UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES.

TEMA:

"Análisis e Implementación de seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información en el Ilustre Municipio del Cantón Pujilí**".**

DIRECTOR: ING. SEGUNDO CORRALES.

POSTULANTES: OÑATE BUSTILLOS FELIX SEBASTIAN
SANGUCHO SANDOVAL ABRAHAN DAVID

Latacunga, 02 de Mayo 2012

ÍNDICE DE CONTENIDOS

ÍNDICE DE CUADROS Y GRÁFICOS

AGRADECIMIENTO

Primeramente quiero dejar impregnado mis más sinceros agradecimientos a la Universidad Técnica de Cotopaxi, la misma que me acogió cuando decidí comenzar mi aventura la cual me vio formar profesionalmente y llegar a ser un ser útil en nuestro país.

A la Ilustre Municipalidad del Cantón Pujilí por haberme abierto sus puertas y permitido realizar mi tesis y culminarla.

Agradezco a todos los profesores que contribuyeron con un granito de arena para guiarme en este largo trayecto, no solo en el ámbito profesional, sino también como seres humanos al Ing. Segundo Corrales quien fue el responsable de darme el último empujón en mi carrera colaborando y guiando durante el desarrollo del presente proyecto.

También quiero mencionar a mis padres quienes con su magnífico y constante apoyo siempre han estado presentes en mi largo caminar en el alcance de mis metas.

También agradezco a mi gran hermano quien siempre me a inspirado y me brindado fuerza para luchar.

A mis primos aquellos quienes han estado presente alentando para cumplir y terminas lo propuesto.

Y por supuesto agradezco a mi abuelita que siempre será la mayor inspiración para nunca rendirme.

Félix Sebastián Oñate Bustillos

AGRADECIMIENTO

La presente Tesis es un esfuerzo en el cual, directa o indirectamente, participaron varias personas leyendo, opinando, corrigiendo, teniéndome paciencia, dándome ánimo, acompañándome en los momentos de crisis y en los momentos de felicidad.

Mi gratitud, principalmente está dirigida al Niñito de Isinche por haberme dado fuerza y permitido llegar al final de esta carrera.

A nuestra casa de estudios la Universidad Técnica de Cotopaxi por haberme dado la oportunidad de ingresar al Sistema de Educación Superior y cumplir este gran sueño.

A todos GRACIAS.

Abrahan David Sangucho Sandoval

DEDICATORIA

A mi Dios por concederme toda la felicidad y tener la dicha de recibir tus bendiciones. Gracias mi dios por no abandonarme.

Te dedico a ti papito Segundo Oñate, lo único que puedo decir gracias por todo tu amor y sacrificio que hiciste por mí, ya que fuiste uno de los pilares fundamentales en mi vida y que sin ti no hubiera podido cumplir todos mis sueños y mis metas.

También con todo mi amor a ti madrecita querida Celinda Bustillos que con tu sublime apoyo diariamente y bendiciones he podido culminar mi carrera y conseguir este tan ansiado título que me lo he propuesto conseguir.

A mi gran hermano Braulio Oñate por todos los momentos inolvidables que hemos pasado juntos, quien también a brinda su gran apoyo que ha sido lo máximo para seguirme superando sin desmayar en el alcance de mis metas.

Como olvidarme de unas de las personas más importantes en mi vida, mi segunda madre que es mi abuelita Irene Martínez quien desde muy pequeño me ha brindado su apoyo para ser siempre luchador en mi vida.

Y por supuesto aquellas personas que han estado siempre a mi lado como son mis primos dándome el ánimo siempre que lo he necesitado.

Félix Sebastián Oñate Bustillos

DEDICATORIA

Es mi deseo como sencillo gesto de agradecimiento, dedicarle mi humilde obra de trabajo de grado plasmada en el presente Informe, en primera instancia a mi Abuelita María Juana Sandoval, (que ya partió a la presencia del Altísimo) quien permanentemente me apoyo con espíritu alentador, contribuyendo incondicionalmente a lograr las metas y objetivos propuestos.

A los docentes que me han acompañado durante el largo camino, brindándome siempre su orientación con profesionalismo ético en la adquisición de conocimientosy afianzando mi formación como estudiante universitario.

A mi familia que me acompañaron a lo largo del camino, brindándome la fuerza necesaria para continuar y momentos de ánimo así mismo ayudándome en lo que fuera posible, dándome consejos y orientación, estoy muy agradecido.

A todos GRACIAS.

Abrahan David Sangucho Sandoval

RESUMEN

Para realizar el análisis e implementación de seguridades ipsec el cual ayudará al traslado y manejo seguro de información del Ilustre Municipio del Cantón Pujilí se ha utilizado muchas fuentes bibliográficas las cuales nos han brindado satisfactoriamente las necesidades requeridas para solucionar el problema propuesto en el proyecto.
La metodología seguir es el método científico para realizar el análisis de IPSec se investigó varias iniciativas sobre cómo probar que un sistema es seguro.

Tomando en cuenta la necesidad del Ilustre Municipio del Cantón Pujilí para el envío y recepción segura de información es factible la implementación de las seguridades IPSec ya que a raíz del avance tecnológico van incrementando su nivel de protección y a su vez proporcionando nuevas herramientas para su configuración, lo cual a futuro será de mayor confiabilidad en las seguridades de la información.
Para el desarrollo del presente trabajo de investigación, se aplicaron herramientas que están dentro del mercado de la informática, como una de las principales tenemos el IPSec (**Internet Protocol Security**), el cual es un pionero en desarrollo en la flexibilidad de los requerimientos, seguridades, estabilidad, y economía al momento de crear estos proyectos.

PROTECCIÓN DE TRANSMISIÓN DE INFORMACIÓN

SUMMARY

To carry out the analysis and implementation of securities ipsec which will help to the transfer and sure handling of information of the Illustrious Municipality of the Canton Pujilí it has been used many bibliographical sources which have offered us satisfactorily the necessities required to solve the problem proposed in the project. The methodology to continue is the scientific method to carry out the analysis of IPSec it was investigated several initiatives on how to prove that a system is safe.

Taking into account the necessity of the Illustrious Municipality of the Canton Pujilí for the shipment and sure reception of information is feasible the implementation of the securities IPSec since soon after the technological advance they go increasing its protection level and in turn providing new tools for its configuration, that which will be of more dependability in the securities of the information to future.

For the development of the present investigation work, tools were applied that they are inside the computer science's market, like one of the main ones has the IPSec (Internet Protocol Security), which is a pioneer in development in the flexibility of the requirements, securities, stability, and economy to the moment to create these projects.

PROTECTION OF TRANSMISSION OF INFORMATION

Introducción

Con la evolución de las tecnologías de la información y el acceso masivo de la sociedad a la Internet ha aumentado exponencialmente el sentimiento de indefensión que tienen las empresas (y más aún los administradores de sistemas) sobre los datos sensibles publicados en sus servidores web.

Habitualmente se utilizan mecanismos de control de accesos de usuarios mediante login/password que verifican contra algún tipo de base de datos la identidad del usuario. Pero de todos es sabido que hoy en día cualquier persona podría mediante un simple vistazo al teclado del usuario conseguir estos datos de autentificación en el sistema y poner en entredicho la seguridad de estos datos de carácter privado.

Al momento de buscar una solución de conectividad entre redes distantes geográficamente, son muchas las alternativas que aparecen como posibles. La clave está en encontrar una solución que supla las necesidades de los usuarios.

El proyecto contiene tres capítulos, el primero, contiene los pasos esquemáticos para desarrollar el estudio propuesto el cual facilita la recopilación de la información para explicar y comprender la realización del mismo; este capítulo consta de: introducción, fundamentación teórica, en la que se detalla todo el contenido del proyecto que, conjuntamente con la metodológica propuesta que es el método científico, y el cronograma de actividades, permiten medir los avances que se generen, concordando con el diseño más adecuado para los análisis respectivos, planteados en el segundo capítulo; de la misma manera la etapa investigativa, en la que utilizamos el tipo de investigación que es la encuesta; esta permitirá la recolección de información para su análisis y requerimiento en la resolución del problema; y en el tercer capítulo, permite detallar a profundidad cada uno de los pasos planteados en los dos capítulos anteriores, estos son una herramienta esencial, que permiten ir puliendo las alternativas existentes, considerando tanto a factores externos como internos, pero que de una u otra

forma afectan al proyecto en su esencia; aquí se detallara, también se mostrara la realización y aplicación de la propuesta planteada en el proyecto el cual dará credibilidad del funcionamiento de la aplicación.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. DEFINICIONES BÁSICA

1.1.1. INFORMATICA

Según **Antonio Ortiz Medina (2004)** dice que Informática es la: "Ciencia que estudia el tratamiento automático de la información. El término procede del francés informatique formado a su vez por la conjunción de las palabras information y automatique" **(pág. 20).**

De acuerdo el sitio web: **www.mastermagazine.info/termino/5368.php** Informática es: "el procesamiento automático de información mediante dispositivos electrónicos **y** sistemas computacionales"**.**

En base al criterio de los investigadores la informática es: un conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadores.

1.1.2. INTERNET

Según el **manual curso de formación internet (2008)**dice que Internet es: "Un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial". (**pág 3)**

Los autores **Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff (2005)** manifiestan que Interned: **"**Es una red de arquitectura abierta, las redes individuales pueden ser diseñadas y desarrolladas separadamente y cada una puede tener su propia y única interfaz, que puede ofrecer a los usuarios y/u otros proveedores, incluyendo otros proveedores de Internet"**(pág 62-71)**.

Según el sitio web: **http://www.civila.com/desenredada/que-es.html**Internet es: "Una red de cómputo sustentada en tecnologías de vanguardia que permiten una alta velocidad en la transmisión de contenidos y funciona independientemente de la Internet comercial actual".

En base al criterio de los investigadores internet es: un conjunto de redes de comunicación con una determinada cantidad de contenidos para transmitir servicios a través de computadores conectados entre ellos mediante un protocolo de red.

1.1.2.1. VENTAJAS DEL INTERNET

En base ala investigación de los autores del proyecto de tesis define las siguientes ventajas del internet son:

- Permanencia en contacto con amigos, parientes y colegas alrededor del mundo, a una fracción del coste de una llamada telefónica o correo aéreo.

- Discusión sobre cualquier tema, desde la arqueología a la zoología, con la gente en varios idiomas diferentes.

- Exploración en millares de bibliotecas y bases de datos de información globalmente.

- Acceso a millares de documentos, diarios, reservas y programas.

- Servicio de Noticias de cualquier tipo, desde noticias deportivas hasta información metereológica.

- Facilita el aprender haciendo, construyendo cosas y resolviendo problemas.

1.2. PROTOCOLOS

1.2.1. PROTOCOLOS DE RED

Según el sitio web:
http://www.monografias.com/trabajos11/reco/reco.shtml Protocolos de red 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".

Según el.sitio.web:
http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29
Un protocolo es: "Una regla o estándar que controla o permite la comunicación en su forma más simple, puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación".

En base al criterio de los investigadores del presente trabajo protocolo de red es: aquel que sirve para enviar y recibir datos entre varios ordenadores, y también pueden una misma máquina coexistir instalados varios protocolos, pues es posible que una pc pertenezca a redes distintas.

1.2.2. CLASIFICACIÓN DE LOS PROTOCOLOS

En base a la investigación de los autores del proyecto de tesis define los siguientes conceptos:

1.2.2.1. TCP/IP

En el sitio web: **http://es.kioskea.net/contents/internet/tcpip.php3** TCP/IP es: "Un conjunto de protocolos, entre ellos los dos que le dan nombre: TCP y IP".

El protocolo IP se refiere a la forma de fraccionar los datos a enviar en bloques (paquetes, datagramas). Como ocurre con IPX, IP es un servicio no confiable (o de mejor esfuerzo), que no garantiza la recepción del paquete. El paquete podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. La confiabilidad es proporcionada por el protocolo de la capa de transporte, trabajando en equipo.

Según el sitio web:
http://www.monografias.com/trabajos15/arquitectura-tcp/.shtml

Protocolo TCP/IP es: "Un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos".

En base al criterio de los investigadores: Un protocolo es aquel que permite estar conectados a la red Internet, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un envió fiable de datos.

1.2.2.2. VENTAJAS

En base a la investigación de los autores del proyecto de tesis define las

siguientes ventajas de TCP/IP son:

- La primera posible consecuencia de este incremento es no es necesario el uso de sistemas NAT, ya que hay direcciones suficientes como para que todas las máquinas se conecten entre sí directamente, volviendo a ser una verdadera red entre extremos.

- Las direcciones IP se podrán obtener de forma totalmente automáticas, lo que facilitará enormemente la creación de redes, tanto a nivel local como a nivel externo.

1.2.2.3. DESVENTAJAS.

En base al criterio de varios autores las desventajas de TCP/IP son:

- Las direcciones solo contienen 32 bits por lo que es muy limitada
- Es lenta para transmitir videos y voz.
- En enlace el protocolo IPv4 supera a IPv6 en un 3,66 % para UDP y un 3,79 % para TCP.

1.2.2.4. MODO DE USO

En base a la investigación de los autores del proyecto de tesis el modo de uso de TCP/IP es: una de las redes más comunes utilizadas para conectar computadoras con sistema UNIX. Las utilidades de red TCP/IP forman parte de la versión 4, muchas facilidades de red como un sistema UUCP, el sistema de correo, RFS y NFS, pueden utilizar una red TCP/CP para comunicarse con otras máquinas.

Para que la red TCP/IP esté activa y funcionando será necesario:

- Obtener una dirección Internet.
- Instalar las utilidades Internet en el sistema

- Configurar la red para TCP/IP
- Configurar los guiones de arranque TCP/IP
- Identificar otras máquinas ante el sistema
- Configurar la base de datos del o y ente de STREAMS
- Comenzar a ejecutar TCP/IP.

1.2.3. IPV4

Según el sitio web: **www.wikipedia.org/wiki/Internet** Protocolo IPV4 es: "La cuarta versión del protocolo de Internet (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791".

Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4.

Según el sitio web: **www.configurarequipos.com**: Protocolo IPV4 es: "Una versión de 32bits y consta de cuatro grupos binarios de 8bits cada uno (8x4=32), o lo que es lo mismo, cuatro grupos decimales, formado cada uno por tres dígitos".

En base al criterio de los investigadores Protocolo IPV4 es:Un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de switches de paquetes (por ejemplo a través de Ethernet).

1.2.3.1. MODO DE USO

Este tipo de conexiones TCP/IP es cada vez más empleado no solo por ordenadores, sino también por dispositivos de otro tipo, tales como, por ejemplo, cámaras IP, comunicaciones de voz del tipo Voz IP, teléfonos móviles, PDA, etc. Para navegar en Internet.

1.3. SEGURIDADES DE RED

1.3.1 SEGURIDAD IP

Según el sitio web:**www.wikipedia.org/wiki/Internet**: seguridad IP es: "La base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa".

1.3.1.1 OBJETIVOS

En base a la investigación de los autores del proyecto de tesis define los siguientes objetivos de las seguridades IP son:

- En las páginas precedentes ha visto que Internet es, por encima de todo, un servicio valioso a nuestro alcance. Lo que se necesita ahora es software capaz de acceder a la red y que permita extraerle el máximo partido. Este Proyecto Fin de Carrera se enmarca en ese contexto.

- El número de protocolos de aplicación es muy elevado, y algunos de ellos son bastante complejos (HTTP), poco difundidos (IMAP4) o de dudosa utilidad en este contexto (Quote of the Day). Por ello, para cubrir adecuadamente las necesidades de los usuarios, es preciso que este Proyecto se diseñe como un entorno abierto y bien documentado, fácilmente mantenible y ampliable.

- Efectuar un diseño cuyos criterios principales sean la eficiencia en ejecución, la economía de recursos y, sobre todo, la portabilidad. Afrontar este reto con dicha actitud ha permitido desarrollar una herramienta lo bastante compacta, modular y portable como para ser recompilada para entornos personales de bajas prestaciones e incluso placas de desarrollo y pequeños prototipos informáticos.

- Alcanzar con este Proyecto era la propia formación del autor. El desarrollo del software ha supuesto un esfuerzo notable, compensado sobradamente por los conocimientos teóricos y prácticos adquiridos durante el proceso.

1.3.1.2 CARACTERÍSTICAS.

En base ala investigación de los autores del proyecto de tesis define las siguientes características de las seguridades IP son:

a) Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

b) La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro.

c) Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino.

d) Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino.

e) Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

f) La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye.

1.3.1.3 VENTAJAS.

En base a la investigación de los autores del proyecto de tesis define las siguientes ventajas de las seguridades IP son:

- El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web.

- Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

- El conjunto TCP/IP se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, como así también en redes pequeñas o domésticas, y hasta en teléfonos móviles y en domótica.

- Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que Net BEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo.

1.4. ARQUITECTURA DEL PROTOCOLO TCP/IP

Según el sitio web:
http://www.monografias.com/trabajos15/arquitecturatcp/arquitectur.
Dice que: La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes.
- Físico: Análogo al nivel físico del OSI.
- Red: Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

CUADRO 1.1 Arquitectura TCP/IP

NIVEL DE APLICACIÓN
NIVEL DE TRANSPORTE
NIVEL DE INTERNET
NIVEL DE RED
NIVEL FÍSICO

Fuente: http://usuarios.multimania.es/janjo/janjo1.html:

1.5. VPN

Según el sitio web: **http://www.configurarequipos.com/doc499.html:** VPN es: "Una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas".

Según el autor: **Roberto Nader Carreón (1996) VPN es:** "Una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte"**(pág 26)**.

En:**http://sistemas.anmat.gov.ar/aplicaciones_net/applications/menu/vpn** Una VPN es: "Una red privada que utiliza redes públicas (generalmente Internet) para conectar varios lugares o usuarios remotos entre ellos. En vez de utilizar una conexión dedicada o líneas alquiladas".

En base al criterio de los investigadores VPN es: Una red privada virtual o VPN (siglas en inglés de virtual prívate network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.

1.6. IP SEC

Según **J.P. Degabriele y K.G. Paterson (2001):** IPSec es: "Un grupo de extensiones de la familia del protocolo IP. Esta provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación"(**pag130)**.

Según el sitio web: **http://es.wikipedia.org/wiki/IPsec**:IPsec (abreviatura de Internet Protocol security) es: "Un conjunto de protocolos cuya función

es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos".

Según el sitio web: **http://www.ipsec-howto.org/spanish/x161.html:** IPsec es: "Una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4".

En base al criterio de los investigadores IPSec es: un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

1.6.1 OBJETIVOS

En base a la investigación de los autores del proyecto de tesis define los siguientes objetivos de IPSec son:

- Control de acceso: previene el uso no autorizado de recursos.
- Integridad sin conexión: detección de modificaciones en un datagrama IP individual.
- Autenticación del origen de los datos.
- Protección anti-replay: una forma de integrabilidad parcial de la secuencia, detecta la llegada de datagramas IP duplicados.
- Confidencialidad: encriptación.
- Confidencialidad limitada del flujo de trafico: el uso del modo túnel permite encriptar las cabeceras IP internas, ocultando las identidades del origen del trafico y del (ultimo) destino. También, se puede usar el "relleno en la carga útil" de ESP para ocultar el tamaño de los paquetes, consiguiendo ocultar las características externas del trafico.

1.6.2 CARACTERÍSTICAS

Según los investigadores del proyecto las características de IPSec son:

- Claves basadas en criptografía. Las claves cifradas, que se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito.

- Administración automática de claves. Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques. IPSec usa el protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar dinámicamente claves cifradas entre los equipos que se comunican.

- Negociación de seguridad automática. IPSec usa *ISAKMP* para negociar de forma dinámica un conjunto de requisitos de seguridad mutuos entre los equipos que se comunican. No es necesario que los equipos tengan directivas idénticas, sólo una directiva configurada con las opciones de negociación necesarias para establecer un conjunto de requisitos con otro equipo.

- Seguridad a nivel de red. IPSec existe en el nivel de red, proporcionando seguridad automática a todas las aplicaciones.

- Autenticación mutua. IPSec permite el intercambio y la comprobación de identidades sin exponer la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los

sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicar con la protección de IPSec.

1.6.3 VENTAJAS

De acuerdo a los investigadores del proyecto las ventajas de IPSec son:

- Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada.

- IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

- La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía principalmente de larga distancia que son usuales de las compañías de la Red Pública Telefónica Conmutada.
- Las llamadas de VozIP a VozIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VozIP a PSTN que generalmente cuestan al usuario de VozIP.

- Transparente a aplicaciones (por debajo de la capa de Transporte)

- Provee seguridad para usuarios individuales.

- Un mensaje proviene de una fuente (ruteador) autorizado.

- Un mensaje redirigido viene del ruteador para el cual fue originalmente enviado.

- Las actualizaciones a las tablas de ruteo no hayan sido falsificadas

1.6.4 DESVENTAJAS

En base al criterio de varios autores la única desventaja: que se le ve a IPSec por el momento, es la dificultad de configuración con sistemas Windows. El Windows 2000 y Windows XP proveen herramientas para configurar túneles con IPSec, pero su configuración es bastante difícil (Microsoft nombra a todas las cosas en forma diferente de lo estándar), y además posee algunas limitaciones (como ser: necesita si o si IP estáticos).

1.6.5 ATAQUES A LA SEGURIDAD

A continuación se presenta una lista parcial de los ataques a las redes más comunes en base al criterio de varios autores:

- Rastreo. Un rastreador de red es una aplicación o un dispositivo que puede supervisar y leer los paquetes de la red. Si los paquetes no están cifrados, un rastreador de red obtiene una vista completa de los datos del paquete. El Monitor de red de Microsoft es un ejemplo de rastreador de red.
- Modificación de datos. Un atacante podría modificar un mensaje en tránsito y enviar datos falsos, que podrían impedir al destinatario recibir la información correcta o permitir al atacante conseguir la información protegida.
- Contraseñas. El atacante podría usar una contraseña o clave robadas, o intentar averiguar la contraseña si es fácil.
- Suplantación de direcciones. El atacante usa programas especiales para construir paquetes IP que parecen provenir de direcciones válidas de la red de confianza.
- Nivel de aplicación. Este ataque va dirigido a servidores de aplicaciones al explotar las debilidades del sistema operativo y de las aplicaciones del servidor.

- Intermediario. En este tipo de ataque, alguien entre los dos equipos comunicantes está supervisando activamente, capturando y controlando los datos de forma desapercibida (por ejemplo, el atacante puede estar cambiando el encaminamiento de un intercambio de datos).
- Denegación de servicio. El objetivo de este ataque es impedir el uso normal de equipos o recursos de la red. Por ejemplo, cuando las cuentas de correo electrónico se ven desbordadas con mensajes no solicitados.

1.7. DESCRIPCIÓN DEL PROTOCOLO

IPsec (abreviatura de Internet Protocol security) es: un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec está implementado por un conjunto de protocolos criptográficos para:

- asegurar el flujo de paquetes,

- garantizar la autenticación mutua y
- establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

1.7.1. DETALLES TÉCNICOS

A consideración de varios autores se detalla lo siguiente:

- Authentication Header (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

- Encapsulating Security Payload (ESP) proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.

- La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50 (ver /etc/protocols). Las siguientes secciones tratarán brevemente sobre sus propiedades.

- AH - Cabecera de autenticación; El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes

inmutables de la cabecera IP (como son las direcciones IP).

- ESP - Carga de Seguridad Encapsulada. El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC.

- El protocolo IKEEl e IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

1.8. LIMITACIONES

En base ala investigación de los autores del proyecto de tesis define las siguientes limitaciones:

- IPSec no es seguro si el sistema no lo es: Los gateways de seguridad deben estar en perfectas condiciones para poder confiar en el buen funcionamiento de IPSec.
- IPSec no provee seguridad de usuario a usuario: no provee la misma clase de seguridad que otros sistemas de niveles superiores. Por ejemplo, el GPG que se utiliza para cifrar mensajes de correo electrónico, si lo que se necesita es que los datos de un usuario los pueda leer otro usuario, IPSec no asegura esto y se tendrá que utilizar otro método.
- IPSec autentica máquinas, no usuarios: el concepto de identificación y contraseña de usuarios no es entendido por IPSec, si lo que se necesita es limitar el acceso a recursos dependiendo del usuario que quiere

ingresar, entonces habrá que utilizar otros mecanismos de autenticación en combinación con IPSec.

- IPSec no evita los ataques DOS: estos ataques se basan en sobrecargar la máquina atacada de tal modo de que sus usuarios no puedan utilizar los servicios que dicha máquina les provee.

1.8.1. REQUISITOS DEL PROTOCOLO DE IPSEC.

En base al criterio de varios autoresRequisitos del protocolo de IPSec son:

El software sólo es compatible con dispositivos que dispongan de sistema operativo MS Windows Mobile 2003.
Los requisitos mínimos del sistema para instalar y ejecutar el cliente IPSec son los siguientes:

- PC: Sistema operativo Windows 95/98/NT/2000/XP. ActiveSync 4.1 o superior
- Dispositivo móvil: Sistema operativo "MS Windows Mobile 2003" y 850Kb libres de memoria.
- Se requiere por lo menos una conexión correctamente configurada (GPRS, Bluetooth, WiFi) para conectar con la RPV-IP.

1.8.2. IDENTIFICACIÓN DE LOS CASOS DE USO

La ayuda de IPsec se pone en ejecución generalmente en núcleo con la gerencia dominante y ISAKMP/IKE negociación realizada de usuario-espacio. Las puestas en práctica existentes de IPsec tienden para incluir ambas funcionalidades. Sin embargo, como hay un interfaz estándar para la gerencia dominante, es posible controlar un apilado de IPsec del núcleo usando las herramientas de gerencia dominantes de una diversa puesta en práctica.

Las nuevas arquitecturas de los procesadores de red, incluyendo procesadores multi-core con los motores integrados del cifrado, cambio la manera los apilados de IPsec se diseñan. Una trayectoria rápida dedicada se utiliza para sacar datos el proceso del proceso de IPsec (las operaciones de búsqueda del SA, del SP, cifrado, etc.).

Estos apilados rápidos de la trayectoria se deben co-integrar en corazones dedicados con Linux o RTOS que funciona en otros corazones. Este el OS es el plano del control que funciona ISAKMP/IKE del apilado rápido de IPsec de la trayectoria.

1.9. DIRECIONES IP A UTILIZAR

En base ala investigación de los autores del proyecto de tesis IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4,294,967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión (Multicast), etc.

1.9.1 CARACTERÍSTICAS

En base al criterio de varios autores las características de las direcciones IP son:

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]), es decir, 16 777 214 hosts.

- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que

sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} - 2, o 65 534 hosts.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^8 - 2, ó 254 hosts.

1.9.2 VENTAJAS

En base al criterio de varios autores las ventajas de las direcciones IP son:

- Permite tener servicios dirigidos directamente a la IP.
- Esta combinación es capaz de generar aproximadamente 4.000 millones de combinaciones.
- Las direcciones solo contienen 32 bits por lo que es muy limitada.
- Es lenta para transmitir videos y vos.
- En enlace el protocolo IPv4 supera a IPv6 en un 3,66 % para UDP y un 3,79 % para TCP.

1.9.3 DESVENTAJAS

En base al criterio de varios autores las desventajas de las direcciones IP son:

- Son más vulnerables al ataque, puesto que el usuario no puede conseguir otra IP.

- Es más caro para los ISPs puesto que esa IP puede no estar usándose las 24 horas del día.

CAPITULO II

ANALISIS DE CAMPO PARA IMPLEMENTACIÓN DE SEGURIDADES IPSEC EN LA TRASMISIÓN DE DATOS EN INTERNET CON IPV4 Y EVITAR EL ACCESO INDEBIDO A LA INFORMACIÓN EN EL ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ.

ENTORNO DEL ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ.

ANTECEDENTES HISTORICOS

GOBIERNO MUNICIPAL DEL CANTON PUJILI

2.1. INTRODUCCIÓN

El 22 de Septiembre de 1852 la Asamblea Constituyente presidida por Don Pedro Moncayo Esparza, jurista e historiador imbabureño, aprueba en tercer y último debate la Cantonización de Pujilí, mediante decreto que fuera sancionado por el general José María Urbina Viteri, Séptimo Presidente Constitucional de la República que ejerció el poder de 1852 a 1856, deduciéndose que la Cantonización de Pujilí quedó firmada y sella en trámite legal el 24 de Septiembre de 1852 pero transcurrieron 10 días más para que el decreto llegara a la Gobernación de León publique por bando hasta que el Juzgado Primero Parroquial de Pujilí sentó en sus libros la histórica razón " Octubre 14 de 1852.- Recibo en esta fecha el presente Decreto; se publicó con la solemnidad debida y en los lugares públicos y acostumbrados, lo que pongo por diligencia para que conste".

El cantón Pujilí se localiza en la zona interandina del Ecuador, se encuentra ubicado a 12 Km al oeste de Latacunga; sus límites son al Norte: Sigchos, Saquisilí y Latacunga; al Sur: Pangua, Bolívar y Tungurahua

(Ambato); al Este: Latacunga y Salcedo y al Oeste: La Maná y Pangua.

2.1.1 RESEÑA HISTÓRICA

ILUSTRE MUNICIPIO DE PUJILI

FUENTE:http://www.municipiopujili.gov.ec/index.php?option=com_content&view=article&id=125:historia-de-pujili&catid=105:historia&Itemid=168

Pujilí al igual que el resto de pueblos situados en los páramos del occidente de la Cordillera de los Andes estuvo habitada por "Aborígenes Panzaleos", estos aborígenes analfabetos a quienes se los describe como personas dedicadas a las labores agrícolas, a la alfarería y al pastoreo del ganado. Cosechaban cereales y frutos, debido a que estas tierras eran bosques de clima templado, cansados de las invasiones a su territorio, decidieron desprenderse de sus lares nativos, llegaron hasta comarca pujilense asentándose en este al pie de la loma de Sinchahuasín. En aquel asiento indígena fueron aprovechados algunos materiales para los trabajos agrícolas.

ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ

DECRETO CANTONIZACIÓN:

"REPÚBLICA DEL ECUADOR.- La Asamblea Nacional del Ecuador,

Considerando:

1.- Que concentrada la acción administrativa, se promueve eficazmente el progreso de los pueblos.

2.- Que la Parroquia de Pujilí y sus anexos tienen elementos para formar un Cantón.

2.1.2 FUNCIONES

CUADRO N 2.1

FUNCIONARIO	**CARGO**
Dr. Milton Molina	DIRECTOR FINANCIERO
Ing. Rodrigo Ramos M.	DIRECTOR DE OBRAS PUBLICAS
Dr. William Rodríguez	PROCURADOR SINDICO MUNICIPAL
Ab. Rubén Cevallos M.	SECRETARIO GENERAL DEL I. CONCEJO
Lic. Luis Yánez V.	TESORERO MUNICIPAL
Sra. Vanessa Moreno R.	ANALISTA DE PERSONAL
Sr. Eduardo Sarzosa J.	RELACIONADOR PUBLICO
Lic. Juan Albán	COORDINADOR GENERAL
Tlga. Verónica Herrera	JEFE DE EDUCACION, CULTURA Y TURISMO
Egdo. Fernando Karolys M.	JEFE DESARROLLO SOCIAL
Srta. Inés Jácome S.	JEFE DE AVALUOS Y CATASTROS
Msc. Fausto Ruiz Sarzosa	JEFE ADMINISTRATIVO
Ing. Carlos Arroyo C.	JEFE DE SISTEMAS y MEDIOS TECNOLOGICOS
Sra. Sonia Arroyo S.	JEFE DE RENTAS
Lic. Elsa León	JEFE DE CONTABILIDAD
Ing. Javier Navarro	JEFE DE MEDIO AMBIENTE
Tlgo. Diego Amaya	INSPECTOR PARQUES Y JARDINES
Ing. Jaime Lozada	PLANIFICACION Y URB.
Arq. Napoleón Romero	FISCALIZACION

Ing. Edgar Neto	COMISARIO MUNICIPAL
Prof. Darwin Naranjo	SECRETARIO COMISIONES
Sr. Manuel Herrera	JEFE DE MAQUINARIA
Sr. Marcelo Cajas	JEFE DE TALERES
Sr. Humberto Chusín	GUARDALAMCEN
Lic. Natalia Lascano	PRESIDENTA DEL PATRONATO MUNICIPAL DE AMPARO SOCIAL

FUENTE:http://www.municipiopujili.gov.ec/index.php?option=com_content&view=article&id=125:historia-de-pujili&catid=105:historia&Itemid=168

REALIZADO POR: LOS INVESTIGADORES

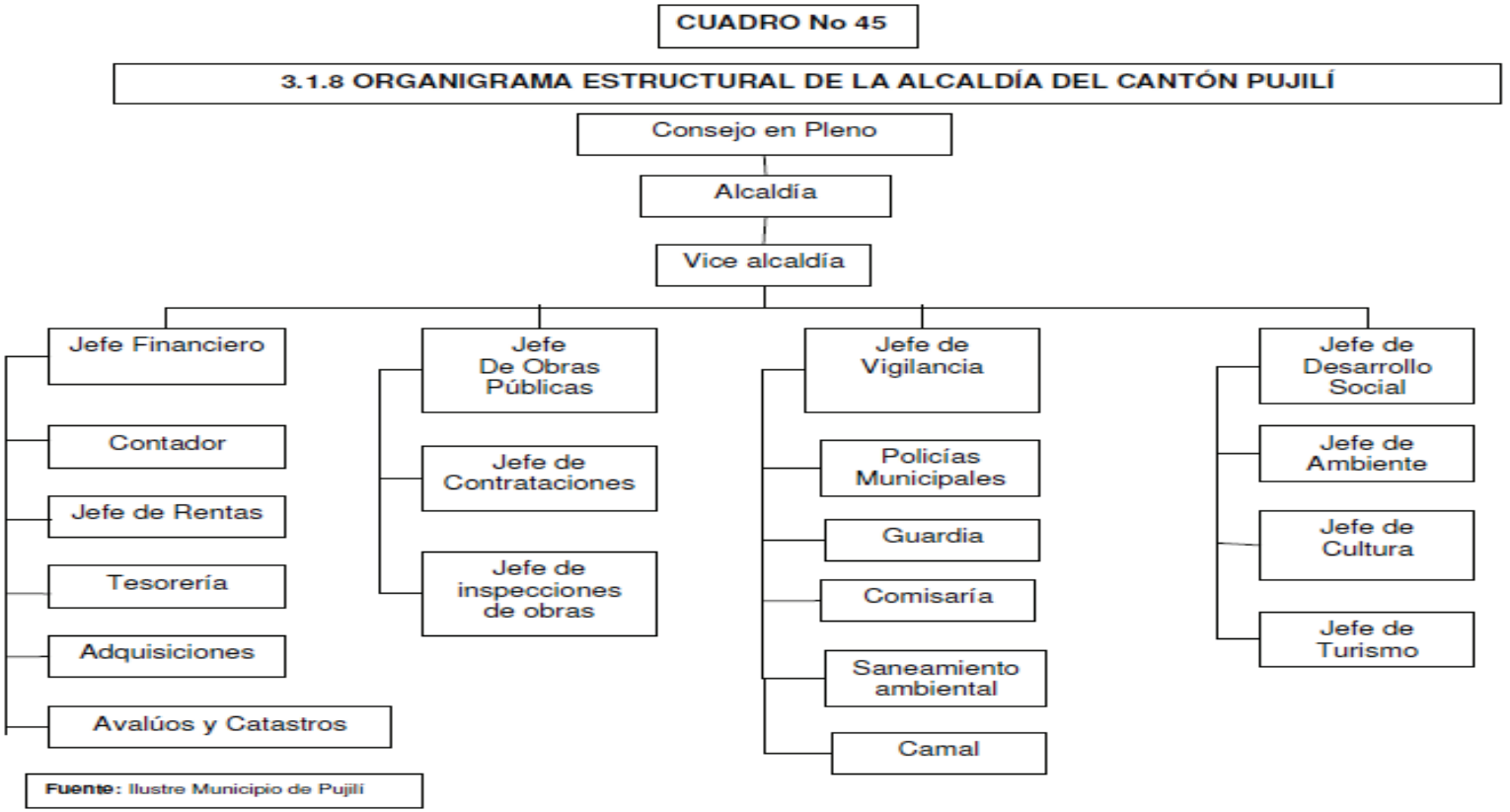
2.1.3 MISIÓN

- Planear, implementar y sostener las acciones del desarrollo del gobierno local.
- Dinamizar los proyectos de obras y servicios con calidad y oportunidad, que aseguren el desarrollo social y económico de la población, con la participación directa y efectiva de los diferentes actores sociales, dentro de un marco de transparencia, ética institucional y el uso óptimo de los recursos humanos altamente comprometidos, capacitados y motivados.

2.1.4 VISIÓN

- El Gobierno Municipal de Pujilí, para los próximos años se constituirá en un ejemplo del desarrollo local y contará con una organización interna, altamente eficiente, que genere productos y servicios compatibles con la demanda de la sociedad, capaz de asumir los nuevos papeles vinculados con el desarrollo, con identidad cultural y de género, descentralizando y optimizando los recursos.

2.1.5 ESTRUCTURA ORGANIZACIONAL



FUENTE:http://www.municipiopujili.gov.ec/index.php?option=com_content&view=article&id=125:historia-de-pujili&catid=105:historia&Itemid=168

2.1.6 OBJETIVOS.

- Contribuir al fomento y protección de los intereses locales.
- Planificar e impulsar el desarrollo físico del Cantón, sus áreas urbanas y rurales, realizando las obras y servicios que fueran necesarios para una convivencia humana, plausible de la comunidad pujilense, obteniendo como fin la dotación de servicios básicos como: agua potable de calidad, alcantarillado, energía eléctrica, adoquinado de calles, aceras y bordillos.
- Acrecentar el espíritu de integración de todos los actores sociales y económicos, el civismo y la confraternidad de la población para lograr el creciente progreso del Cantón.
- Coordinar con otras entidades, el desarrollo y mejoramiento de la cultura, de la educación y la asistencia social.
- Investigar, analizar y recomendar las soluciones más adecuadas a los problemas que enfrenta el Municipio, con arreglo a las condiciones cambiantes, en lo social, político y económico.
- Estudiar la temática municipal y recomendar la adopción de técnicas de gestión racionalizada y empresarial, con procedimientos de trabajo uniformes y flexibles, tendientes a profesionalizar y especializar la gestión del gobierno local.
- Auspiciar y promover la realización de reuniones permanentes para discutir los problemas municipales, mediante el uso de mesas redondas, seminarios, talleres, conferencias, simposios, cursos y otras actividades de integración y trabajo.

2.1.7 POLITICAS.

- Siendo el Gobierno Municipal del Cantón de Pujilí una entidad de Derecho Público, con finalidad social, autonomía administrativa y financiera tiene como objetivo primordial el logro del bienestar de la comunidad de PUJILÍ, a través de la satisfacción de las necesidades

colectivas derivadas de la convivencia urbana y rural.

- Trabajo de calidad optimizando todos y cada uno de los recursos disponibles como son: Talento humano, materiales, económicos y naturales.
- Concertación con los diferentes actores sociales, para el logro de una participación efectiva en el desarrollo de la Comunidad.
- Movilización de esfuerzos para dotar al Municipio de una infraestructura administrativa, material y humana que permita receptar y procesar adecuadamente los efectos de la descentralización.

- Identificación de los problemas prioritarios de la comunidad y búsqueda oportuna de las soluciones más adecuadas, con el menor costo y el mayor beneficio.

2.1.8 GENERALIDADES.

- TURISMO
- PALACIO MUNICIPAL
- IGLESIA MATRIZ
- CENTRO ARTESANAL "EL ROSAL"
- LA HOSTERÍA "EL CAPULÍ"
- COLINA SINCHAHUASÍN
- EL PARQUE CENTRAL "LUIS FERNANDO VIVERO"
- EL DIVINO NIÑO DE ISICHE
- EL MERCADO CENTRAL
- EL DANZANTE
- MONUMENTOS A LA CULTURA PUJILENSE
- EL DANZANTE
- LA ESPOSA DEL DANZANTE
- LOS REYES
- LA HILANDERA
- LA MISHQUERA

2.2. METODOLIGÍA DE INVESTIGACIÓN

2.2.1. METODO DE INVESTIGACIÓN.

Esta investigación está basada en el método científico, El método científico o experimental es una manera de recopilar información y comprobar ideas, La esencia del método científico consiste en el planteamiento de preguntas y búsqueda de respuestas, las cuales deben ser susceptibles de comprobación.

Es una manera de recopilar información y comprobar ideas. A pesar de que el procedimiento puede variar, el método científico consta de los siguientes pasos generales: hacer observaciones; formular hipótesis; someter a prueba las hipótesis y llegar a conclusiones.

2.2.2. TIPO DE INVESTIGACIÓN.

Para la realización de este trabajo, existen diversos tipos de investigación, y hubo que analizarlos todos para saber cuál es el apropiado para este proyecto.

Determinamos que el tipo de investigación que más se acomoda para la realización de este proyecto es la descriptiva la cual permite describir la estructura de los fenómenos y su dinámica. Están en el primer nivel de conocimiento científico. Utilizan básicamente técnicas cualitativas entre las que se puede distinguir:

- Investigación por encuesta.

2.2.3. TECNICA DE INVESTIGACIÓN.

La técnica de investigación fue la encuesta la destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente

por escrito. Ese listado se denomina cuestionario.

Es impersonal porque el cuestionario no lleve el nombre ni otra identificación de la persona que lo responde, ya que no interesan esos datos. Es una técnica que se puede aplicar a sectores más amplios del universo, de manera mucho más económica que mediante entrevistas.

2.3. ANÁLISIS DE LOS RESULTADOS DE LA OBSERVACIÓN DEL OBJETO DE ESTUDIO LA INVESTIGACIÓN.

2.2.1 POBLACION Y MUESTRA

2.2.1.1 POBLACIÓN

Para el desarrollo del proyecto se enfocará de manera directa a la siguiente población:

Empleados	15
Total	15

2.2.1.2 MUESTRA

En el **ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ** de la ciudad de Pujilí, se ha tomado en cuenta a las personas aquellas que utilizan computadoras para realizar las encuestas, las cuales ameritan para la muestra.

2.4. Análisis de los resultados de la encuesta realizada a los administradores y jefe de sistemas del Ilustre Municipio del Cantón Pujilí.

Para el desarrollo del trabajo investigativo se utilizó la técnica de la encuesta que se aplicó aquellos Empleados del **ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ** de la ciudad de Pujilí, con la finalidad de obtener información relevante que satisfaga cada una de las incógnitas planteadas.

1. A manejado usted internet**?**

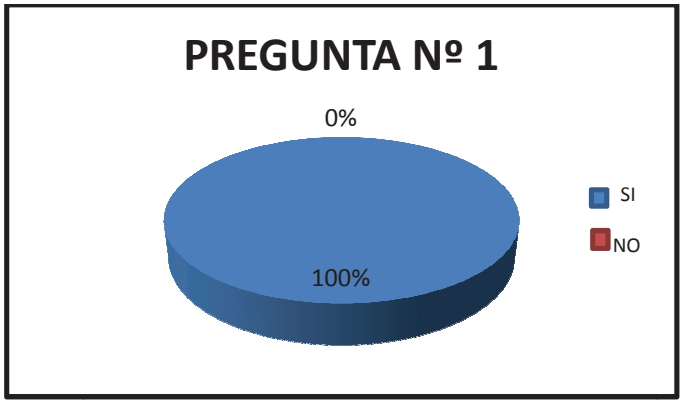
TABLA Nº 1

Internet

Opciones	**Valor**	**%f**
Si	15	100%
No	0	0%
TOTAL	**15**	**100**%

GRAFICO Nº1

Internet



Análisis.

Como se puede observar en el gráfico la respuesta SI alcanza un 100%, y el NO posee un 0% de los encuestados, el cual indica que poseen un conocimiento básico sobre lo que es internet y sobre todo los empleados siempre están conectados a internet.

2. Cree usted que en el Ilustre Municipio del Cantón Pujilí existe la debida seguridad en el envío y recepción de la información?

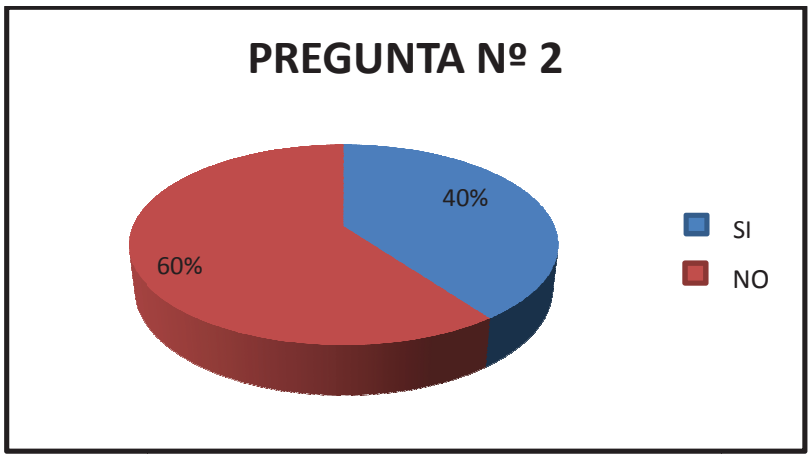
TABLA Nº 2

Seguridad en el envió

Opciones	Valor	%f
Si	6	40%
No	9	60%
TOTAL	**15**	**100%**

GRAFICO Nº2

Seguridad en el envió



Análisis.

Como se puede observar en el gráfico el 40% de los encuestados cree que existe seguridad de los datos en el Municipio y el 60% de los mismos cree que no tienen suficientes seguridades por lo cual sería factible la implementación de seguridades.

3. Que tan seguro es para usted el envío de información a través de la red?

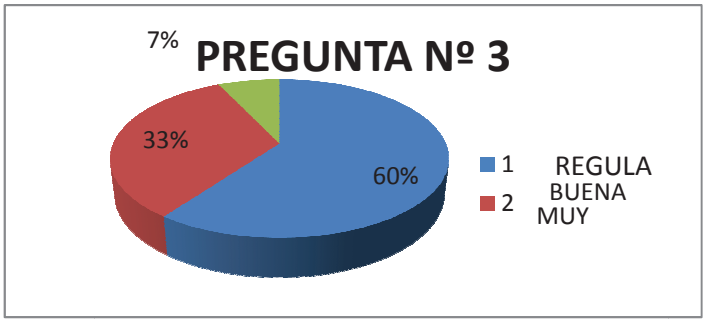
TABLA Nº 3

Envió de información

Opciones	Valor	%f
Regular	9	60%
Buena	5	33%
Muy Buena	1	7%
TOTAL	**15**	**100%**

GRAFICO Nº3

Envió de información



Análisis.

Como se puede observar en el gráfico el 33% de los encuestados cree que el envió de la información es buena que no se realiza con tanta seguridad por el hecho que existen personas que pueden accesar fácilmente a la información y por eso es regular el 60% de los mismos cree que es regular y el 7% muy buena por lo cual necesitan un cien por ciento de confiabilidad para evitar el acceso indeseado a los datos.

4. Conoce usted si existe algún tipo de seguridad que proteja la información importante dentro del Ilustre Municipio del Cantón Pujilí?

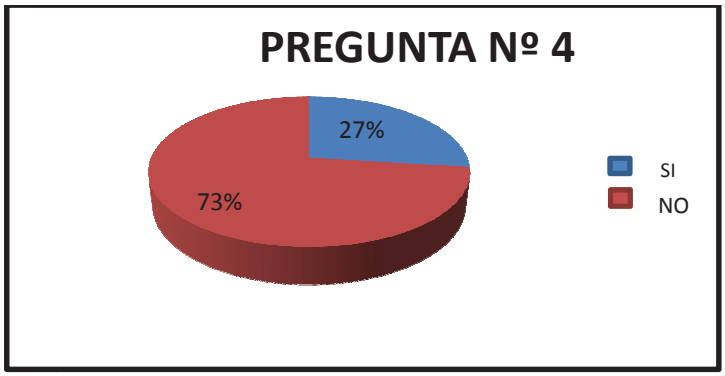
TABLA Nº 4

Existencia de información

Opciones	Valor	%f
Si	4	27%
No	11	73%
TOTAL	**15**	**100%**

GRAFICO Nº4

Existencia de información



Análisis.

Como se puede observar en el gráfico el 27% de los encuestados cree que existen métodos de seguridad para proteger la información y el 73% de los mismos desconocen estos tipos de seguridades debido a esta situación se debería detallarles las seguridades que existen para aplicarlas.

5. Alguna vez ha existido manipulación indebida de información por persona no pertenecientes a la Institución?

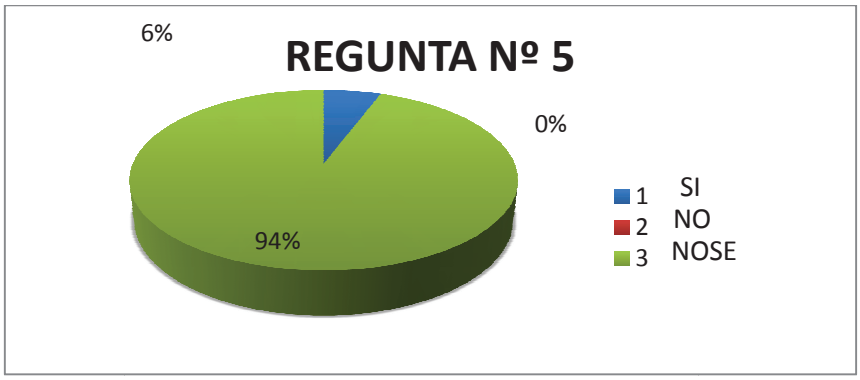
TABLA Nº 5

Manipulación indebida de la información

Opciones	**Valor**	**%f**
Si	1	6%
No	0	0%
NOSE	14	100%
TOTAL	**15**	**100%**

GRAFICO Nº5

Manipulación indebida de la información



I

Análisis.

Como se puede observar en el gráfico el 6% de las personas manifiesta que SI ha existido manipulación de información y el 0% de los encuestados dice que NO ha existido y el 94% dice que NO SABE si ha existido manipulación en la información.

6. Cree que la información manipulada escrupulosamente puede perjudicar al Ilustre Municipio?

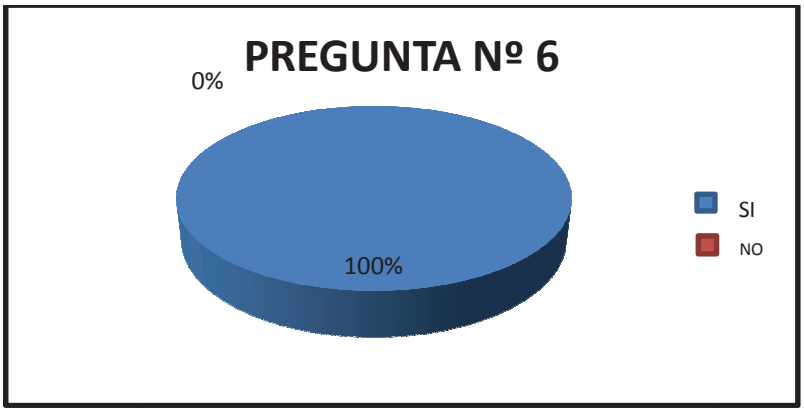
TABLA Nº 6

Perjuicio a la institución

Opciones	**Valor**	**%f**
Si	15	100%
No	0	0%
TOTAL	**15**	**100%**

GRAFICO Nº6

Perjuicio a la institución



Análisis.

El 100% de los encuestados cree que la manipulación indebida de la información puede perjudicar en muchos aspectos al Ilustre Municipio del Cantón Pujilí por lo que requiere la implementación de seguridades en el manejo de información.

7. Alguna vez la información que usted envío no ha llegado a su destino final?

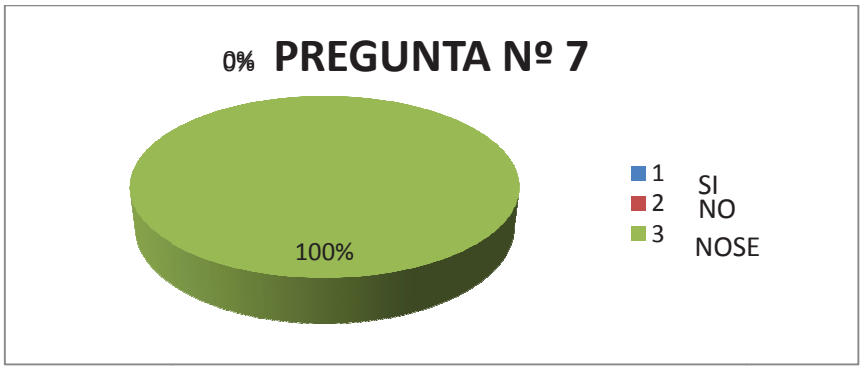
TABLA Nº 7

Destino de la información

Opciones	Valor	%f
Si	0	0%
No	0	0%
No se	15	100%
TOTAL	**15**	**100%**

GRAFICO Nº7

Destino de la información



Análisis.

De acuerdo a la grafica el 0% dice que ha enviado información y no ha llegado a su destinatario, en cambio el 0% no le ha ocurrido este inconveniente pero el 100% dice que no sabe si la información ha llegado a su destino.

8. Alguna vez se ha tratado de implementar algún método de seguridad en el Ilustre Municipio del Cantón Pujilí?

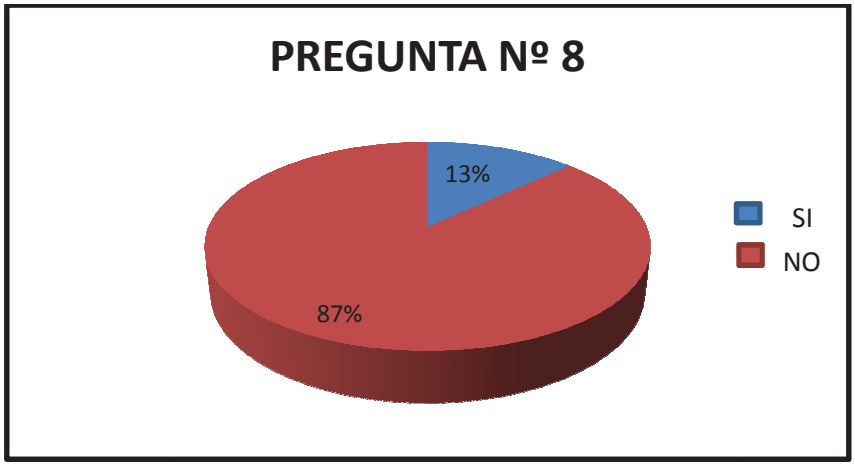
TABLA Nº 8

Implementar seguridades

Opciones	**Valor**	**%f**
Si	2	13%
No	13	87%
TOTAL	**15**	**100%**

GRAFICO Nº8

Implementar seguridades



Análisis.

El 87% de los encuestados dice que nunca se ha tratado el tema de implementar un proyecto de protección a la información en el Ilustre Municipio del Cantón Pujilí y el 13% dice que SI, ya que desconocen se realizara una implementación de seguridad y que sea conocida por los empleados.

9. Estaría de acuerdo que se implementara un método de seguridad para el manejo y traslado de su información?

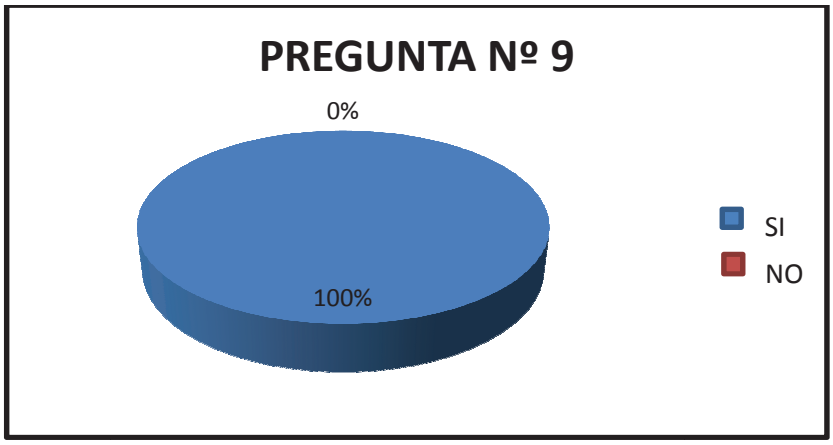
TABLA Nº 9

Implemento de seguridades

Opciones	**Valor**	**%f**
Si	15	100%
No	0	0%
TOTAL	**15**	**100%**

GRAFICO Nº9

Implemento de seguridades



JJILI

Análisis.

El 100% de los encuestados están de acuerdo en implementar un protocolo de seguridad para la protección de datos en el Ilustre Municipio del Cantón Pujilí.

10. Le gustaría tener una comunicación segura con otro usuario sin temor al acceso a su confidencialidad?

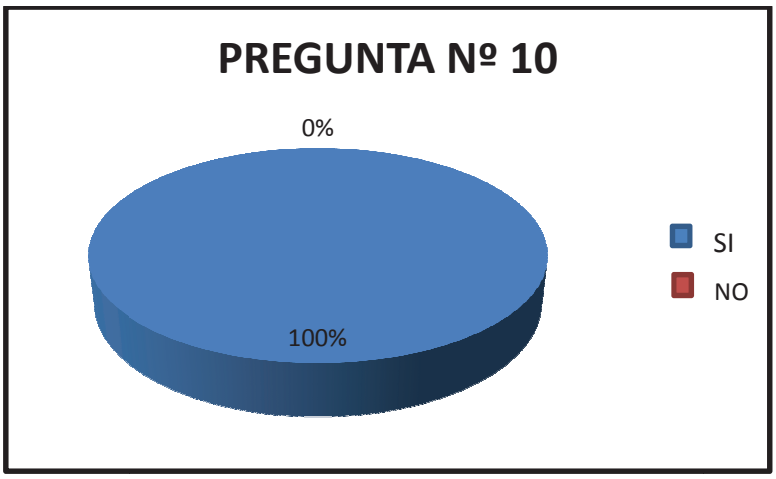
TABLA Nº 10

Comunicación segura

Opciones	**Valor**	**%f**
Si	15	100%
No	0	0%
TOTAL	**15**	**100%**

GRAFICO Nº10

Comunicación segura



Análisis.

Todos aquellos a quienes se ha encuestado manifiestan que desean tener privacidad en la comunicación y envíos de la información que ellos manipulan en su cargo correspondiente por lo cual se realizara la implementación de seguridad.

11. Apoyaría usted este proyecto de seguridad de información sea aplicado con factibilidad en el Ilustre Municipio del Cantón Pujilí?

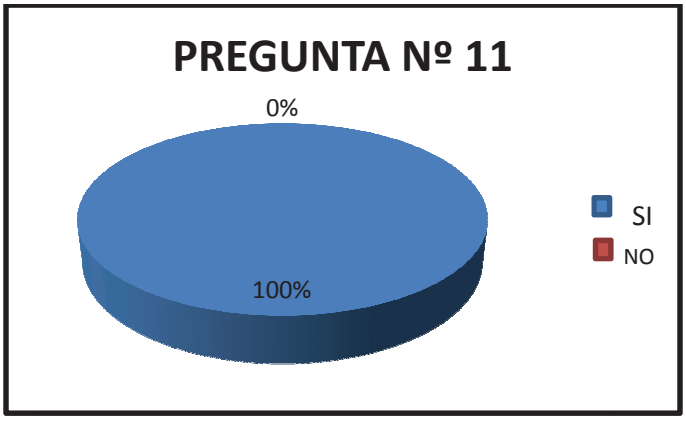
TABLA Nº 11

Apoyo a la investigación

Opciones	**Valor**	**%f**
Si	15	100%
No	0	0%
TOTAL	**15**	**100%**

GRAFICO Nº11

Apoyo a la investigación



LI

Análisis.

El 100% de los encuestados apoya y aprueba nuestro proyecto a ser aplicado en el Ilustre Municipio del Cantón Pujilí, lo cual es más satisfactorio para nosotros como investigadores implementar la seguridad en tan prestigiosa institución.

2.5. Análisis General.

Se pude resaltar que en el ilustre municipio del Cantón Pujilí sus trabajadores apoyan la implementación del protocolo IPSec, el cual brindara protección a la información con la cual trabajan y es muy fundamental para el desarrollo de esta institución. El grupo encuestado tiene la seguridad de que la tecnología en medios que utiliza la computadora es de mucho beneficio para todos.

2.6. VERIFICACIÓN DE HIPÓTESIS

2.6.1. ENUNCIADO

Después de haber aplicado las encuestas a la población involucrada dentro de este estudio, es importante manifestar que una vez analizadas todas y cada una de las preguntas y repuestas, la hipótesis planteada para la investigación es afirmativa; es decir la hipótesis ha sido verificada.

Para la realización de la presente investigación se utilizó la siguiente hipótesis: "Análisis e Implementación de seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información en el Ilustre Municipio del Cantón Pujilí que permitirá mejorar las seguridades de la información, el cual mejorará el envió de información de los usuarios satisfactoriamente sin manipulación indebida o no deseada.

2.6.2. DECISIÓN

De acuerdo a las respuestas de la encuesta realizada por los investigadores, los empleados que trabajan con computadoras no poseen seguridades en la transmisión de información, motivo por el cual se hace necesaria el Análisis e Implementación de seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información, que

mantendrán seguros los datos estando de acuerdo con el personal encuestado manifestando su apoyo con la implementación de las seguridades para la información.

Sobre todo da la seguridad necesaria a la información almacenada diariamente permitiendo la tranquilidad de envió de datos importantes de la institución.

CAPÍTULO III

PROPUESTA

3.1 DESARROLLO.

Para el desarrollo del presente trabajo de investigación, se aplicaron herramientas que están dentro del mercado de la informática, como una de las principales tenemos el IPSec (**Internet Protocol Security**), el cual es un pionero en desarrollo en la flexibilidad de los requerimientos, seguridades, estabilidad, y economía al momento de crear estos proyectos.

Por esta razón se ha propuesto:

3.1.1 Tema: "IMPLEMENTACIÓN DE SEGURIDADES IPSEC EN LA TRASMISIÓN DE DATOS EN INTERNET CON IPV4 PARA EVITAR EL ACCESO INDEBIDO A LA INFORMACIÓN EN EL ILUSTRE MUNICIPIO DEL CANTÓN PUJILÍ."

3.1.2 Presentación.

El trabajo de investigación está destinado en resolver los problemas de acceso indebido a la información privada, así como el manejo de datos y de comunicación segura que brindara a los empleados para dar confiabilidad en él envió de información en el Ilustre Municipio del Cantón Pujilí.

Para concretar con las propuestas planteadas, se pudo obtener herramientas que son designadas con este fin, es decir la utilización del sistema operativo Windows con protocolo ipv4 en el cual será aplicado la configuración de IPSec.

Dentro del proyecto de investigación se utilizó la arquitectura cliente servidor donde la información y datos se alojan en el servidor y las terminarles o empleados de la red solo acceden a la información.

3.1.3 OBJETIVO GENERAL.

- Analizar e Implementar seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información en el Ilustre Municipio del Cantón Pujilí.

3.1.4 OBJETIVOS ESPECÍFICOS.

- Documentar los fundamentos teóricos y conceptuales en los que se basa las seguridades IPSec.

- Diagnosticarlos resultados de las encuestas realizadas al personal del Ilustre Municipio de Pujilí para determinar la necesidad de una seguridad en el manejo de los datos.

- Implementar y configurarlas seguridades IPSec en los equipos del Ilustre Municipio del Cantón Pujilí.

3.1.5 JUSTIFICACIÓN.

Tomando en cuenta la necesidad del Ilustre Municipio del Cantón Pujilí para el envío y recepción segura de información es factible la implementación de las seguridades IPSec ya que a raíz del avance tecnológico van incrementando su nivel de protección y a su vez proporcionando nuevas herramientas para su configuración, lo cual a futuro será de mayor confiabilidad en las seguridades de la información.

Para el desarrollo de las seguridades IPSec se cuenta con suficiente referencia humana, bibliográfica web y entre otros, el mismo que

facilitará el desarrollo del proyecto.

En la implementación del protocolo de seguridad se procederá a la configuración manual mediante las herramientas que se van a utilizar en el desarrollo de la configuración de IPSec, mismas: software (Windows Xp y Server 2003), y hardware de red: internet, router, switch, equipos de prueba, dirección ip de la máquina, máscara de red, si se usan subredes, router por defecto, nombre completo de la máquina.

3.1.6 DESARROLLO DE LA PROPUESTA

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y cifrando cada paquete IP en un flujo de datos. El cual brindara seguridad y confiabilidad a los usuarios del Ilustre Municipio del Cantón Pujilí, lo que se detalla en las siguientes fases.

3.1.6.1 ANÁLISIS

En esta fase empezaremos obteniendo respuestas a varias interrogantes para la configuración de IPSec, que se detallan a continuación:

- ¿Se necesita realmente la configuración de IPSec?

  Si porque mediante este nuevo servicio se brinda seguridad a la información del Ilustre Municipio del Cantón Pujilí.

- ¿Para qué se necesita la seguridad IPSec?

  La seguridad IPSec permitirá enviar y recibir paquetes de datos encriptados cifrados mediante una clave de red.

- ¿Qué es lo que buscarán los usuarios en la implementación de las seguridades IPSec?

  Confiabilidad en cada uno de sus archivos para evitar el acceso indebido a la información.

- ¿Con qué recursos se cuenta para la implementación de la seguridad IPSec?

  El grupo investigativo cuentó con el apoyo y herramientas necesarias por parte del Ilustre municipio del Cantón Pujilí, para esta aplicación de Tesis.

Una vez conocidas todas las interrogantes se pudo listar los siguientes requisitos para la configuración de las seguridades IPSec en el Ilustre Municipio del Cantón Pujilí.

3.1.6.1.1 REQUISITOS FUNCIONALES:

Como requisitos funcionales se detalla las expectativas tanto de los usuarios como de la organización (Ilustre Municipio del Cantón Pujilí)

- **EXPECTATIVAS DE USUARIO**

Los usuarios del Ilustre Municipio del Cantón Pujilí a usar el entorno de red ya configurada tendrán la confiabilidad de manejar su información libremente sin la el acceso indebido de usuarios inescrupulosos.

- **EXPECTATIVAS DE ORGANIZACIÓN**

El Ilustre Municipio del Cantón Pujilí requiere seguridad en el manejo de

su información, la cual debe ser inaccesible a los usuarios indebidos y para evitar perjuicios en la institución.

3.1.6.2 PLANIFICACIÓN

Se planifico mediante requerimientos técnicos, necesarios y suficientes, los cuales son:

3.1.6.2.1 ESTUDIO DE FACTIBILIDAD

El estudio de factibilidad es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señalados, la factibilidad se apoya en 3 aspectos básicos:

3.1.6.2.1.1 FACTIBILIDAD TÉCNICA

Se refiere a los recursos disponibles como herramientas, conocimientos, habilidades, experiencia, que son necesarios para efectuar las actividades o procesos que requiere el proyecto. El proyecto debe considerar si los recursos técnicos actuales son suficientes o deben complementarse.

El Ilustre Municipio del Cantón Pujilí cuenta con equipos y software que trabajan bajo el Sistema Operativo Windows Xp Service Pack 3 y Server 2003, y con los requerimientos de software de instalación como:

- Procesador de 1 GHz
- 1 GB de memoria RAM
- 16 GB de espacio disponible en disco duro
- Tarjeta de video con soporte para DirectX 9 con WDDM 1.0

TABLA 3.1: TABLA DE REQUERIMIENTOS PARA LA CONFIGURACION DE IPSEC EN EL ILUSTRE MUNICIPIO DEL CANTON PUJILI

REQUISITOS	DISPONIBILIDAD EN EL ILUSTRE MUNICIPIO DEL CANTON PUJILI
SOFTWARE	
Software Microsoft Windows 2003 Server.	SI
Software Microsoft Windows XP. Sp2, Sp3	Si
Software Microsoft Windows ME.	No
Software Microsoft Windows 98.	No
Software Microsoft Windows ME.	No
HADWARE	
Cualquier equipo de hardware que no cumple con todos los estándares obligatorios es considerado inapropiado	Si
COMPONENTES DE RED	
Medios de trasmisión (cable de red)	Si
Switch	Si
Servidor	Si
Estaciones de trabajo	Si
Recursos compartidos	Si
Tarjetas de red	Si

FUENTE: LOS INVESTIGADORES

ANÁLISIS

El Ilustre Municipio del Cantón Pujilí cuenta con equipos y software necesarios para la implementación de Ipsec, lo cual facilita para la aplicación de nuestro proyecto de tesis.

3.1.6.2.1.2 FACTIBILIDAD ECONÓMICA

Son los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades o procesos y para obtener los recursos básicos que deben considerarse son el costo del tiempo, el costo de la realización y el costo de adquirir nuevos recursos.

- **Costo de estudio.**

  El tiempo utilizado en la investigación de requerimientos y necesidades del Ilustre Municipio del Cantón Pujilí, para la implementación de seguridades Ipsec.

- **Costos del desarrollo y adquisición.**

  No fue necesario un capital ya que el Ilustre Municipio del Cantón Pujilí cuenta con licencias, software y otras herramientas necesarias para el desarrollo del proyecto de tesis

- **Costos directos.**

  Como mayor costo directo que hemos tenido los investigadores son las capacitaciones, ya que los demás requisitos necesarios fueron facilitados por el Ilustre Municipio del Cantón Pujilí.

ANÁLISIS

En consideración a lo ya detallado podemos ver que es factible financiar y aplicar el proyecto de tesis en el Ilustre Municipio del Cantón Pujilí.

3.1.6.2.1.3 FACTIBILIDAD OPERATIVA

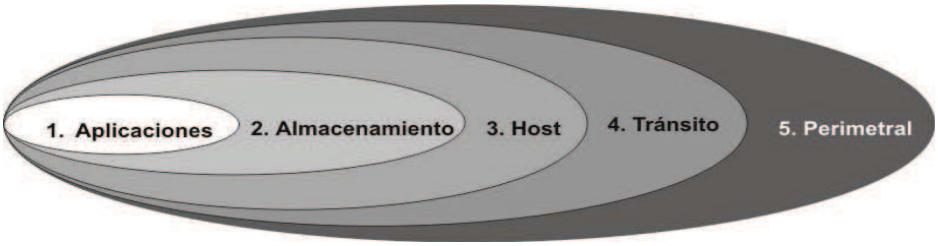
Los usuarios del Ilustre Municipio del Cantón Pujilí requieren equipos seguros, fácil manejo, confiabilidad al momento de envía y recibir información con acceso únicamente a usuarios con seguridad Ipsec, lo cual les permitirán a los mismos tener confianza en la utilización del internet y la confiabilidad de la seguridad de su información, por lo que las seguridades Ipsec satisface las necesidades de los usuarios y han permitido la aplicación de nuestro proyecto de tesis en esta prestigiosa Institución.

3.1.6.3 CONFIGURACIÓN DE IPSEC

3.1.6.3.1 Introducción.

Dado las necesidades del Ilustre Municipio del Cantón Pujilí la motivación principal de este trabajo es contribuir directamente al proyecto de la Institución, cuya red se encuentra en fase de desarrollo con nuevas tecnologías, la misma que presenta ventajas sustantivas para la realización de este trabajo de tesis, motivando el interés por aplicar servicios de seguridad con base en un modelo por capas, en particular en la capa de Tránsito de paquetes IP, fortaleciendo en consecuencia las capas interiores donde se ubican las aplicaciones, bases de datos, es decir, los aspectos de mayor interés de los usuarios de esta nueva red, como se muestra en la figura 3.1

FIGURA 3.1(Modelo de seguridad por capas)



Fuente: http://seguridad.cudi.edu.mx/publications/tesis_comedi.pdf

3.1.6.3.2 Metodología.

Para el planteamiento de la metodología a seguir en el análisis de IPSec se investigó varias iniciativas sobre cómo probar que un sistema es seguro.

Con base en dichas referencias, se plantea en este trabajo un proceso basado en los dos tipos de ataques: pasivo y activo y cuatro conceptos perfectamente aplicables a IPSec:

- **Visibilidad**: cuánto puede verse en Internet, es decir, puertos abiertos, tipo de sistema, arquitectura, aplicaciones instaladas, direcciones de correo, nombres de empleados, etc.

- **Acceso**: qué accesos se brindan al exterior, es decir, servicios públicos como páginas web, servidores DNS, video, correo, etc.

- **Confianza**: tipo y cantidad de mecanismos de autenticación, no repudio, control de acceso, contabilidad, confidencialidad de datos, e integridad de datos.

- **Alarma**: Registro y monitoreo en tiempo y propiedad en búsqueda de actividades que violen los conceptos anteriores, como bitácoras, tráfico, acceso a puertos, etc.

La metodología incluye la instrumentación de un escenario que cubra la configuración de IPSec, generación de pruebas de seguridad y rendimiento para cubrir los enfoques planteados. Las fases se describen a continuación:

3.1.6.3.3 Analisis de la configuracion de Ipsec en windows server 2003 y Xp

Los requerimientos del Ilustre Municipio del Cantón Pujilí en una conexión son mínimos. Los hosts solamente necesitan una conexión dedicada al transportador de red (tal como la Internet).

IPsec se puede configurar para conectar un escritorio o estación de trabajo a otro a través de una conexión clientes-servidor. Este tipo de conexión utiliza la red a la cual están conectados los hosts para crear un túnel seguro entre ellos.

En nuestro caso este análisis se lo realizó en función:

a) Servicio ftp

El primer paso es la configuración de Ipsec en el Ilustre Municipio del Cantón Pujilí se lo realizara en el servidor en el cual activamos el servicio FTP, con el disco de arranque del sistema operativo Windows server 2003 Sp2, el mismo que nos permitirá observarlos a los clientes entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

b) Consola de Windows

La conexión Ipsec en el servidor y clientes del Ilustre Municipio del Cantón Pujilí se enlaza a través de la consola de Windows ejecutando el comando MMC (**Microsoft Management Console**), el mismo que almacena y muestra herramientas administrativas creadas por Microsoft y por otros proveedores de software **(anexo 2 y 46, manual de usuario)**.

Estas herramientas se conocen como complementos y sirven para administrar los componentes de hardware, software y red de Windows.

c) Directivas de seguridad

También agregamos lo que son administrador de directivas de seguridad, en cada cliente y en el respectivo servidor del Ilustre Municipio del Cantón Pujilí, estas se pueden configurar de acuerdo con los requisitos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global. Se pueden definir varias directivas, pero sólo una se asigna a un equipo al mismo tiempo. Windows proporciona directivas predeterminadas para configuraciones de seguridad de grupo y locales, requiere utilizar IPSec para todo el tráfico entrante y saliente. Por tanto siempre requiere que los equipos de destino sean de confianza y utilicen IPSec **(anexo 7 y 53, manual de usuario)**.

d) Claves de seguridad

Una vez creada la directiva de seguridad en el Ilustre Municipio del Cantón Pujilí y con la utilización del asistente, establecemos la clave (llave) de seguridad de comunicación, tienen que proteger el intercambio de datos. Puede utilizar los métodos predefinidos Medio y

Alto, o definir métodos de seguridad personalizados (anexo 11 y 57, manual de usuario).

e) Reglas de seguridad

En las reglas de seguridad se especifica el punto final del túnel que, significa el equipo con protocolo de túnel más cercano al destino del trafico ip.

Un túnel Ipsec permite a los paquetes atravesar una red pública o privada con el nivel de seguridad de una conexión privada y directa entre dos equipos **(anexo 14 y 60, manual de usuario)**.

A continuación se detallan las reglas de seguridad:

1. **Lista de filtros IP**. Define qué tráfico se va a proteger con esta regla. Puede utilizar los filtros predeterminados o crear filtros específicos de directiva para ciertos tipos de tráfico IP o para sobre de específicas.
2. **Acciones de filtrado**. Enumera las acciones de seguridad que se tomarán cuando el tráfico cumpla los criterios de un filtro. La acción especifica si el tráfico se bloquea, se permite o si se negocia la seguridad de la conexión. Se pueden especificar una o varias acciones de filtrado en una lista ordenada por preferencia. Si dicha acción de filtrado no se puede negociar, se intenta la acción de filtrado siguiente.

3. **Métodos de seguridad**. Especifica cómo los equipos que se comunican tienen que proteger el intercambio de datos. Puede utilizar los métodos predefinidos Medio y Alto, o definir métodos de seguridad personalizados.

4. **Configuración de túneles**. En algunas situaciones, como entre en caminadores que sólo están conectados por Internet, es interesante utilizar el modo de túnel en IPSec. Para definir un túnel IPSec tiene que haber dos reglas, una para cada sentido.

5. **Métodos de autenticación**. Los métodos de autenticación definen cómo cada usuario se va a asegurar de que el otro equipo o el otro usuario son realmente quienes dicen ser.

f) Lista de Filtros

Cuando el tráfico corresponde a un origen, destino y tipo de tráfico IP de un filtro, se inician negociaciones de seguridad. Este tipo de filtrado de paquetes IP permite a un administrador de red del Ilustre Municipio del Cantón Pujilí definir con precisión el tráfico IP que se debe proteger.

Cada lista de filtros IP contiene uno o varios filtros, que definen las direcciones y los tipos de tráfico IP. Una lista de filtros IP puede utilizarse para varios escenarios de comunicación.

IPSec requiere tanto un filtro de entrada como un filtro de salida entre los equipos especificados en la lista de filtros (anexo 21 y 67, manual de usuario).

Los filtros de entrada se aplican al tráfico entrante. Los filtros de salida se aplican al tráfico que sale de un equipo hacia un destino. Por ejemplo, si el equipo A desea intercambiar datos de forma segura con el equipo B:

- La directiva IPSec activa en el equipo A debe tener un filtro para cualquier paquete de salida del equipo B. Origen = A y Destino = B.

- La directiva IPSec activa en el equipo A debe tener un filtro para cualquier paquete de entrada del equipo B. Origen = B y Destino = A.
    - Cada interlocutor debe tener también un filtro inverso:

- La directiva IPSec activa en el equipo B debe tener un filtro para cualquier paquete de entrada del equipo A. Origen = A y Destino = B.
- La directiva IPSec activa en el equipo B debe tener un filtro para cualquier paquete de salida al equipo A. Origen = B y Destino = A.

g) Origen del trafico Ip

Especifica el rango de dirección de origen Ip que establece la conexión con los clientes y servidor, en nuestra aplicación utilizamos las direcciones propias del host del Ilustre Municipio del Cantón Pujilí, utiliza el protocolo ESP para proporcionar confidencialidad (cifrado) de datos con el algoritmo triple cifrado de datos estándar (3DES), integridad de datos y autenticación con el algoritmo de hash seguro 1 (SHA1) y la duración de clave predeterminada (100 MB, 1 hora). Si necesita proteger los datos y las direcciones (encabezado IP) pueden crear un método de seguridad personalizado. Si no necesita el cifrado, utilice sólo integridad **(anexo 26 y 72, manual de usuario).**

h) Métodos de seguridad personalizados

En el Ilustre Municipio del Cantón Pujilí debemos especificar métodos de seguridad personalizados. Por ejemplo, puede utilizar métodos personalizados cuando precise especificar cifrado e integridad de direcciones, algoritmos más eficaces o duraciones de clave específicas **(anexo 34 y 79, manual de usuario).**

Al configurar un método de seguridad personalizado, puede establecer

las opciones siguientes:

- Protocolos de seguridad.

  Tanto AH (**Integridad de direcciones y datos sin cifrado**) como ESP (**Integridad de datos y cifrado**) pueden habilitarse en un método de seguridad personalizado cuando se precisa integridad del encabezado IP y cifrado de datos. Si elige habilitar ambas opciones, no es necesario especificar un algoritmo de integridad para ESP. El algoritmo elegido para AH proporciona integridad.

- Algoritmo de integridad.

  - ✓ Síntesis del mensaje 5 (MD5) (abreviatura de Message-Digest-Algorithm *5*, Algoritmo de Resumen del Mensaje 5), que utiliza una clave de 128 bits.

  - ✓ Algoritmo de hash seguro 1 (SHA1), que utiliza una clave de 160 bits. La función SHA1 sirve para encriptar contraseñas. Eso sí, este tipo de encriptación es irreversible, así que si se olvidara la contraseña, se debe de asignar una nueva.

- Algoritmo de cifrado.
- 3DES es la más segura de las combinaciones DES y más lenta en cuanto a rendimiento. 3DES procesa cada bloque tres veces, utilizando tres claves únicas de 56 bits.
- Opciones de clave de sesión.

  Las opciones de clave de sesión determinan cuándo se genera una clave nueva, pero no cómo se genera. Es posible especificar una duración en kilobytes, segundos o ambos. Por ejemplo, si la

comunicación dura 10000 segundos y usted especifica una duración de la clave de 1000 segundos, se generarán 10 claves para completar la transferencia. De este modo se asegura que, incluso aunque un atacante logre determinar una clave de sesión y descifrar parte de una comunicación, no le será posible descifrarla por completo. De forma predeterminada se generan nuevas claves de sesión para cada 100 MB de datos transmitidos o cada hora transcurrida. Tenga en cuenta que cada vez que se agota la duración de una clave, también se vuelve a negociar la asociación de seguridad de modo rápido además de la actualización o la nueva generación de la clave.

i) Al finalizar la configuración Ipsec en los clientes y servidor del Ilustre Municipio del Cantón Pujilí, en la consola de Windows digitamos CMD y en la pantalla que se visualiza se escribe gpupdate/forcé, en la cual nos saldrá un mensaje: se ha completado la actualización de directiva de seguridad, una vez realizado este paso asignamos nuestra directiva creada **(anexo 43-44 y 87-88, manual de usuario)**.

Como se ha podido observar en la configuración de Ipsec la aplicación de seguridad es indispensable en las redes públicas y privadas, ya que tiene enfoque diferente a otros protocolos de seguridad que funcionan en la capa de transporte, y están ligados con una aplicación particular; Ipsec puede realizar conexiones seguras de extremo a extremo de forma flexible y bajo diversas configuraciones, sin importar la aplicación del nivel de usuario.

3.1.6.3.4 PRUEBAS Y RESULTADOS

Las pruebas se fueron desarrollando de forma gradual, en base a los escenarios planteados aplicando la configuración de IPsec y el modo de funcionamiento, enfocamos sobre la vulnerabilidad del punto de acceso,

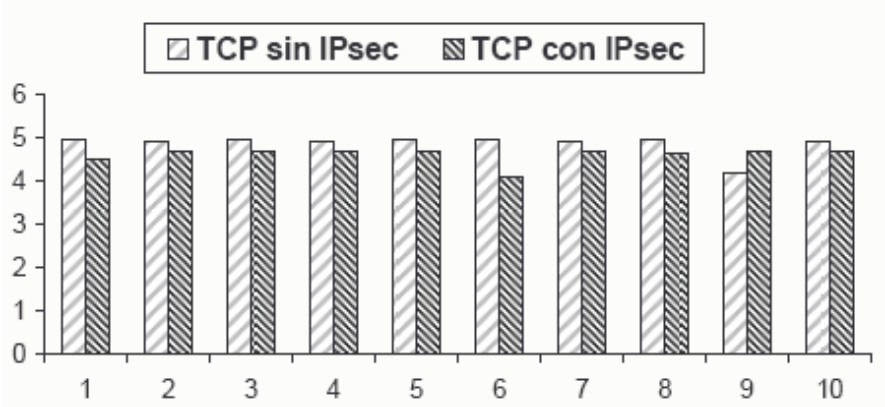
analizando el flujo de paquetes sin servicios de seguridad, y verificar el acceso a cada usuario al aplicar IPsec.

Se utilizó una serie de elementos de hardware y software; como el servidor server 2003 como punto de acceso, estaciones de trabajo con Windows xpy dispositivos de red.

Para el acceso a un cliente que no tenga configuración IPsec obtuvimos un retardo significativo, obviamente no nos permitirá el acceso pero si obtenemos respuesta del servidor como nos muestra en la figura 3.2.

FIGURA 3.2

Número de pruebas de seguridad y tiempo de respuesta



FUENTE: INVESTIGADORES

Se describieron las pruebas realizadas con el protocolo IPSec, la relevancia de aplicar servicios de seguridad ante una evidente y comprobada vulnerabilidad de IP, extraer tráfico de una LAN es sencilla y representa problemas serios. La resistencia a las estrategias de ataques, las prestaciones de una red en donde se ha instrumentado IPSec, bajo una configuración y la evaluación de dichas prestaciones para garantizar la calidad de servicios, sobre todo aquellos que se están manejando.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- Gracias a la abundante fundamentación teórica existente acerca de le realización de nuestro proyecto se analizó e implementó seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información en el Ilustre Municipio del Cantón Pujilí.

- También se documentar los fundamentos teóricos y conceptuales en los que se basa las seguridades IPSec para el mejor entendimiento acerca de nuestro tema.

- Para el diagnostico de resultados de las preguntas realizadas se utilizó el tipo de técnica de investigación que es la encuesta la cual se realizó al personal del Ilustre Municipio de Pujilí para determinar las necesidades de una seguridad en el manejo de los datos.

- La propuesta de nuestro tema permitió la mayor confiabilidad del manejo de información al momento de su envió.

- La presente configuración ayuda en el manejo de la información confiablemente por la red sin alteración alguna de los datos originales.

- La configuración de seguridades IPSec puede ser aplicado en otras instituciones que ofertan servicios a clientes y manejan información sumamente importante.

- Como usuarios tenemos la satisfacción de poseer seguridad y confiabilidad en la transmisión de la información.

RECOMENDACIONES:

- Aanalizar e Implementar seguridades IPSEC en la trasmisión de datos en Internet con IPv4 para evitar el acceso indebido a la información en el Ilustre Municipio del Cantón Pujilí.

- Documentar los fundamentos teóricos y conceptuales en los que se basa las seguridades IPSec para el mejor entendimiento del tema propuesto.

- Diagnosticar los resultados de las encuestas realizadas al personal del Ilustre Municipio de Pujilí para determinar la necesidad de una seguridad en el manejo de los datos.

- Una empresa que necesita seguridad y gran cantidad de servicios en su red podría utilizar las tecnologías actuales como IPSec para la protección de su información.

- Es necesario seguir los pasos establecidos para el correcto funcionamiento de la configuración de IPSec.

- Las empresas deben evaluar las necesidades de comunicación, y niveles de seguridad que se requieren, para así poder implementar soluciones necesarias y no incurrir en gastos que no se necesitan.

- Los usuarios deberán conocer el funcionamiento y beneficios de la configuración IPSec para evitar incógnitas en la aplicación de la tesis.

- Se recomienda configurar equipos nuevos que sean conectados en la red que se halle instalado IPSec porque no se podrá compartir información si no se encuentra habilitado la seguridad.

GLOSARIO DE TÉRMINOS

A:

Autentificación: Proceso mediante el cual el usuario comunica ciertos datos al sistema para que los coteje con una base de datos, verifique su identidad y proporcione un acceso a una zona, información o servicio específico para el usuario.

AH: AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits

C:

Contraseñas.- el uso de un nombre de usuario y una contraseña provee el modo más común de autenticación, esta información se introduce al arrancar el ordenador o acceder a una aplicación.

D:

Directivas.-Windows proporciona directivas predeterminadas para configuraciones de seguridad de grupo y locales, requiere utilizar IPSec para todo el tráfico entrante y saliente. Por tanto siempre requiere que los equipos de destino sean de confianza y utilicen IPSec.

E:

ESP. - El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC.

ENCRIPTACIÓN.-(Cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptado sólo puede leerse aplicándole una clave.

I:

IPsec.- es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IKE.- El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas.

L:

LAN.- Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña.

M:

Modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

MAN.- Redes de Área Metropolitana

Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos.

P:

PROYECTO.- Es una herramienta o instrumento que busca recopilar, crear, analizar en forma sistemática un conjunto de datos y antecedentes, para la obtención de resultados esperados.

R:

Rastreo.- Un rastreador de red es una aplicación o un dispositivo que puede supervisar y leer los paquetes de la red. Si los paquetes no están cifrados, un rastreador de red obtiene una vista completa de los datos del paquete. El Monitor de red de Microsoft es un ejemplo de rastreador de red.

T:

Transporte se utiliza para comunicaciones ordenador a ordenador.

Túnel: En el **modo túnel**, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El **modo túnel** se utiliza para comunicaciones red a red (túneles seguros entre routers, para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

W:

WAN.- Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system).

REFERENCIAS Y BIBLIOGRAFÍA

BIBLIOGRAFÍA CITADA

- Antonio Ortiz Medina (2004, pág. 20)
- J.P. Degabriele y K.G. Paterson(2001, pag130)
- Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff
- manual curso de formación internet (2008, pag 3)
- curso de formación internet (2008, pág. 3)

BIBLIOGRAFÍA CITADA Y ELECTRONICA

- web: www.mastermagazine.info/termino/5368.php
- web: http://es.wikipedia.org/wiki/Inform%C3%A1tica
- web: http://es.wikipedia.org/wiki/Internet
- http://www.civila.com/desenredada/que-es.html
- www.wikipedia.org
- www.gobiernodecanarias.org
- http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/protocol1.htm
- http://es.kioskea.net/contents/internet/tcpip.php3
- www.configurarequipos.com
- www.wikipedia.org
- http://www.monografias.com/trabajos15/arquitectura-tcp/arquitectura-tcp.shtml
- www.rediris.es
- http://www.monografias.com/trabajos11/repri/repri.shtm
- http://sistemas.anmat.gov.ar/aplicaciones_net/applications/menu/menu/vpn/vpn.htm

- http://es.wikipedia.org/wiki/IPsec
- http://www.ipsec-howto.org/spanish/x161.html
- http://www.municipiopujili.gov.ec/index.php?option=com_content&view=article&id=125:historia-de-pujili&catid=105:historia&Itemid=168
- http://dspace.ups.edu.ec/bitstream/123456789/202/4/Capitulo%203.pdf
- http://technet.microsoft.com/es-es/library/cc739580(WS.10).aspx
- http://proteneo.wordpress.com/2009/07/16/ipsec-seguridad-en-la-red/
- http://electronica.udea.edu.co/cursos/redes/IPSec.pdf
- http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml
- http://es.answers.yahoo.com/question/index?qid=20070327075349AAPFMH3
- http://seguridad.cudi.edu.mx/publications/tesis_comedi.pdf
- http://www.municipiopujili.gov.ec/index.php?option=com_content&view=article&id=125:historia-de-ujili&catid=105:historia&Itemid=168

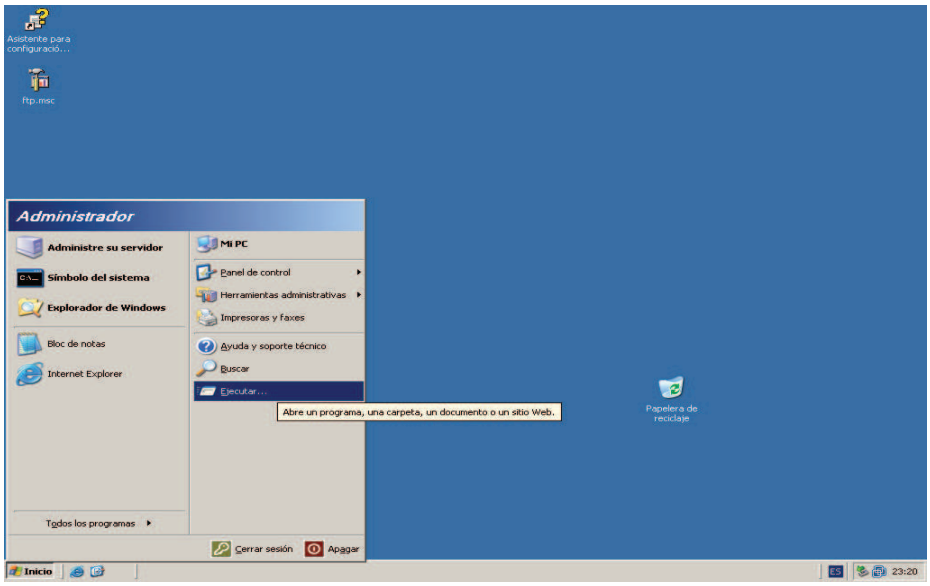
ANEXOS

ANEXOS

CONFIGURACION IPSec EN WIN SERVER 2003 SP2

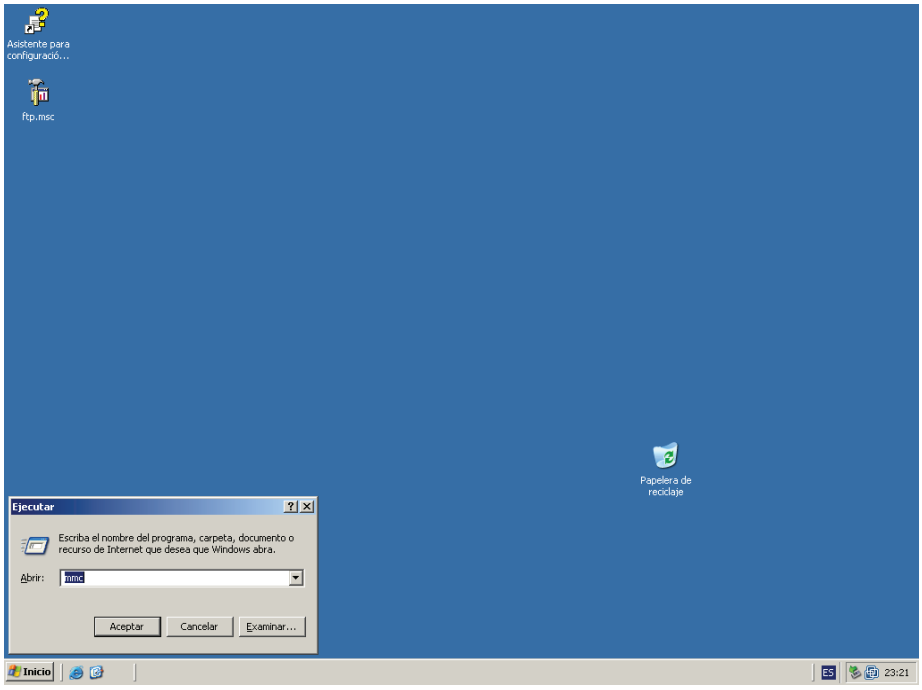
ANEXO1

VAMOS A MENU EJECUTAR



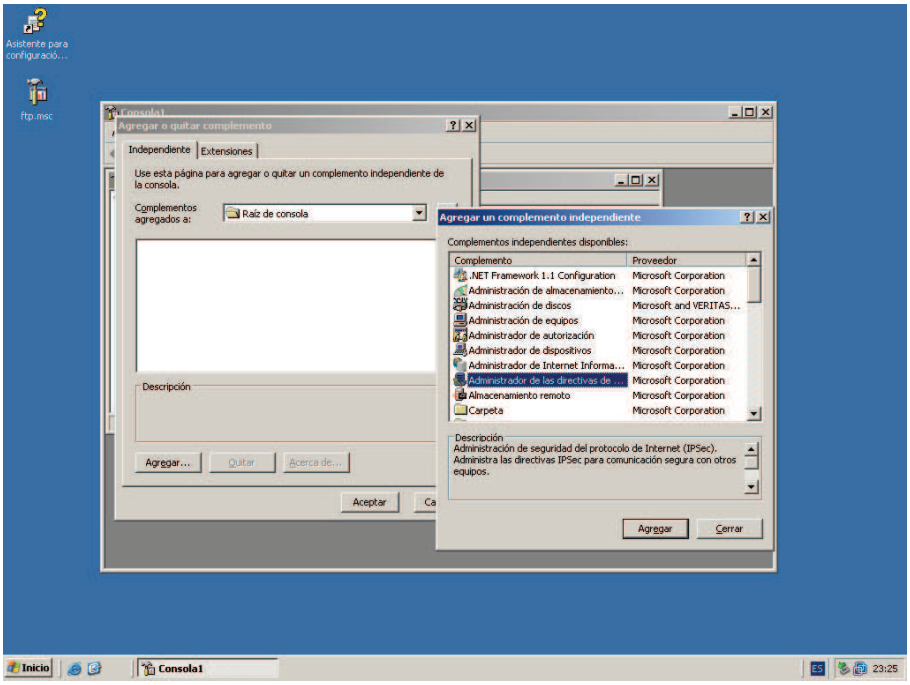
ANEXO 2

EJECUTAMOS EL COMANDO MMC



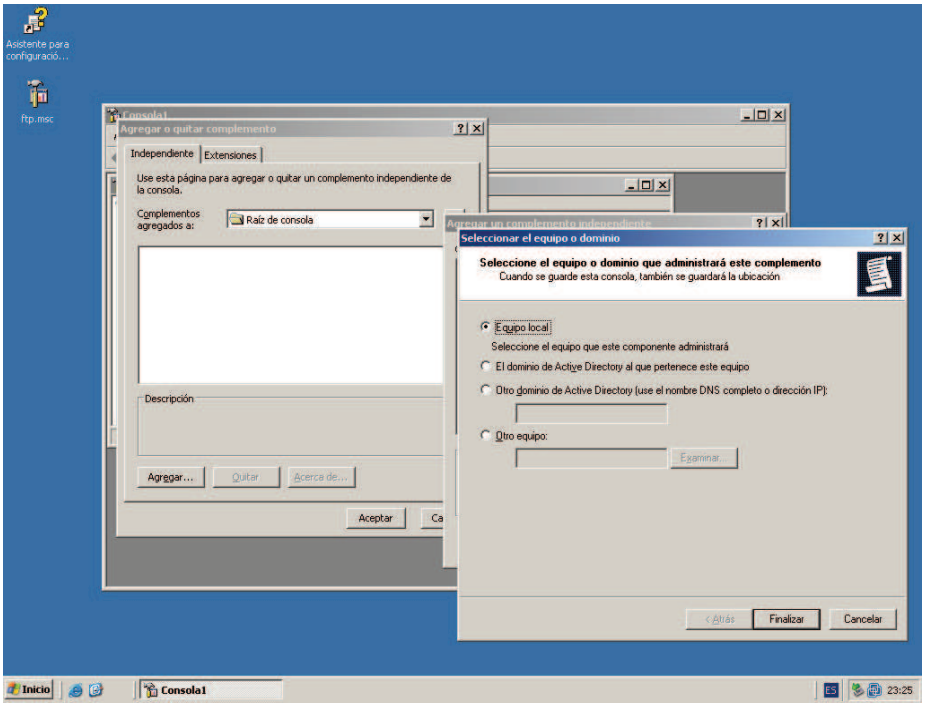
ANEXO 3

NOS DIRIGIMOS A ARCHIVO AGREGAR O QUITAR



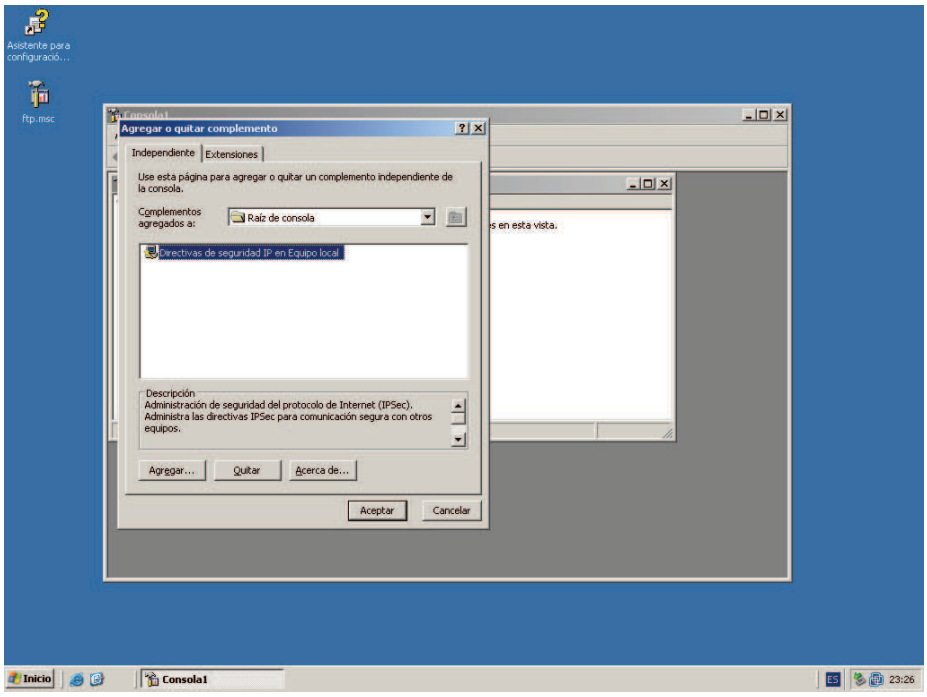
ANEXO 4

ELEGIMOS EQUIPO LOCAL



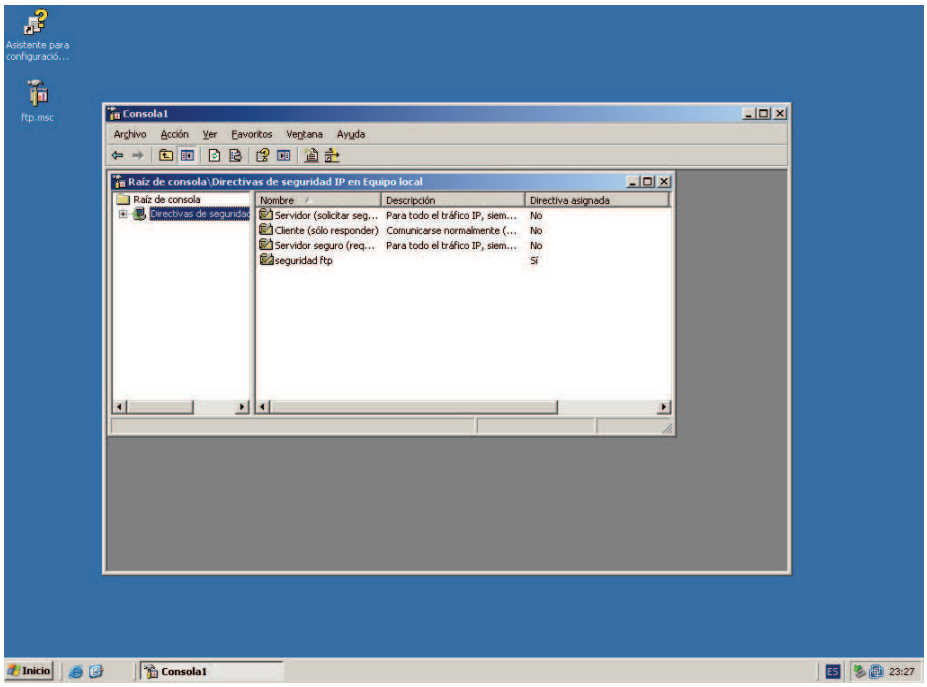
ANEXO 5

COMPLEMENTO Y AGREGAR ADMINISTRADOR DE LAS DIRECTIVAS IPsec



ANEXO 6

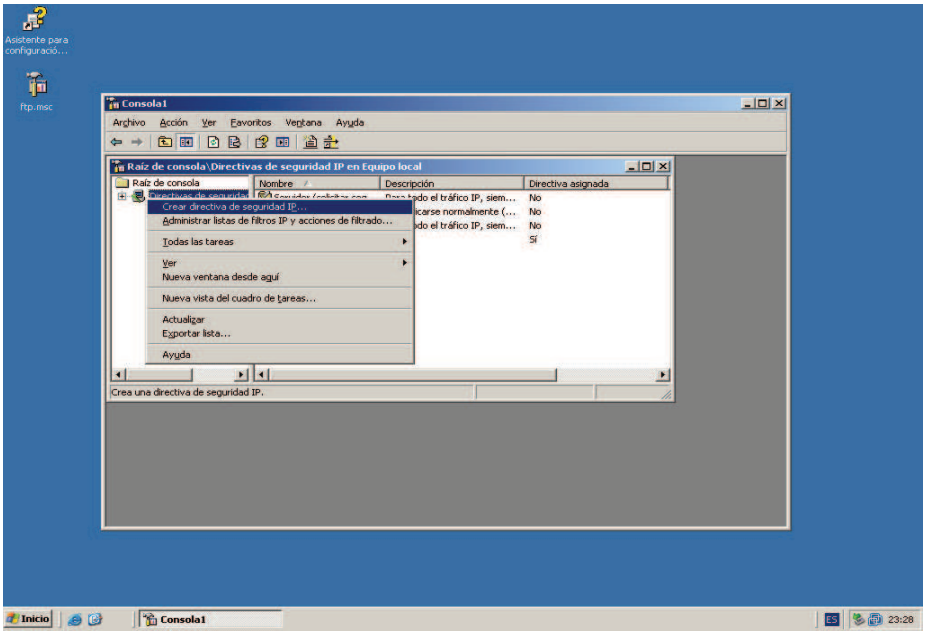
NOS QUEDARA ESTA PANTALLA



ANEXO 7

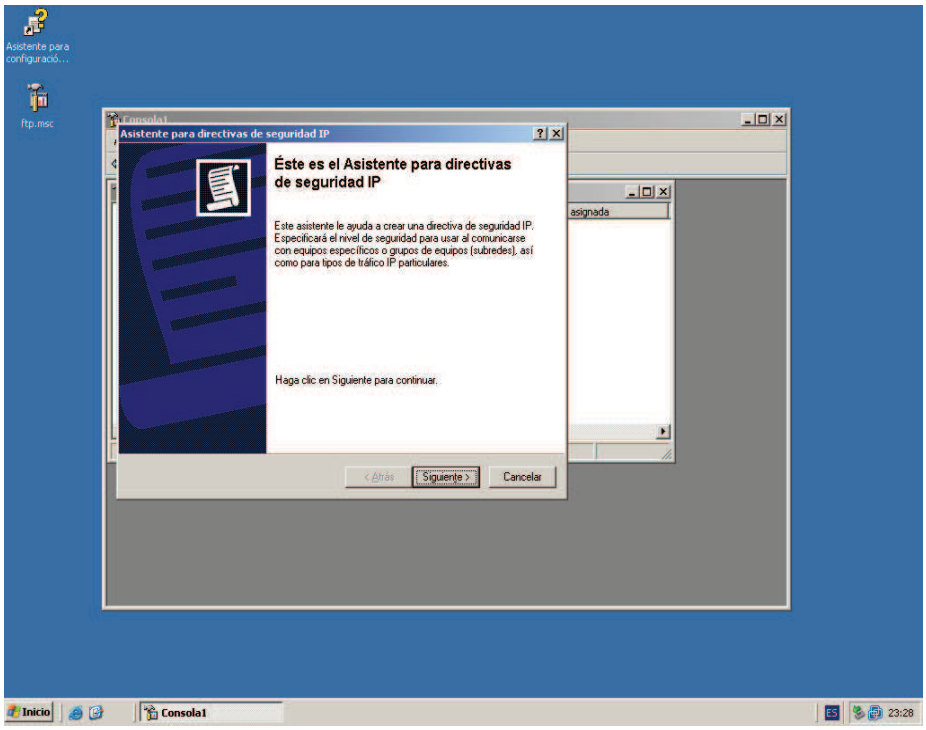
CLIC DERECHO EN LA DIRECTIVA QUE ACABAMOS DE CREAR

Y CREAR DIRECTIVA DE SEGURIDAD IP



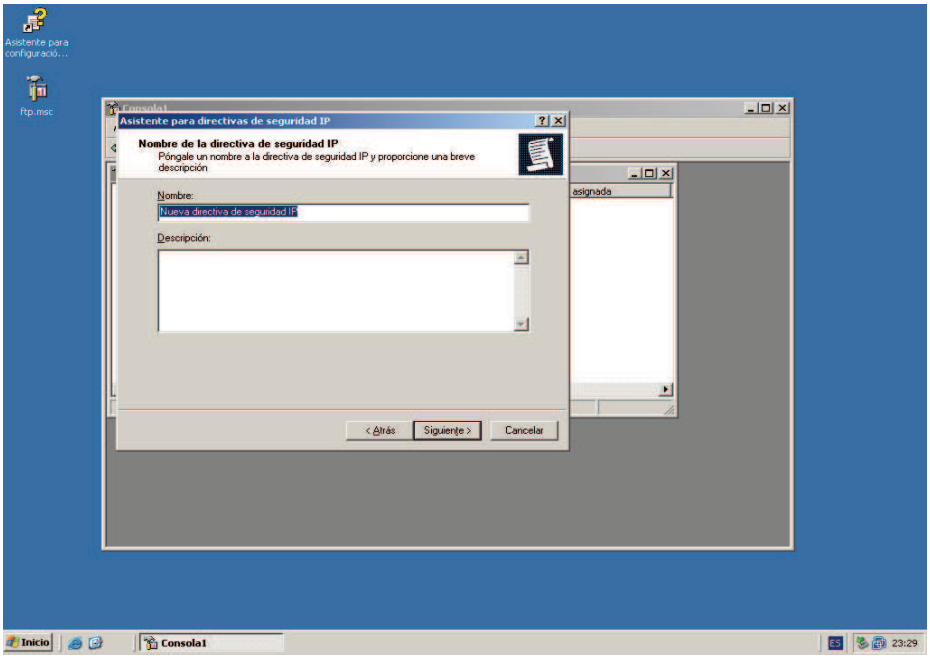
ANEXO 8

CLIC EN SIGUIENTE



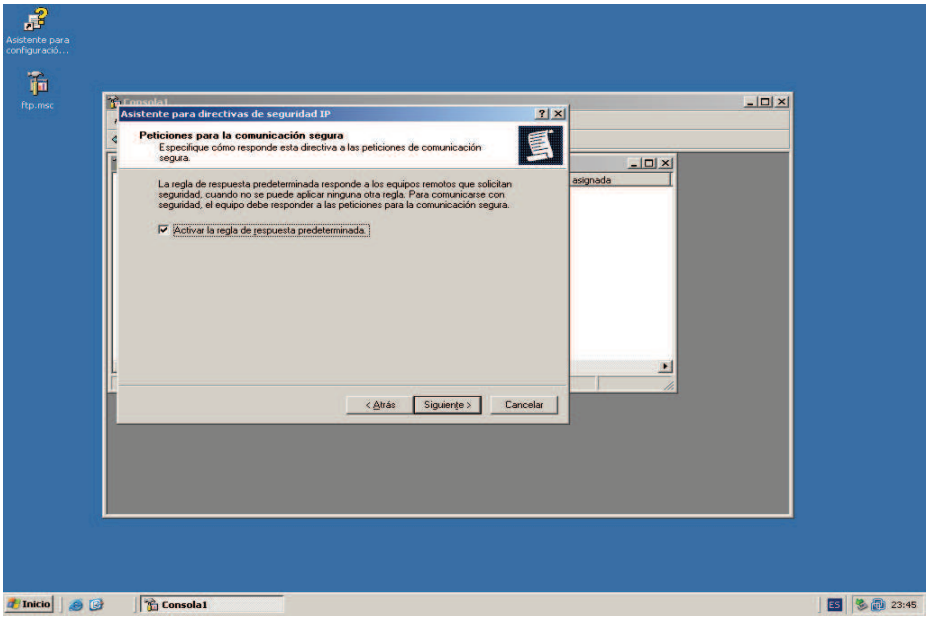
ANEXO 9

DAMOS UN NOMBRE A NUESTRA DIRECTIVA Y SIGUIENTE



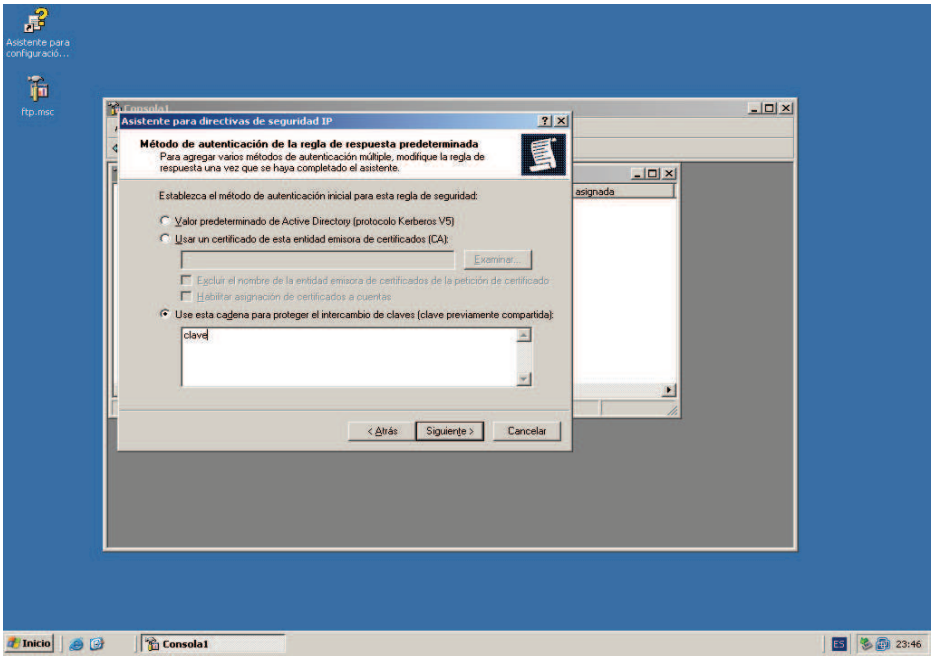
ANEXO 10

CLIC EN SIGUIENTE



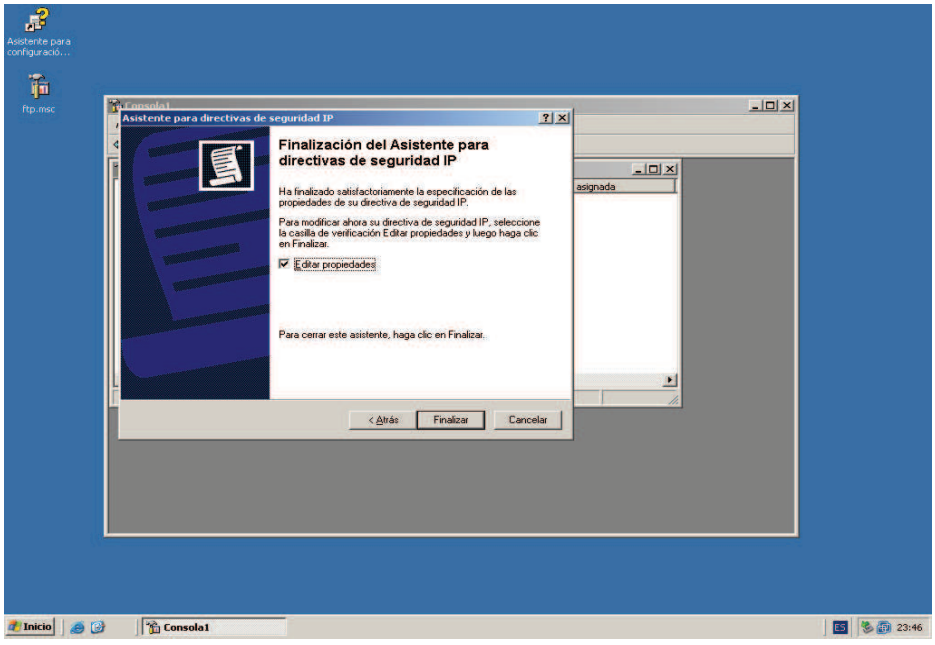
ANEXO 11

ACTIVAMOS LA ULTIMA OPCIÓN Y AGREGAMOS UNA CONTRASEÑA A NUESTRA DIRECTIVA



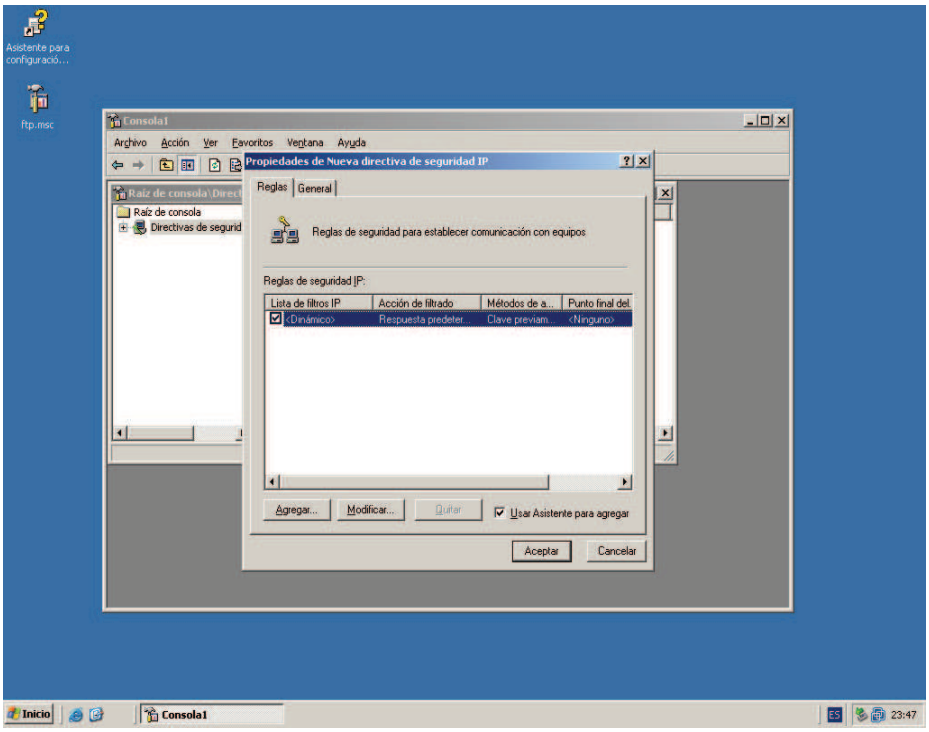
ANEXO 12

FINALIZAMOS



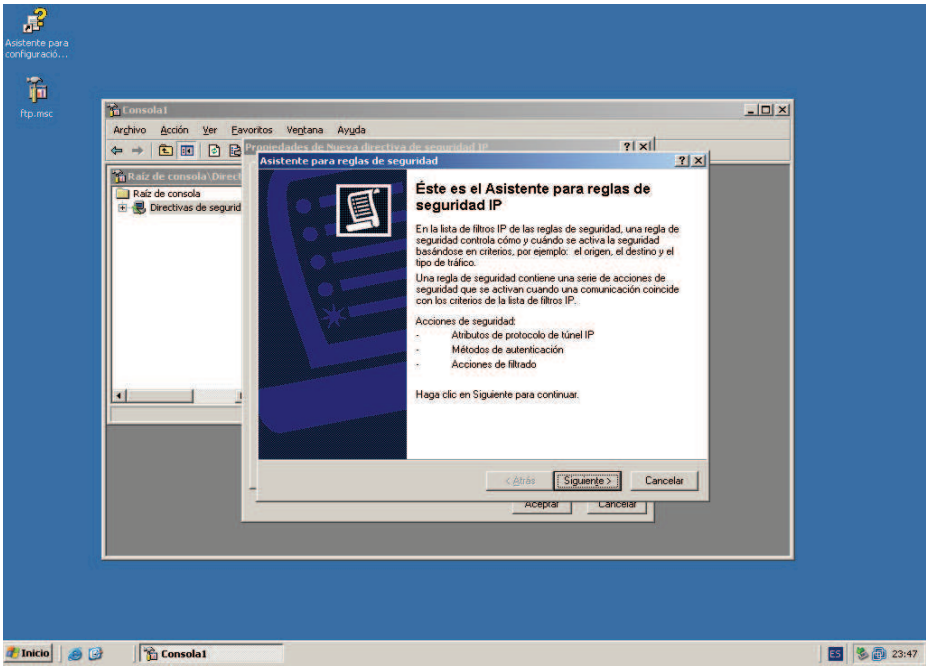
ANEXO 13

CLIC EN AGREGAR



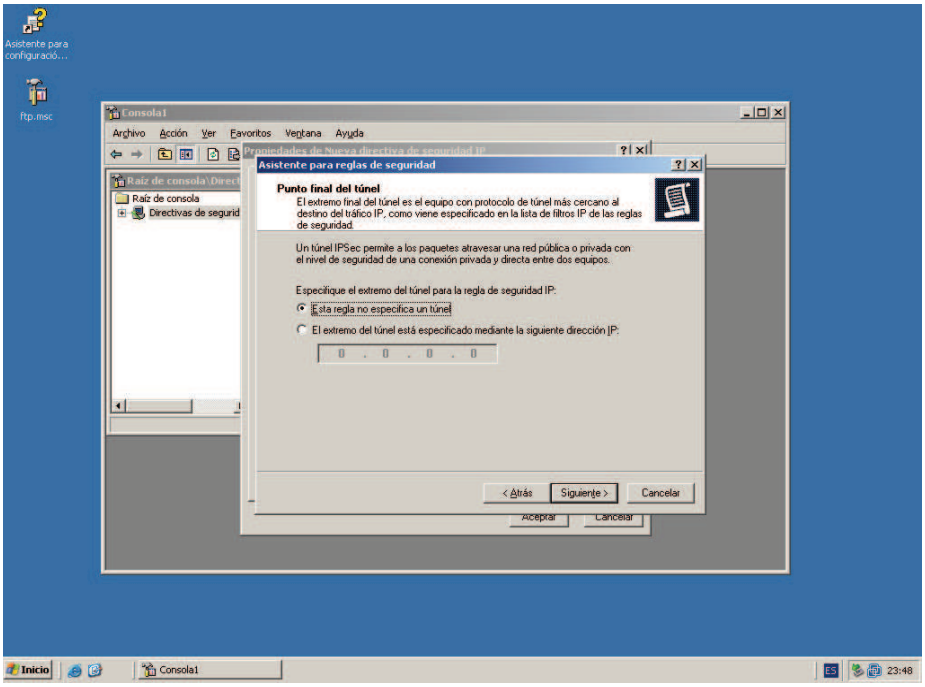
ANEXO 14

CLIC EN SIGUIENTE



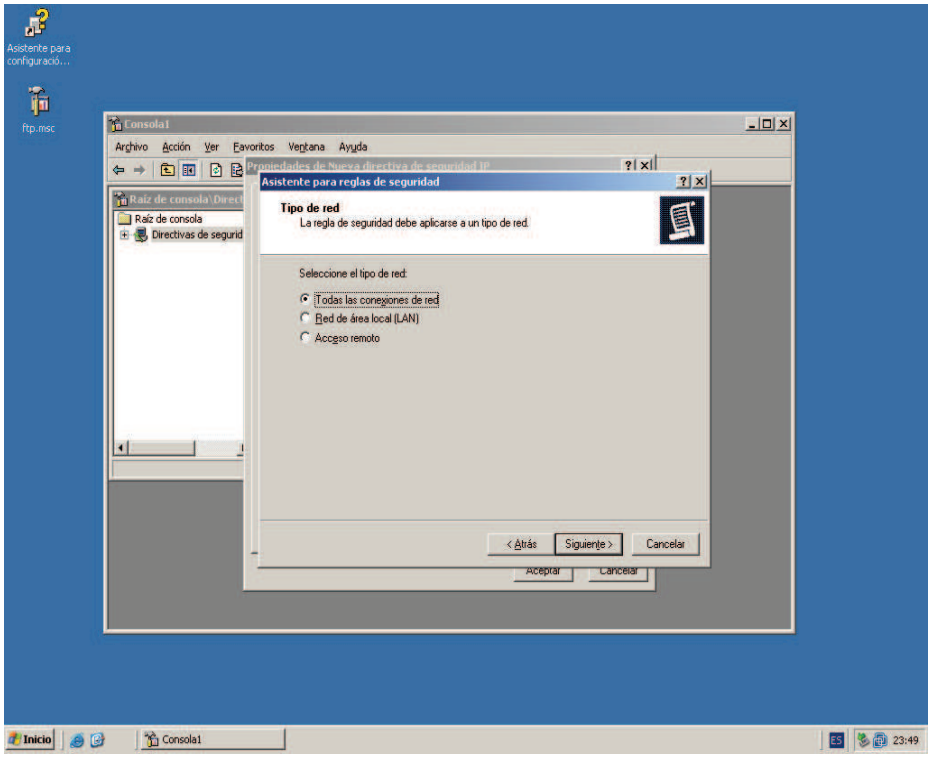
ANEXO 15

ESCOGEMOS LA PRIMERA OPCIÓN



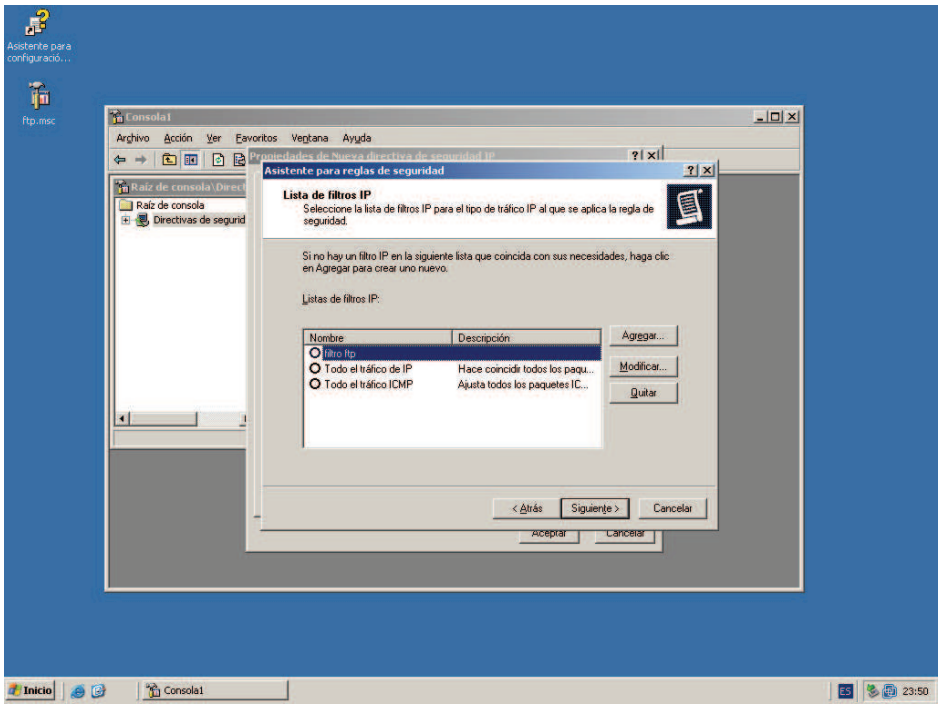
ANEXO 16

ESCOGEMOS LA OPCIÓN TODAS LAS CONEXIONES DE RED



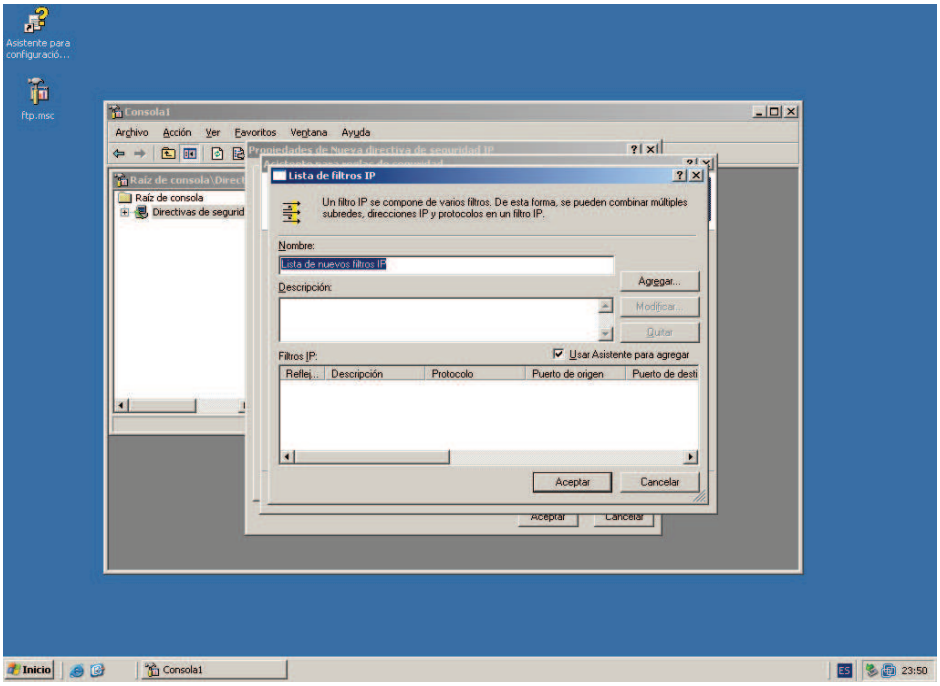
ANEXO 17

CLIC EN AGREGAR



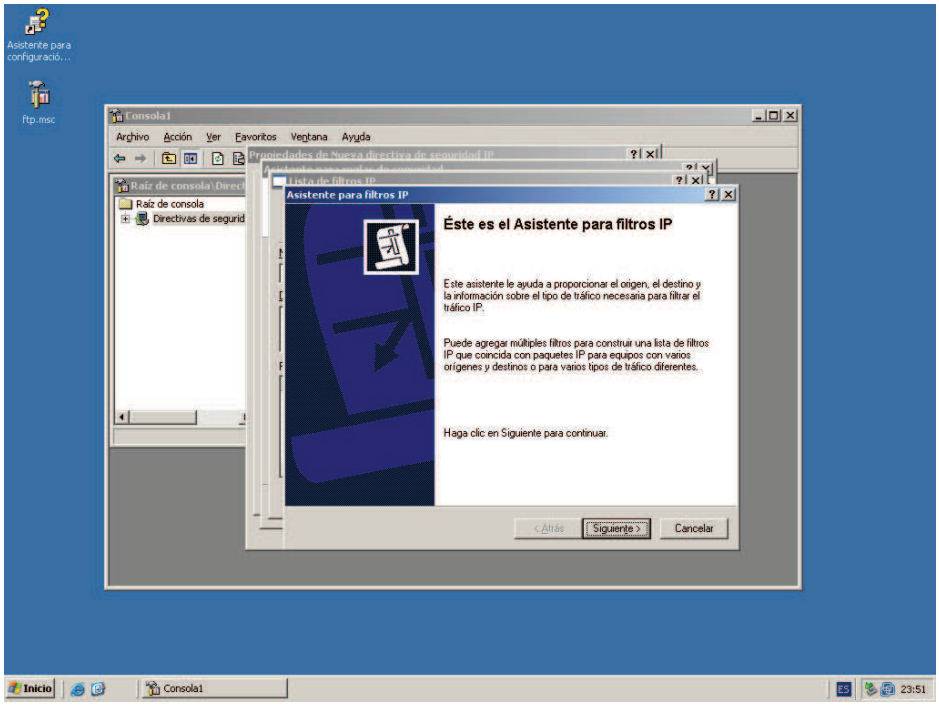
ANEXO 18

DAMOS UN NOMBRE A NUESTRA LISTA DE FILTROS



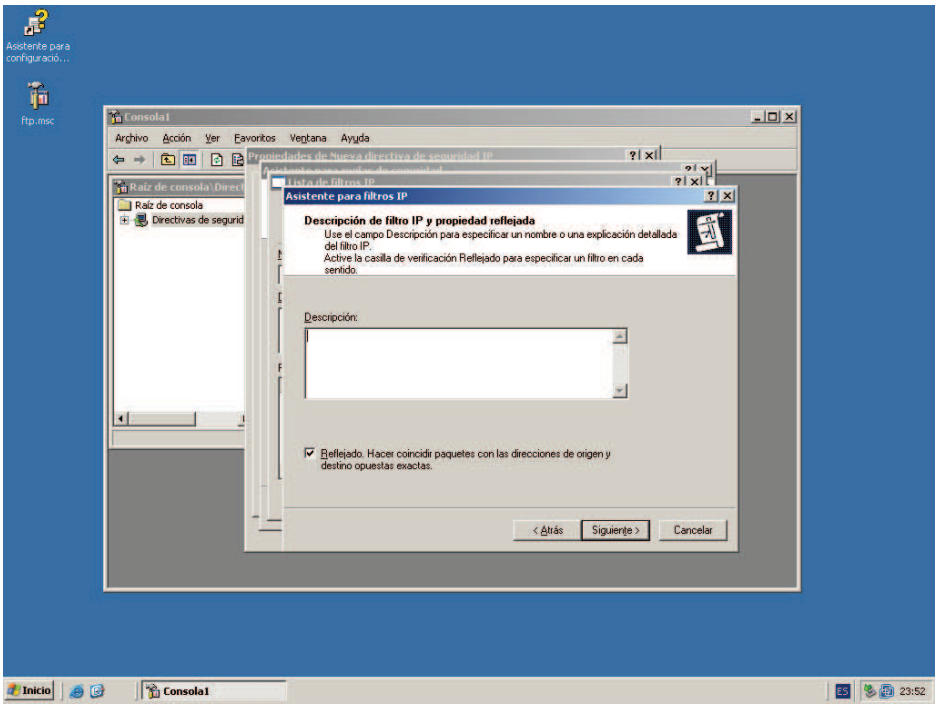
ANEXO 19

CLIC EN SIGUIENTE



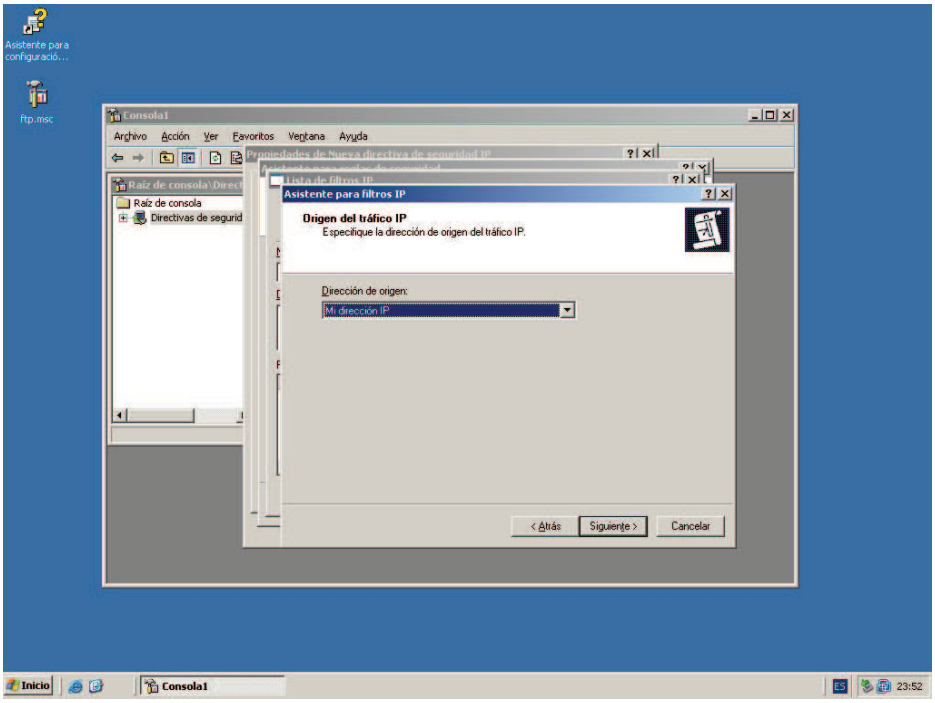
ANEXO 20

AGREGAMOS UN COMENTARIO Y SIGUIENTE



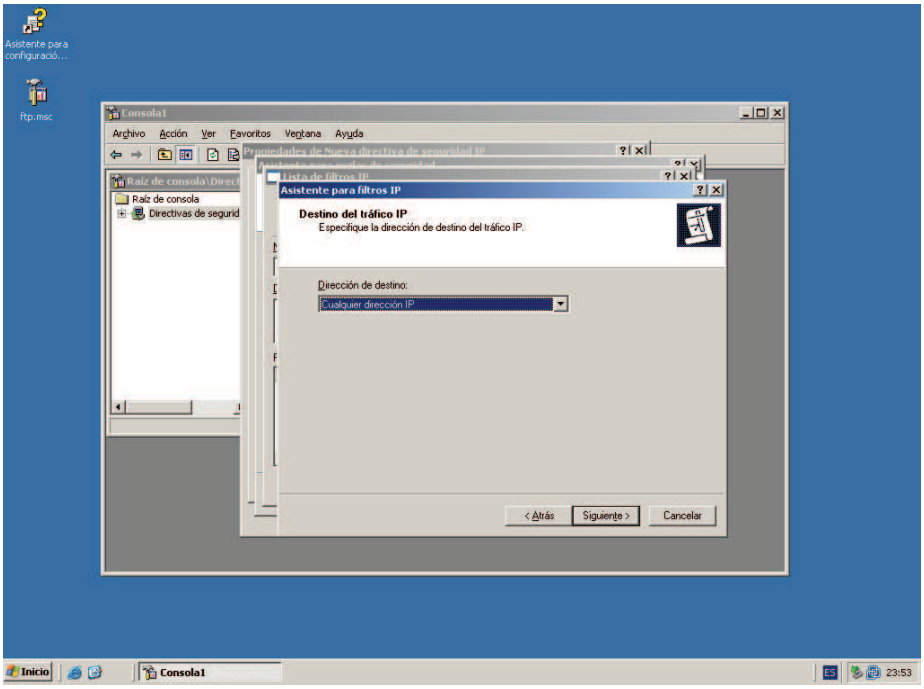
ANEXO 21

ELEGIMOS MI DIRECCIÓN IP



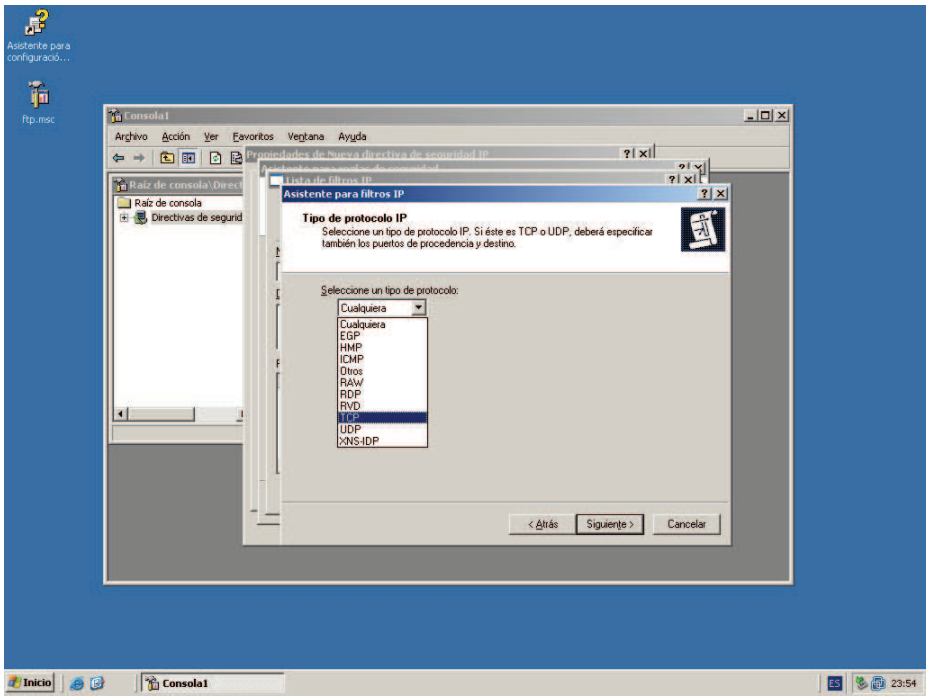
ANEXO 22

A CUALQUIER DIRECCIÓN IP



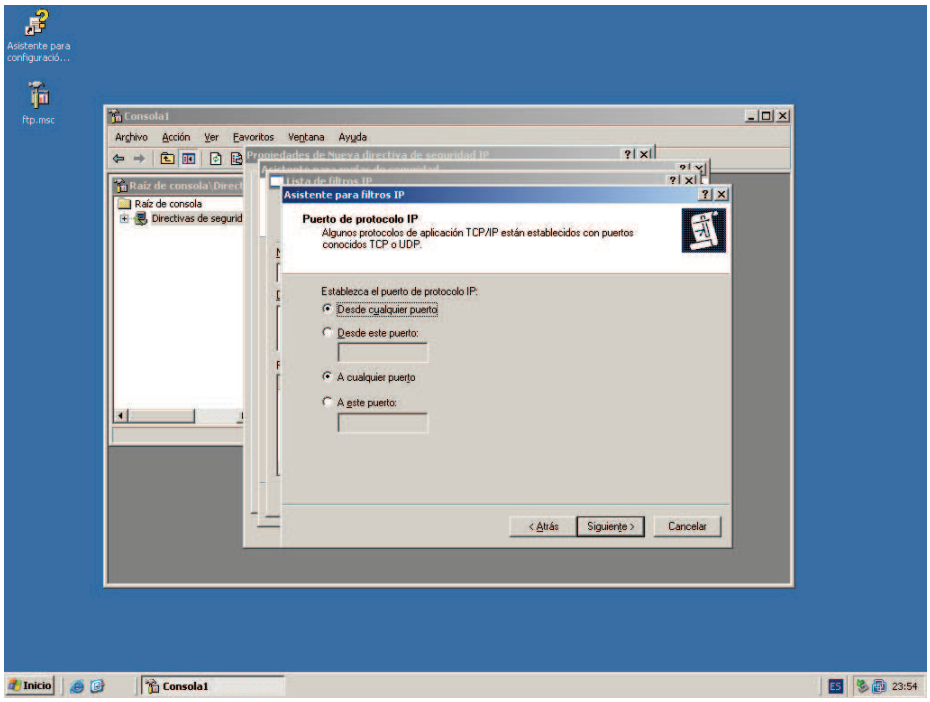
ANEXO 23

SELECCIONAMOS EL PROTOCOLO TCP



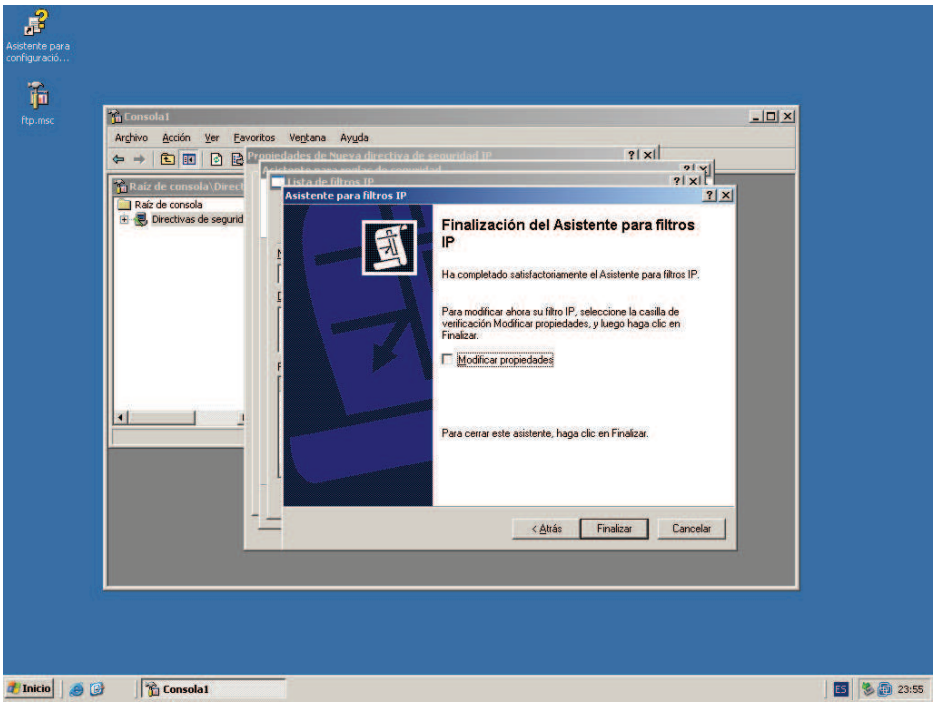
ANEXO 24

ELEGIMOS DESDE CUALQUIER PUERTO A CUALQUIER PUERTO



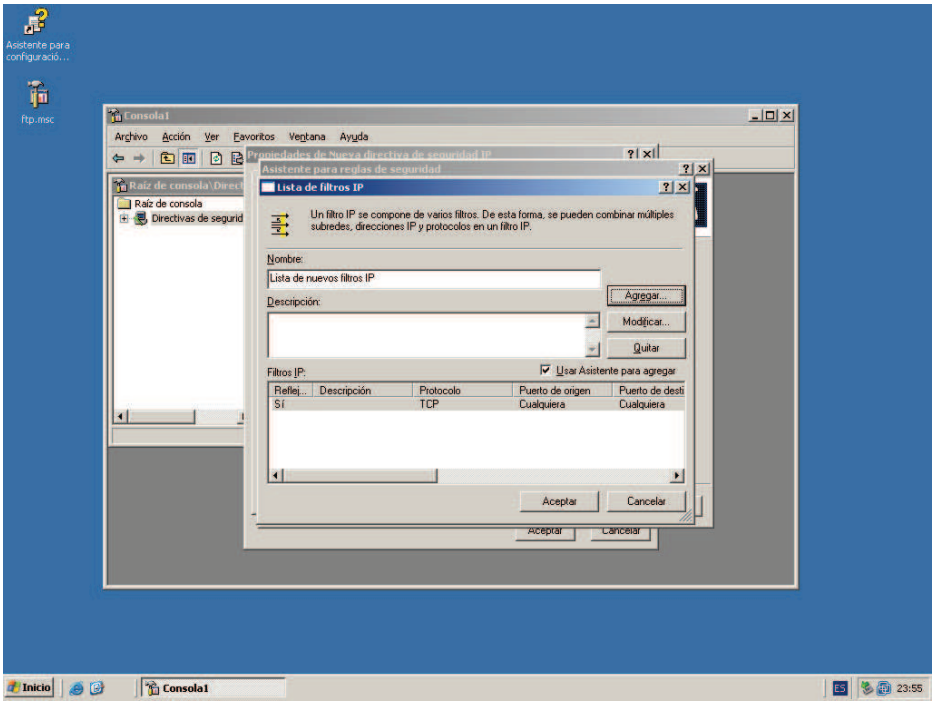
ANEXO 25

CLIC EN FINALIZAR



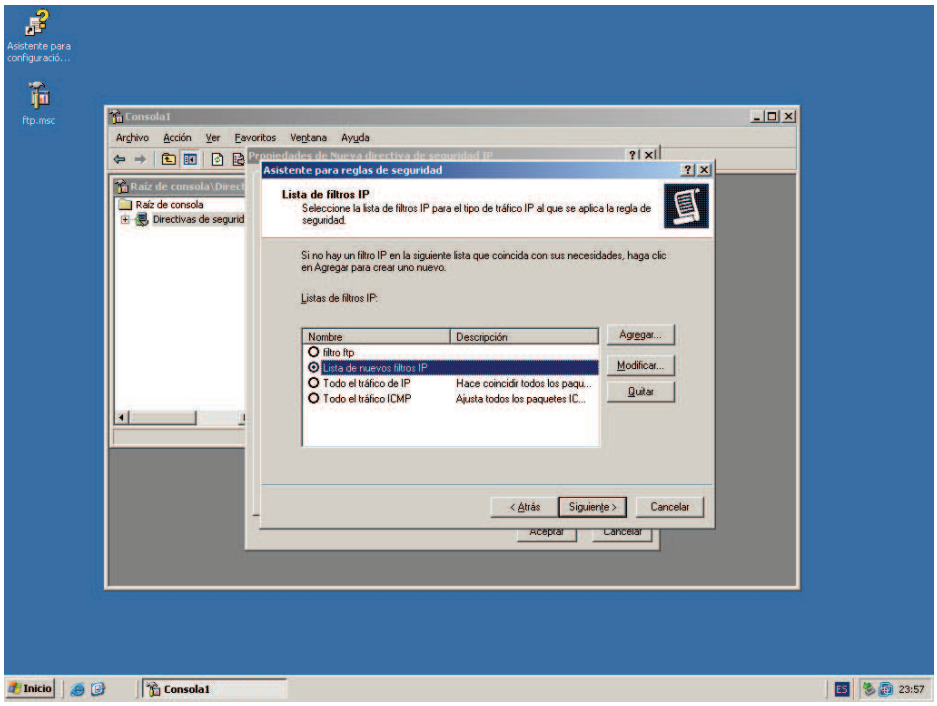
ANEXO 26

CLIC EN ACEPTAR



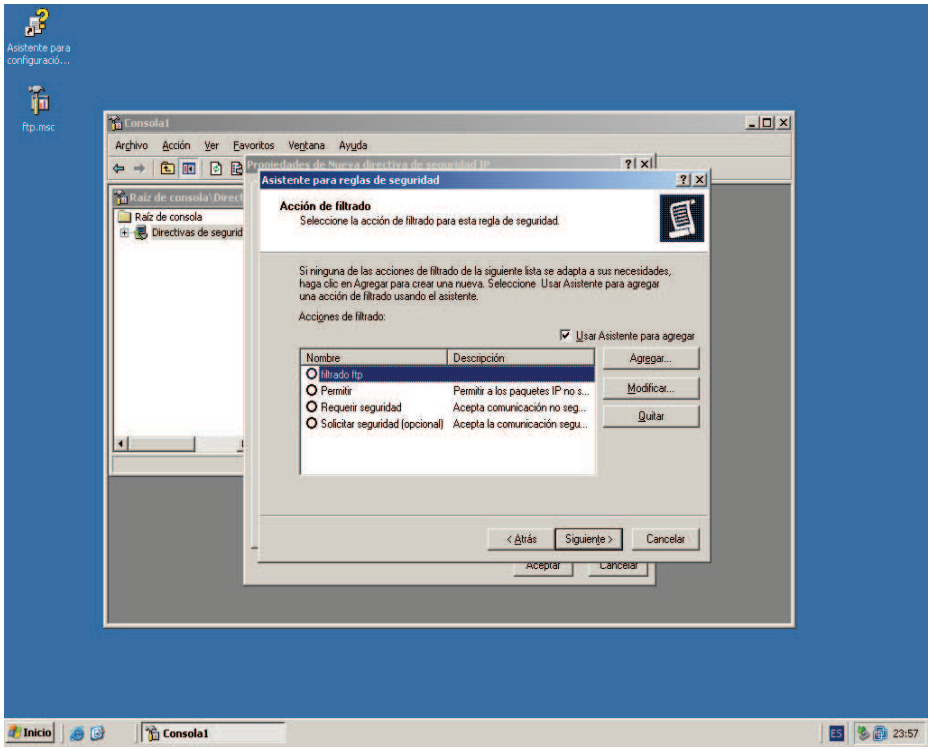
ANEXO 27

SELECCIONAMOS EL FILTRO CREADO Y CLIC EN SIGUIENTE



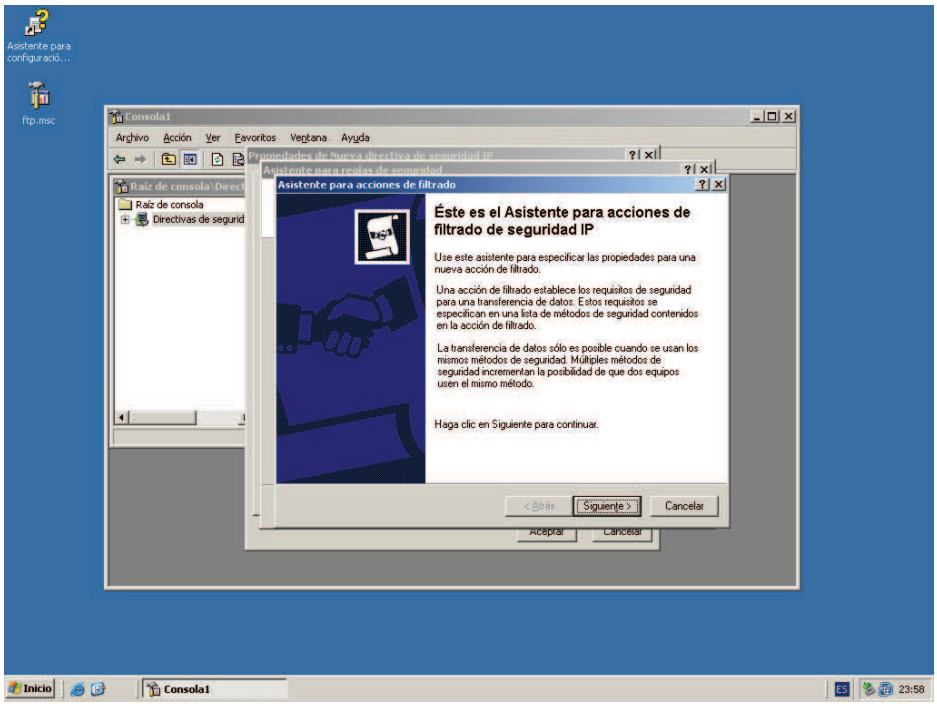
ANEXO 28

CLIC EN AGREGAR



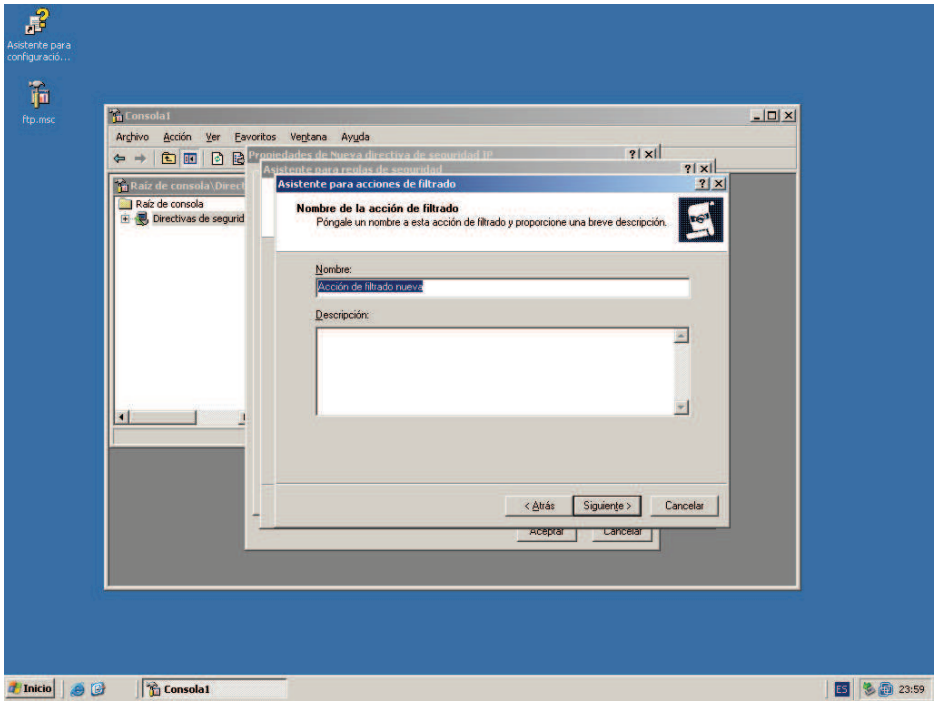
ANEXO 29

CLIC EN SIGUIENTE



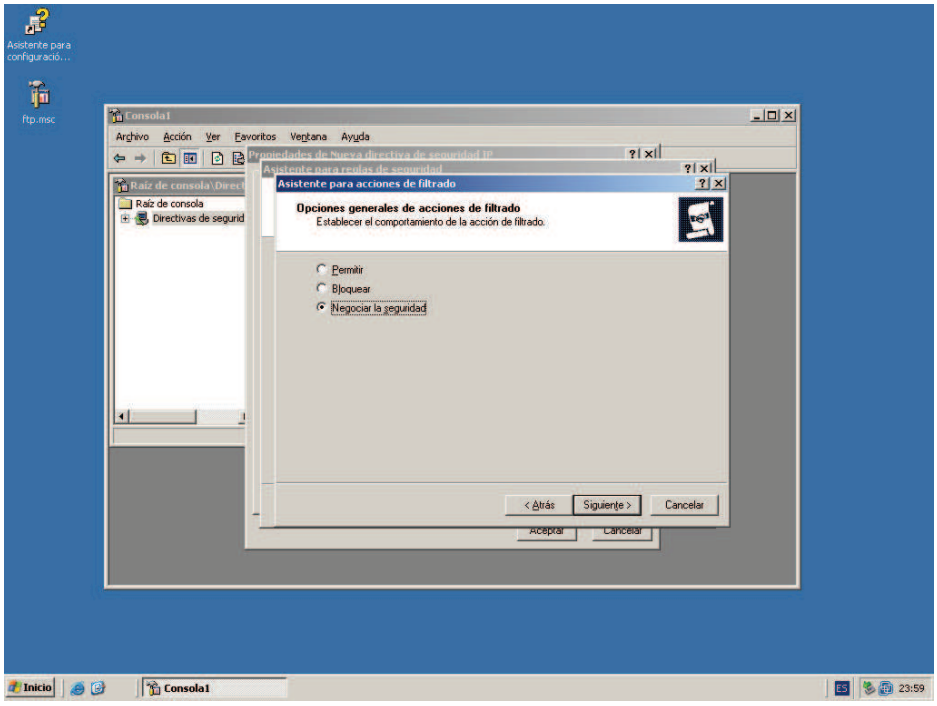
ANEXO 30

DAMOS UN NOMBRE A NUESTRA ACCIÓN DE FILTRADO



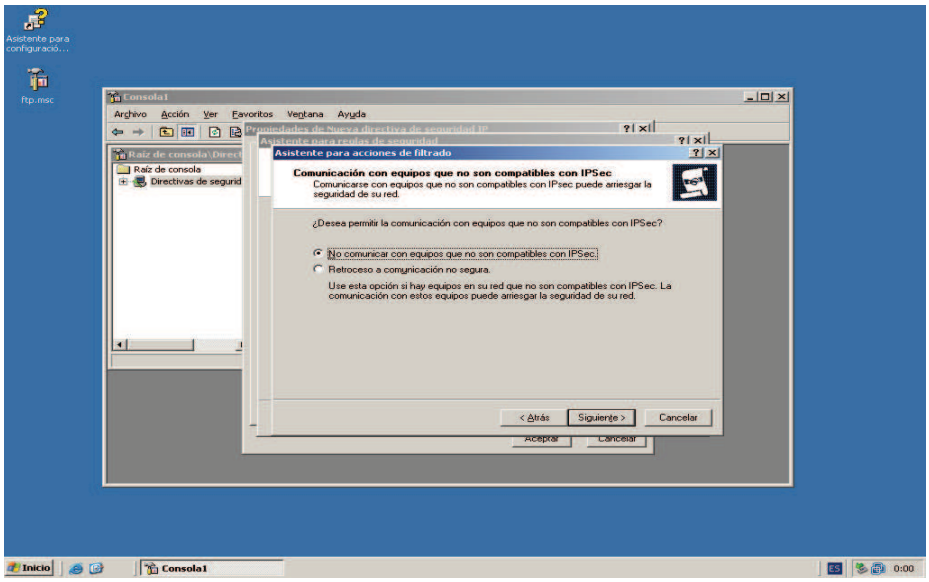
ANEXO 31

SELECCIONAMOS NEGOCIAR SEGURIDAD



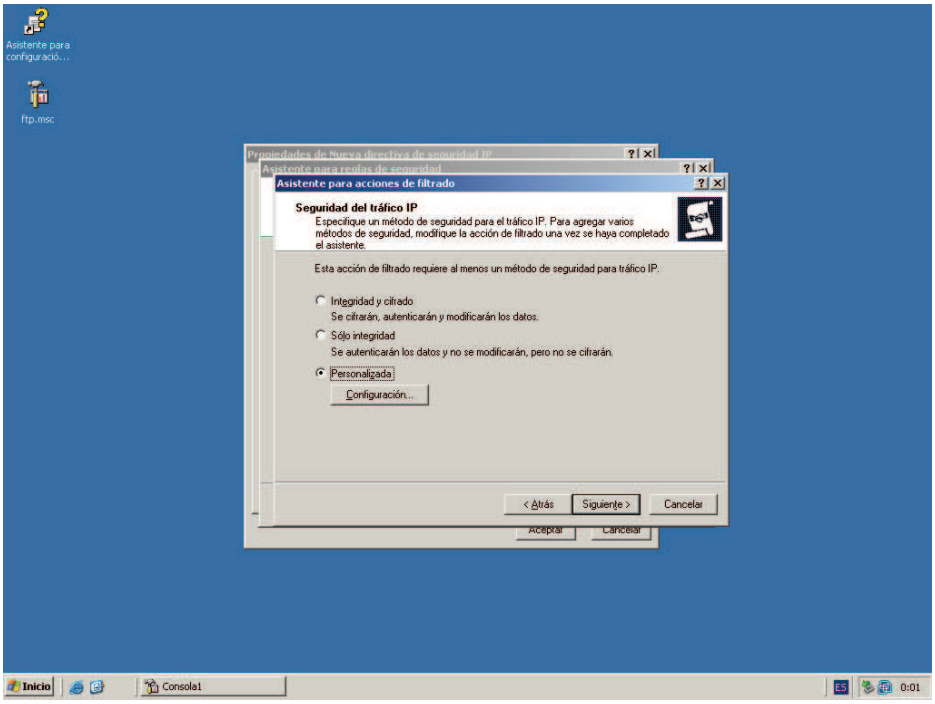
ANEXO 32

ELEGIMOS LA PRIMERA OPCIÓN



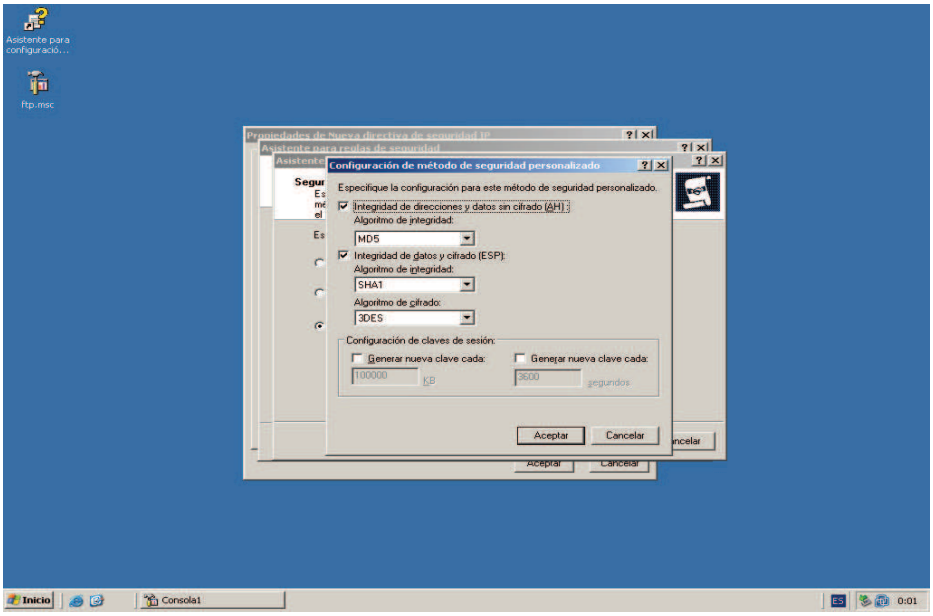
ANEXO 33

SELECCIONAMOS LA ÚLTIMA OPCIÓN Y CONFIGURAR



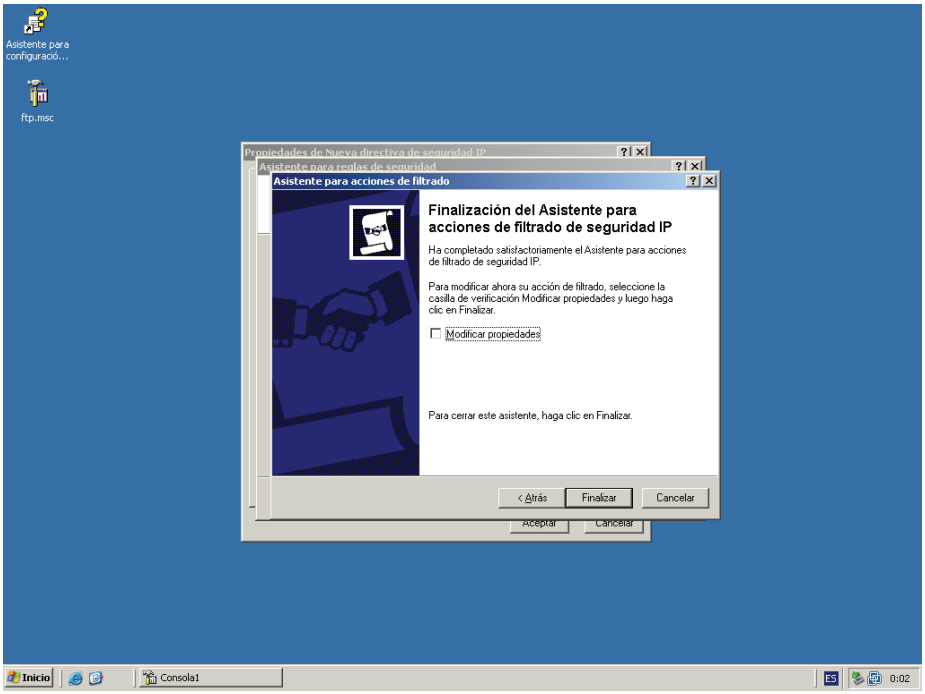
ANEXO 34

ELEGIMOS LAS 2 PRIMERAS OPCIONES Y SELECCIONAMOS EL ALGORITMO DE SEGURIDAD MD5



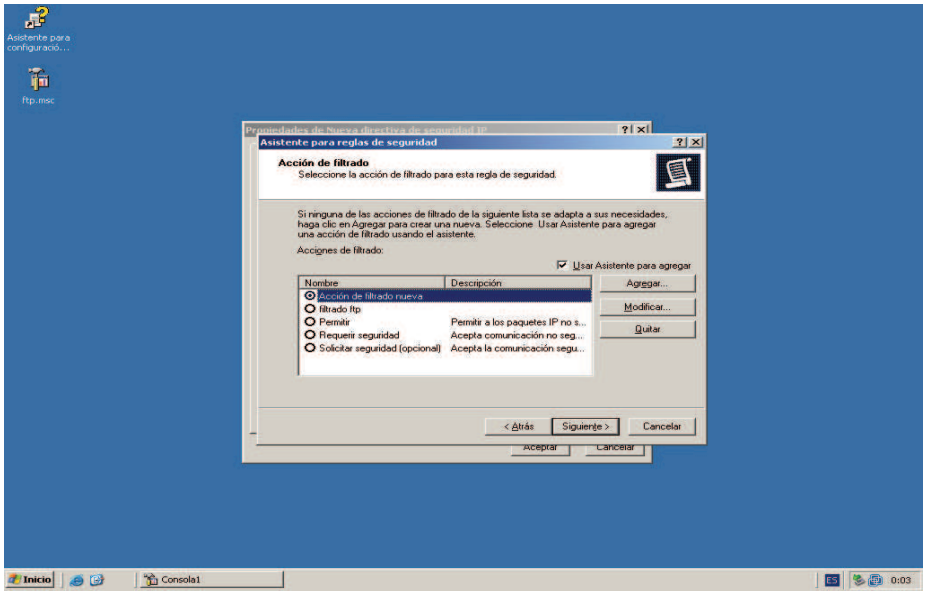
ANEXO 35

FINALIZAMOS



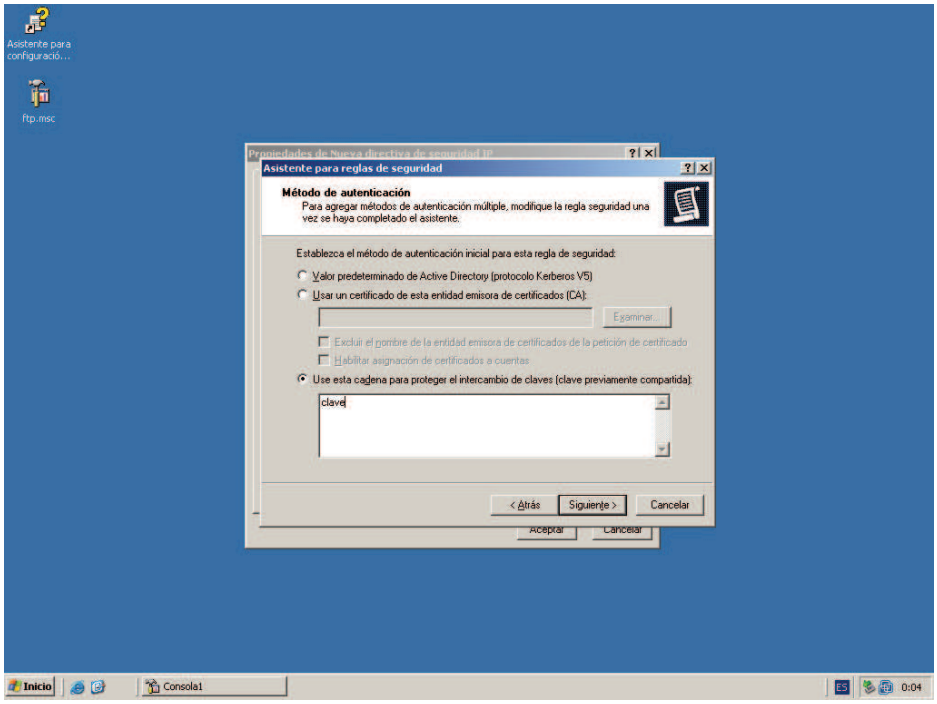
ANEXO 36

SELECCIONAMOS NUESTRA ACCIÓN DE FILTRADO Y CLIC EN SIGUIENTE



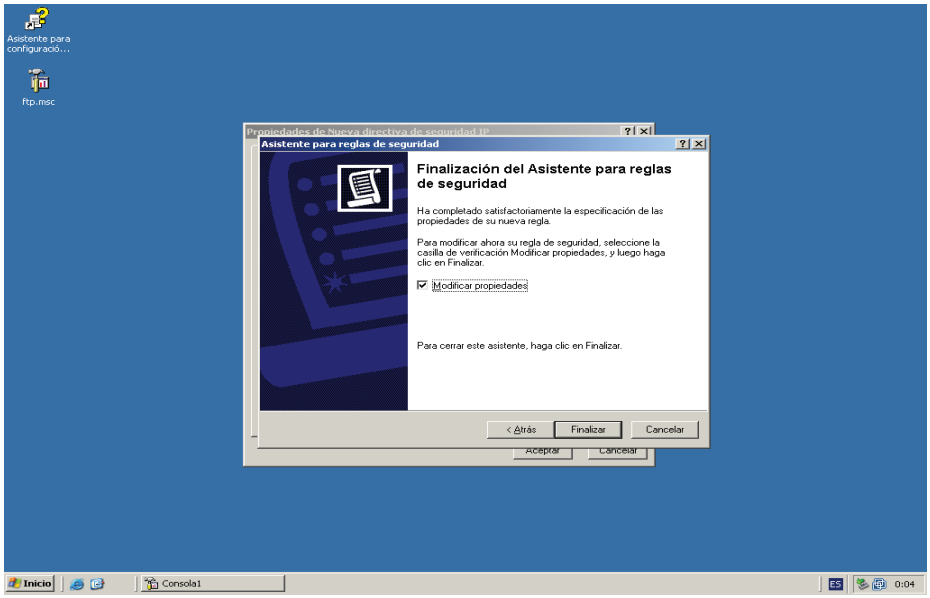
ANEXO 37

ELEGIMOS LA ULTIMA OPCIÓN Y DAMOS UNA CLAVE A NUESTRA LISTA DE FILTROS



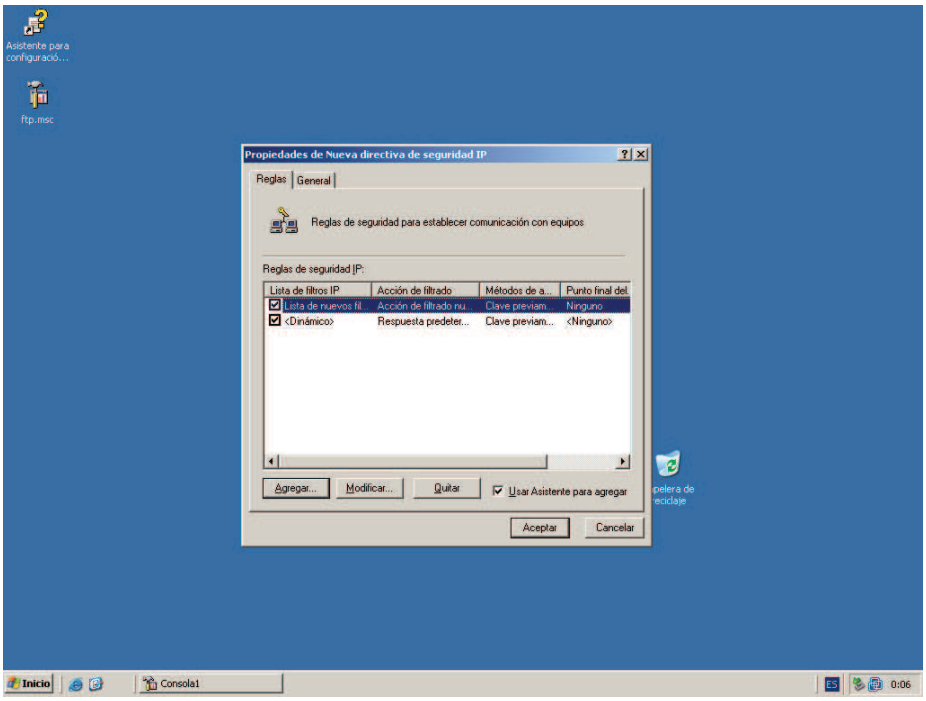
ANEXO 38

CLIC EN FINALIZAR



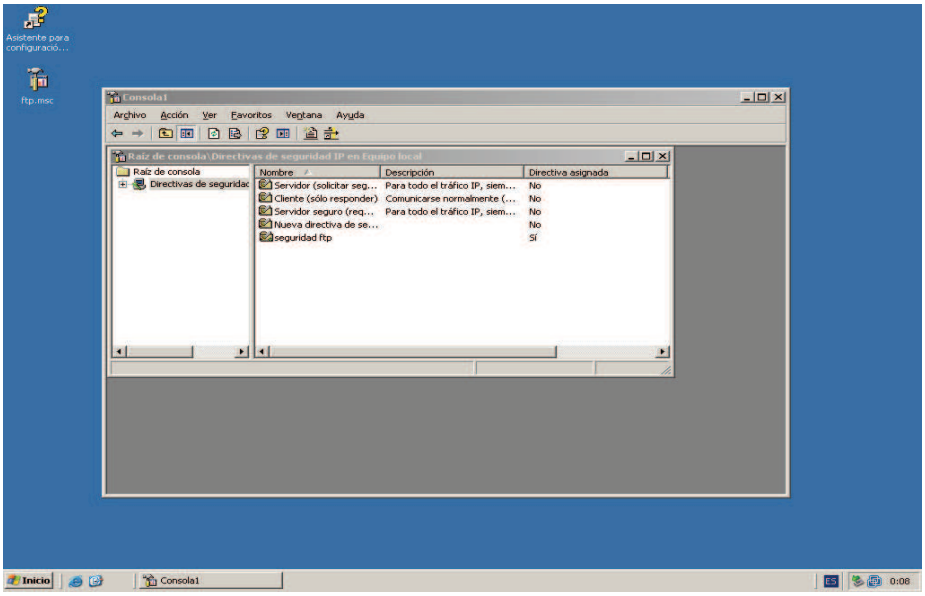
ANEXO 39

CLIC EN ACEPTAR



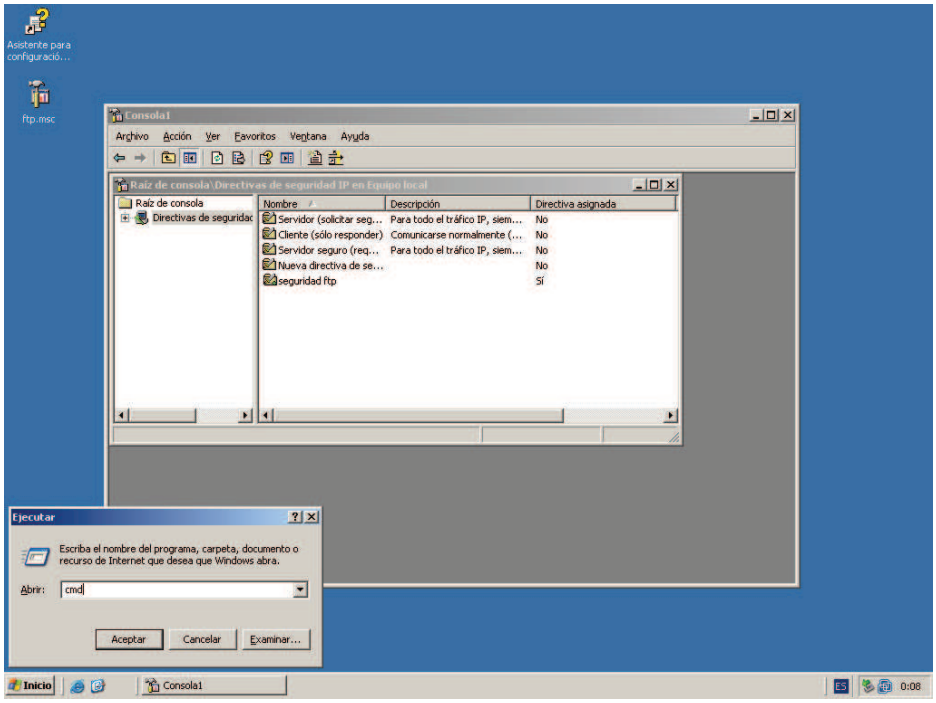
ANEXO 40

OBTENDREMOS UNA PANTALLA COMO ESTA



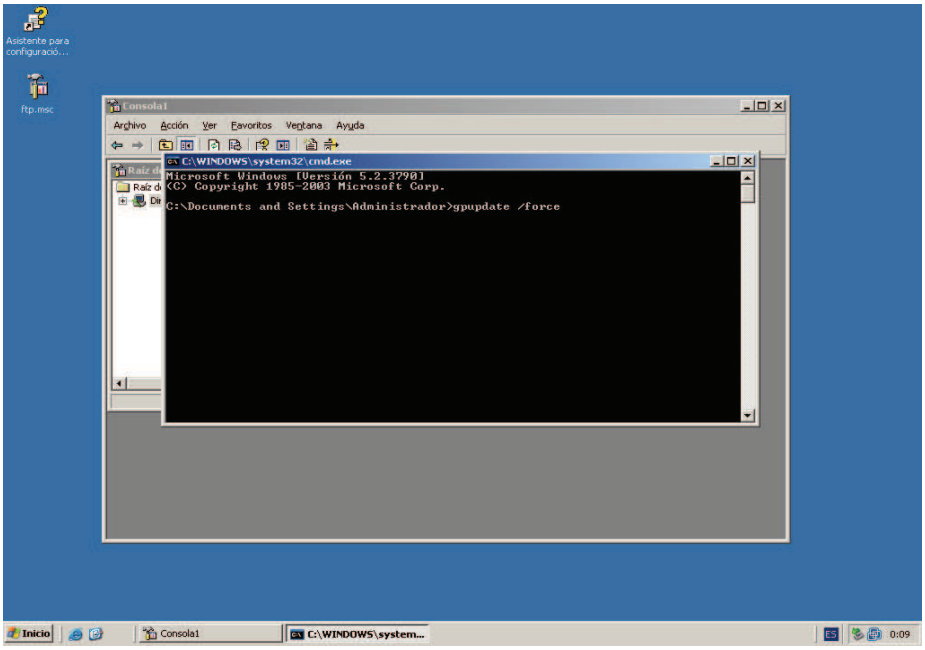
ANEXO 41

NUEVAMENTE INICIO EJECUTAR DIGITAMOS CMD



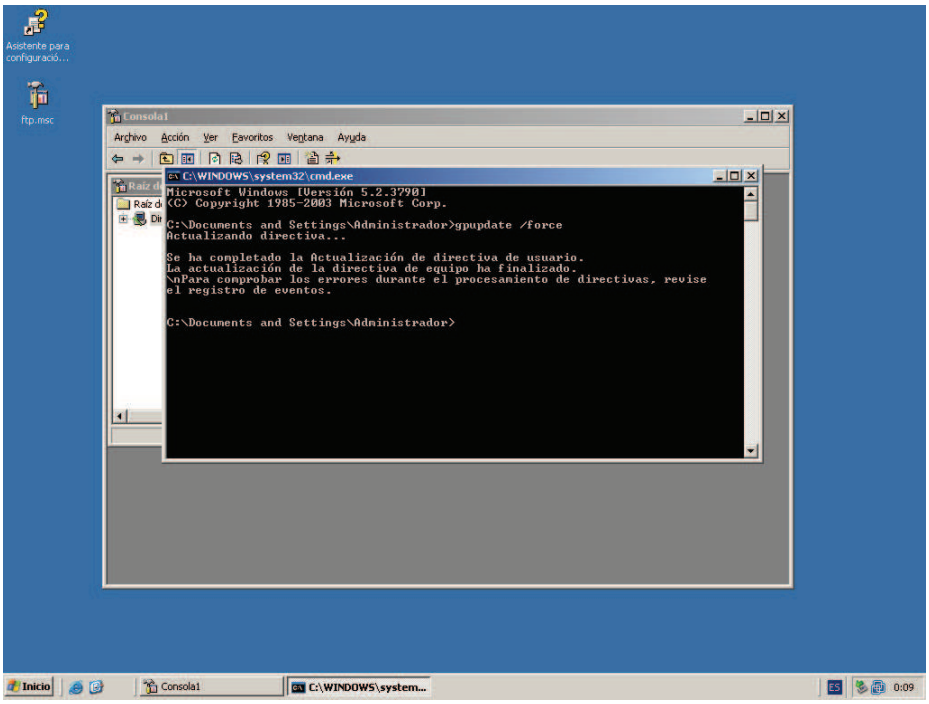
ANEXO 42

DIGITAMOS gpupdate /force



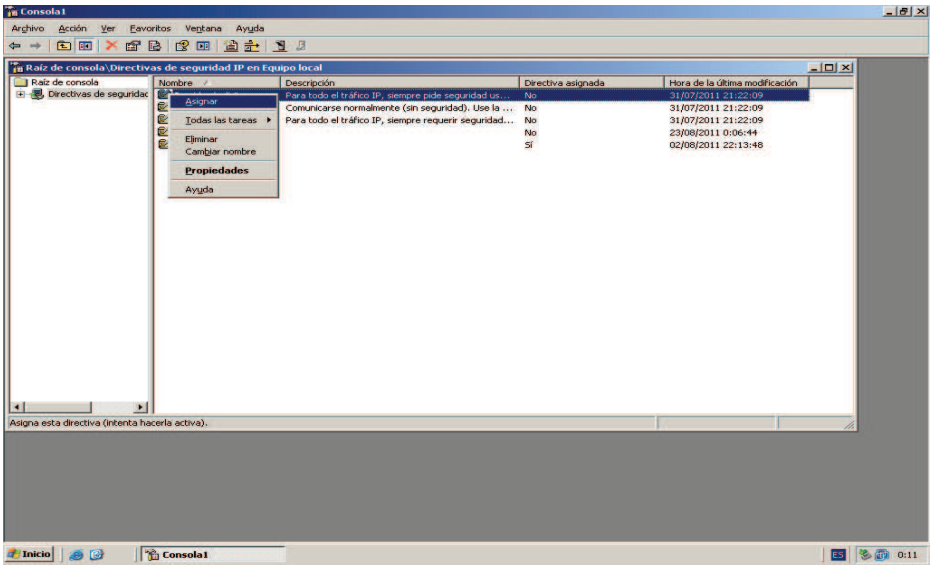
ANEXO 43

NOS SALDRÁ UN MENSAJE DE SE A COMPLETADO LA ACTUALIZACIÓN DE DIRECTIVAS DE SEGURIDAD



ANEXO 44

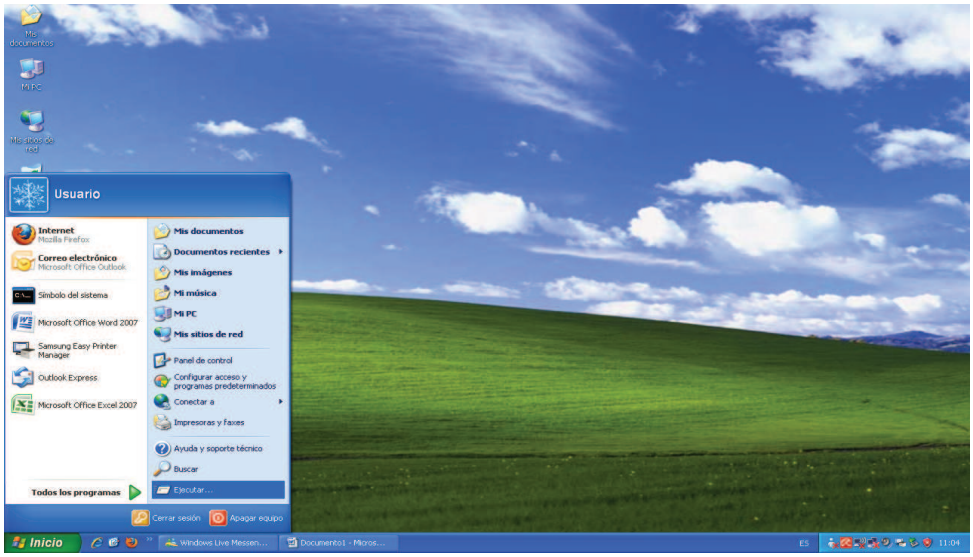
POR ULTIMO CLIC DERECHO EN NUESTRA DIRECTIVA CREADA Y MARCAMOS LA OPCIÓN ASIGNAR



ANEXO 45

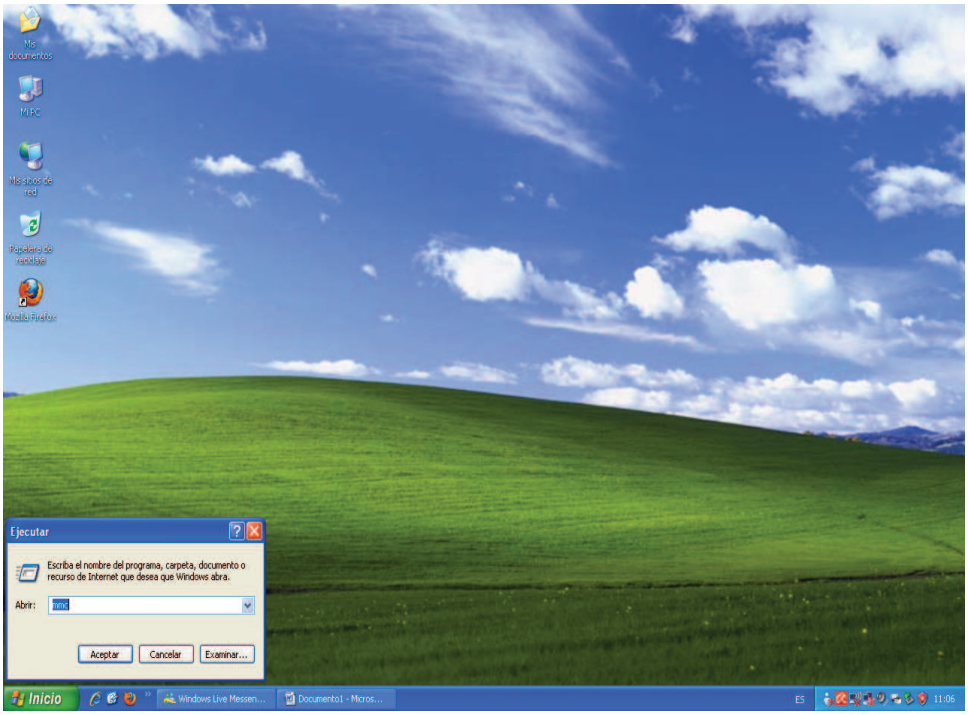
CONFIGURACION PASO A PASO DE IPsec EN WIN XP SP3

EJECUTAR



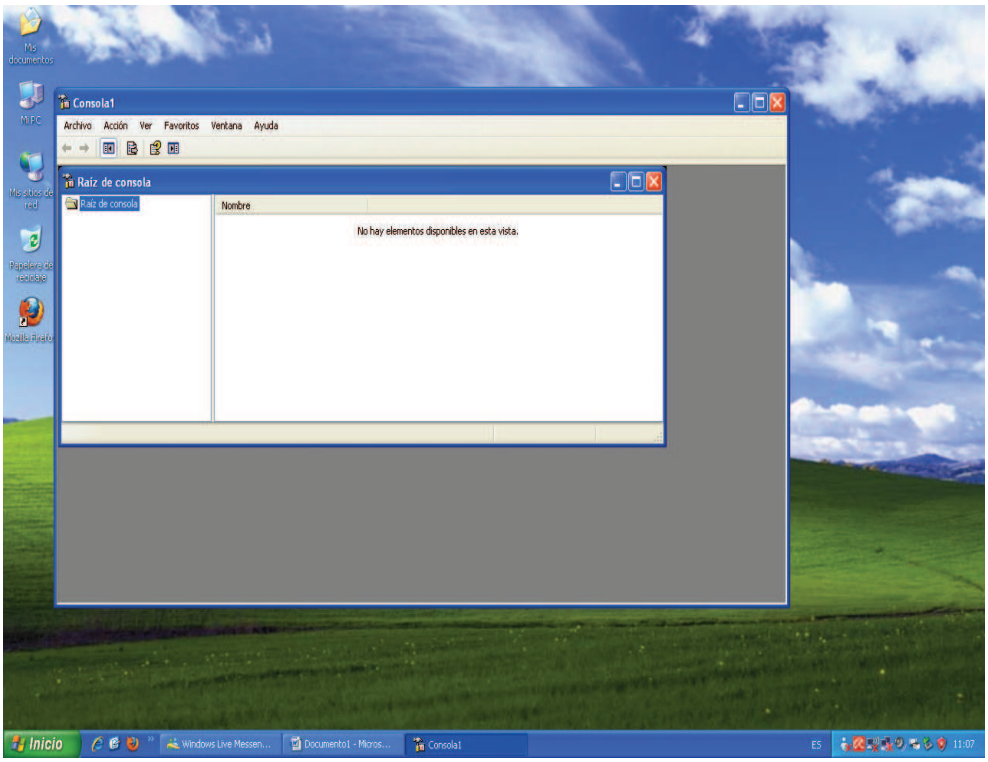
ANEXO 46

DIGITAMOS MMC



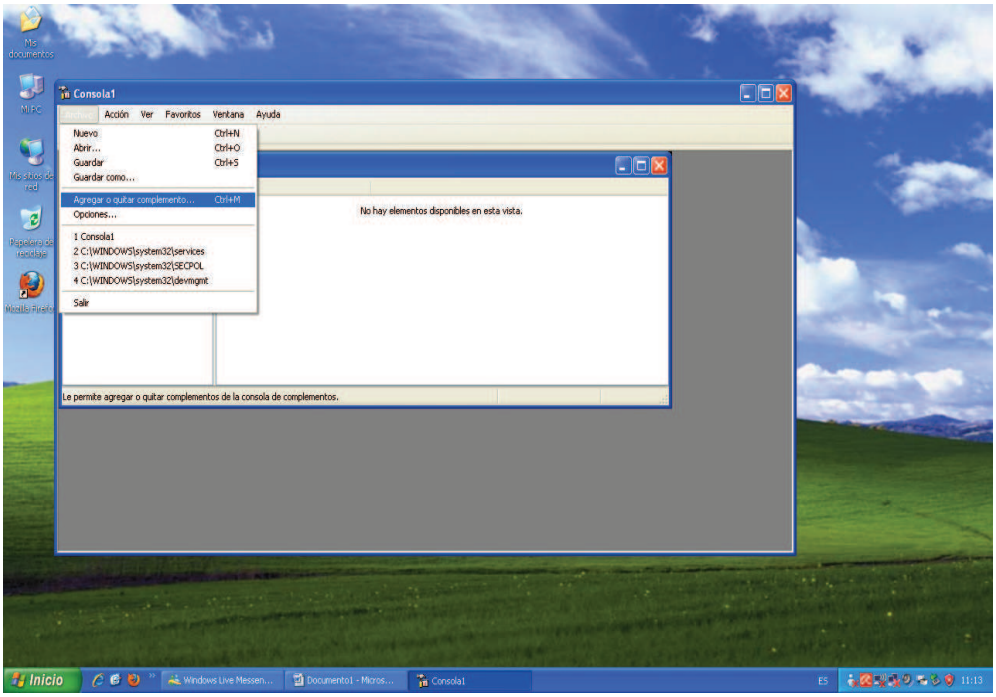
ANEXO 47

OBTENDREMOS UNA CONSOLA



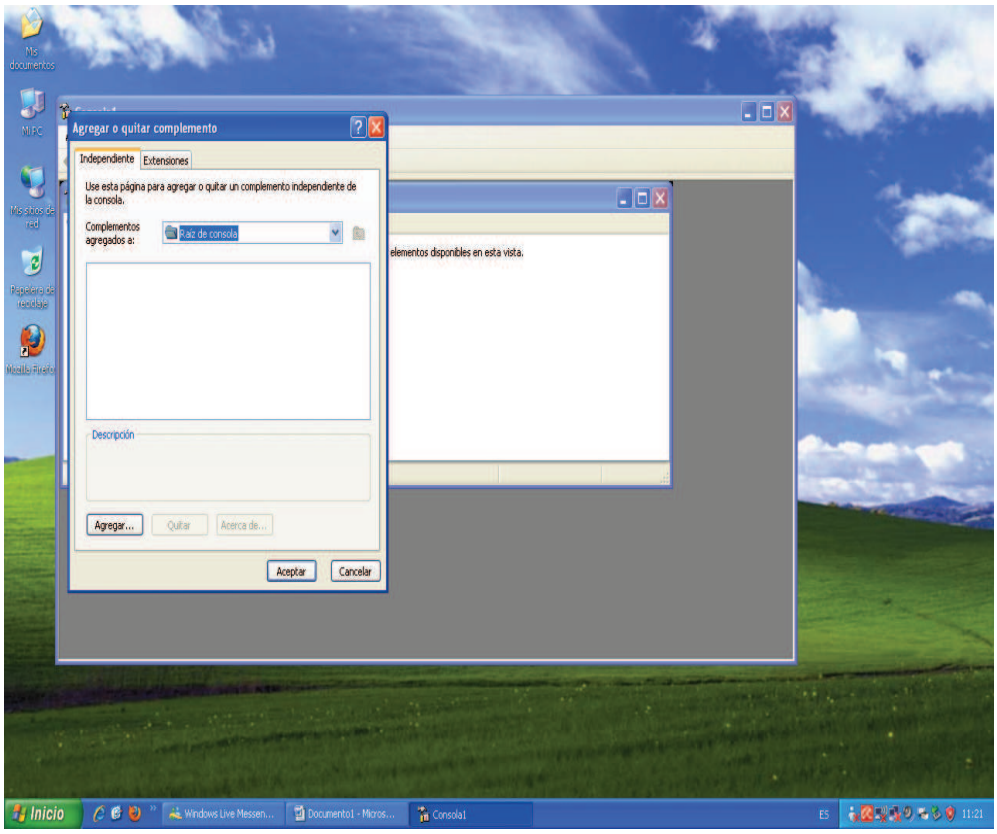
ANEXO 48

AGREGAMOS COMPLEMENTOS



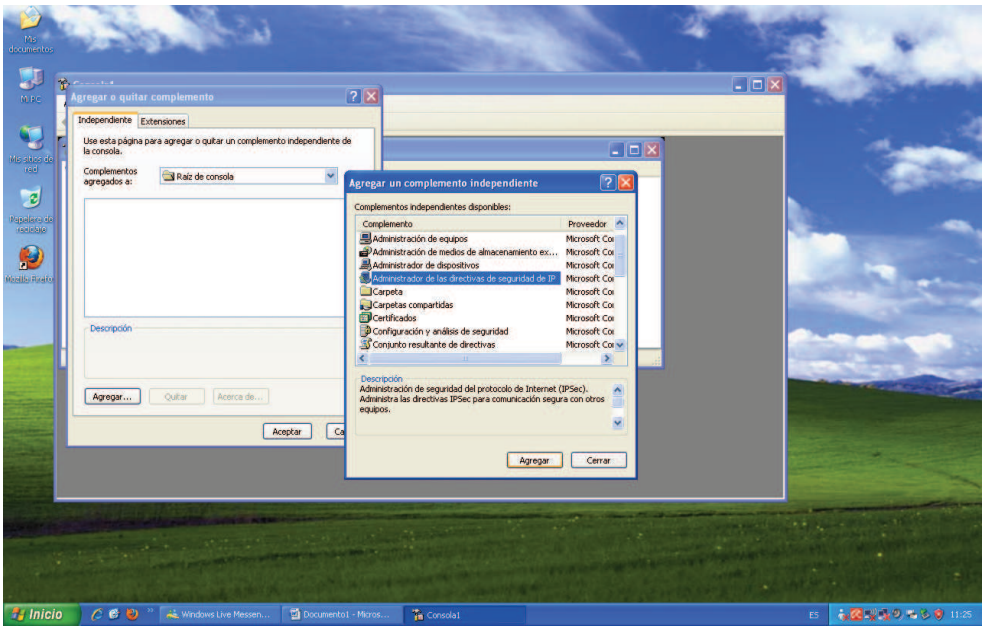
ANEXO 49

OBTENDREMOS UNA PANTALLA ASI



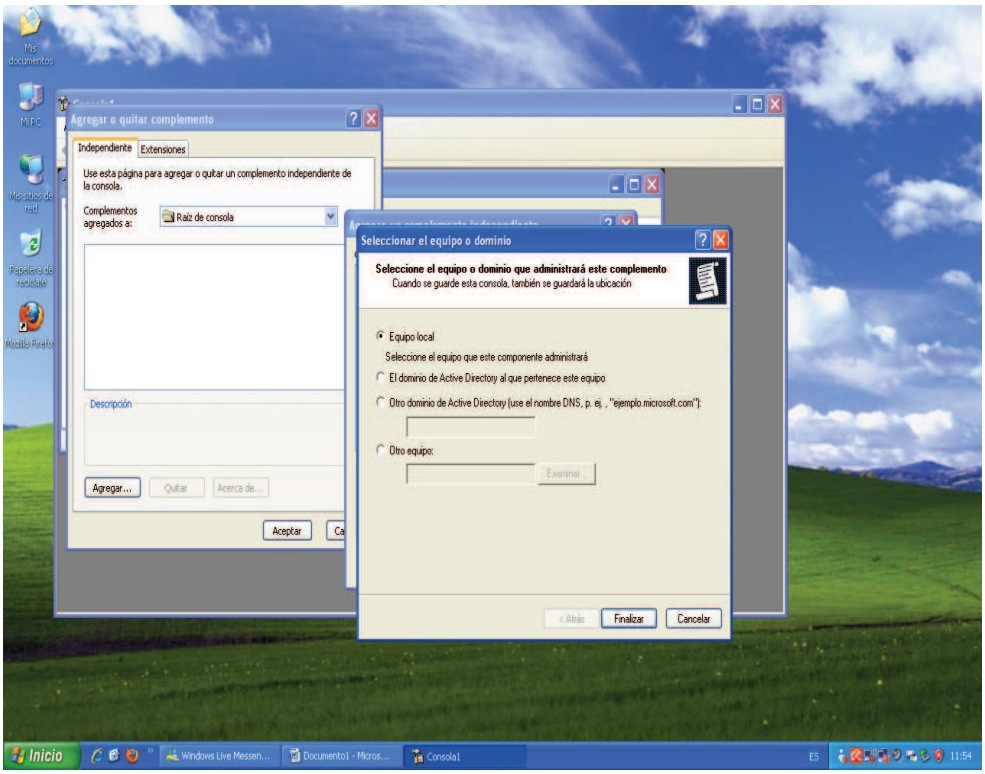
ANEXO 50

AGREGAMOS UNA DIRECTIVA DE SEGURIDAD IP



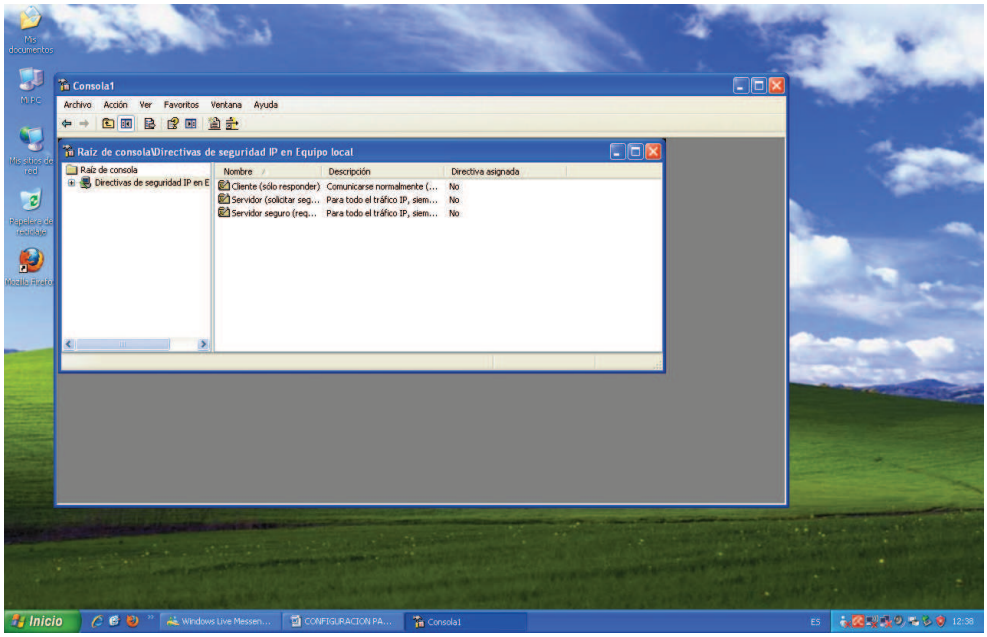
ANEXO 51

ELEGIMOS EQUIPO LOCAL Y FINALIZAR Y ACEPTAR



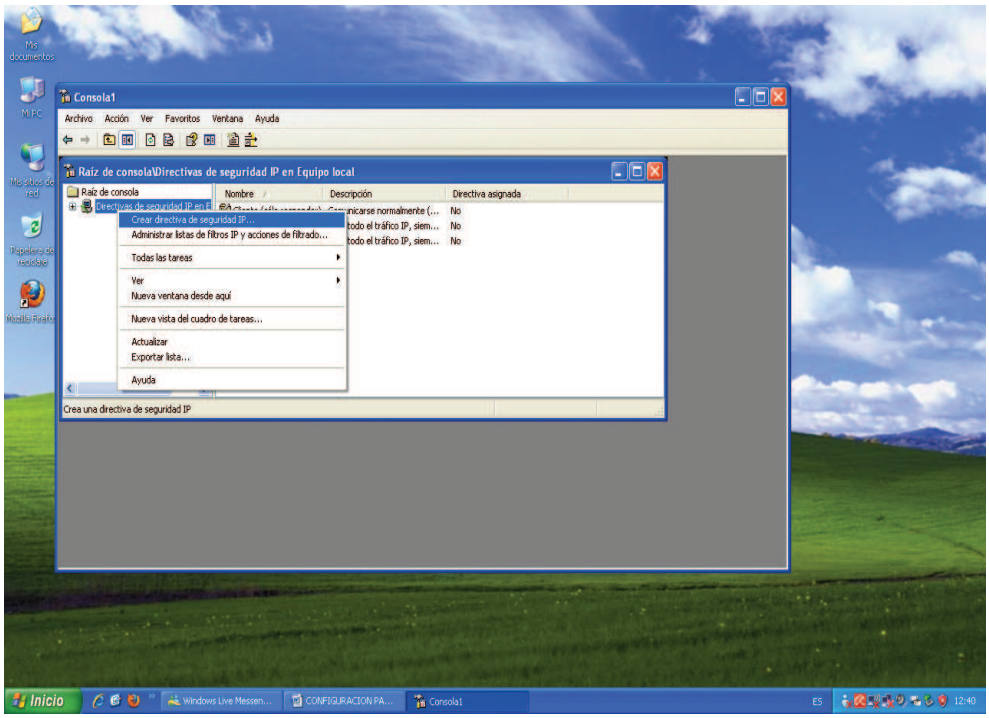
ANEXO 52

OBTENDREMOS LA SIGUIENTE PANTALLA



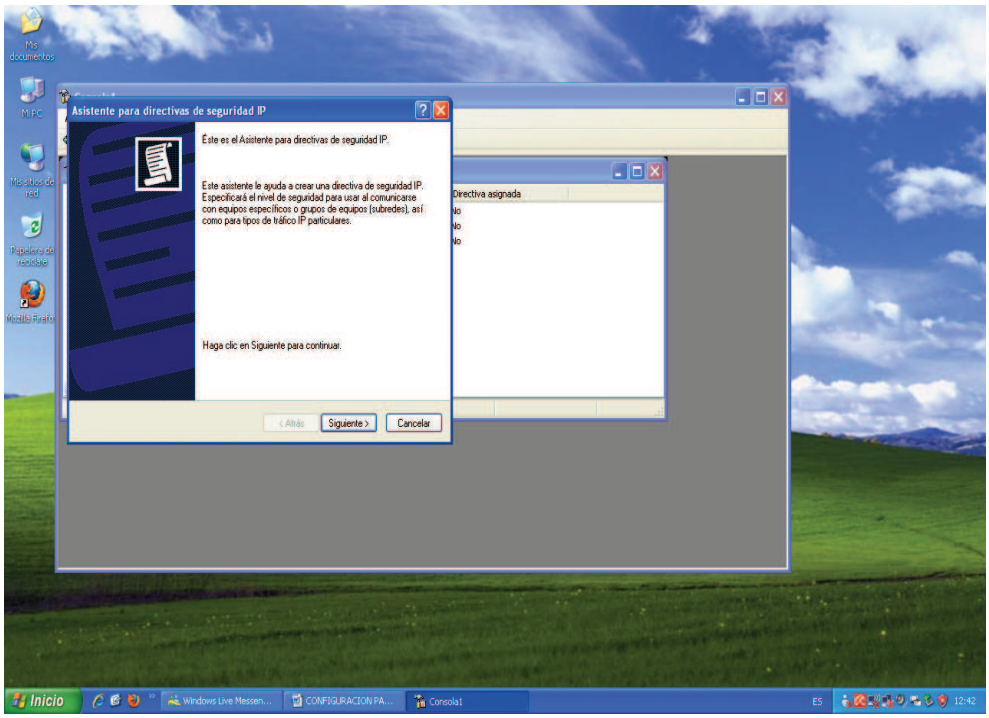
ANEXO 53

CREAMOS UNA DIRECTIVA DE SEGURIDAD IP



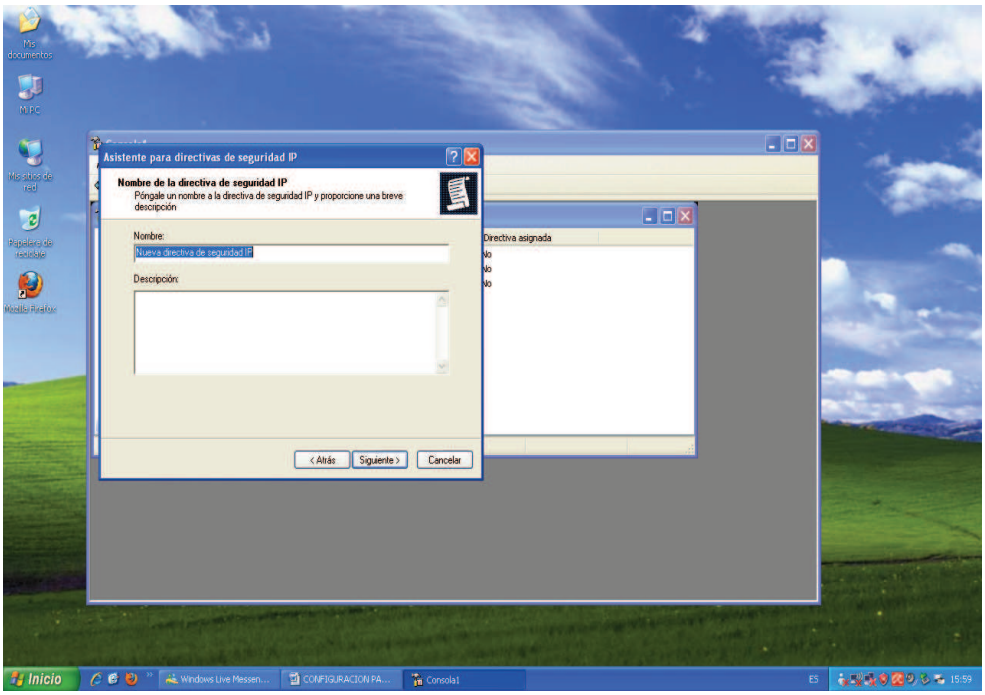
ANEXO 54

SIGUIENTE



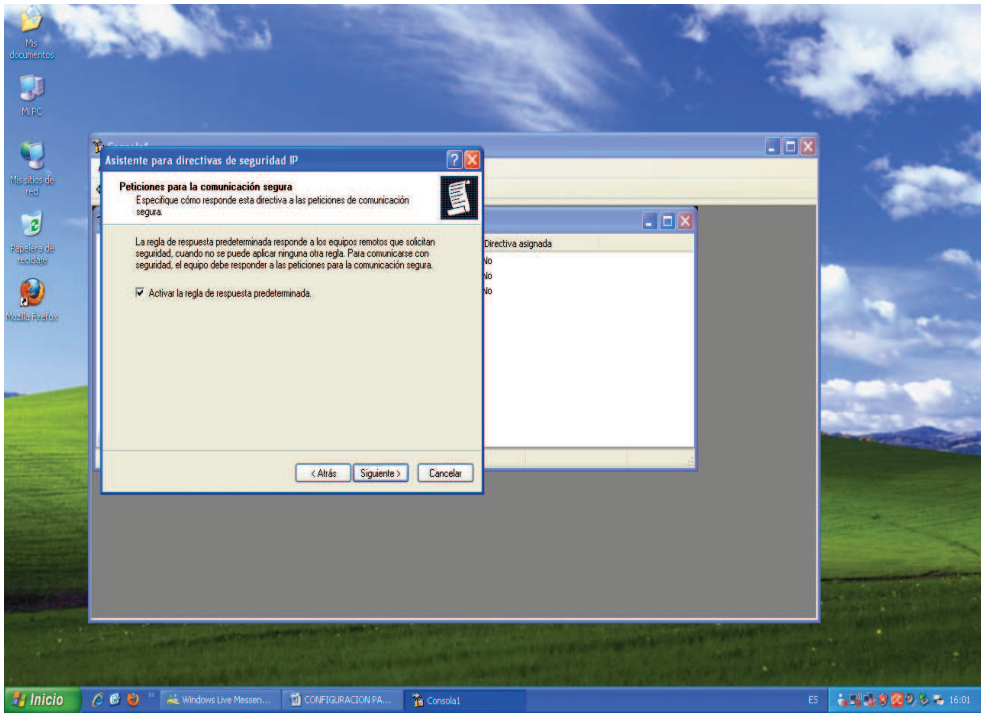
ANEXO 55

LE DAMOS EL NOMBRE A NUESTRA DIRECTIVA



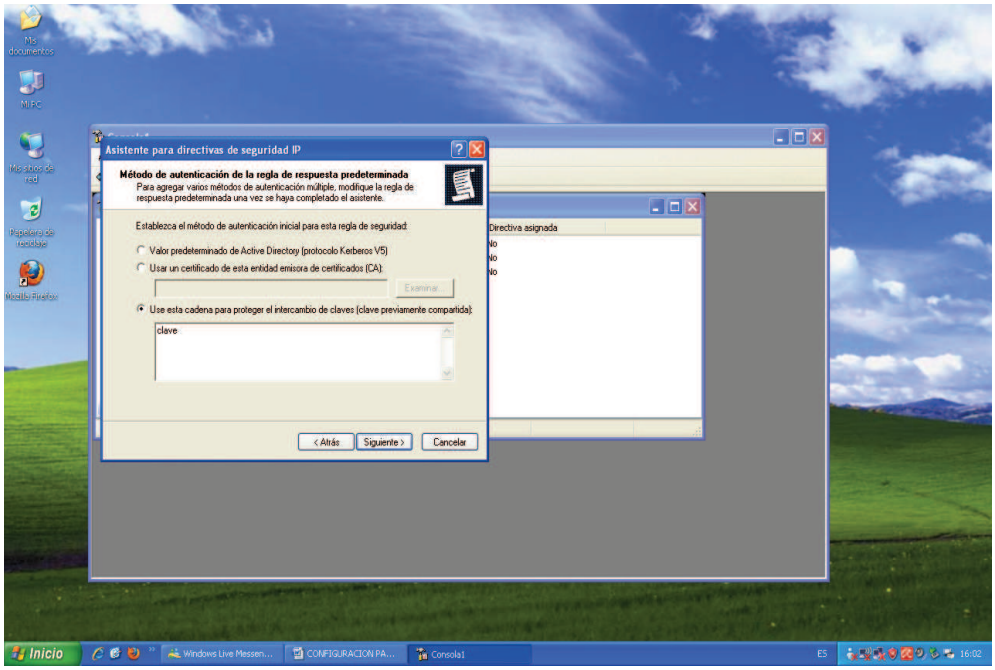
ANEXO 56

DEJAMOS LOS VALORES POR DEFECTO Y SIGUIENTE



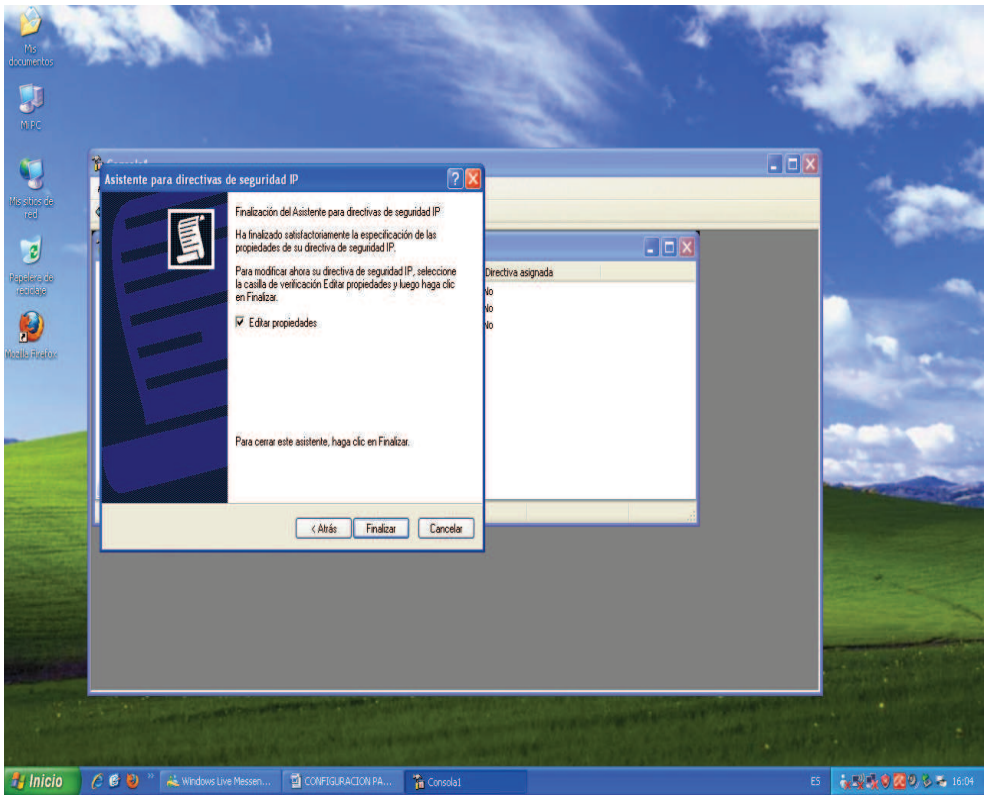
ANEXO 57

ESCOGEMOS LA ULTIMA OPCIÓN DIGITAMOS UNA CLAVE Y SIGUIENTE



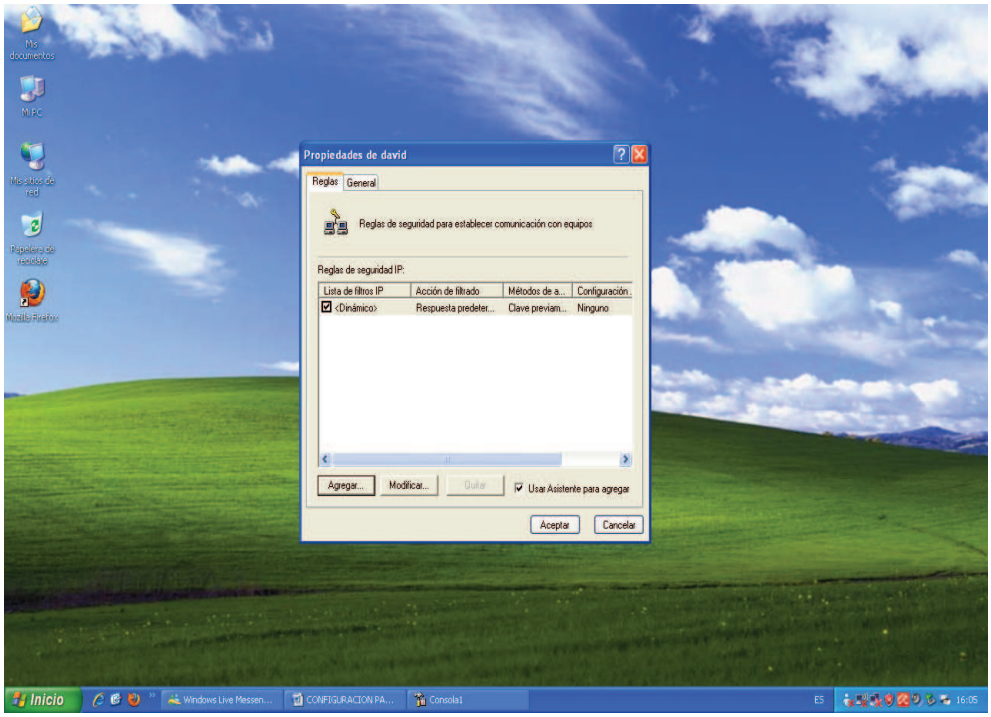
ANEXO 58

DEJAMOS LOS VALORES POR DEFECTO Y FINALIZAR



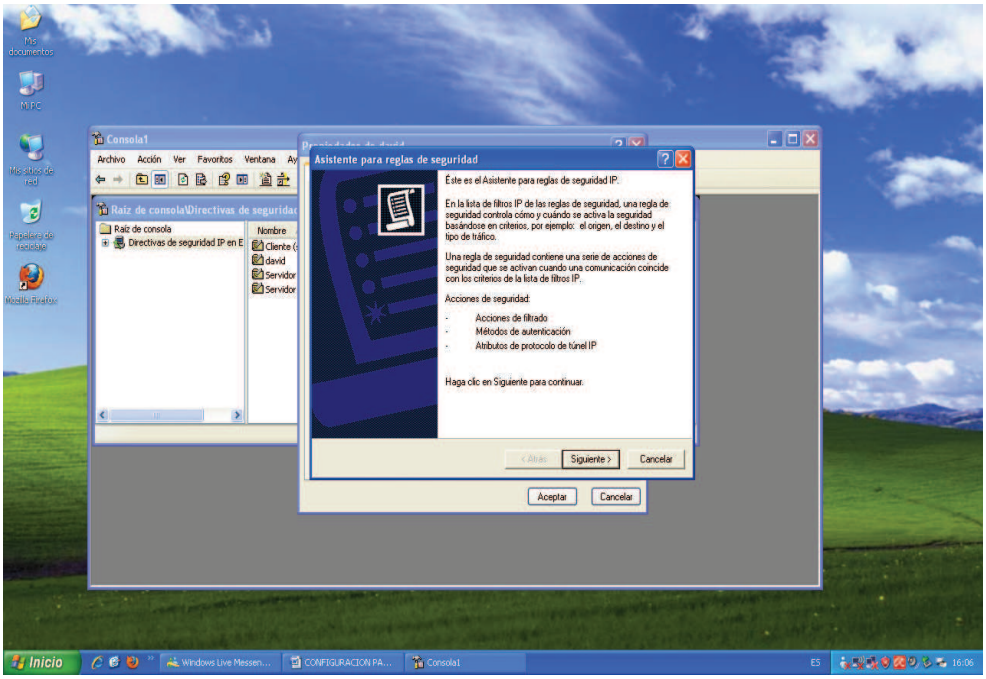
ANEXO 59

AGREGAR



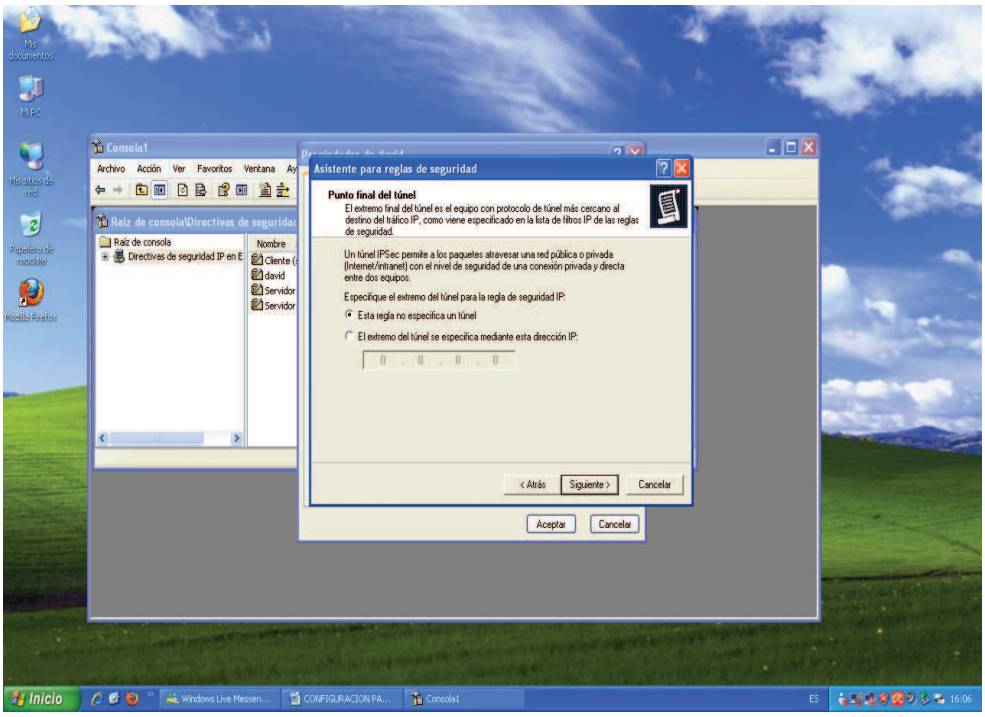
ANEXO 60

SIGUIENTE



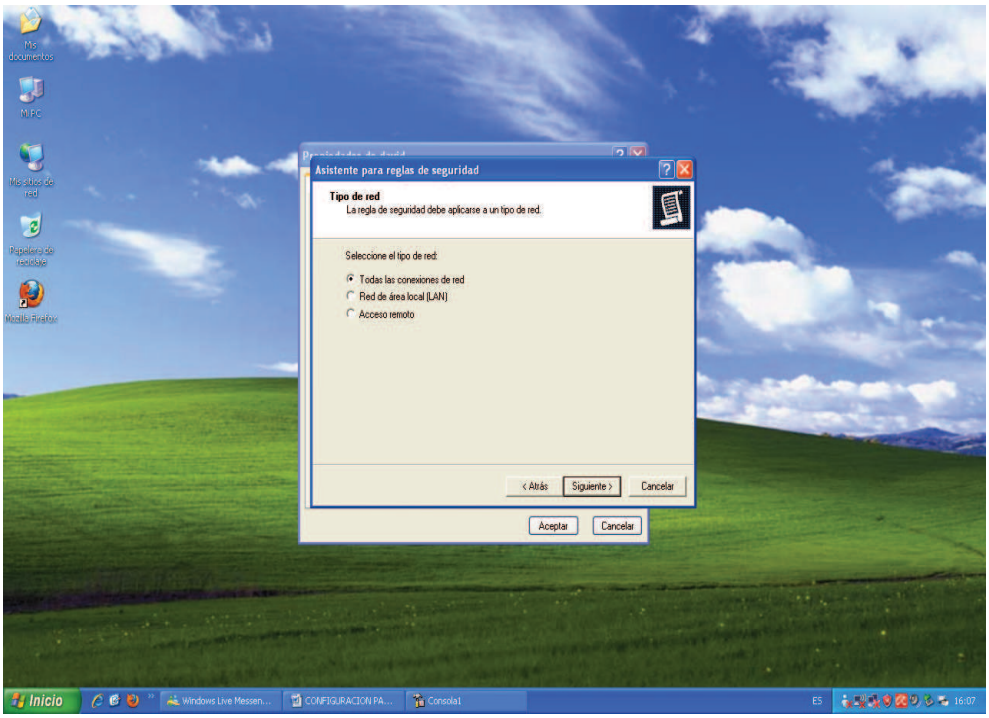
ANEXO 61

ELEGIMOS NO ESPECIFICAR UN TÚNEL



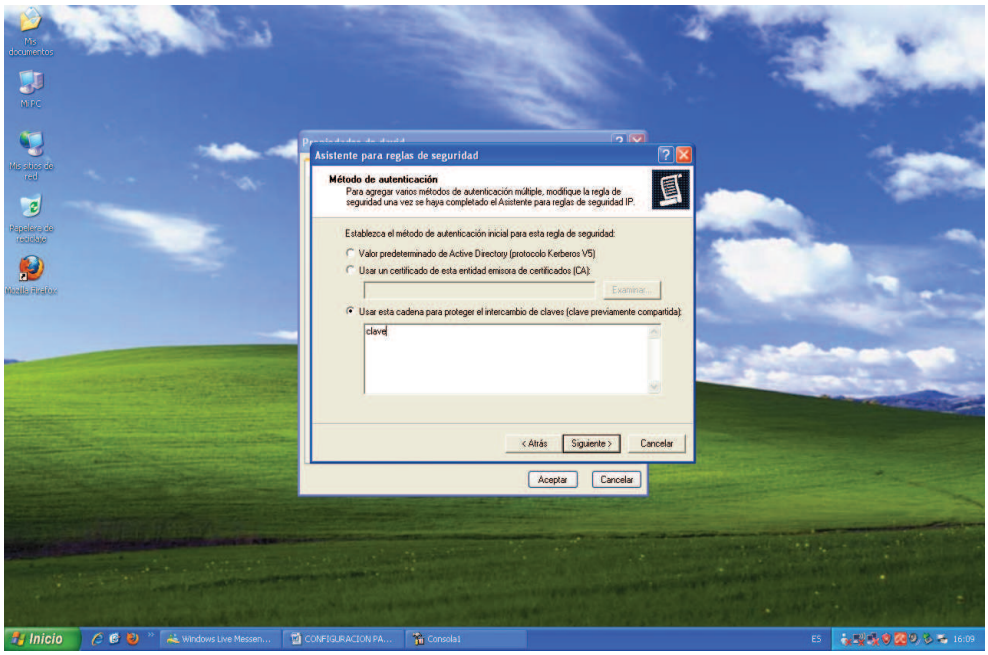
ANEXO 62

TODAS LAS CONEXIONES DE RED



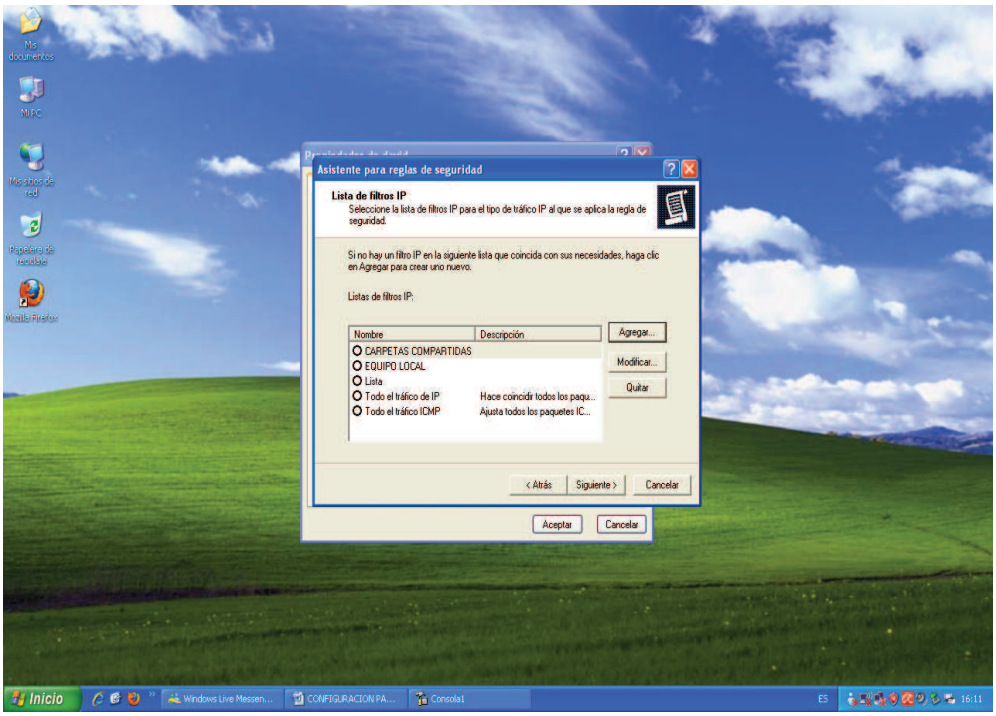
ANEXO 63

1. ESCOGEMOS LA ÚLTIMA OPCIÓN Y DIGITAMOS NUESTRA CLAVE QUE ELEGIMOS EN EL PASO # 13



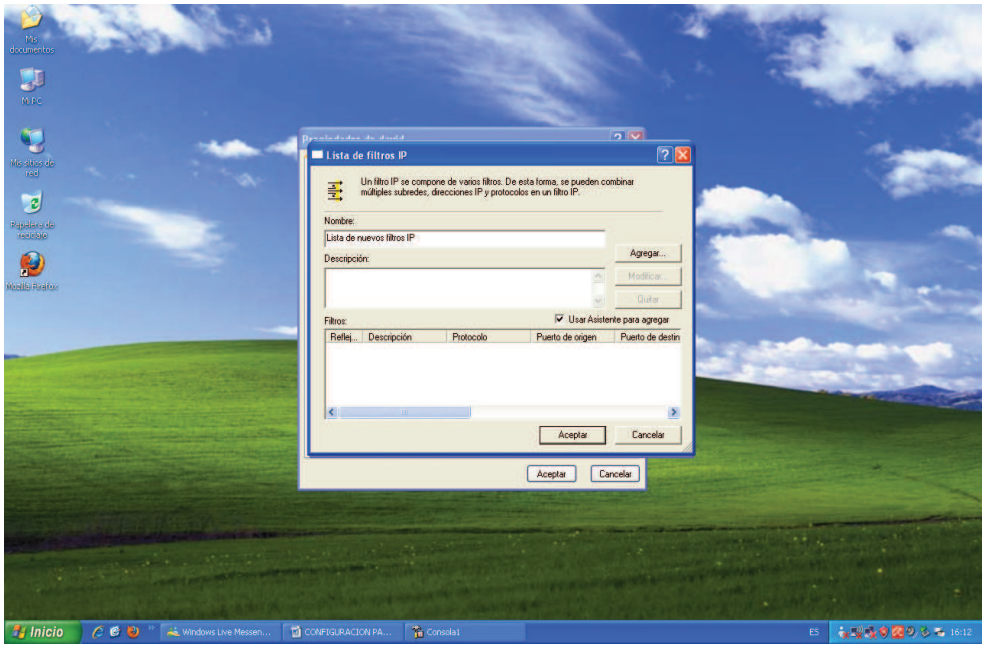
ANEXO 64

2. AGREGAR



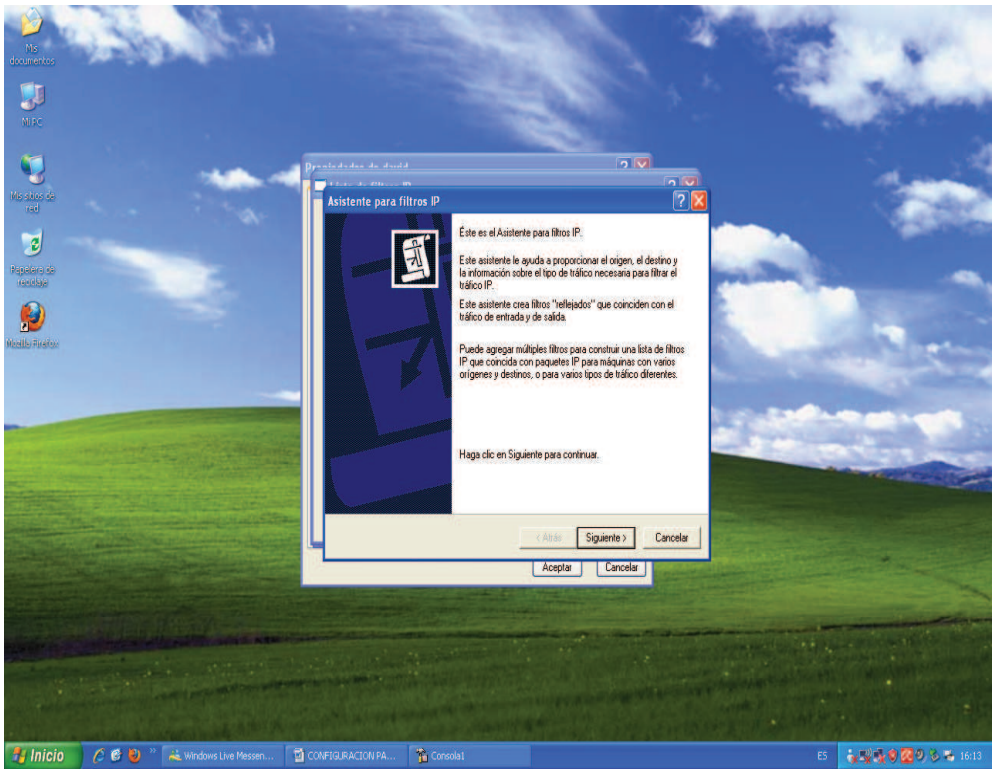
ANEXO 65

3. LE DAMOS UN NOMBRE A NUESTRA LISTA DE FILTROS Y AGREGAR



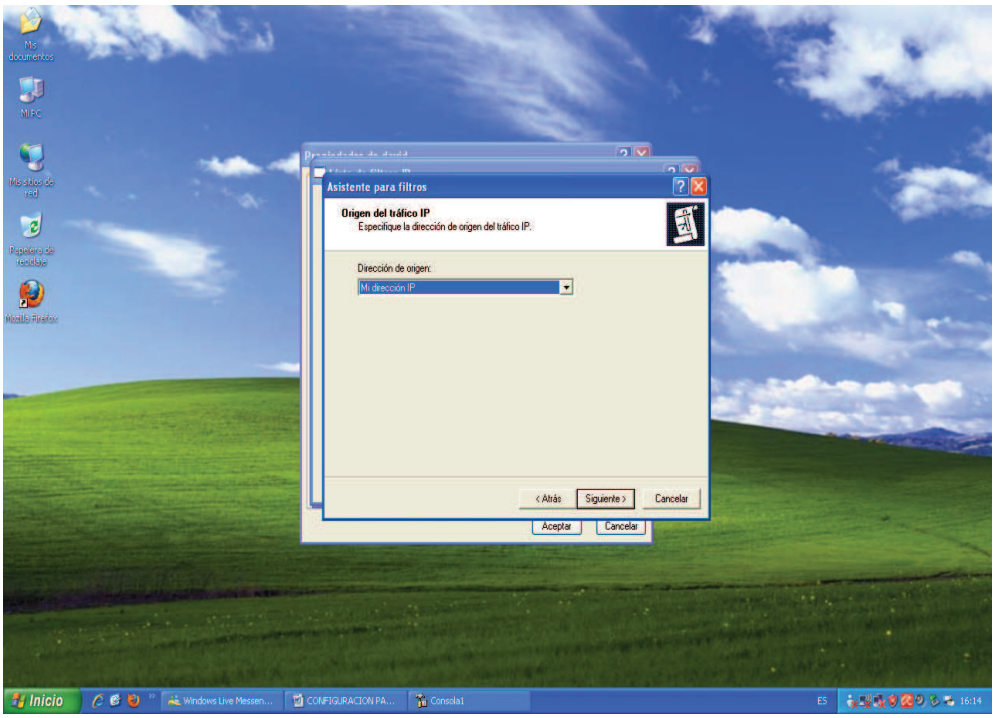
ANEXO 66

4. SIGUIENTE



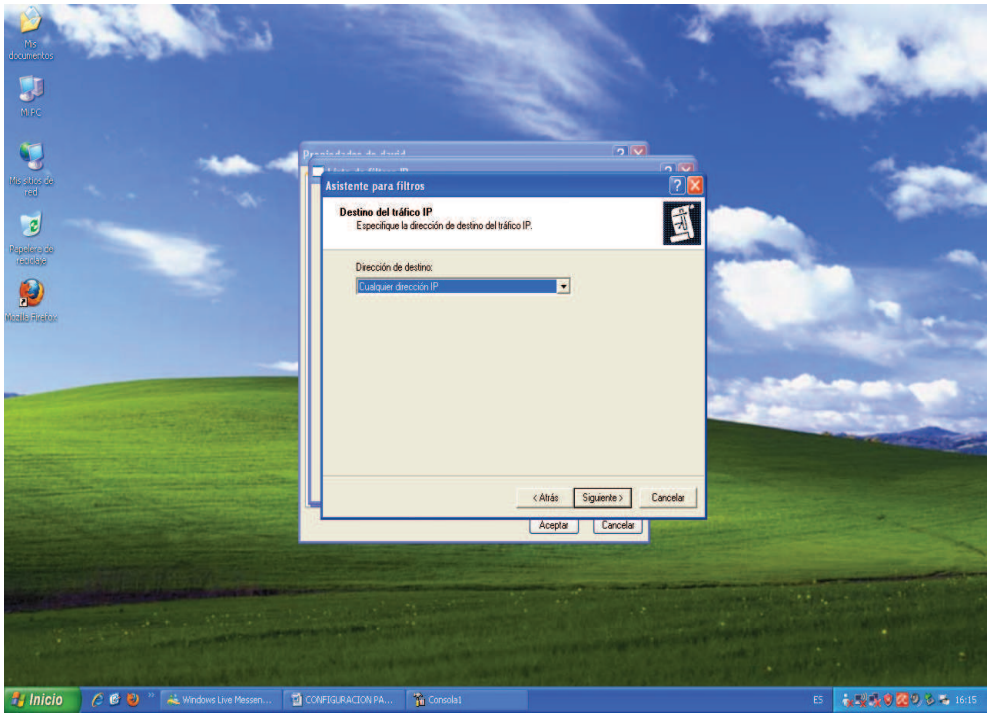
ANEXO 67

5. SELECCIONAMOS LA OPCIÓN MI DIRECCIÓN IP



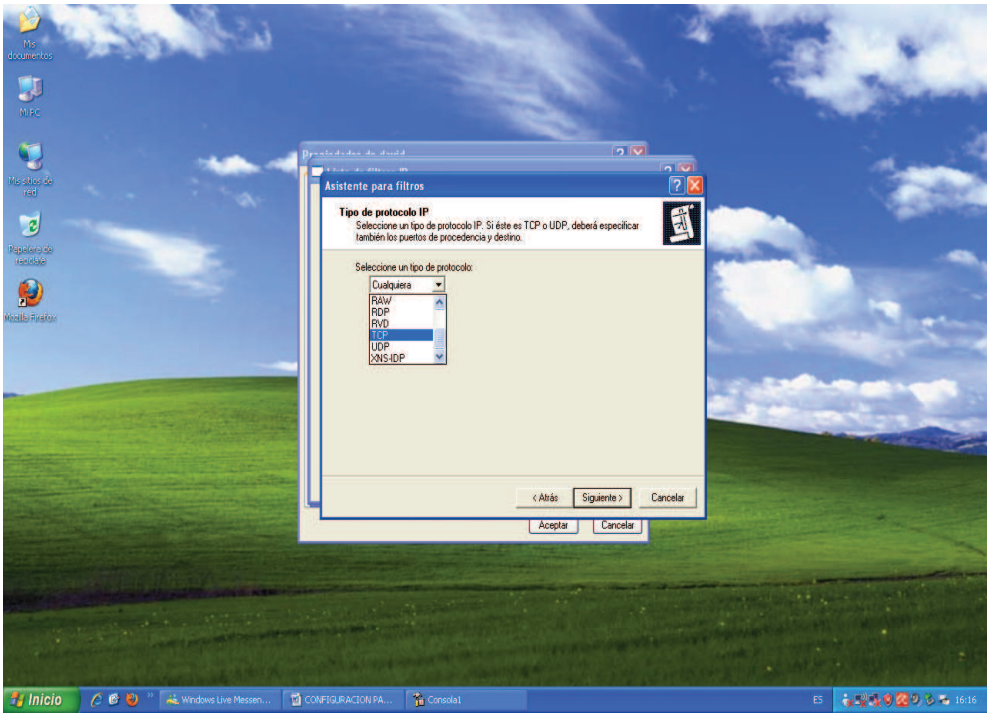
ANEXO 68

6. SELECCIONAMOS LA OPCIÓN A CUALQUIER DIRECCIÓN IP



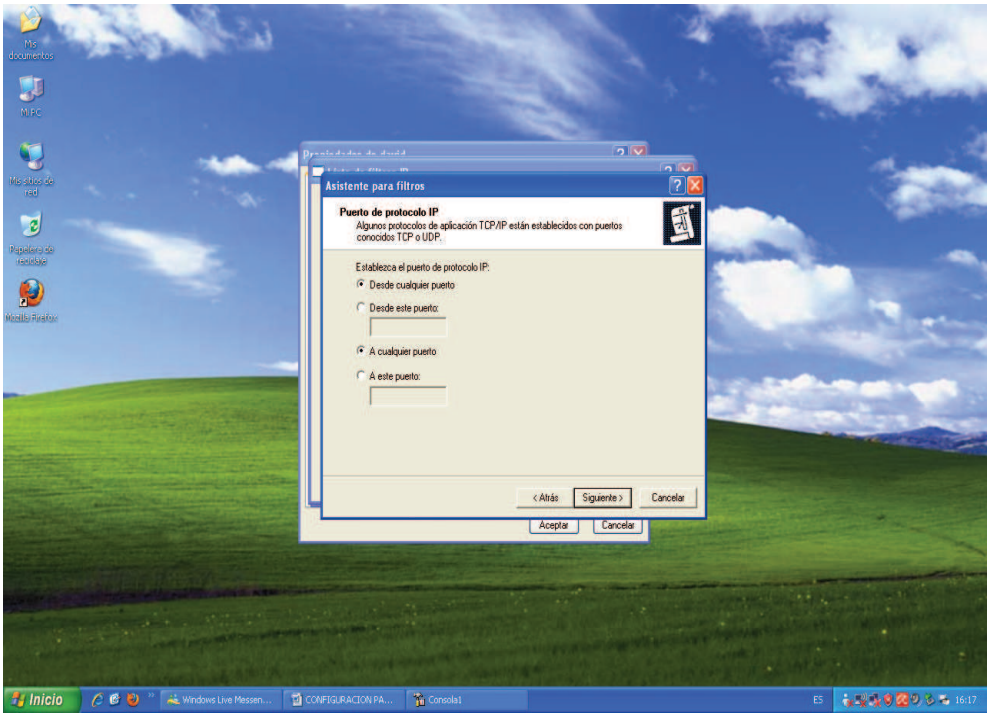
ANEXO 69

7. SELECCIONAMOS EL PROTOCOLO TCP



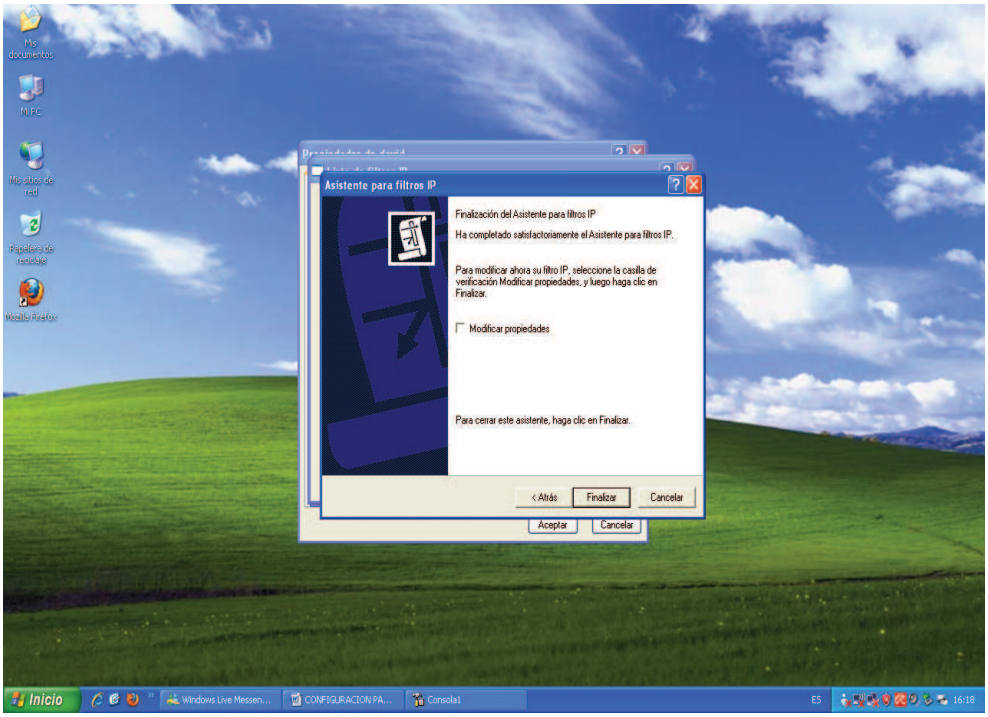
ANEXO 70

8. DEJAMOS LOS VALORES POR DEFECTO



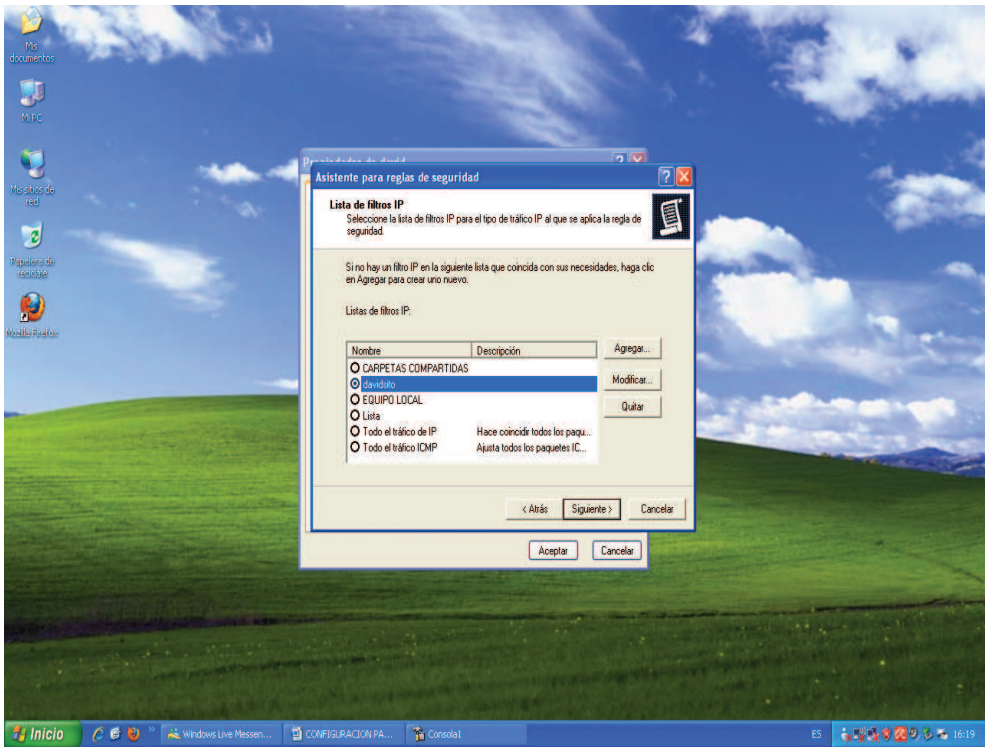
ANEXO 71

9. FINALIZAR Y ACEPTAR



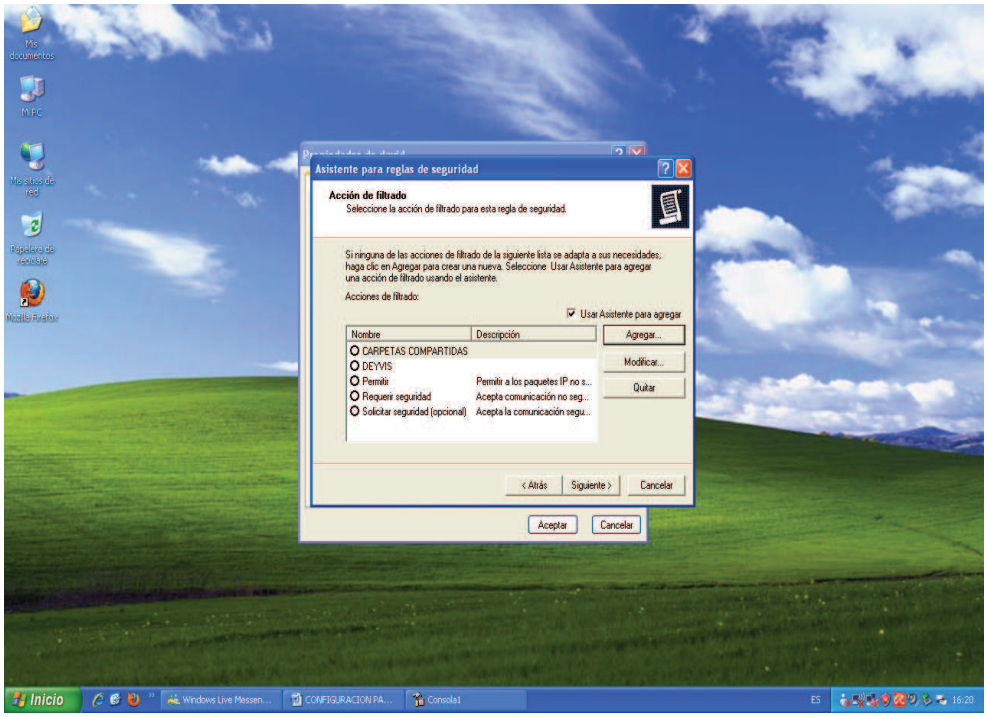
ANEXO 72

10. SELECCIONO MI LIOSTA DE FILTROS CREADA



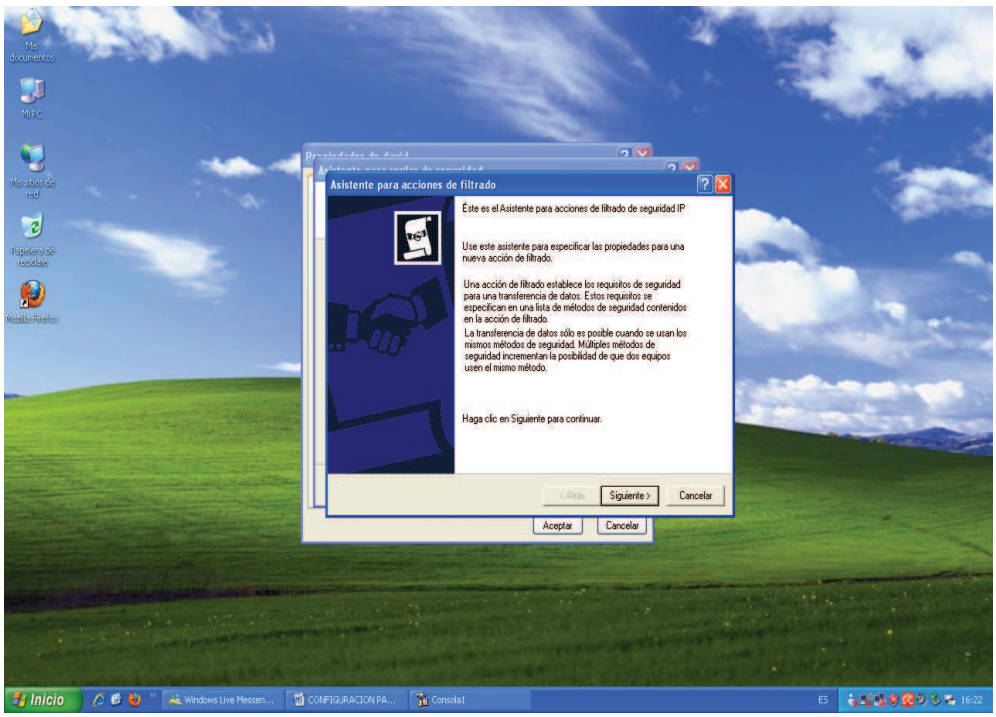
ANEXO 73

11. AGREGAR



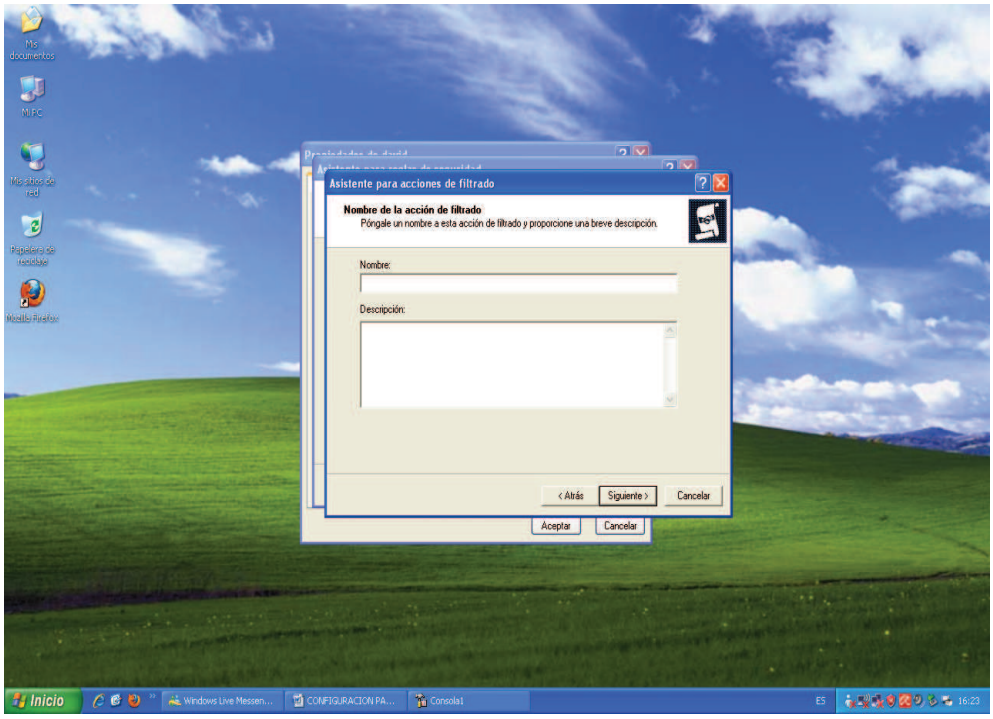
ANEXO 74

12. SIGUIENTE



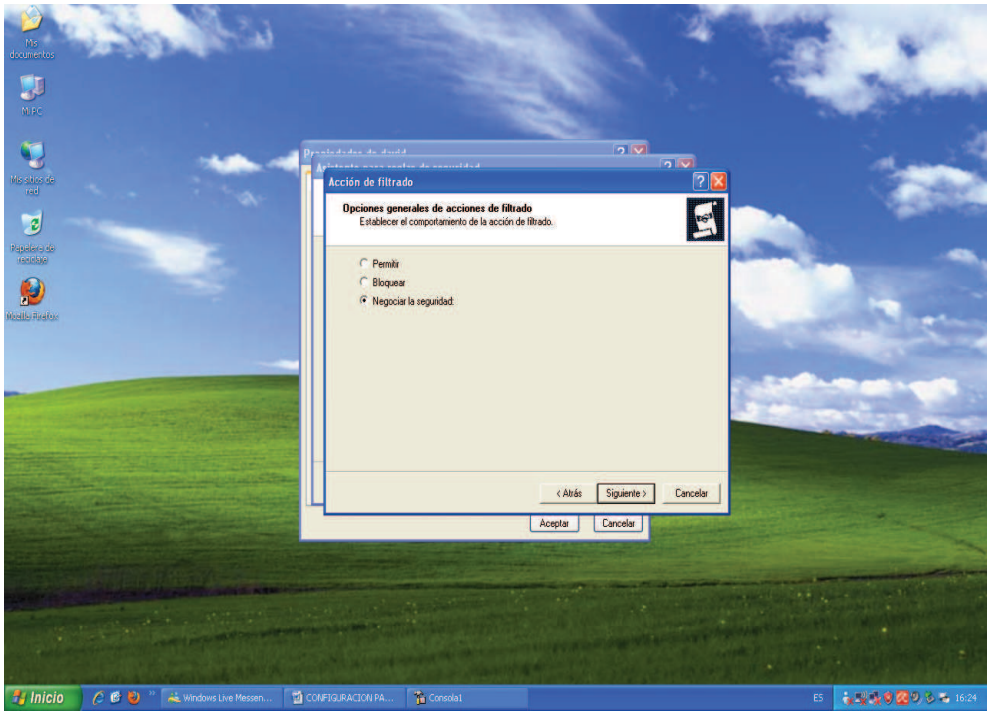
ANEXO 75

13. DAMOS UN NOMBRE A NUESTRA ACCION DE FILTRADO



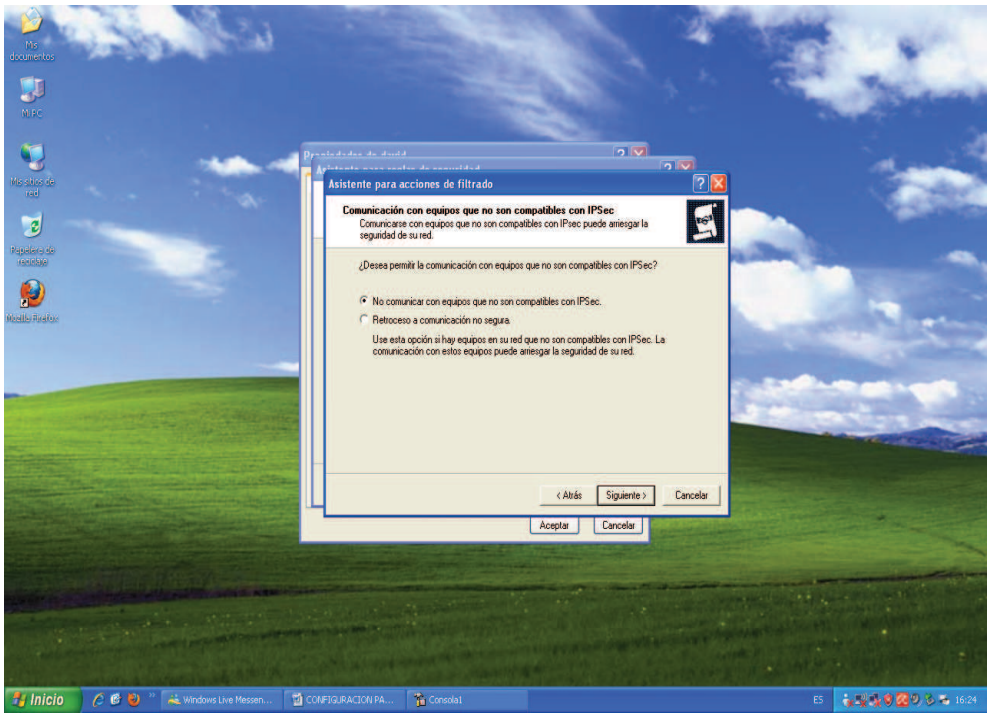
ANEXO 76

14. SELECCIONAMOS LA OPCION NEGOCIAR LA SEGURIDAD



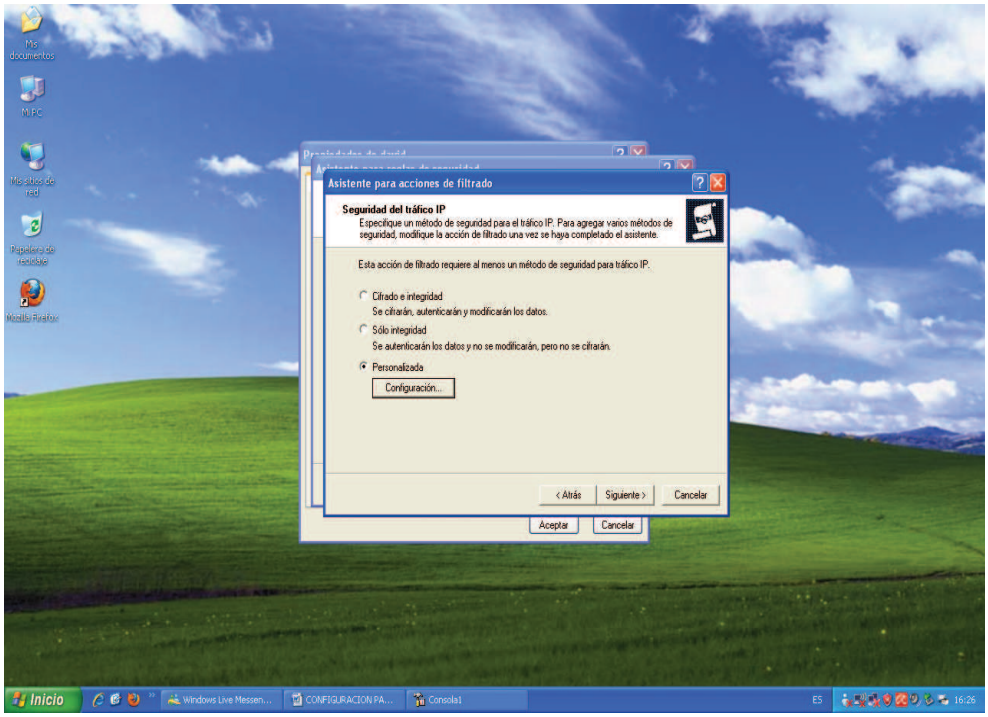
ANEXO 77

15. ELEGIMOS LA PRIMERA OPCIÓN



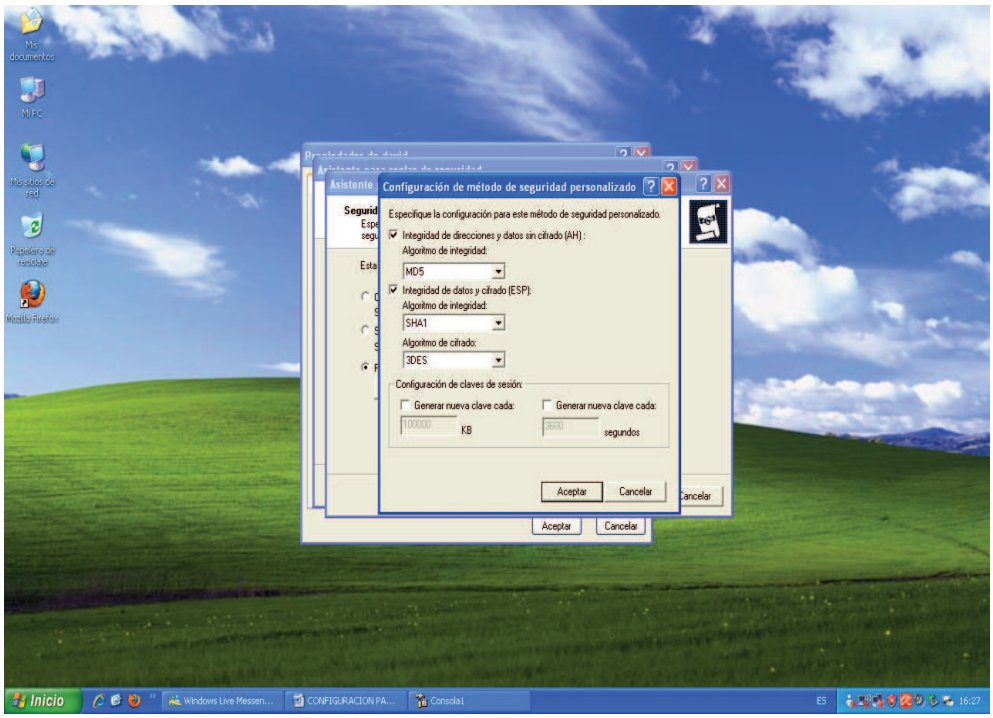
ANEXO 78

16. SELECCIONAMOS LA ULTIMA OPCION Y CONFIGURAMOS



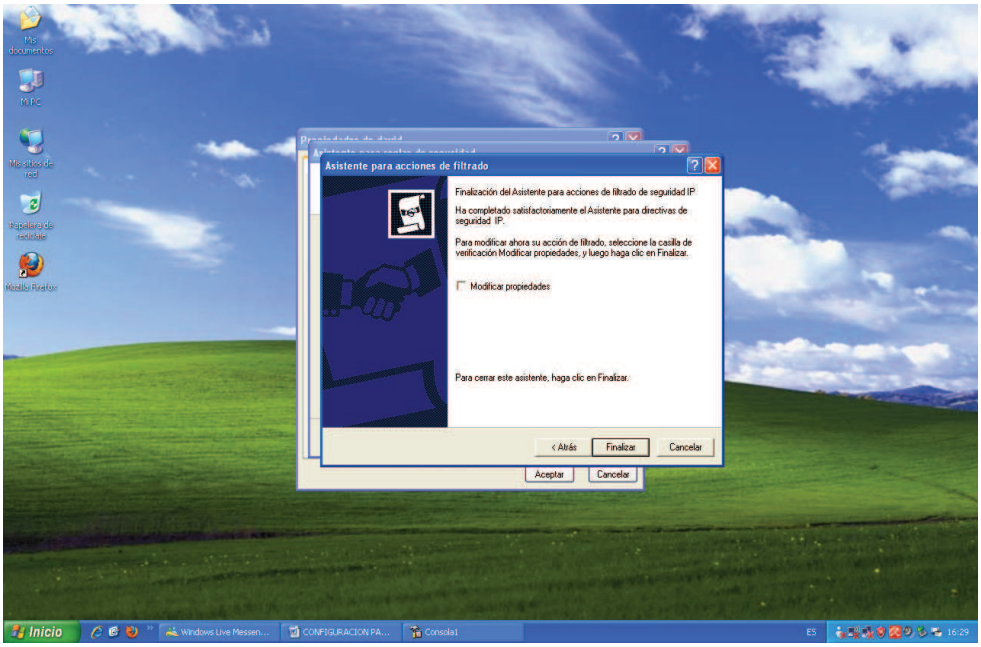
ANEXO 79

17. AVILITAMOS LA PRIMERA OPCIÓN Y ELEGIMOS MD5 Y LAS DEMÁS POR DEFECTO Y ACEPTAR



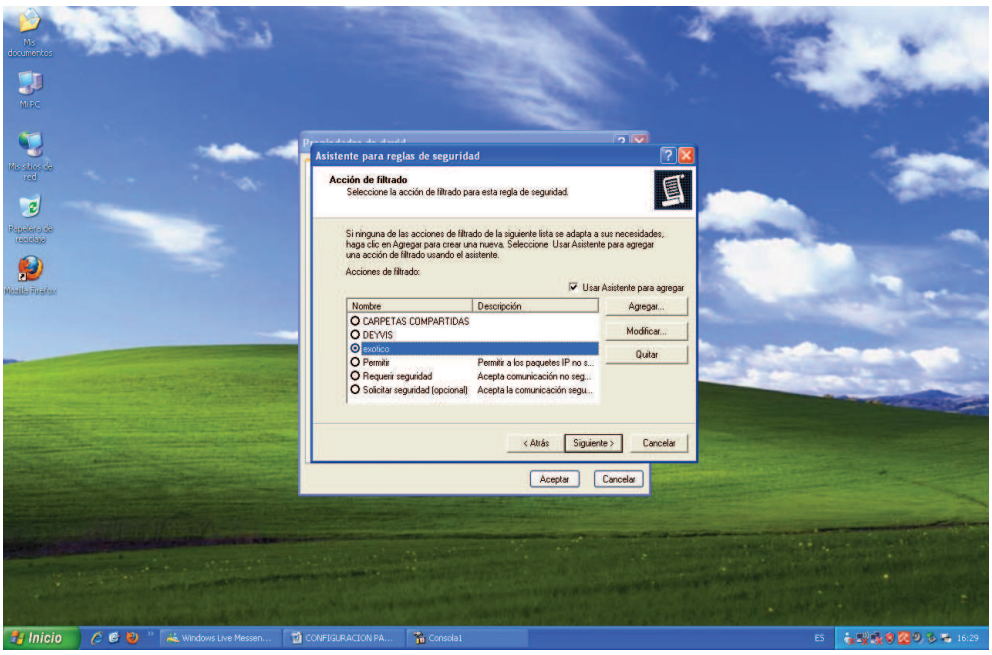
ANEXO 80

18. FINALIZAR



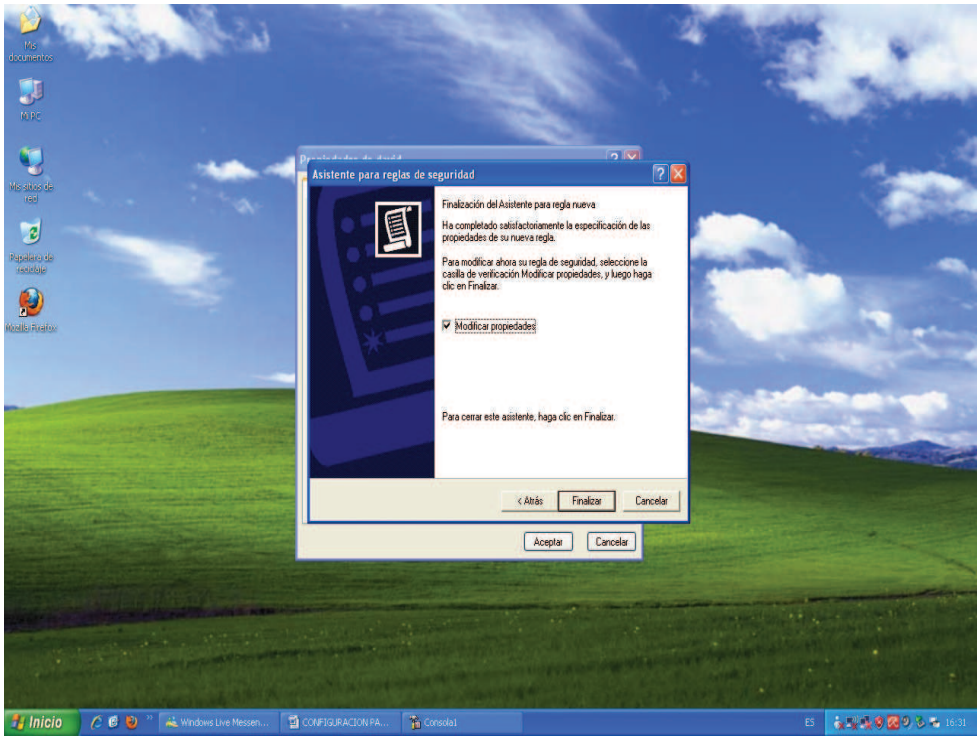
ANEXO 81

19. SELECCIONAMOS LA ACCION DE FILTRADO QUE ACABAMOS DE CREAR Y SIGUIENTE



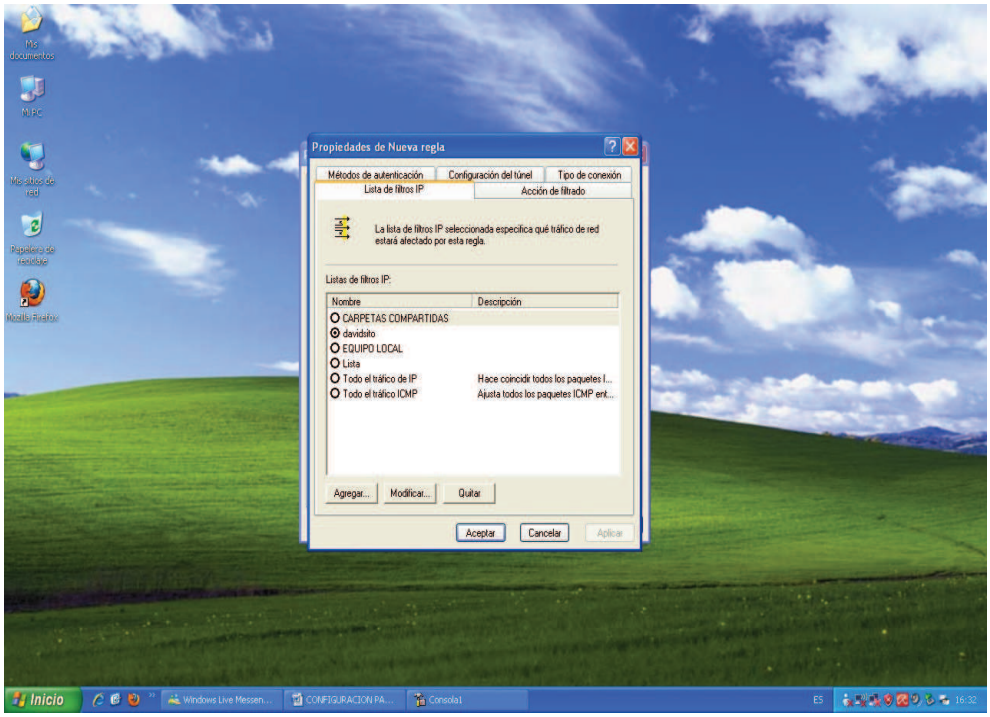
ANEXO 82

20. FINALIZAR



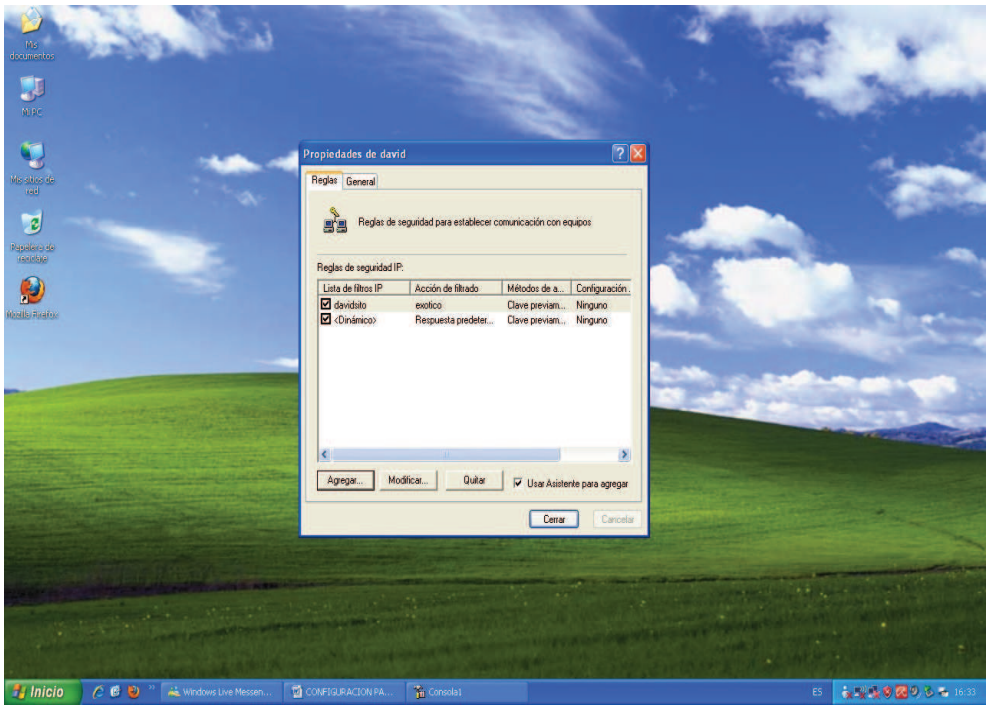
ANEXO 83

21. ACEPTAR



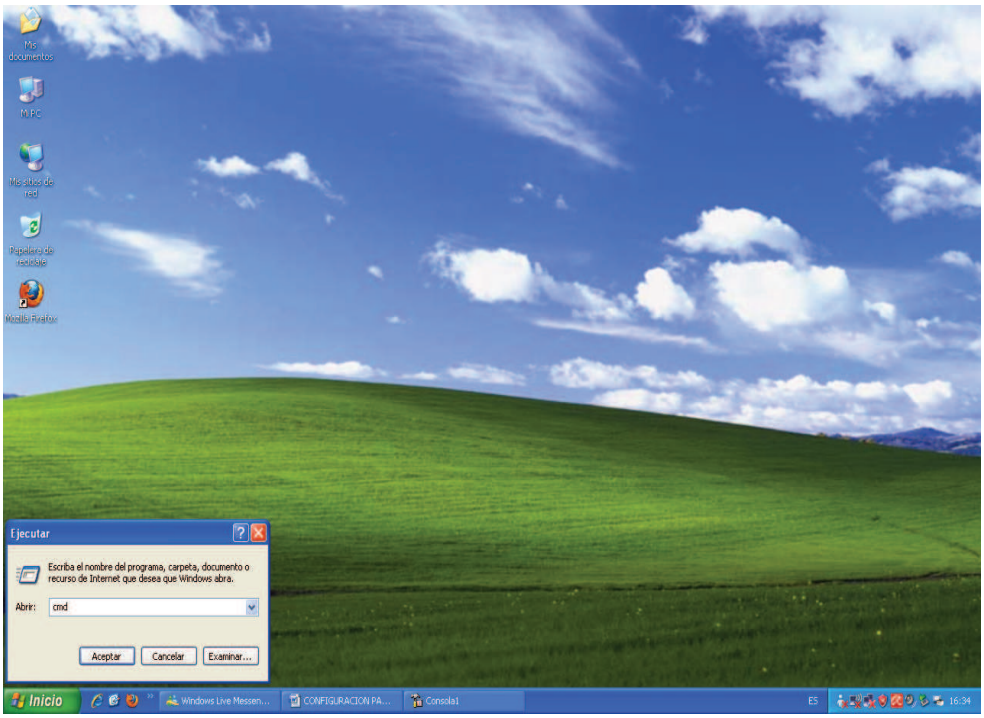
ANEXO 84

22. CERRAR



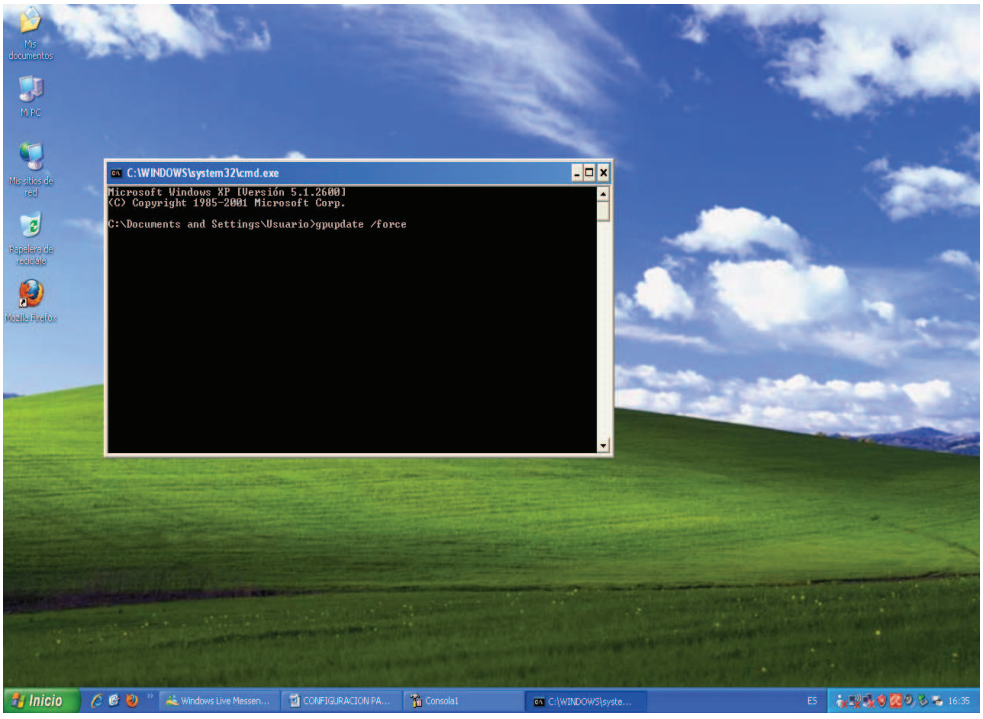
ANEXO 85

23. INICIO, EJECTAR Y DIGITAMOS CMD



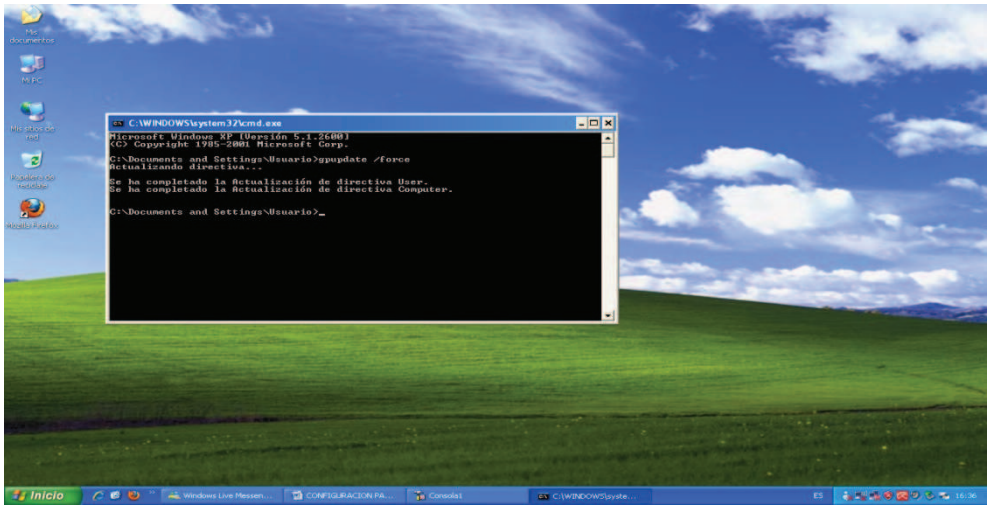
ANEXO 86

24. DIGITAMOS gpupdate/ force



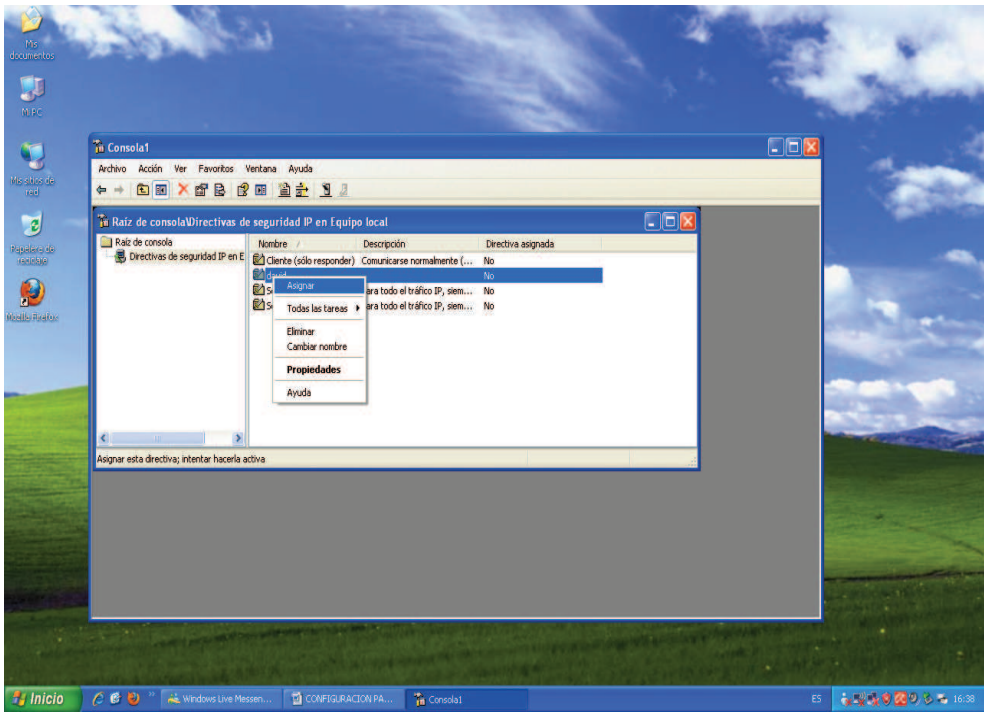
ANEXO 87

25. OPTENDREMOS UN MENSAJE DE: SE HA COMPLETADO LA ACTUALIZACIÓN DE DIRECTIVA



ANEXO 88

26. EN NUESTRA CONSOLA APARECE EL NOMBRE DE LA SEGURIDAD QUE CREAMOS, DAMOS CLICK DERECHO Y ASIGNAR



NUESTRA CONFIGURACIÓN YA TIENE ENLACE CON EL SERVIDOR.