ser utilizado sin la autorización.

Independientemente de ello cada organización tiene que tener conciencia de que es imprescindible contar con un Control de Acceso a Red tanto externa como internamente.

Al crear en un switch como rutas para acceder a varias redes y compartir recursos en base al tipo de equipo se crean esquemas de seguridad a nivel de puertos, cisco posee software propietario y se establece en esta tesis.

Las políticas o sea comandos como que personas pueden acceder a ciertas aplicaciones, o equipos de las redes LAN pero todo a nivel de puertos o sea hardware. No fueran políticas literalmente fueran comandos como rutas de acceso implantadas en el switch.

El problema registrado en la solución FreeNAC es que la compatibilidad entre cisco y software libre, no se pueden establecer como un llamado a los protocolos y códigos de cada uno. Debido a que cisco posee software propietario para la administración de sus equipos y puertos para las políticas, que se lo hacen a nivel de comandos.

CAPITULO V

5 Propuesta Metodológica de Control de Acceso a la Red Corporativa.

5.1 CONTROL DE ACCESO A LAS REDES

Controlar el acceso a los sistemas, aplicaciones y servicios, tanto internos como externos, evitando el acceso no autorizado.

5.2 POLÍTICA DE USO DE LOS SERVICIOS EN RED

Para garantizar que los usuarios accedan únicamente a los servicios a los cuales están autorizados, se establecen los siguientes lineamientos:

a) Los jefes de cada Área del Departamento de Operaciones y Sistemas analizarán sobre las redes y servicios a los que cada usuario de su Área debería

tener acceso. Para el caso de los clientes, el Jefe Operacional será el encargado de dicho análisis.

b) Se incorporarán controles automáticos, que verifiquen el cumplimiento de la presente política. El dispositivo de seguridad, permitirá crear listas de acceso y grupos de autenticación; además facilitará la autorización y registro de las actividades.

c) Para acceder a las redes, se utilizarán los medios proporcionados y autorizados por la empresa; bajo ningún concepto se deberá duplicar o utilizar recursos de los clientes.

5.3 AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

Se incorporará autenticación para todos los usuarios del servicio de Internet y de correo electrónico. Para los usuarios de los servicios dial-up y correo electrónico, se utilizará un servidor; mientras que los usuarios de los servicios de banda ancha y corporativo, estarán asociados a otro servidor , que deberá realizar una autenticación transparente para el usuario. Los servidores, además permitirán el bloqueo de conexiones no deseadas o no autorizadas. Ambos servidores utilizan controles, de modo que la información asociada en la autenticación se transmitirá de manera segura.

Para controlar el acceso de los clientes asociados a nodos inalámbrica, cualquiera sea el servicio proporcionado, se debería optar por el servidor TACACS+, que incorpora mayor seguridad, necesaria para el intercambio de información en un medio inseguro como lo es el inalámbrico.

5.4 IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES

Con el propósito de autenticar conexiones de equipos y ubicaciones específicas, se identificarán todos los equipos en las redes. De manera lógica, se procederá a configurar los equipos, con nombres adecuados, que especifiquen con claridad de qué equipo se trata y qué nivel de importancia tiene. Para la identificación física, se deberá incorporar al equipo, una etiqueta que contenga información sobre las redes a las cuales puede ser conectada, y la sensibilidad de dichas redes.

5.5 PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO

Para proteger los puertos de configuración y diagnóstico remoto, se utilizarán las cuentas asignadas con contraseñas proporcionadas al personal con acceso autorizado a la configuración y diagnóstico de las redes. Se aplicará la Política de Controles de las redes. Se deberá inhabilitar o retirar los puertos, servicios, aplicaciones que no sean necesarias para la entrega y revisión de los servicios.

5.6 SEPARACIÓN EN LAS REDES

Se requerirá separar los entornos de seguridad de la red; para ello se propone la creación de servidores de autenticación diferentes para el personal y los empleados dentro del grupo de autenticación. Tan solo el personal debería tener acceso al dispositivo de seguridad, por ello se plantea la respuesta exclusiva al personal para solicitudes de acceso serial, privilegiado y telnet. Los demás equipos que conforman la red, restringirán el acceso no autorizado, mediante contraseñas.

Existirán entornos de red aislados para la realización de pruebas y desarrollo de sistemas y aplicaciones, eliminando el riesgo de cambios no autorizados e

incorporación de fallas. Se deberán separar las redes inalámbricas, a través de controles adicionales como los descritos en la Política de Autenticación de usuarios para conexiones externas.

5.7 CONTROL DE CONEXIÓN A LAS REDES

Conforme a la Política de Control de acceso, se deberán mantener y actualizar los derechos de acceso a la red. Dichos controles deberán ser aplicados a la mensajería, transferencia de archivos, acceso interactivo, acceso a las aplicaciones. Además se deberán revisar las conexiones establecidas y fallidas, mediante los servidores de autenticación y el dispositivo de seguridad incorporado.

5.8 CONTROL DEL ENRUTAMIENTO EN LA RED

Para controlar el enrutamiento correcto en la red, se cuenta con protocolos de capa 3 que proporcionan un nivel confiable de enrutamiento, verificándose las direcciones fuente y destino. El dispositivo de seguridad generará mensajes Syslog en caso de detectar errores en el envío o recepción de información, sospechando un posible ataque o riesgo.

5.9 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Evitar que usuarios no autorizados accedan a los sistemas operativos que permiten proporcionar los servicios a los clientes.

5.9.1 PROCEDIMIENTOS DE REGISTRO DE INICIO SEGURO

Para garantizar un buen procedimiento de registro de inicio, los encargados de su mantenimiento deberán evitar la publicación de información hasta que el proceso de

registro de inicio se haya completado satisfactoriamente; además se deberá mostrar una advertencia sobre la restricción del acceso.

No se deberán suministrar mensajes de ayuda durante el registro de inicio, pues usuarios no autorizados podrían beneficiarse de ellos y lograr el acceso. La validación de la información de registro deberá ser efectuada una vez que se hayan terminado todos los datos de entrada; en caso de que el sistema detectara un error, no se deberá indicar al usuario qué información fue correcta e incorrecta.

Para el acceso, se limitará la cantidad de intentos permitidos a 3; los servidores de autenticación serán los encargados de esta función. Resultaría conveniente establecer en los servidores, tiempos de dilación antes de permitir intentos adicionales de registro de inicio. También convendría utilizar el sistema de contraseñas ocultas mediante símbolos y la criptografía para transmitir las contraseñas por la red.

Dado que el dispositivo de seguridad trabaja en conjunto con los servidores de autenticación, será posible que se almacenen los registros exitosos y fallidos, junto a los detalles respectivos, posibilitando a los administradores del sistema acceder a dicha información.

5.9.2 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Cada jefe de Área concederá identificadores de usuario (ID) a los empleados de los cuales es responsable. Los identificadores serán utilizados por el jefe del Área para controlar el acceso físico y lógico de los usuarios; además servirán para rastrear y monitorear sus actividades.

Se utilizarán identificadores de usuario compartido; lo que evitará la dependencia de un solo usuario en determinadas funciones en el Departamento de Operaciones.

Los servidores de autenticación TACACS+ y RADIUS proporcionan verificación sólida de autenticidad, pues emplean al protocolo CHAP durante el proceso de autenticación. Para reforzar la seguridad de la autenticación en el acceso físico a los nodos y al Centro de Datos, será conveniente implementar medios biométricos, como un lector de huellas digitales que contenga almacenada la información del personal con acceso autorizado; de modo que cuando se registre un acceso, se registren también los detalles del mismo.

5.9.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS

El sistema de gestión de contraseñas, con el fin de monitorear las actividades de los usuarios y conservar responsabilidades, se basará en identificadores de usuario (ID) y contraseñas.

El sistema deberá permitir el cambio de contraseñas de los usuarios, imponiendo que éstas sean contraseñas de calidad. En caso de que se detectara la intención de utilizar una contraseña que no cumpla con las condiciones requeridas, el sistema deberá indicar al usuario que la contraseña ingresada no cumple con las condiciones y que deberá utilizar otra. Se deberá incorporar un timer de validez de contraseñas de los sistemas empleados por el personal para la entrega de los servicios; de manera que cada dos meses el sistema obligue a los usuarios a cambiar de contraseñas. El sistema deberá conservar un registro de las contraseñas empleadas. Para el almacenamiento

de las contraseñas, se deberán utilizar controles criptográficos y localidades de disco diferentes a las que contengan los datos del sistema de aplicación.

5.9.4 USO DE LAS UTILIDADES DEL SISTEMA

Para acceder a las utilidades del sistema, se deberán seguir las siguientes directrices:

a) Atravesar por un procedimiento de autenticación y autorización, mediante el uso de identificadores de usuario y contraseña, los cuales deberán ser limitados a una cantidad mínima de usuarios, de preferencia.

b) Todo uso de las utilidades del sistema, deberá ser registrado; dicho registro servirá para verificar que los niveles de autorización para las utilidades del sistema sean los adecuados y que estén siendo empleadas adecuadamente.

c) Todas las utilidades o software del sistema que sea innecesario para la prestación o revisión de los servicios, deberá ser retirado, puesto que podrían representar una vulnerabilidad para que se presenten amenazas.

5.10 TIEMPO DE INACTIVIDAD DE LA SESIÓN

En base a la sensibilidad de la información asociada a los sistemas o aplicaciones utilizadas para la entrega de los servicios, se determinará el tiempo de dilación adecuado para suspender las sesiones inactivas.

5.10.1 LIMITACIÓN DEL TIEMPO DE CONEXIÓN

Se deberá limitar el tiempo de conexión para las aplicaciones consideradas como de alto riesgo. Los trabajos efectuados en el dispositivo de seguridad deberán ser

considerados como de alto riesgo, para lo cual se establece el tiempo agotado absoluto.

Será conveniente conservar los tiempos límite de conexión, con que actualmente cuentan los equipos que conforman la red.

Se procederá a restringir los tiempos de conexión a las horas normales de oficina, a menos que se requiera tiempo extra u operaciones de horario prolongado; para ello, el jefe del Área que requiera la prolongación de tiempo, será el responsable de la autorización respectiva.

No se utilizará repetición de autenticación a intervalos determinados, excepto si el sistema detectara inactividad en la sesión, en cuyo caso se aplicará el tiempo agotado de inactividad.

5.11 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

Evitar que usuarios no autorizados accedan a la información de los sistemas de aplicación.

5.11.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

En base a la Política de Control de acceso, se restringirá el ingreso de los usuarios a la información. Para controlar el acceso a las funciones del sistema de aplicación, se deberá proporcionar menús a los usuarios, de modo que sea más sencillo ingresar a la función necesaria y evitar errores involuntarios.

Además se deberá restringir los derechos de acceso, como leer, escribir, eliminar y ejecutar, dependiente del usuario que haya accedido al sistema.

La información generada por los sistemas de aplicación, deberá ser manejada adecuadamente, evitando que sea enviada a terminales o sitios no autorizados

5.11.2 AISLAMIENTO DE SISTEMAS SENSIBLES

Será necesario aislar los sistemas sensibles, en un entorno dedicado. Una vez que los propietarios de los sistemas y aplicaciones evalúen sus sensibilidades y los riesgos a los cuales se exponen, deberán determinar si se requiere o no aislamiento.

Se deberá proceder al aislamiento del ingreso a los equipos de backbone y al dispositivo de seguridad, de forma que solo el personal autorizado del Departamento de Operaciones y Sistemas pueda acceder a los mismos. Además se propone la determinación de niveles de seguridad diferentes en las interfaces , creando un aislamiento en las interfaces; de modo que toda la red de la empresa quede aislada de las redes externas, y se posibilite la comunicación solo para las redes especificadas como permitidas.

Mediante medios biométricos se podrá incorporar aislamiento físico en los lugares en los que se procesen sistemas sensibles.

5.11.3 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Incorporar a la seguridad como parte esencial de los sistemas de información.

Los sistemas de información deben incorporar un control de detección de caracteres inválidos, datos incompletos, datos de control inconsistentes, de modo que presenten al usuario el aviso correspondiente.

Se realizará la verificación de los procedimientos de respuesta ante errores de validación. Todo el personal tendrá la obligación de verificar los sistemas de acceso por contraseña, realizando cuatro pruebas, al menos una vez al mes:

- Ingresar el nombre de usuario correcto y una contraseña incorrecta.
- Ingresar el nombre de usuario incorrecto y la contraseña correcta.
- Ingresar tanto el nombre de usuario y de contraseña incorrectos.
- Ingresar tanto el nombre de usuario y de contraseña correctos.

5.12 VALIDACIÓN DE LOS DATOS DE SALIDA

Para la validación de los datos de salida:

a) Todo el personal que maneje datos de salida, debe suministrar la información suficiente para su futura comprensión y determinación de exactitud, totalidad, precisión y clasificación.

b) Los asesores del Encargado de seguridad de la información, deben verificar la verosimilitud de la información de salida, constatando que sea razonable. Además, deben comprobar el procesamiento total de todos los datos de salida, realizando verificaciones en las aplicaciones y servidores necesarios. En caso de que se detectara alguna anomalía, deberán informar inmediatamente al Encargado de seguridad de la información de la empresa.

c) Se verificará que los anchos de banda que constan en los contratos, son los que se les proporciona a los clientes y que el servicio no es intermitente. La verificación para cada cliente, se llevará a cabo durante un día, mediante el monitoreo , la constatación

dentro de la configuración del switch y la ejecución de un ping extendido, garantizando así que los anchos de banda contratados, sean los que se les proporciona a los clientes y que el servicio sea continuo. Cada asesor tecnológico e ingeniero de soporte, será el encargado de verificar el ancho de banda proporcionado a los clientes de los cuales está a cargo. Si se detectara alguna anomalía, se documentará el evento y se informará al Encargado de seguridad de la información.

d) Se manejará un registro de todas las actividades del proceso de validación de la salida de los datos; esta información estará bajo el control del Encargado de la seguridad de la información de la empresa

5.13 GESTIÓN DE CLAVES

Para proteger las claves criptográficas, privadas y secretas se presenta la Política de gestión de claves:

a) Los diferentes sistemas criptográficos y aplicaciones empleadas, tendrán asociadas sus claves únicas e irrepetibles.

b) Los asesores del Encargado de seguridad de la información generarán y obtendrán certificados para las claves o llaves públicas necesarias.

c) El Encargado de seguridad deberá entregar un documento a los futuros usuarios de claves; en él se solicita la firma de aceptación del uso de las mismas y se especifica la forma de activación de las claves. Una vez aceptadas las condiciones, el Encargado de seguridad de la información enviará la información de las claves en un correo

electrónico, debiendo percatarse de que el archivo se encuentre encriptado y que las claves sean enviadas a los destinos correctos.

d) Las claves serán almacenadas por el Encargado de seguridad de la información, en archivos encriptados en la Intranet y con acceso exclusivo para cada usuario. Cuando un usuario autorizado, ingrese en su archivo correspondiente, solo él dispondrá de la llave, recibida previamente en el Documento de aceptación, permitiendo así su desencriptación. La selección de claves para cada caso, será realizada en base a la Política de privilegios de acceso. La llave de desencriptación no deberá ser almacenada electrónicamente, en lo posible debe ser recordada o registrada de manera segura.

e) Las claves serán cambiadas al menos trimestralmente. Si se presentara algún incidente por descubrimiento de alguna clave, todas deberán ser cambiadas inmediatamente. También se requerirá un cambio absoluto cuando algún empleado abandone sus funciones en la empresa. Todo cambio deberá ser autorizado por el Encargado de seguridad de la información.

f) Los asesores del Encargado de seguridad de la información deberán archivar todas las claves, inclusive aquellas que ya no se utilicen. El archivo deberá ser protegido. Para la destrucción segura de claves, se verificará que no se encuentre almacenada en ningún dispositivo o configuración. Tan solo deberá permanecer en el archivo de claves.

g) Cada seis meses se realizará una revisión interna de la gestión de claves, garantizando que todas están siendo bien utilizadas, sin riesgos asociados. Además se revisarán los archivos y registros necesarios.

5.14 Políticas Implementadas en el Servidor

Se ha considerado establecer las siguientes políticas de seguridad que permitirán un uso apropiado del sistema; estas políticas serán aplicables a todos los usuarios y equipos que requieran utilizar el sistema.

5.15 Condiciones del cuarto de equipos

El cuarto de equipos deberá proporcionar las condiciones adecuadas para la instalación de los equipos, es decir proporcionar sistemas de control de temperatura como sistemas de aire acondicionado, una adecuada instalación eléctrica y seguridad física adecuada para el acceso hacia el cuarto de equipos.

5.16 Sistema de respaldo de energía eléctrica

Se deberá proporcionar sistemas de respaldo de energía eléctrica de tal manera que si se suscitara un corte de energía se pueda apagar de forma adecuada los sistemas de comunicaciones, evitando daños por cortes eléctricos abruptos.

5.17 Sistema de control de incendios

El sistema de control de incendios a ser implementado, deberá emplear elementos químicos que no afecten los sistemas de comunicaciones.

Deberá proporcionar de señales tanto visuales como sonoras de algún evento de combustión detectado.

Deberá proporcionar sistemas de evacuación de emergencia y mecanismos de retardo en la expulsión de los químicos, en caso de que algún operario quede atrapado en el cuarto de equipos.

5.18 Control de acceso mediante dirección MAC en los clientes

El usuario para acceder a cualquier servicio de la red (Internet) debe tener asignada una dirección IP válida, la cual será otorgada por el servidor DHCP configurado en el cliente del servidor, para ello el usuario debe configurar su computador como cliente DHCP.

Para evitar accesos no autorizado a la red, el servidor DHCP estará configurado para otorgar una dirección IP únicamente a los usuarios cuya dirección MAC haya sido previamente registrada en un listado de direcciones MAC autorizadas. Se podrá registrar, modificar y eliminar la dirección MAC de los usuarios en el listado mediante el uso de la interfaz de administración.

Al momento de registrar las direcciones MAC será posible también indicar una dirección IP fija para cada dirección MAC; si no se indica ninguna, el sistema asignará al usuario una dirección IP disponible del rango que se haya definido en la configuración del servidor DHCP.

5.19 Filtros de direcciones MAC en puntos de acceso inalámbricos

Con el propósito de evitar que usuarios no autorizados hagan uso indebido del sistema, se va a configurar en los puntos de acceso inalámbricos (AP) un filtro de direcciones MAC de tal forma que únicamente lo usuarios autorizados puedan hacer uso del segmento de red inalámbrico.

Para conseguir esto se requiere que el equipo a emplearse sea compatible con esta funcionalidad.

5.20 Autorización de acceso a usuarios con dirección IP configurada de forma estática

Una vulnerabilidad identificada durante el proceso de implementación fue que cuando se configuraba una dirección IP perteneciente al segmento de red de los usuarios, de forma estática en un computador, era posible el acceso a la página de autenticación del cliente en el servidor.

Para evitar que esto suceda es necesario, permitir el acceso a usuarios que hayan configurado su dirección IP de forma estática, únicamente si su dirección MAC fue previamente registrada en el sistema.

5.21 Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios

Una vez que el usuario disponga de una dirección IP, podrá acceder al sistema de autenticación.

El sistema de autenticación solicitará que se ingresen un “nombre de usuario” y una “clave”, a estos dos parámetros estará asociado un perfil que será asignado de acuerdo a los requerimientos y/o necesidades del usuario.

El nombre de usuario será asignado por el administrador del sistema; una vez que el usuario haya solicitado el servicio.

Para la creación del nombre de usuario se considerará utilizar la primera letra del primer nombre del usuario seguido de su apellido, en caso de no encontrarse disponible este nombre de usuario se deja a consideración del administrador alguna otra combinación.

Para garantizar que la clave de acceso de usuario sea segura, ésta deberá ser de al menos ocho caracteres alfanuméricos, de los cuales al menos tres y no más de cinco serán números.

Para la creación de la cuenta y asignación de un “nombre de usuario” y “clave”, el usuario deberá indicar la siguiente información que será empleada para la creación de la cuenta de usuario en el servidor:

Primeramente la información general del usuario que se lista a continuación:

- Nombre de usuarios (*Username*)
- Clave (*Password*)
- Grupo (*Group*)
- Nombre compuesto por el nombre y seudónimo [*Name* (*First Name Surname*)]
- Correo (*Mail*)
- Departamento (*Department*)
- Teléfono de casa (*Home Phone*)
- Teléfono del trabajo (*Work Phone*)
- Teléfono móvil (*Mobile Phone*)

Además se debe configurar la información que será intercambiada en el *Access-Accept*, enviado por el servidor, misma que se lista a continuación.

- Protocolo (*Protocol*), que puede ser PPP, L2TP o IP; este campo no se empleará en la implementación.
- Dirección IP (IP *Address*), corresponde al campo de la dirección IP del usuario.

- Máscara de red de la dirección IP (IP *Netmask*), corresponde a la máscara de red empleada para el usuario.
- Tramado MTU (*Framed*-MTU), corresponde al tamaño de la trama el valor por defecto empleado en el campo es de 1500
- Compresión usada (*Compression Used*), el valor por defecto es *Van-Jacobson-TCP-IP*, este campo no se lo emplea en la implementación.
- Tipo de servicio (*Service Type*), campo que se empleará para enviar la información de perfil.
- Duración de la sesión (*Session Timeout*), campo empleado para indicar el tiempo máximo de duración de una sesión del usuario.
- Tiempo máximo de inactividad (*Idle Timeout*), campo empleado para indicar el período de tiempo en el cual se considerará un usuario como inactivo.
- Número máximo de sesiones (*Port Limit*), por política de utilización el número máximo de sesiones por usuario será de una sesión.
- Mensaje presentado (*Lock Message*), campo opcional de tipo descriptivo

Por defecto si el usuario no se ha autenticado y desea acceder a una dirección web externa a la red a través de su navegador, en lugar de la dirección solicitada se le mostrará una página de autenticación alojada en el cliente del servidor, en esta página se le solicitará ingresar el “nombre de usuario” y la “clave” que le fueron asignados. Una vez ingresada esta información se enviará una petición de *Access-Request* al servidor, y dependiendo del resultado que el servidor envié en respuesta a esta petición el usuario será aceptado o rechazado.

Si la respuesta es un *Access-Reject* se le mostrará al usuario una página de error y se le solicitará ingresar nuevamente el “nombre de usuario” y la “clave”.

Si la respuesta del servidor es un *Access-Accept* en el cliente se crearán las reglas apropiadas que permitirán al usuario utilizar al cliente como *gateway* para el acceso a Internet y se ejecutarán un conjunto de comandos dependiendo del perfil asociado al usuario, los cuales permitirán el acceso hacia el Internet según su perfil; restringiendo y/o permitiéndole acceso a los servicios y controlando el uso del ancho de banda.

El sistema se ha diseñado para permitir una sola sesión simultanea por usuario, por lo cual si otro usuario intenta hacer uso del sistema con un “nombre de usuario” y “clave” que en ese momento estén siendo empleados, se le presentará un error indicando la dirección IP y la dirección MAC del usuario que se encuentra empleando las credenciales ingresadas y solicitando que se envíe esta información al administrador de red.

5.22 Definir diferentes perfiles de acceso para los usuarios

En el sistema se establecerán distintas categorías de usuarios en función de las actividades que el usuario realizará.

A cada perfil estará asociado un conjunto de reglas que permitirán al usuario realizar únicamente peticiones a ciertos puertos, dependiendo del perfil asignado a cada usuario del sistema se le asignarán los permisos correspondientes.

Todos los perfiles tendrán acceso al puerto http (80) y https (443) del cliente, ya que el sistema empleará estos dos puertos para realizar la negociación de intercambio de credenciales, entre el usuario y el cliente, credenciales que posteriormente serán enviadas al servidor.

Por defecto se definirán tres perfiles, según el perfil asociado el usuario podrá acceder únicamente a cierto tipo de protocolos y/o aplicaciones como se describe a continuación:

- Acceso Total: Podrá utilizar todos los servicios disponibles en la red.
- Acceso Restringido: Se le permitirá acceso http, SMTP, pop3 y ftp.
- Invitado: Solo tendrá acceso http.

Para el caso de usuarios que no pertenezcan a ninguno de los perfiles no tendrán acceso a ninguno de los servicios de la red.

El administrador del sistema podrá hacer uso de la interfaz de administración del cliente para la creación y/o modificación de los perfiles de usuario existentes; esta interfaz permitirá asignar un nivel de acceso a la red diferente a cada grupo de usuarios pertenecientes a un determinado perfil, así como también limitar el uso del ancho de banda disponible.

El paso de trafico DNS hacia el Internet estará permitido para todos los usuarios, de esta forma se permitirá al usuario emplear el servidor DNS de su elección, en caso que no desee emplear el servidor DNS que se configura vía DHCP.

5.23 Protección de la información que viaja por el segmento de red inalámbrico

La información de los usuarios que se conecten por medio inalámbrico viajará encriptado, para prevenir cualquier tipo de ataque que se pueda dar en este segmento de la red.

Para proteger la confidencialidad de la información, se podrá emplear mecanismos de encriptación de información utilizados en comunicación inalámbrica como por ejemplo: WEP, TKIP, 802.1X/EAP, WPA y WPA2/802.11i.

5.24 Protección de la información de autenticación que el usuario envía al cliente

Será un requisito obligatorio el emplear un mecanismo de inscripción en el intercambio de información confidencial como son nombres de usuario y clave.

Por lo cual en la implementación se considerará emplear https con el objetivo de proteger la confidencialidad de la información importante intercambiada con el sistema de autenticación del cliente. Es decir, la información que envíe el usuario viajará encriptada mediante el uso de Certificados Digitales.

El sistema de autenticación deberá presentar de forma automática la página de autenticación empleando https, de tal manera que para el usuario sea transparente la utilización de encripción.

5.25 Protección de la información de autenticación que el cliente, enviada al servidor

La información intercambiada entre el cliente y el servidor deberá ser encriptado, ya que esta información corresponde a datos confidenciales de los usuarios.

Con el objetivo de encriptar la información que se intercambia entre el cliente y el servidor, se ha decidido levantar un túnel IPSec entre esos dos servidores, de tal manera que la información intercambiada sea únicamente comprendida entre estos dos participantes.

5.26 Registro del tiempo de conexión y el consumo medido en bytes que realice el Usuario

El tiempo de conexión en segundos y la cantidad de información que el usuario intercambie en *bytes* serán registrados en una base de datos, para poder tarifar la utilización del sistema.

Con el fin de registrar la utilización del sistema se definió un mecanismo automático, que permita ir actualizando el tiempo de conexión y los *bytes* consumidos en la base de datos.

El sistema debe determinar de forma automática, si un usuario se encuentra o no en actividad, esto se lo realiza mediante la comparación del consumo acumulado medido cinco segundos antes con el consumo acumulado hasta ese instante; en caso que no se registre consumo del usuario por un tiempo mayor al tiempo máximo de inactividad configurado (*Idle Timeout*), el sistema finalizara la sesión actual del usuario y procederá a aplicar las restricciones de acceso correspondientes.

5.27 Verificar el Cumplimiento de las Políticas de Seguridad Establecidas

A continuación se describe el procedimiento empleado para verificar cada una de las políticas de seguridad implementadas en el presente proyecto de titulación.

Se excluyen de la verificación que se realiza las siguientes políticas: protección de la información de autenticación que el cliente, envía al servidor; protección de la información de autenticación que el usuario envía al cliente y protección de la información que viaja por el segmento de red inalámbrico.

5.28 Control de Acceso Mediante Dirección MAC

Para realizar esta comprobación se ingresó en la red un equipo cuya dirección MAC no se encontraba registrada en la base de datos de direcciones MAC autorizadas; se comprobó en primera instancia al estar el equipo configurado como cliente DHCP y conectado mediante un cable de red al HUB, no le fue asignada una dirección IP del segmento de red LOCAL.

Posteriormente se ejecutó en la línea de comandos del sistema operativo el comando:

C:\>ipconfig /renew

Mediante el cual se le indica al computador que solicite una dirección IP a cualquier servidor DHCP disponible, luego de varios segundos se observó que el sistema no asigno ninguna dirección IP válida para acceder a los servicio de la red.

Por lo cual queda comprobada la correcta aplicación de la política de seguridad; permitiendo únicamente que los computadores cuyas direcciones MAC hayan sido registradas previamente obtengan una dirección IP válida para el acceso a la página de autenticación del cliente.

5.29 Filtros de Direcciones MAC en Puntos de Acceso

Para el cumplimiento de esta política de seguridad se hace uso de la funcionalidad del Punto de Acceso Inalámbrico que permite dar acceso únicamente a usuarios cuyas direcciones MAC hayan sido previamente registradas.

5.30 Autorización de Acceso a Usuarios en Dirección IP Configurada Forma Estática

Deben realizarse las pruebas de acceso empleando para este fin la dirección IP x.x.x.x configurada de forma estática en el computador del usuario que intentará acceder a los servicios de red.

Para que el computador del usuario pueda acceder al sistema de autenticación el cliente verifica que la dirección MAC del usuario sea una dirección válida, es decir, que se encuentre registrada en la base de datos de usuarios válidos.

Si algún usuario con su dirección IP configurada de forma estática, tratase de acceder al sistema, pese a que este usuario tenga configurada una dirección IP válida del

segmento de red LOCAL, el sistema no le permitirá ingresar a la página de autenticación, a menos que su dirección MAC haya sido registrada en la base de datos.
En esta circunstancia, al usuario que intente acceder al sistema en lugar de la página de autenticación se le presentará una página indicando que no está autorizado a utilizar el sistema.

5.31 Empleo de Nombre de Usuario y Clave de Acceso Segura para la Autenticación de Usuarios

Se verificará el funcionamiento del sistema de autenticación, empleando para las pruebas nombres de usuarios y contraseñas válidos, verificando que el sistema permitía el acceso de estos usuarios.
De igual forma al emplear usuarios no válidos, se debe verificar que los mismos no puedan obtener acceso a ningún servicio de red y únicamente se obtenía un mensaje indicando un error de autenticación.

Será responsabilidad del administrador del sistema, generar claves lo suficientemente seguras, que cumplan con un esquema de seguridad adecuado y eficiente. Por ejemplo crear nombres de usuarios de forma estándar y contraseñas que contengan al menos ocho caracteres alfanuméricos y que no sean palabras conocidas

5.32 DEFINIR DIFERENTES PERFILES DE ACCESO PARA LOS USUARIOS

Para verificar que los permisos de cada uno de los perfiles están siendo asignados de forma adecuada, se procederá a crear dos perfiles en el cliente perfil *Premium* y perfil *Gold*, configurando cada uno de los perfiles con diferentes servicios.

Una vez creados los perfiles se añadieron dos usuarios de prueba en el servidor, uno configurado para acceder con perfil *Premium* y el otro con perfil *Gold*.

Desde dos computadores configurados como usuarios del cliente, se procederá a ingresar el nombre de usuario y contraseña de los dos usuarios de prueba.

Además, desde el computador de cada usuario se arán pruebas de conexión a los servicios configurados en cada perfil, comprobando que únicamente se podía acceder a los servicios que se encontraban definidos en el perfil y el acceso a otros servicios se encontraba bloqueado.

5.33 Registro del Tiempo de Conexión y el Consumo Medido en *Bytes q*ue realice el usuario

El tiempo y *bytes* consumidos por cada uno de los usuarios registrados en el sistema, se lo podrá obtener desde la interfaz de administración.

6 POLÍTICAS SOBRE EL USO Y MANEJO DE INTERNET

Regular y Normar el uso del Servicio de Acceso a Internet a fin de asegurar el manejo de información clasificada a nivel de la red Corporativa.

6.1 Normas de seguridad informática

- Es responsabilidad y competencia exclusiva del departamento de administración y servicio técnico, la configuración, gestión y monitoreo del Servicio de Acceso a Internet, con el fin de proporcionar un servicio de red eficiente.

- Los usuarios están en la obligación de proteger y vigilar el equipo de cómputo asignado por el departamento, responsabilizándose por el uso indebido de terceras personas y manipulación inadecuada de los mismos.
- Se consideran como conductas de uso indebido:
    - Intentar apoderarse de claves de acceso de otros usuarios.
    - Violar o intentar violar los sistemas de seguridad de las máquinas conectadas a la red, tanto a nivel interno como externo.
    - Violar las reglas y restricciones impuestas por los diferentes administradores de red, cualquiera que sea el ordenador al que se tenga acceso.
    - No reportar el uso indebido por parte de otro usuario del que se tenga conocimiento.

- Queda estrictamente prohibido el uso, autorizado o no, del servicio de Internet para fines o efectos ilícitos de los derechos e intereses de terceros, o que de cualquier forma puedan dañar, inutilizar, sobrecargar o deteriorar los servicios, los equipos informáticos y usuarios de Internet (hardware y software) así como los documentos, archivos y toda clase de contenidos almacenados en sus equipos informáticos.
- Las actividades que quedan expresamente prohibidas, no sólo porque son conductas socialmente reprobables que contribuyen al deterioro del buen funcionamiento del servicio de Internet sino porque son actos constitutivos de ilícito penal. En concreto y a titulo enunciativo, se prohíbe:

- Visualización de Pornografía.
- Establecer enlaces o mecanismos de tipo SPAM.
- Infringir el secreto de las comunicaciones y la protección de datos de carácter personal.
- Derechos de la propiedad intelectual.
- Actividades de hacking y similares.

- La realización de cualquier actividad relacionada con la pornografía, salvo en lo que respecta a su erradicación, es ilegal. El Departamento tomará las iniciativas y acciones necesarias para evitar que en sus sistemas se almacene, publique, divulgue, o intercambie materiales en cualquier tipo formato.
- El Departamento monitoreara los equipos de la institución, si así lo considera oportuno, podrá tomar aquellas medidas viables técnicamente que, cumpliendo la regulación relacionada con el Decreto de las Telecomunicaciones, traten de minimizar el impacto ocasionado en el servicio prestado a sus usuarios, por acciones o actividades contrarias a esta política.
- El Servicio de Correo Electrónico Hotmail, Yahoo, Hi5, YouTube, Windows Messenger y otros de características similares serán restringidos en horas de oficina a nivel Institucional.
- Las descargas de paquetes, programas o actualizaciones tendrán sus limitaciones en base a un proceso de nivelación de carga implantado a nivel de servidor a fin de cubrir requerimientos sobre la gestión de aplicaciones institucionales.

- El incumplimiento con las presentes políticas asociadas, estándares, guías y procedimientos, ocasionará recomendación de acciones disciplinarias, según lo establece el reglamento.

7 Políticas Sobre el Manejo de Claves de Acceso de Equipos Informáticos

Regular y Normar el uso de claves de acceso o passwords a fin de asegurar el manejo de información clasificada a nivel de la red Corporativa.

- Es responsabilidad y competencia exclusiva del Departamento de administración y servicio técnico, la configuración, gestión y control del equipamiento de acceso a la Red (puentes, concentradores, enrutadores, etc), y como tal los Puntos de Acceso.
- Las claves de acceso o passwords son las "llaves" que permiten a los usuarios abrir las "puertas" de acceso a los diferentes servicios que ofrece la red; es por esta misma metáfora que cada usuario es responsable sobre su clave de acceso, y por tanto asume toda responsabilidad sobre las actividades realizadas por terceros haciendo uso de su clave de acceso y de su cuenta.
- Los usuarios están en la obligación de renovar sus claves de acceso en forma mensual, siendo de responsabilidad absoluta del usuario su manipulación.
- Queda estrictamente prohibido el uso, autorizado o no, de un código de usuario distinto al propio con el fin de evadir normas de control de recursos escasos.

- Los equipos de cómputo dispondrán de un esquema de claves de usuario, sujeto a dos parámetros:
    - ADMINISTRADOR: Gestión del Departamento.
    - USER DOMAIN: Usuario Permanente del Equipo.

Además de la cuenta de propósito general, habrá otras cuentas específicas, para determinadas prácticas, que se abrirán en los sistemas informáticos que se determinen en su momento bajo autorización del Departamento.

Estas cuentas se renovarán anualmente. La cuentas que no se renueven serán canceladas, perdiéndose toda su información.

- Las Claves de Administrador a nivel de servidores serán renovadas trimestralmente bajo parámetros de seguridad y esquemas funcionales gestionadas por el Personal del Departamento de administración y servicio técnico.
- Se consideran como conductas de uso indebido:
    - Intentar apoderarse de claves de acceso de otros usuarios.
    - Violar o intentar violar los sistemas de seguridad de las máquinas conectadas a la red, tanto a nivel interno como externo.
    - Violar las reglas y restricciones impuestas por los diferentes administradores de red, cualquiera que sea el ordenador al que se tenga acceso.
    - No reportar el uso indebido por parte de otro usuario del que se tenga conocimiento.

- El incumplimiento de las políticas asociadas, estándares, guías y procedimientos, ocasionará recomendación de acciones disciplinarias, según lo establece el reglamento interno.

CONCLUSIONES

- De acuerdo al estudio realizado, se cumplió con establecer una metodología de red para cumplir los parámetros de seguridad, esto se lo hace con el fin de preservar la información fuera de los peligros de posibles ataques y de optimizar la gestión de administración de la misma de una manera más eficiente que la utilizada actualmente.
- La elección de una alternativa de código abierto, es una solución que en general; no tiene buena aceptación.Por lo menos en las grandes empresas privadas, ya que prefieren adoptar tecnologías provistas por sus proveedores tecnológicos y no tener que lidiar con soluciones en las que tengan que invertir horas de sus equipos de desarrollo, ya que de una u otra manera forman parte o tiene estrechas relaciones con las grandes multinacionales y están atadas a seguir los lineamientos que dictan sus casas matrices.
- Las herramientas para soluciones de administración y gestión al acceso inseguro a la red, son propietarias de cisco ya que una solución libre no ofrece garantía ni no soporte técnico
- Uno de los conceptos básicos que manejan los equipos de seguridad para su funcionamiento es el uso de niveles de seguridad, los cuales permiten otorgar cierto nivel de seguridad a las interfaces. Una interfaz con un nivel de seguridad mayor puede acceder a una con un nivel inferior y ésta no podrá acceder a una interfaz con un nivel de seguridad superior. Otra herramienta fundamental

para estos equipos son las listas de acceso, mediante las cuales se permite o restringe el acceso a determinado usuario.

- La implementación de una Política de seguridad permitirá controlar de mejor manera las actividades realizadas por los usuarios y garantizar la seguridad de la información asociada a la entrega de los servicios. Mediante la documentación y registro de todos los procedimientos será posible monitorear las actividades, disponer de información útil para futuros eventos y conservar la información necesaria para auditorías.

RECOMENDACIONES

- Se debe considerar que la información siempre está expuesta a posibles amenazas, sea humanas, tecnológicas o ambientales.
- Cuando se está trabajando en la etapa de configuración de los equipos de red, y realizando el establecimiento de las VLANs, hay que tomar en cuenta que existe una VLAN única para la administración de los equipos, es por esta por donde se envían y reciben las solicitudes de asignación, es muy diferente a las VLANs de cada una de las Direcciones en donde se ubican los equipos de los usuarios.
- Para seleccionar el equipo de seguridad adecuado, se recomienda considerar el tamaño de la red a la cual se desea proteger, las aplicaciones que en ésta se manejan y el análisis de costos correspondiente. Para el caso de un ISP, dado que su producto final es la entrega de servicios que atraviesan por redes, es recomendable adquirir un equipo o sistema que proporcione la mayor cantidad de seguridades posibles, procurando que el costo de la implementación tenga relación con el valor de los activos que se desea proteger.

- Todos los controles deberían ser probados antes de ser implementados, puesto que podrían no funcionar como se espera, y por el contrario se podrían incorporar nuevas vulnerabilidades en los sistemas o aplicaciones.

- Lar herramientas para la administración y gestión de red proporcionadas por cisco son intuitivas para el administrador, facilitando el control de acceso a la red como su monitoreo.
- Se recomienda capacitar a los usuarios en el uso y confidencialidad de sus cuentas de acceso al sistema, por lo menos 2 veces al año.
- Una vez implementados los controles, se deberá dar fiel cumplimiento a las políticas de seguridad establecidas en la empresa; solo así se podrá garantizar el funcionamiento exitoso.

RESUMEN

Se realizó una metodología de solución al acceso inseguro de los recursos de las redes LAN corporativas, el cual se desarrollo mediante aplicaciones NAC.

En la investigación se usa el método deductivo que parte de la identificación del problema en precautelar el acceso inseguro a las redes, su planteamiento, la formulación de la hipótesis y su posterior solución. Para la elaboración de la metodología se realizó un escenario de pruebas usando equipos cisco como switch y router; utilizando el software Cisco Secure ACS que utiliza los protocolos TACACS con niveles de seguridad básicos de Cisco Secure ACS*;* PAP con el que los usuarios se autentican una sola vez y CHAP permite un nivel de seguridad mayor, con contraseñas encriptadas, cuando el cliente se comunica con el NAS. Usa la infraestructura de la red para reforzar el cumplimiento de las políticas de seguridad en todos los dispositivos.

Los resultados obtenidos en la propuesta metodológica demuestran que presenta un 98% de aplicabilidad lo que indica que es una solución bastante confiable, además presenta la mayor flexibilidad y movilidad para el control de acceso al administrador de la red.

La propuesta de la metodología al acceso inseguro constituye un importante aporte para los administradores en el campo de las redes. Además Cisco Secure ACS el que se encarga de centralizar el control de los privilegios de usuario y los distribuye a cientos o miles de puntos de acceso a lo largo de la red y la seguridad.

Se recomienda se dé fiel cumplimiento a las políticas de seguridad establecidas en la empresa; solo así se podrá garantizar el funcionamiento exitoso de la seguridad de la Red.

SUMMARY

It was done an access solution methodology unsure of the resources of corporate LANs, which was developed by NAC applications.

The research uses the deductive method by the identification of the problem in precautionary insecure access to networks, their approach, the hypothesis formulation and its subsequent solution. For obtaining the methodology a test scenario was carried out using equipment as cisco switch and router, also using the Cisco Secure ACS which uses TACACS protocols with basic levels of security with Cisco Secure ACS; PAP to authenticate users to a once and CHAP allows a higher level of security with encrypted passwords, when the customer communicates with the NAS. Use the network infrastructure to enforce compliance with security policies on all devices.

The results show that the proposed methodology provides 98% of applicability which indicates that it is a fairly reliable solution also provides greater flexibility and mobility to control access to the network administrator.

The proposed methodology to insecure access is an important contribution to managers in the field of networks. In addition to Cisco Secure ACS that is responsible for centralizing control of user privileges and distributed to hundreds or thousands of access points along the network and security.

It is recommended to be given full compliance with established security policies in the company, the only way we can ensure the successful operation of the network security.

BIBLIOGRAFÍA GENERAL

1. BARRIOS DUEÑAS, JOEL. Implementación de Servidores con GNU/Linux . Guadalajara, Mexican, 2003. pp. 55-224

2. ROBLES, GREGORIO y GONZALES BARAHONA, JESUS. Introducción al Software libre . Barcelona, Eureca Media, 2003. pp. 100-150

3. CISCO NETWORKING SECURITY

   http://www.cisco.com/cisco/software/release.html?mdfid=282450822&flowid=4363&softwareid=282562545
   [08-03-2011]

4. INTRANET CORPORATIVA

   http://es.wikipedia.org/wiki/Intranet_Corporativa
   [05-03-2011]

5. INTRODUCCION A LAS REDES

   http:// macedoniamagazine.frodrig.com/redes1.htm
   [05-03-2011]

6. MECANISMOS DE SEGURIDAD

   http://www.buenastareas.com/ensayos/Mecanismos-De-Seguridad/229947.html
   [10-03-2011]

7. RED CORPORATIVA

http://technet.microsoft.com/es-s/library/cc782833%28WS.10%29.aspx
[05-03-2011]

8. REDES LAN

http://www.monografias.com/trabajos11/reco/reco.shtml
[08-03-2011]

9. TOPOLOGÍAS

http://hugoenriquecastrocruz615.blogspot.com/2009/02/topologia- malla-se-la-llama-asi-pues.html
[08-03-2011]

10. SOFTWARE LIBRE GNU

http://www.visuarama.com/gnuino/gnuino.html
[13-03-2011]

GLOSARIO

ACL (Access control list) . Lista de control de acceso es una tabla que le indica al sistema operativo de la computadora que derechos de acceso tiene un usuario hacia un objeto en particular, como un directorio o archivo.

Autenticación. Proceso de determinar la identificación de un usuario que intenta accesar un sistema.

Autorización. Proceso de determinar que tipos de actividades son permitidas. Una vez que un usuario haya sido autenticado, es autorizado para tener diferentes tipos de acceso.

Cracker. Es una persona no autorizada que accesa a la computadora de alguien más por medio de una red. Un cracker puede hacer esto con fines de robar información, por alguna causa altruista o por diversión.

Inalámbrico. Dicho de un sistema de comunicación eléctrica: Sin alambres conductores.

Intranet. Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

Ethernet. Es la tecnología más usada para redes locales, típicamente utiliza cable coaxial o cables twisted pair. Existen tres tipos de sistemas Ethernet según su

velocidad: 10BASE-T provee velocidad de 10 mbps, Fast Ethernet de 100 Mbps y Gigabit Ethernet de 100 Mbps.

Host. Es toda computadora que tiene una dirección IP y acceso de doble vía con otras computadoras en la red. Un host es un nodo en una red.

Políticas. Son las reglas de la organización o empresa que gobiernan el uso de los recursos tecnológicos, practicas de seguridad y procedimientos de operación.

Proxy. Es un agente de software que actúa en lugar de un usuario. Los proxies aceptan la conexión de un usuario, toman la decisión de permitir o no a la IP del cliente hacer uso de ellos. También hace una autenticación adicional y completa la conexión en nombre del usuario hacia su destino.

SSL. Es un protocolo usado para administrar seguridad en la transmisión de datos por internet.

Router. Ruteador o en caminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres.

ANEXOS

ANEXO 1. Politicas que rigen a la institución ESMIL

Guía básica de seguridad para Windows NT

Windows NT fue, según Microsoft, diseñado y desarrollado con la seguridad en mente "por lo tanto - podríamos pensar - no tengo que preocuparme de su seguridad"; **esto es falso.**

Lo primero es que ningún programa nos va dar la solución a la seguridad definitiva y total (y el que lo prometa miente). Todos tienen fallos y vulnerabilidades que para cuando son parcheados, el programa será tildado de obsoleto. Lo segundo es que la seguridad de un sistema depende en gran medida de nuestras políticas y de la configuración del sistema.

Esta guía trata de las recomendaciones de configuración que debes tener si estás usando Windows NT. No es objetivo de esta guía el enseñarle a usar Windows NT, aunque si se hace una pequeña introducción con conceptos básicos para unificar términos.

INDICE:

1.- Conceptos Básicos:

Dominio

Es un grupo lógico de máquinas que comparten cuentas de usuarios y seguridad de los recursos. Un dominio está integrado por una máquina NT **servidor de dominio** que administra las cuentas y recursos del dominio en cuestión, y/o servidores y /o estaciones de trabajo. Los usuarios de un mismo dominio tendrán un inicio de sesión único en el **servidor del dominio** para acceder a los recursos de cualquier parte de la red, una cuenta única para acceder a las máquinas del dominio...

Cuentas de usuarios

En las cuentas de los usuarios se establecen datos como el propietario de la misma, contraseña de acceso, localización de su directorio de inicio de sesión, grupo al que pertenece etc. Windows NT distingue las **cuentas locales** y las **cuentas de dominio**:

- **Cuenta local de usuario:** pertenecen a una única estación Windows NT. El procedimiento de login de las mismas se valida en una base de datos local de la estación. La herramienta administrativa de la estación para crearlas, modificarlas, borrarlas y establecer políticas de

seguridad es el **Administrador de usuarios** o el **Administrador de usuarios para dominios**.

- **Cuenta de dominio :** pertenecen al dominio en cuestión. El procedimiento de login requiere, además del nombre de usuario y contraseña, el dominio al que se está haciendo login. La validación se hace en una base de datos existente en el servidor de dominio. La herramienta administrativa del servidor para crearlas, modificarlas, borrarlas y establecer políticas de seguridad del dominio es el **Administrador de usuarios para dominios**.

Tanto si se hace login en un tipo de cuenta u otro, para acceder al menú de seguridad de la estación o el servidor (para cambiar el password, bloquear el terminal, o cierre de sesión e incluso del sistema) teclear CRTL+ALT+SUPR

Las cuentas que por defecto crea NT son la de **Invitado** (guest), deshabilitada por defecto -, y la del **Administrador**, para configuración y control de usuarios y recursos.

Cuentas de grupos

Las cuentas de usuarios se organizan en grupos. Cuando se añade un usuario a un grupo, el usuario tendrá los **derechos y permisos** asignados a ese grupo.

Windows NT distingue dentro del concepto de grupo, dos categorías: **grupos locales y globales**.

- **Grupo local:** lo forman cuentas locales de usuarios y grupos globales de otros dominios. Se usan para asignar a grupos de usuarios permisos para acceder a un recurso.
- **Grupo global:** lo forman únicamente cuentas de dominio. Aunque los grupos globales pueden usarse para asignar permisos a los recursos, su funcionalidad principal es agrupar las cuentas de un dominio. Para lo primero es mejor añadir los grupos globales como locales.

NT crea por defecto ciertos grupos locales - con ciertos derechos ya adquiridos, globales y de sistema. Los grupos locales que existen por defecto en cualquier máquina NT son:

- **Usuarios:** Usuarios normales con cuenta.
- **Administradores:** Usuarios con derechos para administrar el sistema.
- **Invitados:** Usuarios sin cuentas que tienen derechos muy limitados.
- **Operadores de copia de seguridad:** Usuarios con derechos de copia de seguridad y restauración de archivos.

Si es servidora de dominio, además de los anteriores grupos locales, NT crea:

- **Operadores de cuentas:** Usuarios con derechos para administrar cuentas de usuarios.
- **Operadores de servidores:** Usuarios con derechos para administrar servidores.
- **Operadores de impresión:** Usuarios con derechos para administrar impresoras

y los siguientes grupos globales:

- **Admins de dominio**
- **Usuarios de dominio**
- **Invitados de dominio**

Los usuarios se convierten en miembros de los grupos de sistema automáticamente al acceder a la red. Los grupos de sistema en cualquier máquina NT son:

- TODOS: incluye a todos los usuarios que acceden a la red. No se puede controlar quién pertenece a este grupo, pero sí los permisos y derechos de este grupo.
- CREATOR OWNER (propietario): usuario que creó el recurso o es propietario del mismo.

Es conveniente revisar qué derechos tienen todos estos grupos por defecto dentro del menú de políticas de derechos de usuarios

2.- Políticas de passwords y cuentas:

El administrador de la red debe establecer una política de passwords en la que se especifique:

- Una duración máxima de la contraseña (aconsejable unos 90 días).
- Una longitud mínima (aconsejable un mínimo de 8 caracteres).
- Un histórico de la contraseña (unos 5 passwords).
- Un bloqueo automático tras sucesivos fallos de login (unos 5 fallos de login).

La política se establece dentro del menú de Administrador de usuarios para dominios->Directivas->Cuentas->Plan de cuentas

Para desbloquear una cuenta, acceder dentro del menú de:
Administrador de usuarios para dominios->Usuario->Propiedades->Cuenta desactivada

También es útil establecer en el **Administrador de usuarios para dominios** restricciones de:

- Horas de login al dominio.
- Estaciones desde las que se puede acceder al dominio.
- Expiración de la cuenta si es temporal.
- Restricción de acceso dial-in.

así como templates para las cuentas de nueva creación.

3.- Permisos y derechos de usuario:

Los **derechos de usuario** definen qué pueden hacer los usuarios . Algunos de los derechos más comunes son:

- El derecho de inicio de una sesión local.
- Derechos de administración de auditoria.
- Derecho de apagar el equipo.
- Derecho de acceder al equipo desde la red (Log On).
- Derecho de hacer copias de seguridad o de recuperación de ficheros.

Para configurar los derechos de usuarios , se elige Derechos de usuarios del menú Directivas del Administrador de usuarios de Dominio y se autorizan para cada derecho los usuarios o grupos apropiados.

Hay que tener en cuenta que:

Es conveniente eliminar al grupo TODOS el derecho de LogOn (acceso desde red)

Los permisos definen qué recursos pueden usar los usuarios o grupos de usuarios , entendiendo por recurso un fichero, directorio o una impresora. Los permisos controlan el acceso a directorios y ficheros locales, y compartidos en la red y son configurados por el administrador o por el propietario de los mismos. Hay permisos estándar y permisos individuales. Los permisos estándar son una combinación de los permisos individuales.

Permisos para directorios

Permisos estándar	Permisos individuales	Permisos para nuevos ficheros
Sin acceso	Ninguno	Ninguno
Listar	R,X	-
Lectura	R,X	R,X
Añadir	W,X	-
Añadir y Lectura	R,W,X	R,X
Cambio	R,W,X,D	R,W,X,D
Control total	Todo	Todo

Permisos para ficheros

Permisos estándar para archivos	Permisos individuales
Sin acceso	Ninguno
Lectura	R,X
Cambio	R,W,X,D
Control total	Todos

En un sistema de ficheros NTFS, el administrador puede configurar los permisos de ficheros y directorios pulsando con el botón derecho del ratón sobre el fichero o directorio que se que desee proteger, y luego la secuencia:
propiedades -> seguridad -> permisos .

NOTA: ¡¡¡Cuando se formatea un volumen con NTFS, el grupo TODOS adquiere Control Total del volumen!!!

Así, los directorios systemroot (normalmente C:\winnt), systemroot\system32 y systemroot\temp, tienen derechos de CONTROL TOTAL , CAMBIO Y CONTROL TOTAL respectivamente al grupo TODOS.

Para corregirlo, una vez comprobado que el ADMINISTRADOR tiene CONTROL TOTAL sobre los mismos, cambiar a sólo LECTURA systemroot sin propagar estos cambios a los subdirectorios, y systemroot\system32 a sólo LECTURA propagándolos, con la precaución de poner permiso de CAMBIO a TODOS a \winnt\system32\RAS y \winnt\system32\spool\Printer.

De la misma manera, el volumen C: donde se encuentran ficheros relacionados con el arranque de la máquina, debería ser formateado NTFS y los ficheros críticos deberían tener:

C:\boot.ini -> Control total para Administradores y Sistema.
C:\ntdetect.com -> Control total para Administradores y Sistema.
C:\autoexec.bat -> Control total para Administradores y Sistema y Lectura a Todos.

C:\config.sys -> Control total para Administradores y Sistema y Lectura a Todos.

4. - Compartición de recursos de red:

Para compartir recursos a la red solo tendremos que pinchar con el botón derecho sobre un directorio o una impresora y veremos una opción que será compartir. Nos aparecerá un menú desde donde podremos compartir el recurso. Pulsaremos ahora en permisos...

Los recursos de la red se comparten de forma segura con los siguientes permisos:

- **CONTROL TOTAL:** permite modificar permisos, tomar en propiedad y permisos de CAMBIO
- **CAMBIO:** permite crear directorios, añadir ficheros, modificar datos y permisos de éstos, borrar ficheros y directorios, y permisos de READ.
- **LECTURA:** permiten listar directorios, ficheros.
- **SIN ACCESO:** este permiso sobreescribe cualquier otro y deniega el acceso al recurso.

OJO!!! : estos permisos sólo son efectivos cuando se hace login en la red; en nada influyen si el usuario accede localmente. Para los accesos locales se usan los permisos NTFS. El grupo TODOS tiene asignado automáticamente CONTROL TOTAL ante cualquier recurso compartido. Nunca debe pues compartir directorios que contengan información crítica del sistema.

A diferencia de los permisos NTFS, no se pueden asignar diferentes permisos a distintos ficheros de un mismo directorio compartido.

Cuando se combinan los permisos de recursos compartidos y los permisos en un volumen NTFS, prevalece el más restrictivo.

5.- Seguridad del registro:

El registro es una base de datos que mantiene información sobre la configuración hardware, software y de entorno de la máquina. Se puede ver con REGEDT32. Windows NT 4.0 no permite el acceso remoto al registro por defecto. Es conveniente pues:

- Deshabilitar el acceso remoto al registro, chequeando la existencia de la siguiente entrada en el registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

- Deshabilitar (poner a 0) si es necesario el apagado del equipo en la opción ShutdownWithoutLogon de:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

- Proteger adecuadamente el registro de usuarios no autorizados.
- Hacer copias periódicas del mismo con la utilidad REGBACK.EXE

6.- Auditorías.

El Sistema de auditorías de Windows NT permite rastrear sucesos que ocurren en una máquina NT, servidor de dominio o estación o servidor NT . Las auditorías son esenciales para mantener la seguridad de los servidores y redes. Permiten un seguimiento de las actividades realizadas por los usuarios .

La política de auditorías se establece en cada máquina NT. Se pueden realizar tres tipos de auditorías en NT:

a) Auditoría de cuentas de usuario: rastrea los sucesos de seguridad y escribe apuntes en el registro de seguridad. Se activa en Administrador de usuarios en dominios -> Directivas -> Auditoría. PLAN DE AUDITORIAS.

Los eventos que se pueden auditar son:

- Logon y logoff en la red
- Acceso a ficheros , directorios o impresoras
- Ejercicio de los derechos de un usuario
- Seguimiento de procesos
- Tirada o arranque del sistema...

b) Auditoría del sistema de archivos: rastrea sucesos del sistema de archivos. Se activa esta opción en Propiedades, tras pulsar con el botón derecho sobre el fichero o directorio que se desee auditar y luego seleccione Seguridad -> Auditorías.

Los eventos que se pueden auditar son: LECTURA, ESCRITURA, EJECUCIóN, ELIMINACIóN, CAMBIO DE PERMISOS Y TOMA DE POSESIóN.

Para auditar ficheros y directorios, éstos deben estar localizados en un volumen NTFS.

c) Auditoría de impresoras: primero se establece la política de auditorías haciendo doble click en la impresora en cuestión, dentro del menú Impresoras, y luego seleccionar Seguridad -> Auditorías.

Algunos de los eventos que se pueden auditar son: uso de la impresora, cancelar trabajos de impresión, control total de la impresora...

Se debe tener derechos de administrador para configurar propiedades de auditoría.

Una vez que se activa una auditoría se utiliza el Visor de sucesos dentro de Herramientas administrativas para ver los eventos auditados.

Se debería tener cuidado y proteger los archivos de auditoría que están almacenados en el directorio \winnt\system32\CONFIG en los archivos:

- APPEVENT.EVT : Registro de sucesos en aplicaciones.
- SECEVENT.EVT : Registro de sucesos de seguridad.
- SYSEVENT.EVT : Registro de sucesos del sistema.

Algo **muy importante** a la hora de mirar los registros es que la máquina tenga la hora correcta, ya que si tenemos que comparar con los registros de otras máquinas, si ambas no están sincronizadas será muy difícil. Para esto podemos usar NTP (Network Time Protocol) que sirve para poner en hora ordenadores. Tecnologías de la Información ofrece este servicio a todas las máquinas de la UAM y podrás encontrar más información pulsando aquí. Lo único que

necesitas es un software que puedes bajarte pincharlo aquí y configurarlo.

7.- Seguridad de los Protocolos. Seguridad de los servicios.

Debemos usar solo los protocolos que vayamos a necesitar. En principio y salvo que tengamos necesidad de usar más protocolos, podríamos dejar solo dos:

- NetBEUI
- TCP/IP

Con estos dos protocolos son solo de dos tipos los servicios que estamos ofreciendo a la red:

- SMB: (**B**loques de **M**ensajes de **S**ervidor) de Microsoft que son servicios de archivos y red. Estos servicios están instalados por defecto normalmente.
- Servicios TCP/IP e Internet como servidores Web y FTP. Se pueden instalar de modo opcional.

Estos son algunos de los puertos TCP/IP que podemos instalar en una máquina NT:

Servicio / Puerto / Protocolo	Descripción
FTP / 21 / tcp	Servidor FTP.
SMTP / 25 /tcp	Gestiona la distribución del correo de la máquina.
DNS / 53 / tcp-udp	Servidor de nombres (DNS)
GOPHER / 70 / tcp	Sistema de indexación de los servidores FTP (obsoleto)
HTTP (WWW) / 80 / tcp	Servidor WWW
POP2 / 109 / tcp	Servidor de correo Pop versión 2
POP3 / 110 / tcp	Servidor de correo Pop versión 3
NEWS / 119 / tcp	Servidor de News
NETBIOS / 137-138-139 / tcp-udp	Windows for Workgroups

Conviene tener abiertos el menor número de servicios. Al ser estos opcionales, no vienen instalados por defecto y hay que instalarlos a posteriori. Salvo que se necesiten y que se sepa lo que se está haciendo, conviene no instalar ninguno.

También se pueden configurar las opciones de seguridad TCP/IP para permitir o bloquear la dirección del (los) puerto(s) que se necesiten según los servicios que se quieran ejecutar. Para hacer esto, siga la siguiente secuencia:

Panel de Control -> Red -> Protocolos -> Protocolo TCP/IP -> Propiedades -> Avanzadas
Marque: Activar seguridad
Pulse el botón Configurar
Seleccione el adaptador correspondiente y marque el número de puerto/s del servicio/s que quiera permitir.

8.- Services Pack

Los Services Pack (SP) no son más que un conjunto de parches que Microsoft saca de vez en cuando para solucionar fallos, bugs, dar nuevas funcionalidades, etc... Lo bueno de estos parches es que de una sola vez aplicas todos (a veces más de 100) rápida y fácilmente.

Todo NT debería tener instalado al menos el SP5. En la actualidad ya ha salido el SP6a. La versión española del SP6a también está disponible.

IMPORTANTE: Nunca instalar un SP en ingles en un NT en español. Nos causará un sinfín de problemas y en algunos casos habrá que reinstalar el sistema.

Puedes bajarte el SP que necesites aquí:

	SP5	SP6a
Castellano	SP5i386-español	SP6ai386-español
Ingles	SP5i386-ingles	SP6i386-ingles

9.- Para acabar...

- No conviene que NT esté instalado en una máquina con arranque dual, ya que esto haría que muchas de sus garantías de seguridad perdieran efectividad.
- Es casi obligado que la partición sea NTFS, no encontraremos ninguna razón para instalar NT en una partición FAT.
- Conviene dar a cada uno de los usuarios del sistema unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esta explícitamente permitido, esta prohibido" y continuar explicando todo lo que está permitido. Si se dejan las cosas claras desde un principio, no ahorraremos muchos quebraderos de cabeza.
- Administrador no hay más que uno. Aunque NT permite que haya varios administradores para tareas determinadas, es muy importante delimitar estas tareas al máximo si son de una persona las que administran la máquina. A medida que el número de administradores tiende a infinito, la funcionalidad en la máquina tiende a cero.
- Los usuarios solo deben tener los privilegios necesarios para ser usuarios. En un exceso de celo, podemos cometer el error de limitar demasiado los privilegios de los usuarios. Esto hace que el usuario no pueda usar la máquina normalmente y perdamos de vista el objetivo por el que hacemos todo esto. Por otro lado, si los usuarios tienen excesivos privilegios (algunos administradores irresponsables lo permiten para no tener que hacer las cosas ellos y que las hagan los usuarios) nos podemos encontrar que por desconocimiento, experimentación o maldad se cause daño al sistema.
- Como decíamos arriba, una buena política de passwds es conveniente: obligar a cambiar el passwd cada 3 meses, chequear las passwd de los usuarios contra diccionarios para encontrar passwds fáciles, no dejar repetir passwds, etc.
- Por último decir que esta guía no es por supuesto exhaustiva, así que donde esta no llegue, puede pedir más información a cau@uam.es. De todas formas recomendamos como receta general, una búsqueda exhaustiva de información, una buena dosis de sentido común y un pellizco de paranoia.