PROTOTIPO DE IMPLEMENTACION NAP – DHCP EN UNA RED WINDOWS

JUAN CARLOS RAMIREZ

DANIEL SANTA OSPINA

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO

FACULTAD DE INGENIERÍAS

TECNOLOGÍA EN GESTIÓN DE REDES

ENVIGADO

2012

PROTOTIPO DE IMPLEMENTACION NAP – DHCP EN UNA RED WINDOWS

JUAN CARLOS RAMIREZ

DANIEL SANTA OSPINA

Trabajo presentado como requisito para el cuarto semestre de la Tecnología en Gestión de Redes

Asesores

Ing. Marta Lucia Hernández Ángel

Ing. Héctor Fernando Vargas Montoya

Ing. Diego Alexander Duque Marín

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO

FACULTAD DE INGENIERÍAS

TECNOLOGÍA EN GESTIÓN DE REDES

ENVIGADO

2012

RESUMEN

En la realización de este proyecto se implementa un servidor Windows 2008 junto con la característica NAP, la cual brinda una plataforma de control de acceso y protección a la red a través de políticas de estado de salud de las máquinas cliente que van desde poseer un firewall activado, un antivirus y antispyware instalado y actualizado hasta tener activo los servicios de Windows Update. NAP involucra varios métodos de cumplimiento, para este proyecto se hizo uso del método DHCP el cual a través de controles NAP brinda diferentes parámetros de red según sea el estado del equipo cliente: Acceso total, restringido o simplemente no compatible con NAP y por ende sin acceso a la red.

Luego de analizar los requerimientos para el funcionamiento del servidor se instalan máquinas virtuales en un computador con todos los servicios para la puesta en marcha del servidor NAP y también se instala una máquina virtual Windows 7 que sirve para realizar las pruebas de funcionamiento.

Luego de realizadas todas las configuraciones requeridas para NAP se realizan pruebas de conectividad entre maquinas, se comprueba el funcionamiento de NAP en DHCP activando y desactivando el Firewall de Windows y comprobando los diferentes estados del cliente Windows 7.

ABSTRAC

In this project implement Windows 2008 server with the feature NAP, which provides a platform for access control and network protection through policies of health status of client machines that go from having a firewall on, an antivirus and antispyware installed and updated until have active Windows Update services. Network Access Protection involves various methods of compliance for this project was done using the DHCP method which controls through provides different network parameters depending on the client machine status: Full Access, restricted or simply not compatible with and therefore no network access.

After analyzing the requirements for the server running virtual machines install in a computer with all the services for the correct implementation of the server NAP and also installs a virtual machine Windows 7 that serves to perform functional tests.

Then were made all the required settings for NAP, was done connectivity tests between machines, checking the performance of NAP in DHCP enabling and disabling the firewall and checking the different states of Windows 7 client.

TABLA DE CONTENIDO

1. INTRODUCCIÓN 9
2. PLANTEAMIENTO DEL PROBLEMA 10
3. OBJETIVOS 11
3.1. GENERAL 11
3.2. ESPECIFICOS 11
4. JUSTIFICACION 12
5. MARCO TEORICO 13
6. DISEÑO METODOLOGICO 25
6.1. TIPO DE INVESTIGACION 25
6.2. PROCESO 25
7. IMPLEMENTACION 26
7.1. ANTECEDENTES 26
7.2. MONTAJE 26
8. PRESUPUESTO 80
8.1. Equipos y software 80
8.2. Costos de personal 80
CONCLUSIONES Y RECOMENDACIONES 81
BIBLIOGRAFIA 82

LISTA DE FIGURAS

Figura 1 Administración de Unidades Organizativas 16
Figura 2 Un Dominio en Windows 17
Figura 3 Estructura gráfica de una base de datos DNS 18
Figura 4 Servidor DHCP 19
Figura 5 Componentes NAP 22
Figura 6 Instalar Ahora Windows 26
Figura 7 Términos de Licencia 27
Figura 8 Versión a Instalar 27
Figura 9 Tipo de Instalación 28
Figura 10 Progreso de la Instalación de Windows Server 28
Figura 11 Primera Contraseña de Administrador 29
Figura 12 Primer Inicio de Sesión 29
Figura 13 Administrador del Servidor 30
Figura 14 Comprobando Instalador de Active Directory 30
Figura 15 Instalación AD DS 31
Figura 16 Compatibilidad del sistema operativo 31
Figura 17 Configuración de Implementación 32
Figura 18 Nombre del Dominio 32
Figura 19 Selección de Servicios 33
Figura 20 Introducción DHCP 33
Figura 21 Enlaces de conexión de red 34
Figura 22 Configuración servidor DHCP 34
Figura 23 Ámbito DHCP 35
Figura 24 Resumen de instalación DHCP 35
Figura 25 Progreso Instalación DHCP 36
Figura 26 Selección Servicios NPS 36
Figura 27 Introducción a NPS 37
Figura 28 Progreso instalación NPS 37
Figura 29 Primer inicio NPS 38
Figura 30 Unión al dominio 38
Figura 31 Usuario Valido en el Dominio 39
Figura 32 Acceso Correcto al dominio 39
Figura 33 Directiva NAP 40
Figura 34 Agente NAP 40
Figura 35 Cliente de Cumplimiento DHCP 41
Figura 36 Centro de Seguridad 41
Figura 37 Prohibir Configuración TCP / IP 42
Figura 38 Creación de usuario 1 42

Figura 39 Creación de usuario 2 43
Figura 40 Grupo de seguridad NAP 43
Figura 41 Método NAP 44
Figura 42 Servidores de Cumplimiento 44
Figura 43 Ámbito DHCP en el NPS 45
Figura 44 Configurar Grupo 45
Figura 45 Selección grupo NAP 46
Figura 46 Servidores de remediación 46
Figura 47 Directivas de mantenimiento 47
Figura 48 Resumen de configuración NAP en NPS 47
Figura 49 Validador de mantenimiento 48
Figura 50 Configuración de Validador de mantenimiento 48
Figura 51 Requisitos para equipos cliente 49
Figura 52 Propiedades ámbito DHCP 49
Figura 53 Ámbito DHCP para NAP 50
Figura 54 Dominio Restringido 50
Figura 55 Estado del Agente NAP 51
Figura 56 Firewall activado - Windows Update Automático 51
Figura 57 Antivirus/Antispyware Instalado y Activado 52
Figura 58 Desactivación de MSE 52
Figura 59 Estado de riesgo del Equipo 53
Figura 60 Dominio restringido.proyecto.local 53
Figura 61 Acceso a la red limitado 54
Figura 62 Activación de Seccurity Essentials 54
Figura 63 Acceso completo a la red 55
Figura 64 Dominio proyecto.local 55
Figura 65 Preparando Instalación de Actualizaciones 56
Figura 66 Actualizaciones Disponibles 56
Figura 67 Configurando Actualizaciones 57
Figura 68 Windows esta Actualizado 57
Figura 69 Instalar Actualizaciones Automáticamente 58
Figura 70 Usuarios y Equipos de AD 58
Figura 71 OU Administradores 59
Figura 72 OU Gerencia 59
Figura 73 OU Equipos NAP 60
Figura 74 OU Presidencia 60
Figura 75 OU Sistemas 61
Figura 76 OU Mercadeo 61
Figura 77 OU Gestión Humana 62
Figura 78 Segmentación Por OU 62

Figura 79 GPO Prohibir propiedades de LAN 63
Figura 80 Propiedades de conexión LAN Prohibidas 63
Figura 81 Desactivación Cuenta Invitado 64
Figura 82 Deshabilitar COM+ 64
Figura 83 Deshabilitar RPC 65
Figura 84 Ejecutar regedit 65
Figura 85 Editor de registro 66
Figura 86 Servicio W32TIME 66
Figura 87 Tipo de servicio NTP 67
Figura 88 Annouce Flags NTP 67
Figura 89 Activar NTP 68
Figura 90 Dirección NTP Server 68
Figura 91 Special Poll Interval 69
Figura 92 Max Pos Phase Correction 69
Figura 93 Max Neg Phase Correction 70
Figura 94 Detención e iniciación de W32Time 70
Figura 95 Bloqueo puerto FTP datos 71
Figura 96 Bloqueo puerto FTP control 71
Figura 97 Bloqueo puerto Telnet 72
Figura 98 Visor de Eventos 72
Figura 99 Sucesos servicios instalados 73
Figura 100 Sucesos de Seguridad 73
Figura 101 Firewall de Windows 74
Figura 102 Excepciones en el Firewall 74
Figura 103 Firewall Activado 75
Figura 104 Administración Grupo Esquema 75
Figura 105 Administración Grupo del Dominio 76
Figura 106 Administración de Grupo Empresa 76
Figura 107 GPO Proteger con contraseña 77
Figura 108 Activación del protector de pantalla 77
Figura 109 Tiempo de espera para bloquear equipo 78
Figura 110 Cambio de Contraseña 78
Figura 111 Nueva contraseña de administrador 79

1. INTRODUCCIÓN

NAP (“Network Access Protection - Protección de acceso a la red”) es una característica de Windows Server 2008 utilizada para asegurar dominios basados en Windows, optimiza el nivel de protección de la red corporativa a través de políticas de salud y agentes software que monitorean el estado de los equipos cliente acorde a parámetros preestablecidos como lo son firewall habilitado, antivirus y antispyware instalado y actualización automática del sistema, para así permitir un acceso completo a la red interna o un acceso limitado en una red restringida hasta que todos los parámetros NAP sean cumplidos.

Se precisó de un computador con las características mínimas de hardware para soportar dos máquinas virtuales como lo son 4 GB de memoria RAM, un disco duro con espacio libre de al menos 40 GB y procesador de al menos 2,0 GHz. De igual manera fue necesario disponer de una copia del sistema operativo Windows Server 2008 en un medio óptico para la posterior instalación.

Este trabajo se efectúa sobre la plataforma Windows Server 2008 en su edición estándar y con su primer paquete de servicios que proporciona mejoras en seguridad y desempeño, antes de haber instalado las características necesarias para NAP que requiere del Servidor de Directivas de Redes se activaron funciones básicas en el servidor tales como Directorio Activo, DNS y DHCP.

2. PLANTEAMIENTO DEL PROBLEMA

Actualmente las redes de compañías y otras entidades se han hecho muy difíciles de administrar e implementar medidas de protección contra código malicioso y conexiones no autorizadas, igualmente hay un aumento en dispositivos móviles y portables que crean mayor dificultad de administración en la red, además por su migración en diferentes entornos informáticos que van desde hogares, o sitios de acceso público, al momento de reconectasen a la red corporativa pueden ser causantes de riesgo.

Todas estas situaciones incrementan considerablemente las amenazas de seguridad como la propagación de malware, y la probabilidad de ataques o intrusiones entre otros, capaces de perjudicar en gran medida los sistemas informáticos de la organización.

Los administradores de TI realizan esfuerzos muy grandes para proteger las empresas, implementando firewalls para prevenir el acceso de intrusos a los servidores y estaciones de trabajo, mantienen activos los sistemas de actualización e instalan software antivirus y antispyware, para prevenir infecciones dentro de la empresa.

Un riesgo muy típico es que llegue un usuario con un computador portátil contenedor de código malicioso, además su antivirus no se encuentra actualizado o precisamente le hace falta una actualización de seguridad crítica. El equipo se conecta a la red ya sea de manera cableada o inalámbrica y el servidor DHCP hará una concesión de dirección IP. Casi automáticamente el virus o malware puede propagarse por todo el entorno de red.[1]

¿En la actualidad que medidas pueden tomar las compañías para proteger y controlar el acceso de los clientes en la red?

[1]Pablo Campos. NAP Con dhcp paso a paso. Disponible en: http://pacampos.wordpress.com/2008/02/06/nap-con-dhcp-paso-a-paso/ El 12/03/12

3. OBJETIVOS

3.1. GENERAL

Implementar el componente NAP de Windows Server 2008 a través de DHCP reforzando las políticas de seguridad y controlando el acceso a la red interna.

3.2. ESPECIFICOS

- Configurar el equipo Windows Server 2008 como servidor de directivas de redes y DHCP.
- Implantar políticas de seguridad y acceso a la red para equipos que se configuren a través del protocolo DHCP restringiendo el acceso a la red para toda máquina que no cumpla con las políticas establecidas
- Instalar sistemas operativos clientes de Windows que posean software de firewall para que simulen las maquinas conectadas a la red.
- Establecer una red restringida para que contenga las máquinas que no cumplan los parámetros de NAP.

4. JUSTIFICACION

Uno de los mayores retos de las empresas actuales es la cada vez mayor exposición de los dispositivos cliente a software malicioso, como virus y gusanos. Este software puede obtener acceso libre a sistemas desprotegidos o que se encuentran configurados incorrectamente y usar dichos sistemas como medio para propagarse a otros dispositivos de la red de la organización.

NAP ("Network Access Protection - Protección de acceso a la red") es una característica de Windows Server 2008 utilizada para asegurar dominios basados en Windows, optimizando el nivel de protección de la red corporativa y la información que se posee. Los administradores de IT pueden usar la plataforma NAP para proteger su red garantizando que los sistemas cliente mantengan actualizaciones de software y configuraciones de sistema adecuadas que les ayuden a protegerse del software malintencionado.

Con la implementación de NAP en Windows se permite establecer políticas de salud en la red para protección de las estaciones cliente, de esta forma se facilita a los administradores el monitoreo del estado de los clientes y se facilita el control de acceso a la red para que tanto los nuevos equipos como los ya pertenecientes siempre estén cumpliendo con las políticas definidas para la organización.

5. MARCO TEORICO

5.1. Conceptos de Servidores

- **Arquitectura Cliente/Servidor**[2]

Una arquitectura es un conjunto de reglas, definiciones, términos y modelos que se emplean para producir un producto. La arquitectura Cliente/Servidor agrupa conjuntos de elementos que efectúan procesos distribuidos y computo cooperativo.

Entre los grandes beneficios de esta arquitectura esta el mejor aprovechamiento de la potencia de cómputo pues se reparte el trabajo, se reduce el tráfico en la red, se opera bajo sistemas abiertos, se permite el uso de interfaces gráficas variadas y versátiles.

- **Cliente**

Conjunto de Software y Hardware que invoca los servicios de uno o varios servidores. Características: El Cliente oculta al Servidor y la Red. Detecta e intercepta peticiones de otras aplicaciones y puede redirigirlas. Dedicado a la cesión del usuario (Inicia…Termina).

El método más común por el que se solicitan los servicios es a través de RPC (Remote Procedure Calls). Funciones Comunes del Cliente: Mantener y procesar todo el dialogo con el usuario. Manejo de pantallas. Menús e interpretación de comandos. Entrada de datos y validación. Procesamiento de ayudas. Recuperación de errores.

- **Servidor**

Conjunto de Hardware y Software que responde a los requerimientos de un cliente, Algunos tipos comunes de servidores: Servidor de Archivos, Servidor de Bases de Datos, Servidor de Impresión, Servidor de transferencia de archivos. Servidor de Aplicaciones.

Algunas funciones comunes de servidor son: Acceso, almacenamiento y organización de datos, actualización de datos almacenados, administración de recursos compartidos, ejecución de toda la lógica para procesar una transacción.

[2] Juansa. Introducción a redes, Arquitectura Cliente/Servidor. Disponible en: http://www.juansa.net/Admin2003/cliser.htm El 08/05/12

- **VirtualBox**[3]

VirtualBox es un poderoso producto de virtualización para arquitecturas x86 y AMD64/Intel64 para uso empresarial como en el hogar. Es un producto de alto rendimiento usuarios empresariales, este es también la única solución profesional disponible como Open Source bajo los términos de licencia de GNU General Public License (GPL) versión 2.

Actualmente, VirtualBox corre en host Windows, Linux, Macintosh, y Solaris y soporta también un largo numero de sistemas operativos guest incluyendo aunque no limitado a Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7), DOS/Windows 3.x, Linux (2.4 y 2.6), Solaris y OpenSolaris, OS/2, y OpenBSD.

VirtualBox está siendo desarrollado activamente con lanzamientos frecuentes y tiene una lista creciente de características, con el apoyo de sistemas operativos invitados y las plataformas que puede correr. VirtualBox es un esfuerzo de la comunidad respaldada por una empresa dedicada: todo el mundo está invitado a aportar mientras que Oracle asegura que el producto siempre cumple con los criterios de calidad profesional.

- **Microsoft Windows Server 2008**[4]

Windows Server 2008 es el nombre de un sistema operativo de Microsoft diseñado para servidor. Es el sucesor de Windows Server 2003. Se basa en el núcleo Windows NT 6.0. Posteriormente se lanzó una segunda versión, denominada Windows Server 2008 R2.

Está diseñado para ofrecer a las organizaciones la plataforma productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, "Windows Server 2008" incluye nuevas funciones de gran valor y eficacia además de mejoras impactantes en el sistema operativo base.

Fue conocido como Windows Server "Longhorn" hasta el 16 de mayo de 2007, cuando Bill Gates, presidente de Microsoft, anunció su título oficial (Windows Server 2008) usa la interfaz clásica de versiones anteriores de Windows. Su lanzamiento fue el 27 de febrero de 2008.

[3] Oracle. VirtualBox. Disponible en: https://www.virtualbox.org/ El 14/05/12
[4] Microsoft. Introducción técnica a Windows Server 2008. Disponible en: http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx El 14/05/12

- **Active Directory**[5]

El directorio activo es una manera de manejar todos los elementos de una red, incluidos ordenadores, grupos, usuarios, dominios, políticas de seguridad, y cualquier tipo de objetos definidos para el usuario Además de esto, provee de funciones adicionales más allá de estas herramientas y servicios

El directorio activo está construido alrededor de la tecnología DNS y LDAP, los clientes de directorio activo usan DNS y LDAP para localizar y acceder a cualquier tipo recurso de la red. Al ser protocolos de plataforma independiente, Los ordenadores Unix, Linux y Macintosh pueden tener acceso a los recursos de igual modo que los clientes de Windows.

La consola MMC (Microsoft Management Console*)* se usa para implementar y gestionar el directorio activo. Las metas de directorio activo tienen dos acercamientos importantes. La estructura de directorio activo tiene una forma jerárquica donde se localizan los objetos. Estos objetos caen en tres tipos de categorías:

- Un objeto es únicamente identificado por su nombre y tiene una serie de atributos definidos por un esquema, que también determina la clase de objetos que se pueden almacenar en el directorio. Los atributos son las características y la información que el objeto contiene.

- Cada atributo del objeto puede ser usado en diferentes clases de objetos dentro del esquema del objeto. Dicho esquema existe para que se pueda hacer modificaciones o extensiones cuando sea necesario. Hay que tener cuidado al cambiar estos atributos una vez que estén creados, ya que se puede cambiar la estructura ya creada del directorio activo, por lo que hay que hacerlo de un modo planeado.

- El dominio se observa desde un número de niveles. En la parte más alta se tiene el bosque – la colección de todos los objetos, sus atributos y reglas en el directorio activo. Los dominios se identifican por su nombre de estructura DNS. Un dominio tiene un solo nombre DNS.

[5] Ordenadores-y-Portátiles. ¿Qué es el *directorio activo* de Windows?. Disponible en: http://www.ordenadores.-y-portatiles.com/directorio-activo.html El 08/05/12

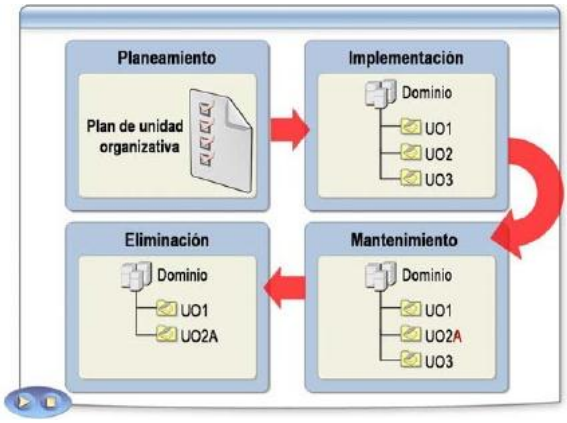
- **Organizational Unit**[6]

Los objetos dentro de un dominio pueden estar agrupados en contenedores llamados unidades organizacionales (OU). Estas unidades dan al dominio una jerarquía, facilita la administración y proporciona una imagen de la compañía en términos organizativos y geográficos.

Estas unidades organizacionales pueden contener a su vez otras unidades organizacionales. Normalmente, se suelen aplicar las políticas de grupo a nivel de OU, aunque también pueden ser aplicados a dominios. Se suelen dar poderes de administrador a estos OU y todo los que contienen por debajo, aunque también se pueden delegar funciones de administrador a objetos individuales o atributos. Ver figura 1

El directorio activo también soporta la creación de sitios, los cuales son grupos físicos más que lógicos, definidos por una o más subredes. Estos sitios son independientes del dominio y la estructura de OU, y son comunes por todo el bosque. Se utilizan para controlar el tráfico de red generado por replicación, y también para referir a los clientes al controlador de dominio más cercano.

Figura 1 Administración de Unidades Organizativas



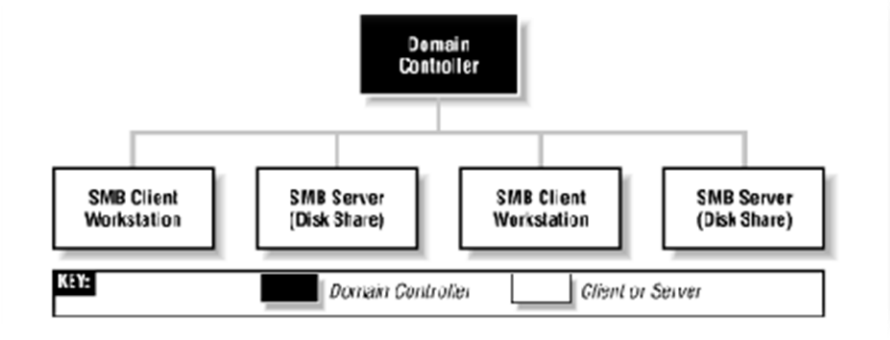
Fuente: Scrib. Implementación de la estructura de una unidad organizativa. Disponible en: http://es.scribd.com/doc/86009669/11-Implementacion-de-La-Estructura-de-Una-Unidad-Organizativa El 15/05/12

[6]Ordenadores-y-Portátiles. ¿Qué es el *directorio activo* de Windows?. Disponible en:http://www.ordenadores-y-portatiles.com/directorio-activo.html El 08/05/12

- **Dominio en Windows**[7]

Un grupo de trabajo es una colección de computadoras SMB, las cuales residen todas en la misma subred y se encuentran suscritas al mismo grupo SMB. Un Dominio Windows va un paso más allá. Es un grupo de trabajo de máquinas SMB que tienen una añadido: un servidor que actúa como controlador de dominio. Se debe tener un controlador de dominio para poder tener un dominio Windows. Por otra parte, se trata sólo de un grupo de trabajo. Ver la figura 2. Los dominios Windows son llamados "Dominios Windows NT" por Microsoft porque ellos asumen que serán máquinas Windows NT las que asuman el papel de controladoras de dominio.

Figura 2 Un Dominio en Windows



Fuente: Linux-cd. Dominio Windows. Disponible en: http://linux-cd.com.ar/manuales/usando-samba/node17.html El 08/05/12

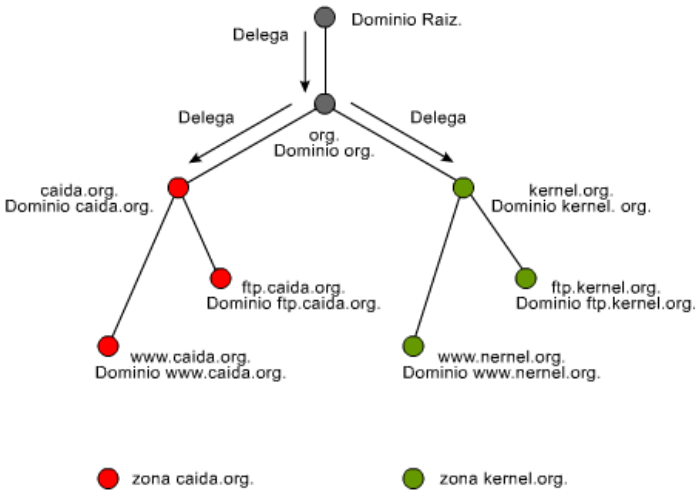
- **DNS**[8]

El DNS (*Domain Name Service*) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa. Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los humanos usen nombres de dominio que son más simples de recordar. El sistema de nombres de dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallos. Aunque parece muy difícil lograr todos esos objetivos, la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los sub-dominios.

[7] Linux-cd. Dominio Windows. Disponible en: http://linux-cd.com.ar/manuales/usando-samba/node17.html El 08/05/12
[8] José M. Piquer. El DNS. Disponible en: http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html El 08/05/12

En un nombre de dominio, la jerarquía se lee de derecha a izquierda. Para que exista una raíz del árbol y todos los dominios están bajo esa raíz. Cada componente del dominio (y también la raíz) tiene un servidor primario y varios servidores secundarios. Todos estos servidores tienen la misma autoridad para responder por ese dominio, pero el primario es el único con derecho para hacer modificaciones en él. Por ello, el primario tiene la copia maestra y los secundarios copian la información desde él. El servidor de nombres es un programa que típicamente es una versión de BIND (*Berkeley Internet Name Daemon*). La raíz del sistema de dominios es servida por algunos servidores ``bien conocidos''. Todo servidor de nombres debe ser configurado con la lista de los servidores raíz bien conocidos (en general lo vienen de fábrica). Estos servidores dicen qué dominios de primer nivel existen y cuáles son sus servidores de nombres. Ver figura 3.

Figura 3 Estructura gráfica de una base de datos DNS



Fuente: NewDevices. Protocolo DNS. Disponible en: http://www.newdevices.com/tutoriales/dns/images/1d.png El 15/05/12

- **DHCP**[9]

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración de red en forma dinámica, sin intervención particular. Sólo tiene que especificar al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

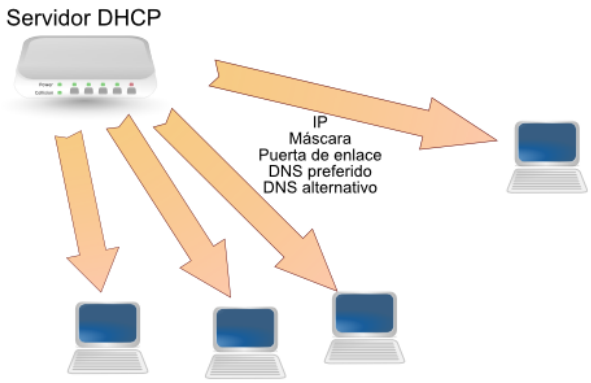
[9]IETF. RFC 2131. Disponible en: http://www.ietf.org/rfc/rfc2131.txt El 27/05/12

- ***Funcionamiento del protocolo DHCP***

Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP fija. El sistema básico de comunicación es BOOTP (con la trama UDP). Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en 255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local.

Cuando el DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión, sin olvidar que el cliente no tiene una dirección IP y, por lo tanto, no es posible conectarse directamente con él, el paquete contiene toda la información solicitada por el cliente. Ver figura 4

Figura 4 Servidor DHCP



Fuente: Juanlu991. Como crear un servidor dhcp. Disponible en: http://2.bp.blogspot.com/_xpi2MxMdjek/TUcAYWIYOeI/AAAAAAAAAFo/lxb9ExTwNO8/s1600/servidor-dhcp.png El 15/05/12

5.2. Conceptos De Seguridad

- **Firewall**[10]

Un cortafuegos o firewall, es un elemento de software o hardware utilizado en una red para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red.

Un firewall correctamente configurado es un sistema adecuado para tener una protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Su modo de funcionar es definido por la recomendación RFC 2979, la cual define las características de comportamiento y requerimientos de interoperabilidad. Protege de intrusiones: El acceso a los servidores en la red sólo se hace desde máquinas autorizadas.

Protección de información privada: Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

- **Antivirus**[11]

Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas peligrosos para los ordenadores llamados malware. Un antivirus compara el código de cada archivo con una BD de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus o la verificación contra virus en redes de computadores.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real.

---

[10] Miguel Ángel Álvarez. Que es un firewall. Disponible en: http://www.desarrolloweb.com/articulos/513.php El 17/05/12

[11] Definiciones ABC. Definición de antivirus. Disponible en: http://www.definicionabc.com/tecnologia/antivirus.php El 17/05/12

Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web.

Los virus, spyware, gusanos, son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen las características de ejecutar recursos, consumir memoria e incluso eliminar la información.

- **Servidor de directivas de redes**[12]

Servidor de directivas de redes (NPS) permite crear y aplicar directivas de acceso a la red en toda la organización con fines de mantenimiento de clientes, autenticación de solicitudes de conexión y autorización de solicitudes de conexión. NPS permite configurar y administrar de forma centralizada directivas de autenticación de acceso a la red, autorización y mantenimiento de clientes con las tres características siguientes:

RADIUS server. NPS realiza la autenticación, autorización y administración de conexiones de forma centralizada para los conmutadores de autenticación inalámbricos, conexiones de acceso remoto telefónico y red privada virtual (VPN).

RADIUS proxy. Cuando se usa NPS como un proxy RADIUS, puede configurarse las directivas de solicitud de conexión que indican al servidor NPS qué solicitudes de conexión debe renviar a otros servidores RADIUS y a qué servidores RADIUS desea renviar las solicitudes de conexión.

Network Access Protection (NAP) policy server. Cuando se configura NPS como un servidor de directivas de NAP, NPS evalúa los informes de mantenimiento (SoH) enviados por equipos cliente compatibles con NAP que desean conectarse a la red. NPS también actúa como un servidor RADIUS cuando está configurado con NAP, realizando tareas de autenticación y autorización para las solicitudes de conexión. Puede configurarse directivas y opciones de NAP en NPS, lo que incluye validadores de mantenimiento del sistema (SHV), directivas de mantenimiento.

- **Protección de Acceso a la Red (NAP)**[13]

La Protección de acceso a redes (NAP) es una de las características del sistema operativo Windows Server ® 2008. NAP es una nueva plataforma que permite a los administradores de red definir niveles de acceso a red en función de la

[12]Technet. Servidor de directivas de redes. Disponible en: http://technet.microsoft.com/es-es/library/cc732912.aspx El 09/05/12
[13] Technet. Introducción a NAP. Disponible en: http://technet.microsoft.com/es-es/library/dd759127.aspx El 10/03/12

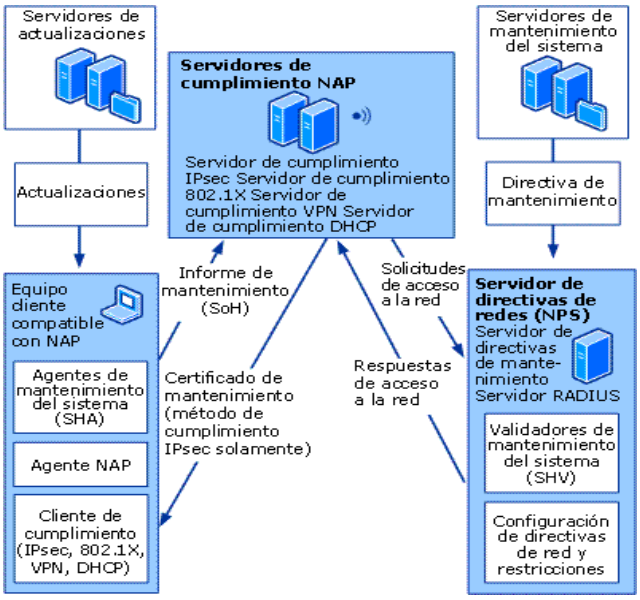
identidad del cliente, los grupos a los que pertenece el cliente y el grado de cumplimiento de la directiva de gobierno corporativo por parte del cliente.

Si un cliente no es compatible, NAP ofrece un mecanismo para hacer que el cliente sea compatible de forma automática (un proceso llamado corrección) y posteriormente aumentar su nivel de acceso a red. NAP es compatible con Windows®7, Windows Vista®, Windows® XP con Service Pack 3, Windows Server2008 y WindowsServer®2008R2.

- ***Componentes NAP***

NAP incluye varios componentes de cliente y servidor. Existen componentes NAP comunes que se usan en todas las implementaciones NAP y existen componentes que se usan sólo para implementaciones específicas, según el método o los métodos de cumplimiento NAP que seleccione. Ver figura 5.

Figura 5 Componentes NAP



Technet. Protección de Acceso a redes. Disponible en: http://i.technet.microsoft.com/dynimg/IC233149.gif El 17/05/12

Entre los métodos de cumplimiento NAP se incluye el protocolo DHCP. Los componentes NAP comunes son componentes de cliente y servidor que se usan en todos los métodos de cumplimiento NAP.

- **Informe de mantenimiento (SoH)**

Componente cliente, es una declaración sobre el estado de mantenimiento del equipo cliente. Los agentes de mantenimiento del sistema (SHA) crean informes

de mantenimiento (SoH) y los envían al Validador de mantenimiento del sistema (SHV) correspondiente de un servidor NPS.

- ***Agente de mantenimiento del sistema (SHA)***

Un componente cliente que comprueba el estado del equipo para determinar si las opciones que supervisa están actualizadas y configuradas correctamente. Por ejemplo, el Agente de mantenimiento de seguridad de Windows (WSHA) puede supervisar Firewall de Windows si se ha instalado, habilitado al igual que software antivirus y antispyware o si el servicio Microsoft Update está habilitado.

- ***Agente NAP***

Un servicio del sistema cliente que recopila y administra información de mantenimiento. Procesa informes de mantenimiento de diversos agentes de mantenimiento del sistema y envía el mantenimiento del cliente al servidor de administración de NAP.

- ***Cliente de cumplimiento***

Software cliente que se integra con tecnologías de acceso a la red, como DHCP, VPN e IPsec. Para usar NAP, se debe instalar y habilitar al menos un cliente de cumplimiento NAP en los equipos cliente. Un cliente de cumplimiento NAP solicita el acceso a una red, comunica el estado de mantenimiento de un equipo cliente al servidor NAP que autoriza el acceso a la red, como el servidor NPS, y comunica el estado restringido del equipo cliente a otros componentes de la arquitectura de cliente de NAP.

- ***Validadores de mantenimiento del sistema (SHV)***

El software de servidor tiene los agentes de mantenimiento del sistema correspondientes. Cada agente de mantenimiento del sistema (SHA) tiene el Validador de mantenimiento del sistema (SHV) correspondiente en NPS. NPS usa SHV para comprobar el informe de mantenimiento que realiza el SHA correspondiente en el equipo cliente.

Además, el SHV puede detectar que no se ha recibido ningún informe de mantenimiento (por ejemplo, si nunca se ha instalado el SHA o si se ha dañado o eliminado). Si el informe de mantenimiento no cumple la directiva definida, el SHV envía un mensaje con una respuesta al informe de mantenimiento (SoHR) al SHA.
Una red puede tener más de un tipo de SHV. En este caso, el servidor NPS debe coordinar la salida de todos los SHV y determinar si se limita el acceso de un equipo que no cumple requisitos. Esto precisa un cuidadoso planeamiento a la hora de definir directivas de mantenimiento para el entorno y una evaluación sobre cómo interactúan los distintos SHV.

- ***Directivas de mantenimiento***

Reglas creadas mediante la configuración de SHV individuales para agregarlas a una directiva de mantenimiento y, a continuación, configurar las condiciones de la directiva. NPS implementa y aplica las directivas de mantenimiento cuando se agregan a la configuración de una directiva de red.

- ***Respuesta al informe de mantenimiento (SoHR)***

Es la validación de un informe de mantenimiento (SoH). Si el equipo cliente no cumple los requisitos, la SoHR contiene instrucciones de actualizaciones que los SHA del cliente usan para que la configuración del equipo cliente cumpla con la directiva de mantenimiento.

Cada tipo de SoH almacena diferentes tipos de información acerca del estado de mantenimiento del sistema y los mensajes de SoHR almacenan diferentes tipos de información acerca del procedimiento para cumplir con los requisitos de las directivas de mantenimiento que se configuran en NPS.

6. DISEÑO METODOLOGICO

6.1. TIPO DE INVESTIGACION - INVESTIGACION EXPLORATORIA[14]

Explorar significa incursionar en un territorio desconocido. Se emprende en una investigación exploratoria cuando no se conoce el tema por investigar, o cuando el conocimiento es tan indeterminado e impreciso que imposibilita conseguir siquiera provisionalmente conclusiones sobre qué aspectos son relevantes y cuáles no.

En este proyecto es obligatoria una investigación exploratoria pues en un principio quienes lo llevan a cabo desconocen por completo todos los conceptos en que se basa la plataforma NAP, como se debe implementar, que requiere para su correcto funcionamiento; todas estas son interrogantes y por lo tanto es muy necesario el proceso de explorar para que posteriormente se distinga todo aquello que involucra la protección de acceso a la red a través de NAP.

6.2. PROCESO

Se investiga cuales eran los requisitos para ofrecer una plataforma NAP que auditaría el acceso a la red de los equipos cliente y validar su estado según aspectos de seguridad como firewall y antivirus, inicialmente se instaló el sistema operativo Windows Server 2008, al igual que Windows 7. Se hizo uso de maquinas virtuales, el servidor Windows 2008 se promovió a controlador de dominio, se configuraron directivas de grupo para que la activación del agente NAP, el centro de seguridad y el cliente de cumplimiento DHCP en los equipos clientes fuera automático, el servidor también incorpora los roles de DHCP y NPS, posteriormente se lleva a cabo la configuración en cada uno de estos para el correcto funcionamiento de NAP.

Se crea el grupo de seguridad NAP en el Active Directory, se agrega como miembro de ese grupo la cuenta de maquina del cliente Windows 7, sobre el cual se hacen las pruebas de funcionamiento. Se configura un filtrado para que las GPO solo se apliquen a los equipos que pertenezcan al grupo antes creado.

La configuración en el servidor NPS es casi automática pues se presentan las opciones de correr un asistente que genera las configuraciones deseadas para el método de cumplimiento DCHP.

Pro ultimo se realizan pruebas para comprobar el comportamiento de la red si el equipo cliente tiene el Firewall de Windows habilitado, anti virus y spyware instalado y las actualizaciones automáticas de Windows Update.

---

[14] Felipe Nieves Cruz. La Investigación Exploratoria. Disponible en: http://www.gestiopolis.com/canales7/mkt/investigacion-exploratoria-y-algunos-aportes-a-la-investigacion-de-mercados.htm El 27/05/12

7. IMPLEMENTACION

7.1. ANTECEDENTES

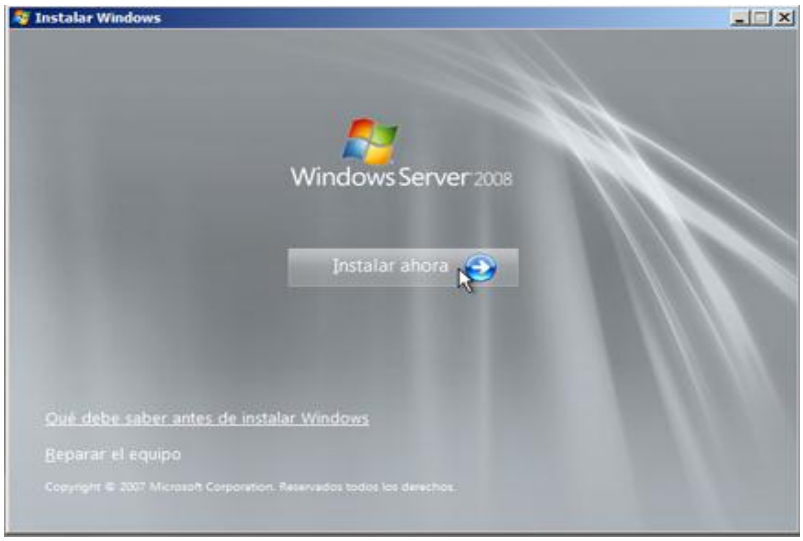
Se cuenta con una máquina de 4 Gigabytes de memoria RAM, disco duro de 250 Gigabytes, procesador AMD Athlon Dual Core de 2,2 GigaHertz, tarjeta grafica ATI Radeon HD 3200, características requeridas para soportar dos maquinas virtuales, tenia ya instalado un sistema operativo Windows 7 Ultimate de 32 bits, el cual funcionará sistema operativo anfitrión para las otras maquinas, era necesario instalar un software de virtualización en este caso será VirtualBox.

7.2. MONTAJE

7.2.1. Instalación de Windows Server 2008 Estándar

En las figuras 6 a la 13 se evidencia el proceso de instalación del sistema operativo Windows server 2008.

Figura 6 Instalar Ahora Windows

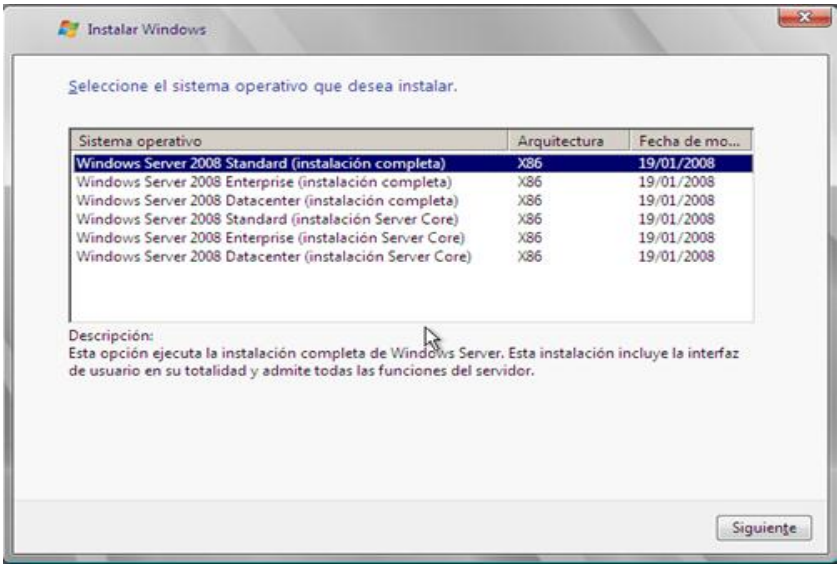


Insertar disco de instalación y luego esperar el arranque del proceso de instalación.

Figura 7 Términos de Licencia

Aceptar los términos de licencia de Windows y continuar con la instalación.

Figura 8 Versión a Instalar



Seleccionar la versión de Windows server que se acomode mas a los requerimientos y servicios a montar

Figura 9 Tipo de Instalación

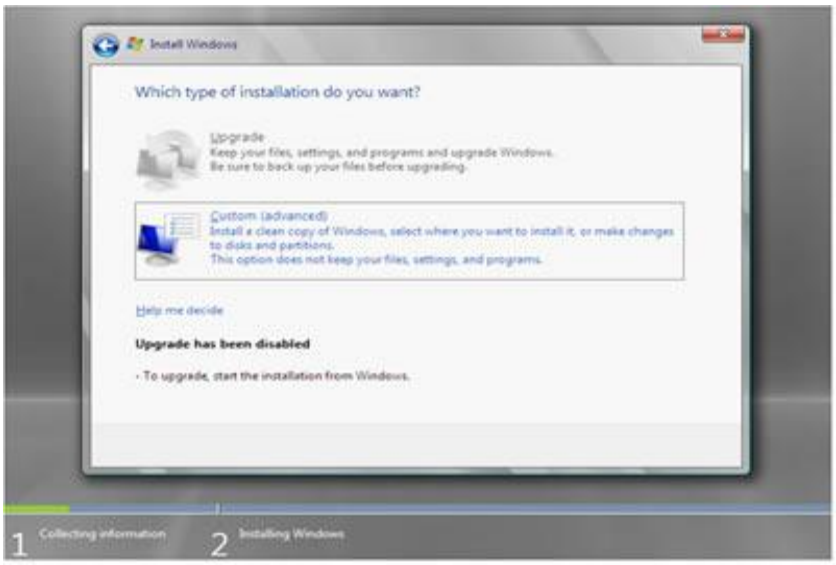


Figura 10 Progreso de la Instalación de Windows Server

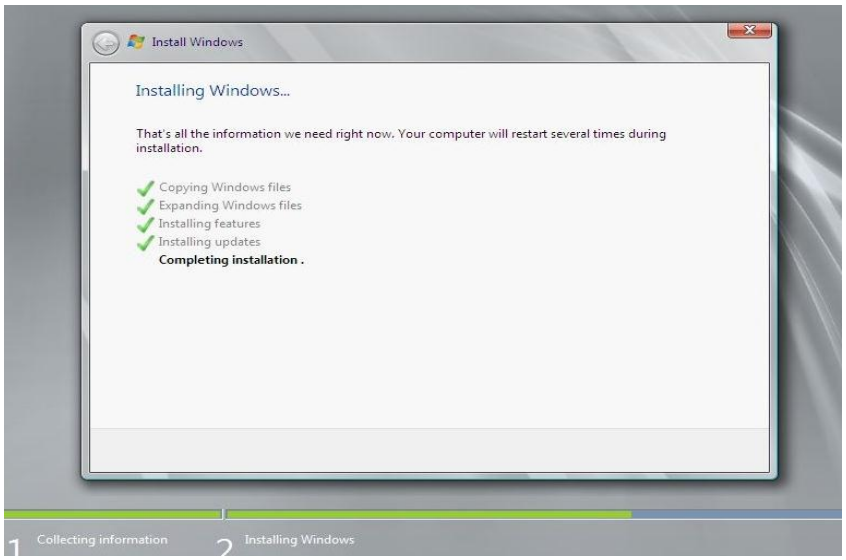
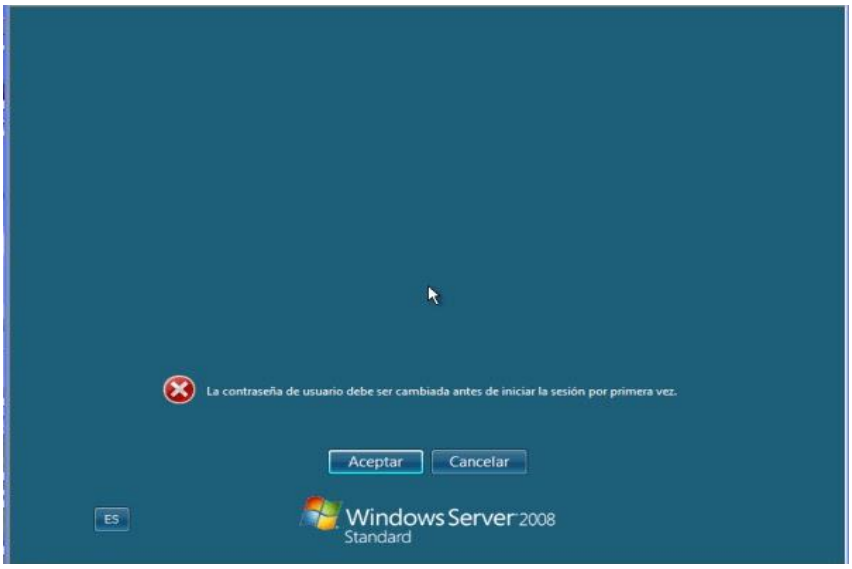


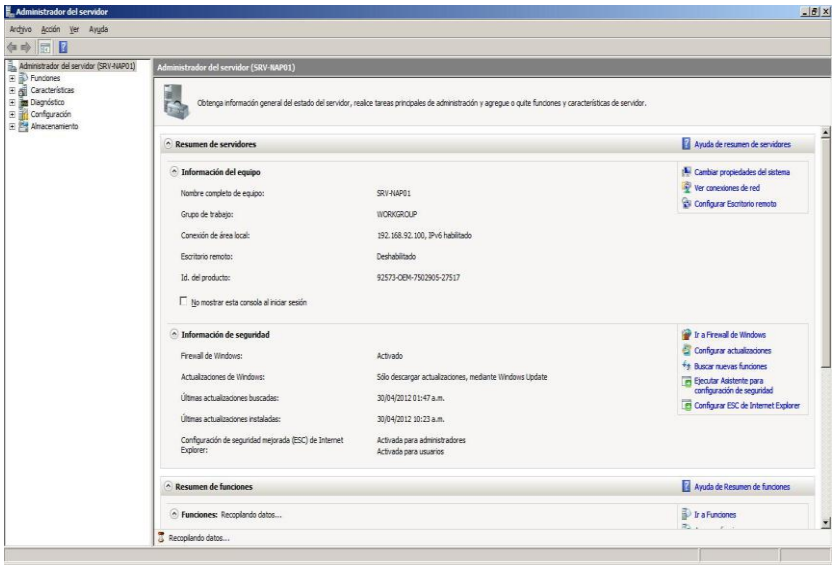
Figura 11 Primera Contraseña de Administrador



Se escribe la primera contraseña para administrador con la que se ingresara al equipo para tareas de administración.

Figura 12 Primer Inicio de Sesión

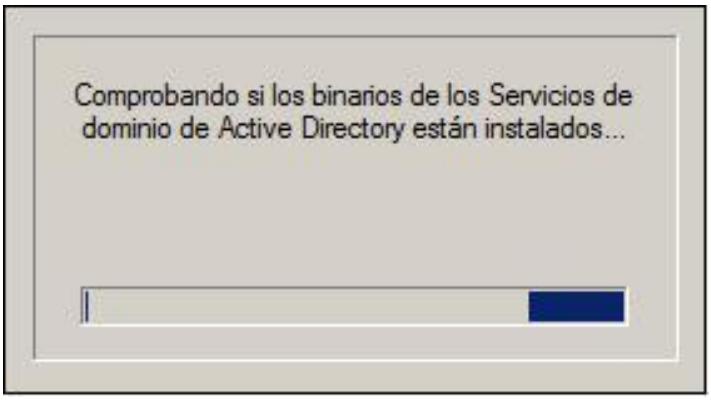
Figura 13 Administrador del Servidor



7.2.2. Instalación Domain Controller y DNS

En las siguientes figuras de la 14 a la 18 se muestra el proceso de promoción a controlador de dominio y la instalación de los servicios DNS.

Figura 14 Comprobando Instalador de Active Directory



En la consola de administración se ejecuta el comando dcpromo para promover la maquina a controlador de dominio

Figura 15 Instalación AD DS

Figura 16 Compatibilidad del sistema operativo

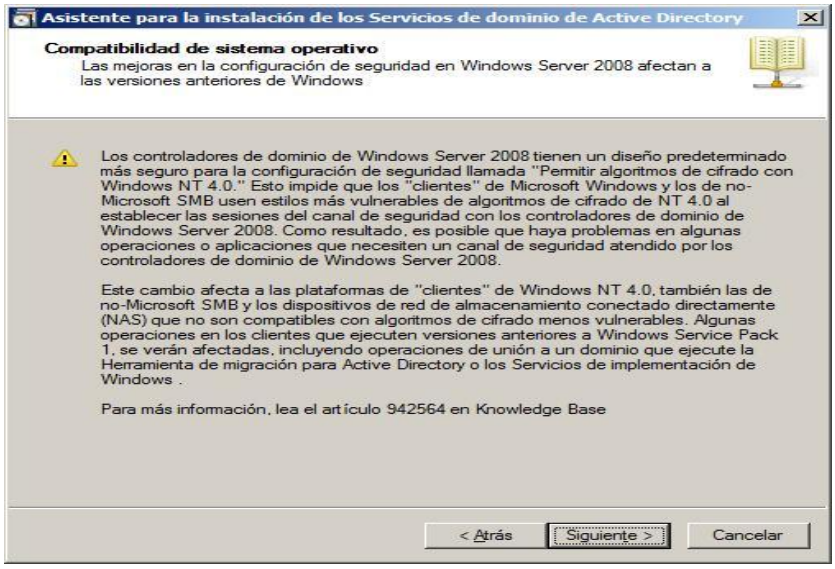


Figura 17 Configuración de Implementación

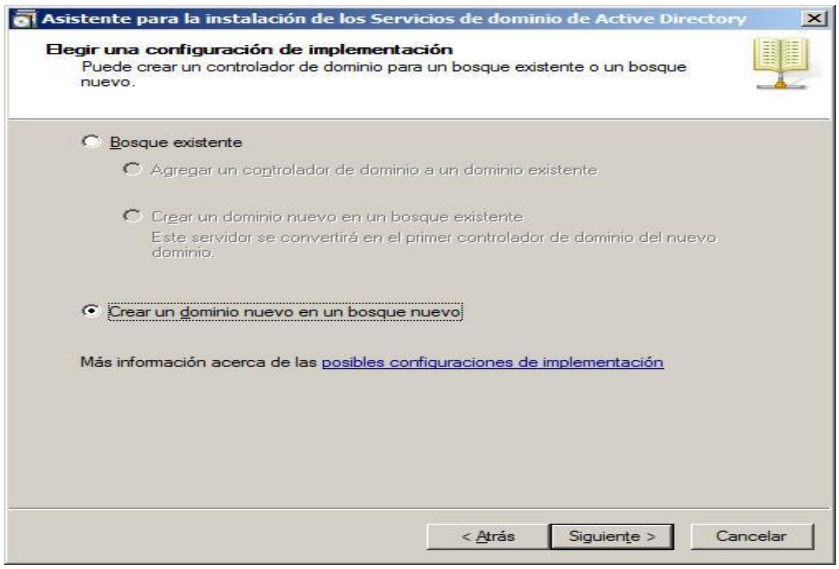
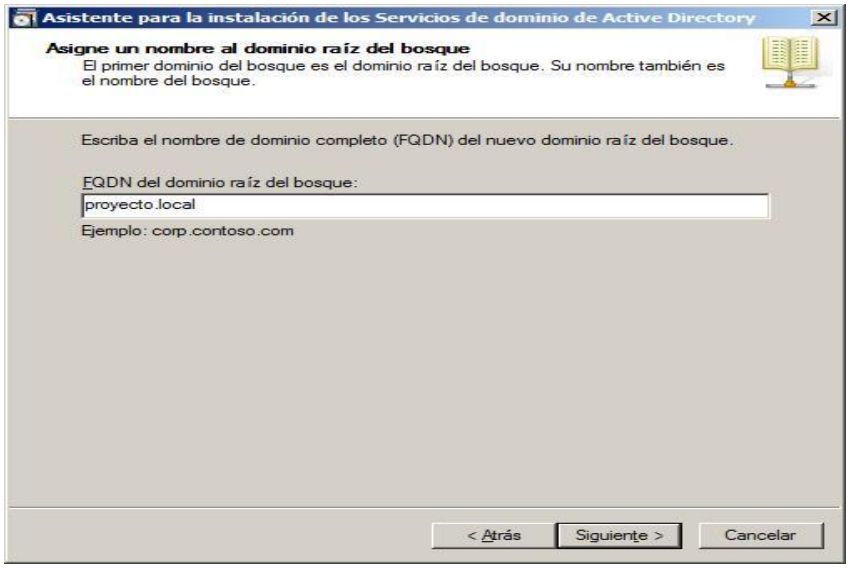


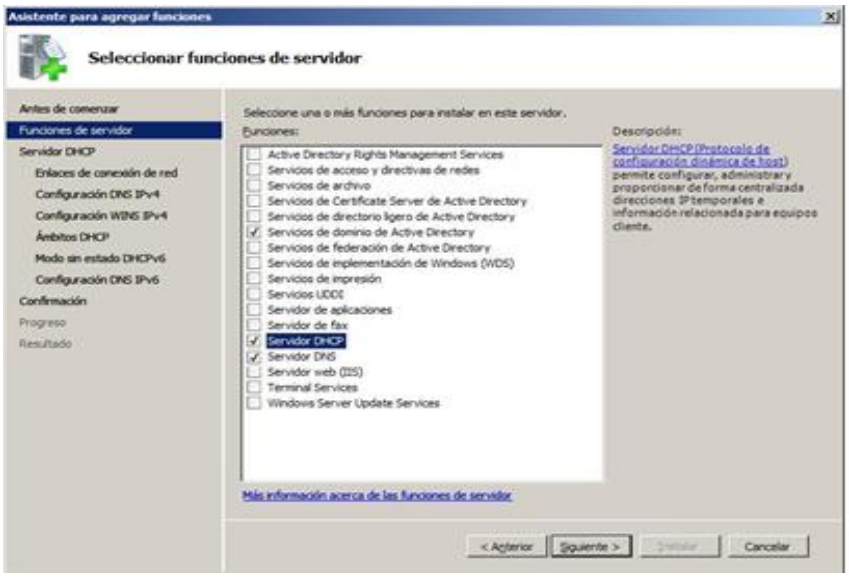
Figura 18 Nombre del Dominio



7.2.3. Instalación Servidores DHCP y NPS

En las siguientes figuras se muestra todo el proceso de instalación de los servidores DHCP y NPS con sus respectivos pasos a seguir.

Figura 19 Selección de Servicios



Se seleccionan las características DHCP para su posterior instalación.

Figura 20 Introducción DHCP

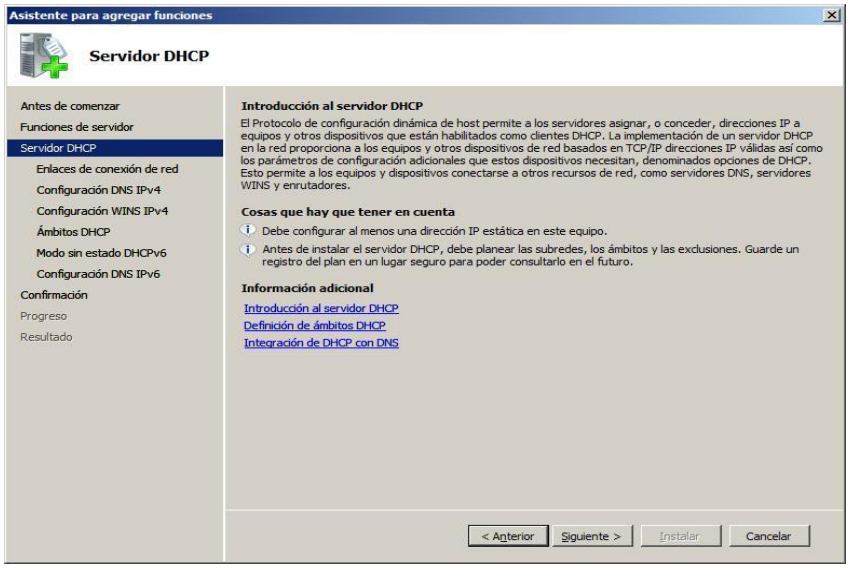


Figura 21 Enlaces de conexión de red

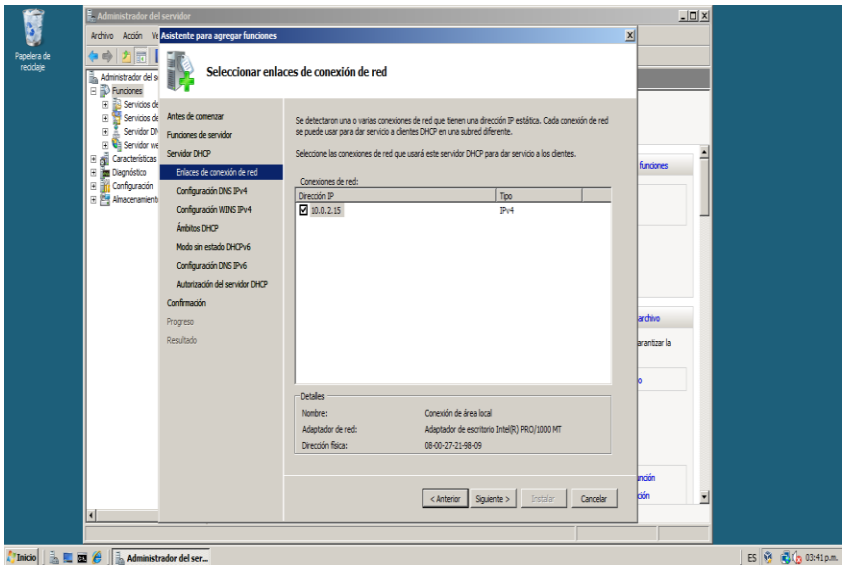


Figura 22 Configuración servidor DHCP

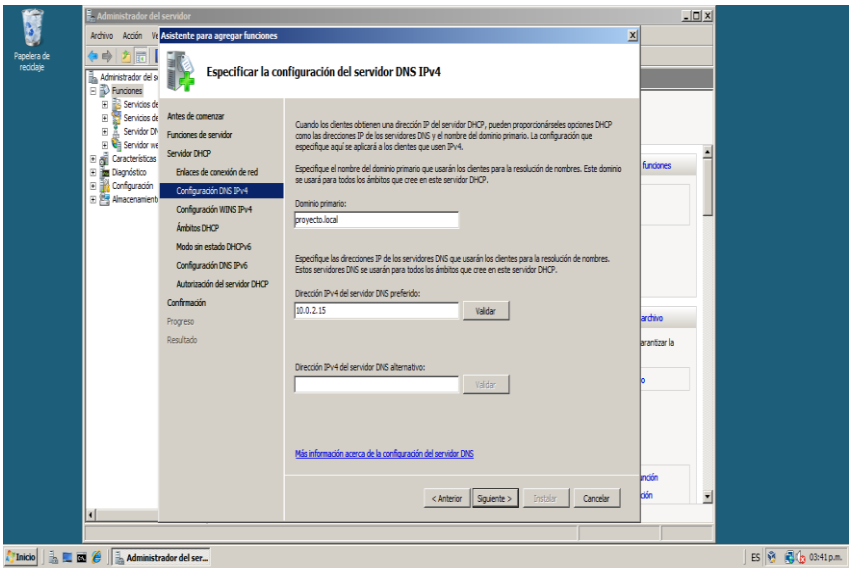
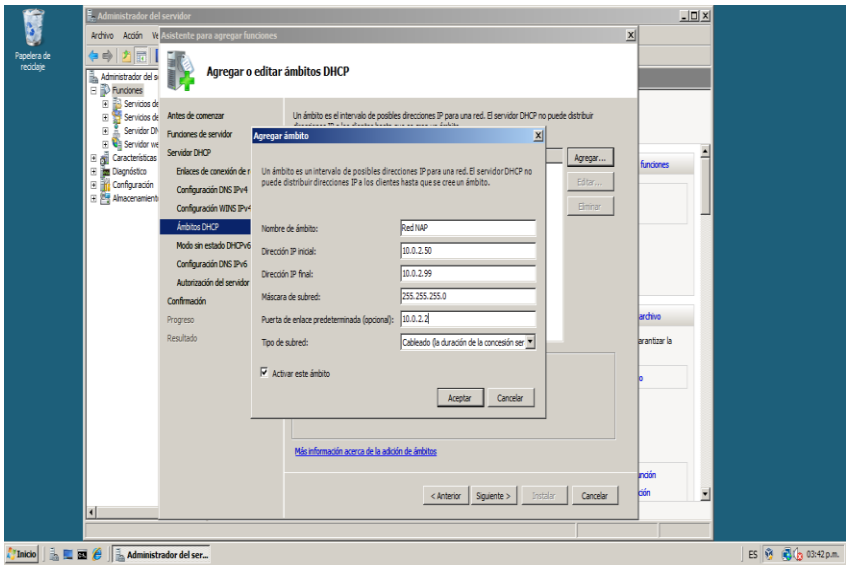


Figura 23 Ámbito DHCP



Se configuran los parámetros que el servidor DHCP entregara a los clientes que hagan peticiones.

Figura 24 Resumen de instalación DHCP

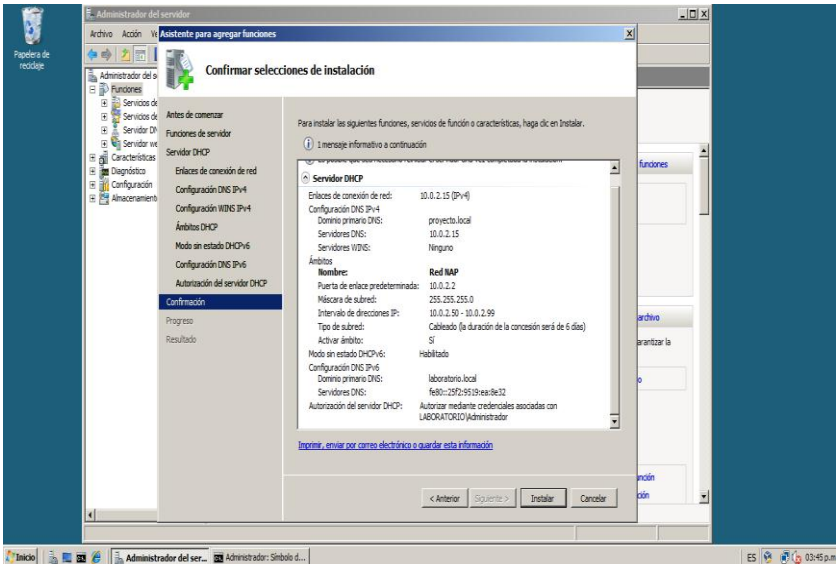
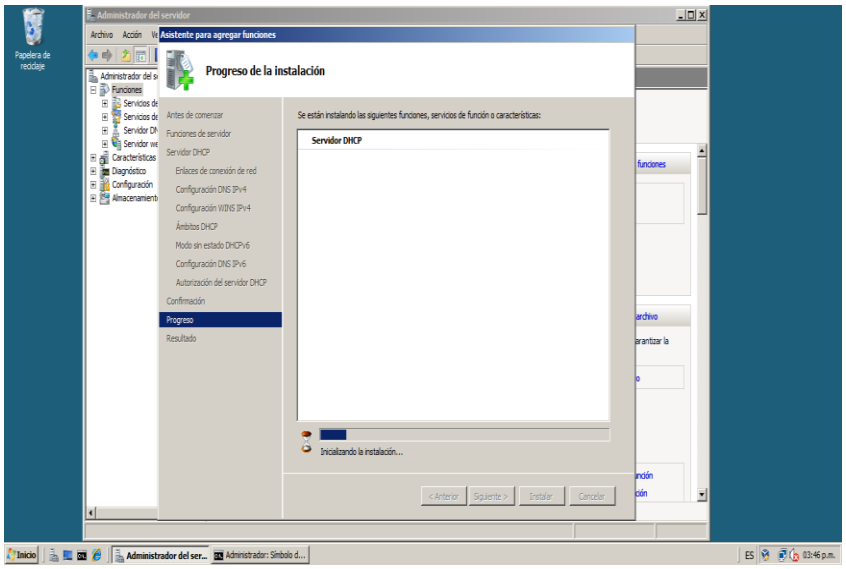
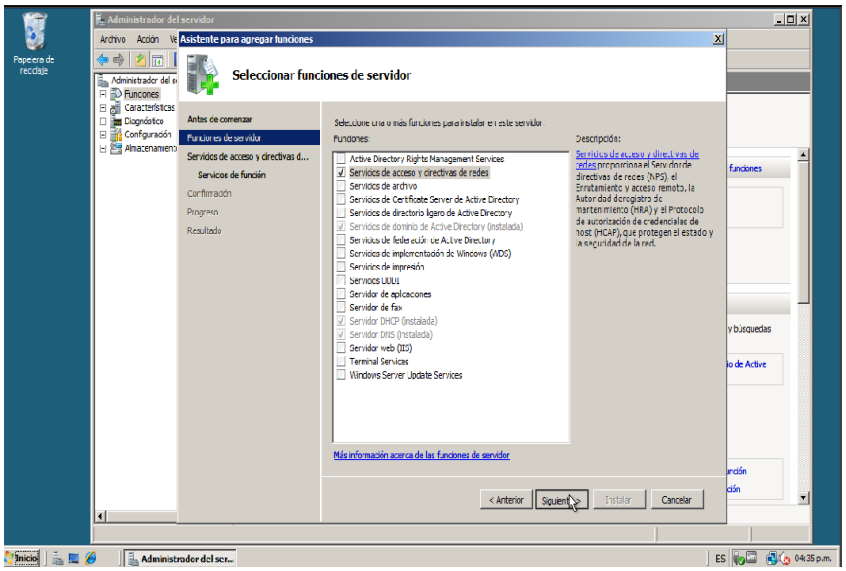


Figura 25 Progreso Instalación DHCP



Network Policy Server

Figura 26 Selección Servicios NPS



Se seleccionan las características NPS para realizar la instalación.

Figura 27 Introducción a NPS

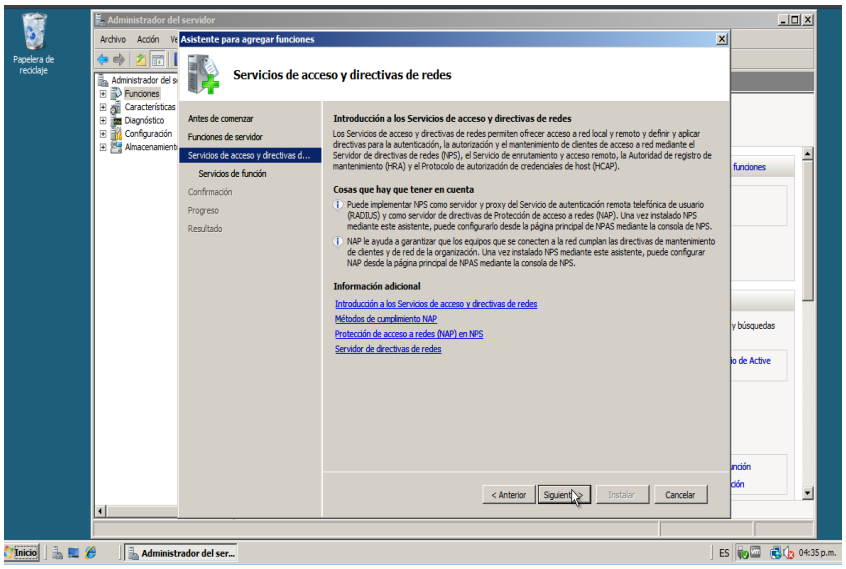


Figura 28 Progreso instalación NPS

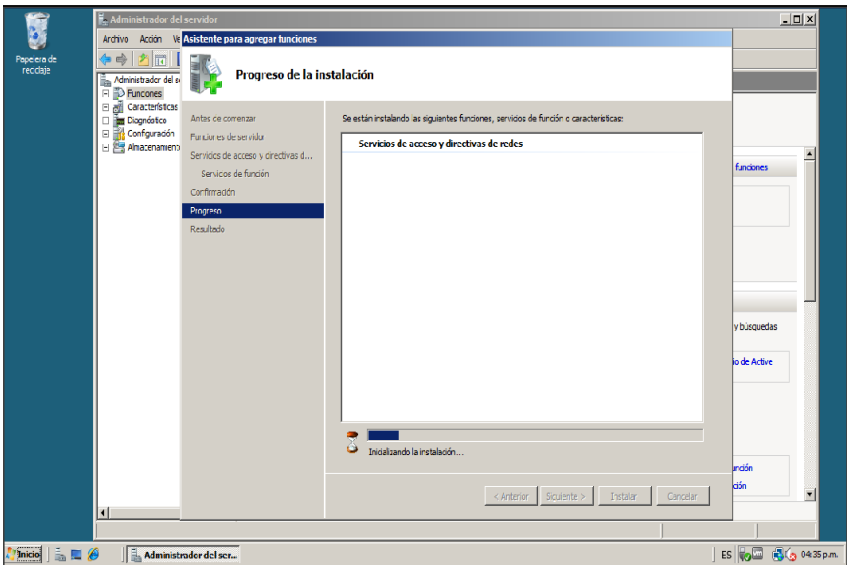
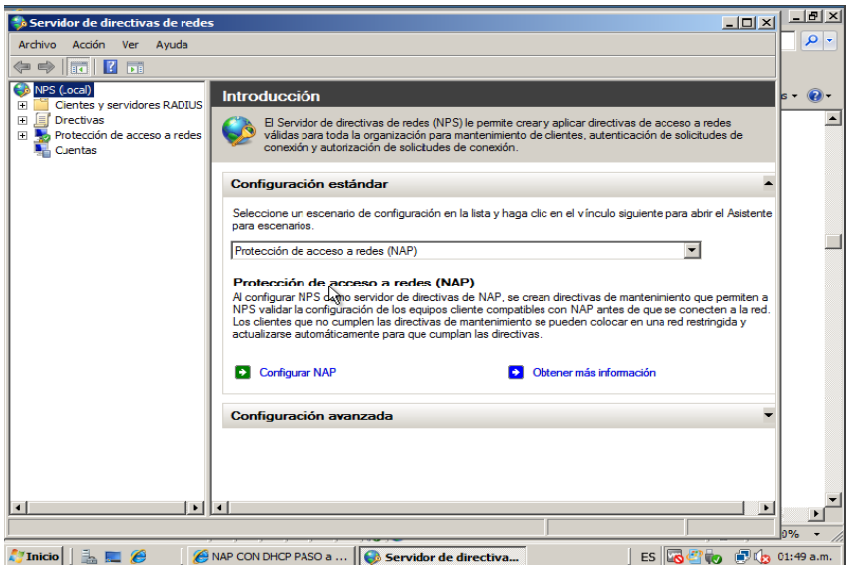


Figura 29 Primer inicio NPS



7.2.4. Unión del equipo cliente al dominio

En las siguientes figuras se evidencia el proceso de unión del equipo cliente Windows 7 al dominio proyecto.local a través de un usuario valido para el ingreso.

Figura 30 Unión al dominio

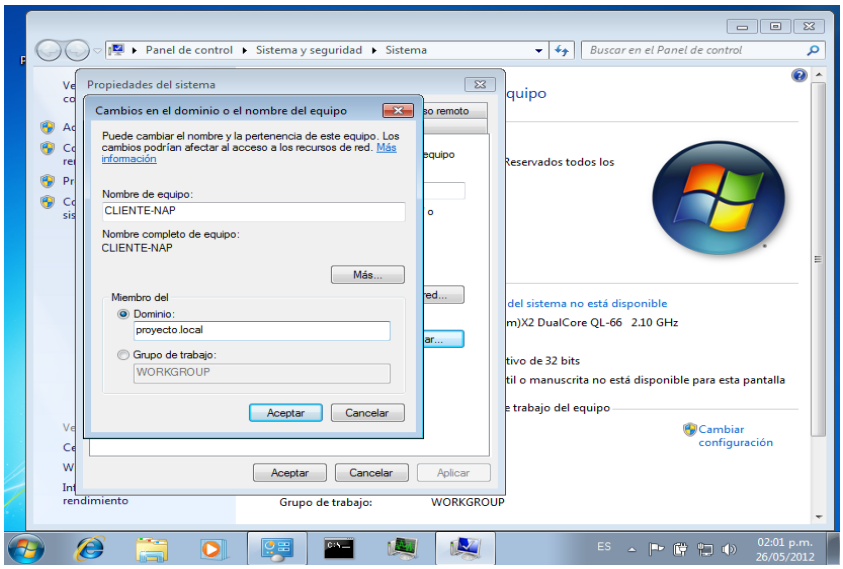


Figura 31 Usuario Valido en el Dominio

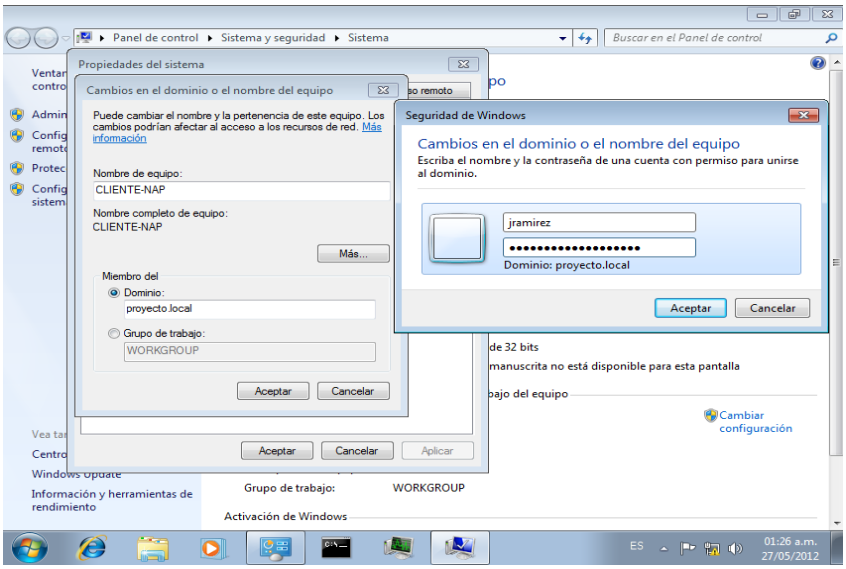
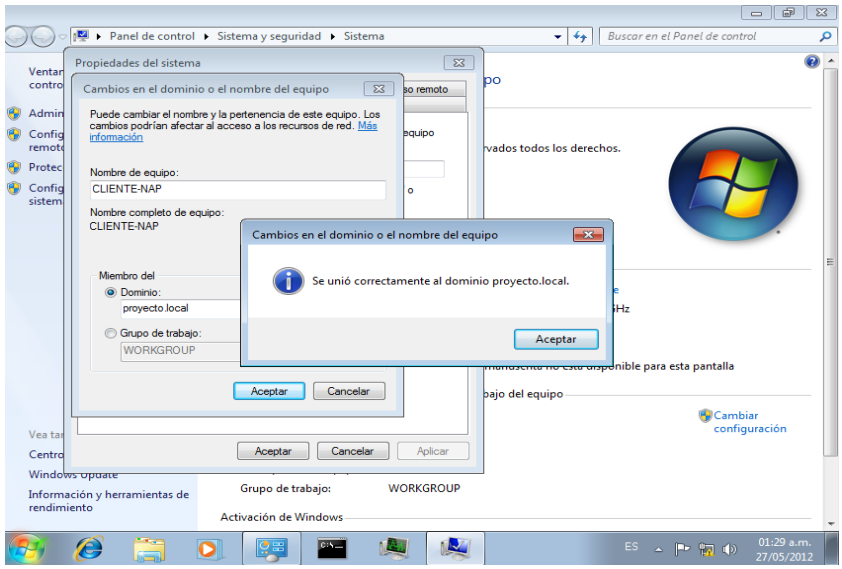


Figura 32 Acceso Correcto al dominio



7.2.5. Configuración Directivas de Grupo

Se evidencia el proceso de creación de directivas de grupo para el correcto funcionamiento de NAP. Involucran el agente NAP, centro de seguridad y el cliente de cumplimiento específico para DHCP.

Figura 33 Directiva NAP

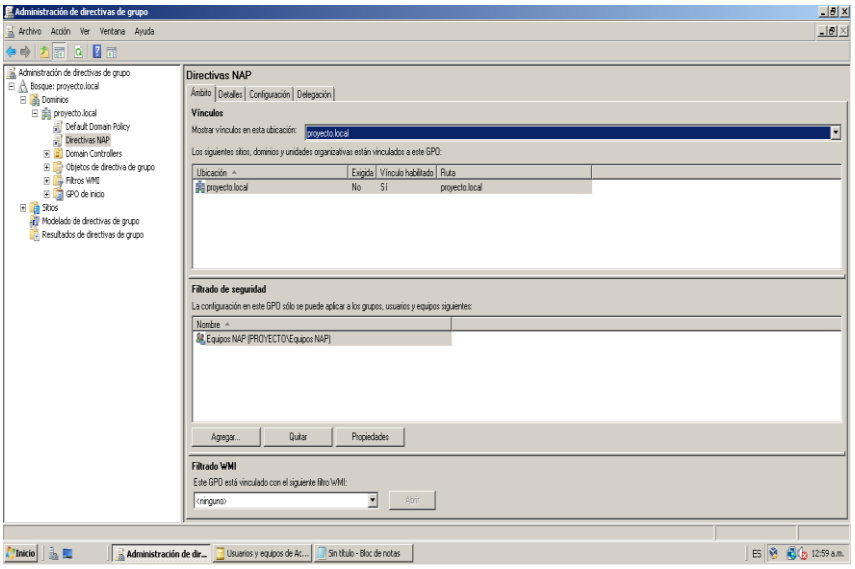


Figura 34 Agente NAP

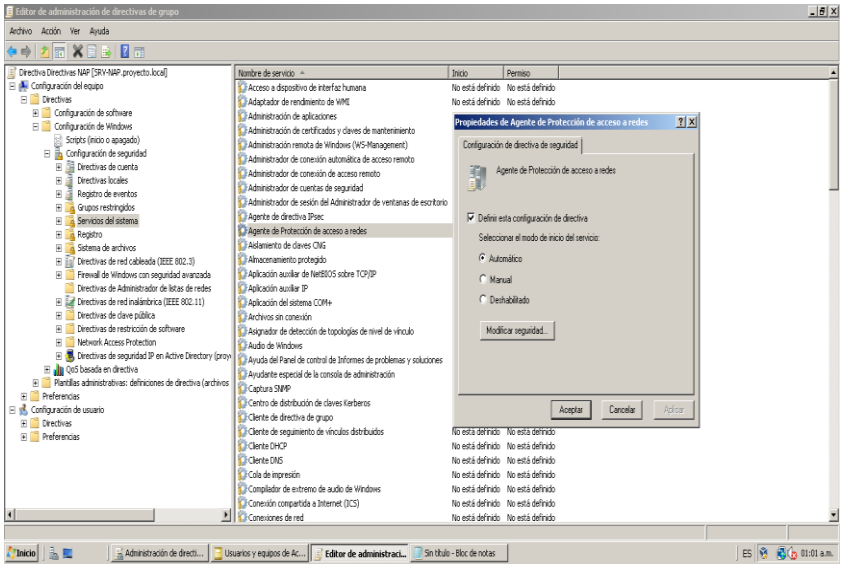


Figura 35 Cliente de Cumplimiento DHCP

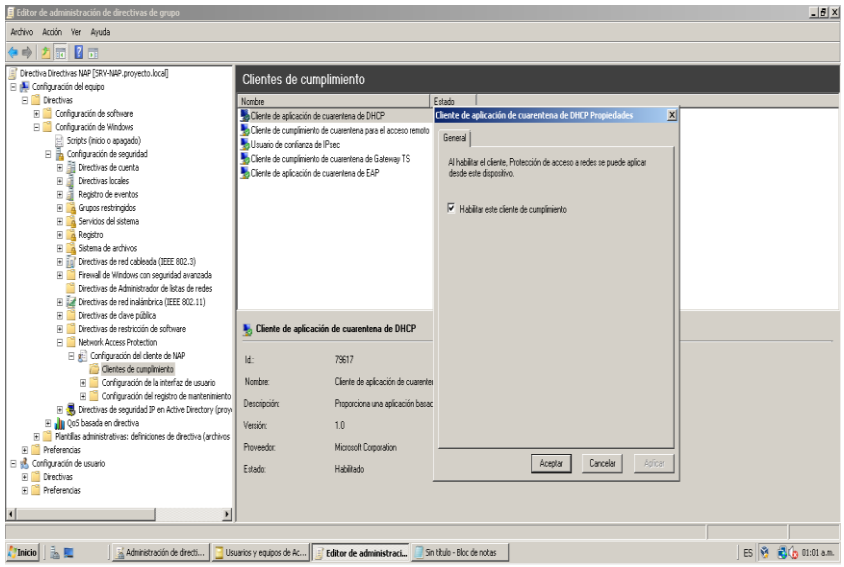


Figura 36 Centro de Seguridad

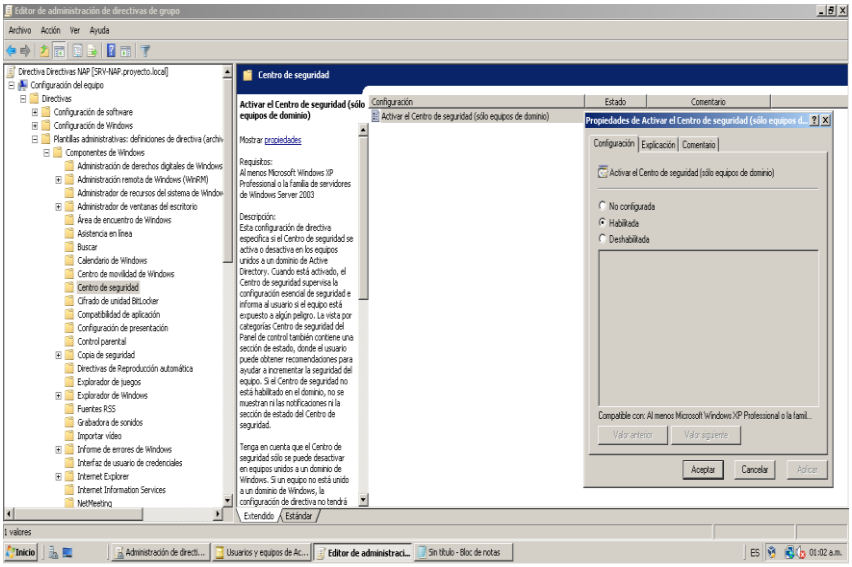
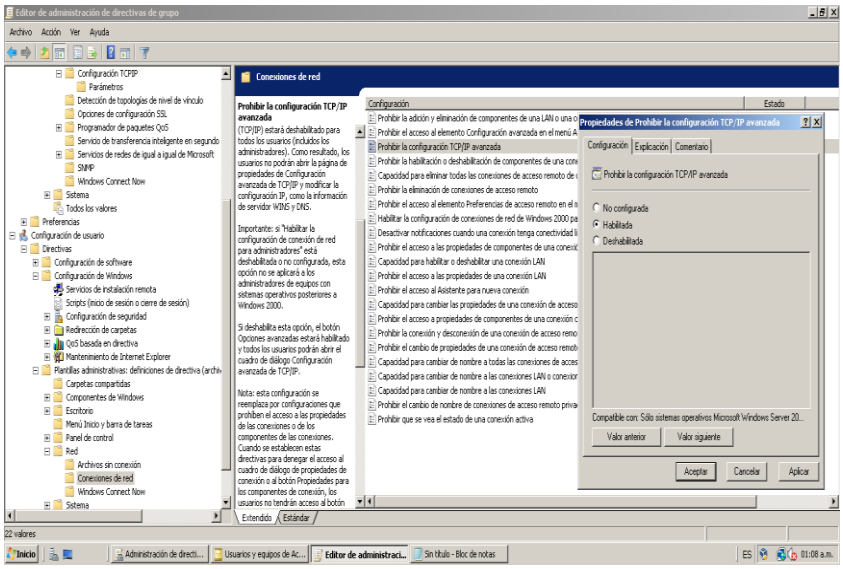


Figura 37 Prohibir Configuración TCP / IP



7.2.6. Configuración de cuentas de usuario y equipos AD

Creación de cuentas de usuario para los equipos cliente y un grupo de seguridad especifico para NAP.

Figura 38 Creación de usuario 1

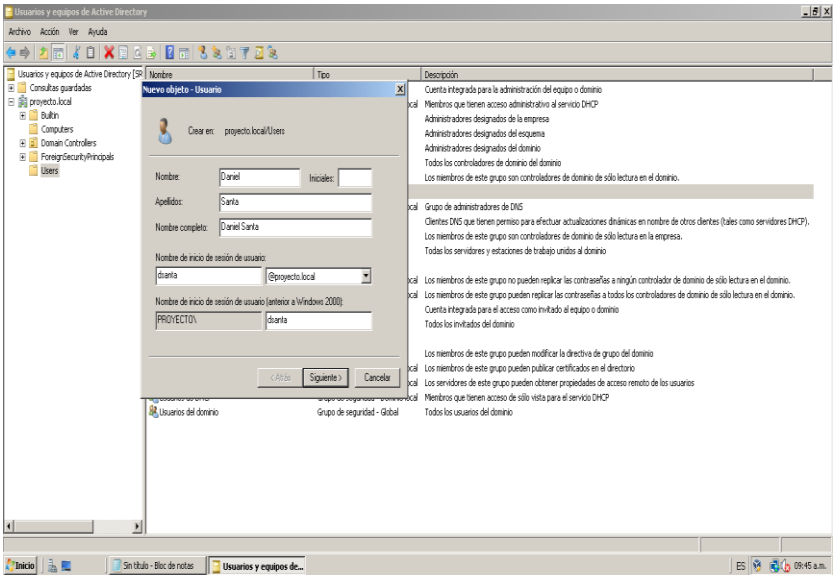


Figura 39 Creación de usuario 2

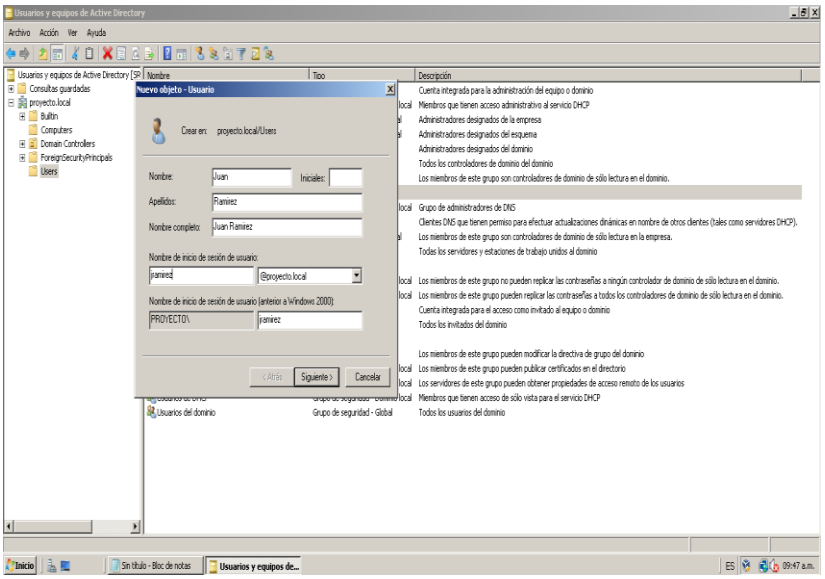
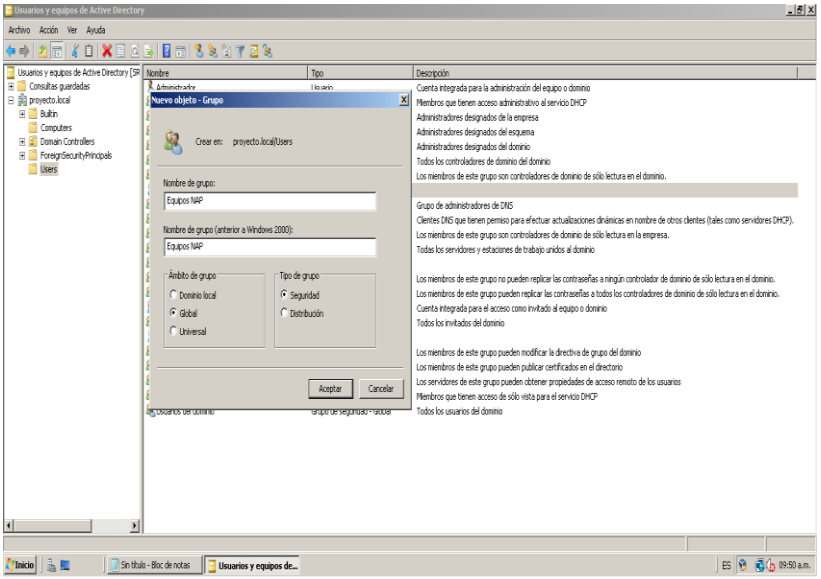


Figura 40 Grupo de seguridad NAP



7.2.7. Configuración Network Access Protection en el servidor NPS

En las siguientes figuras se evidencia el asistente para configurar Network Access Protection en el servidor de Directivas de Redes NPS y la creación de directivas de red y acceso además de la configuración del validador de mantenimiento de seguridad de Windows.

Figura 41 Método NAP

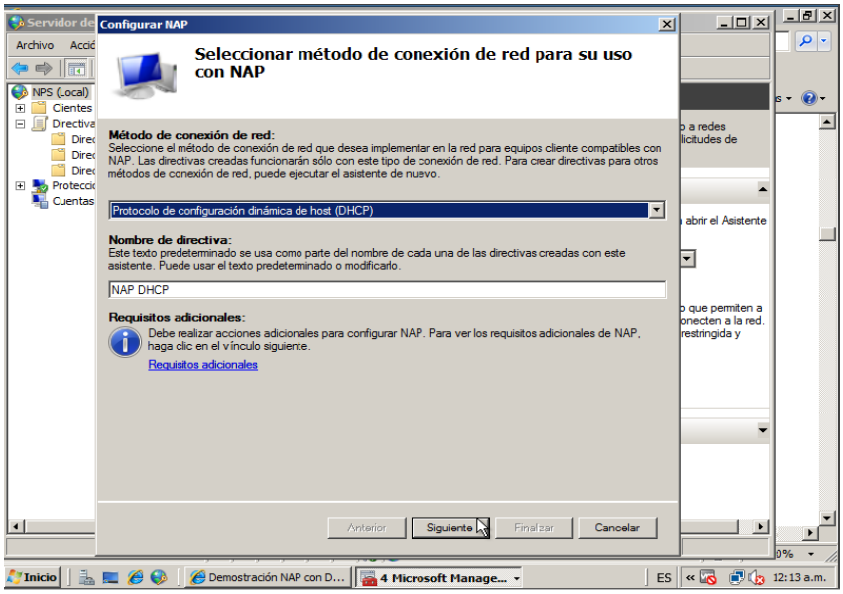


Figura 42 Servidores de Cumplimiento

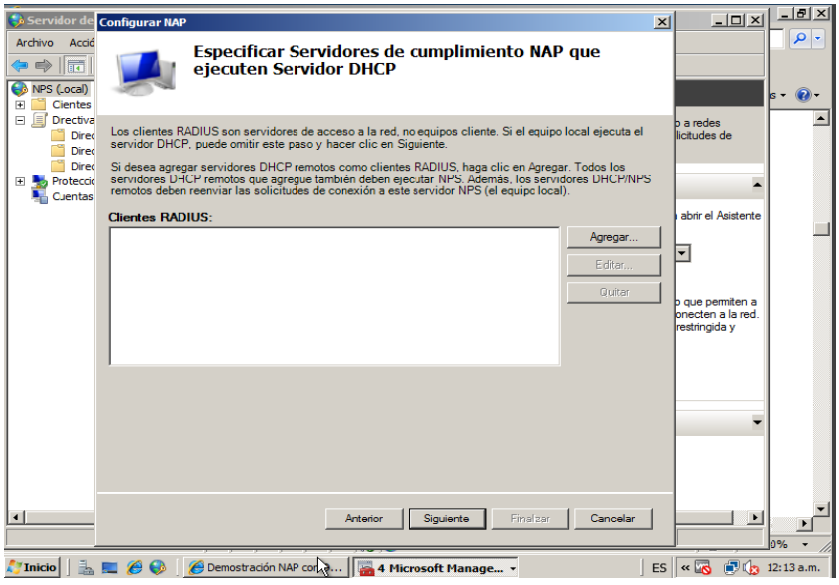


Figura 43 Ámbito DHCP en el NPS

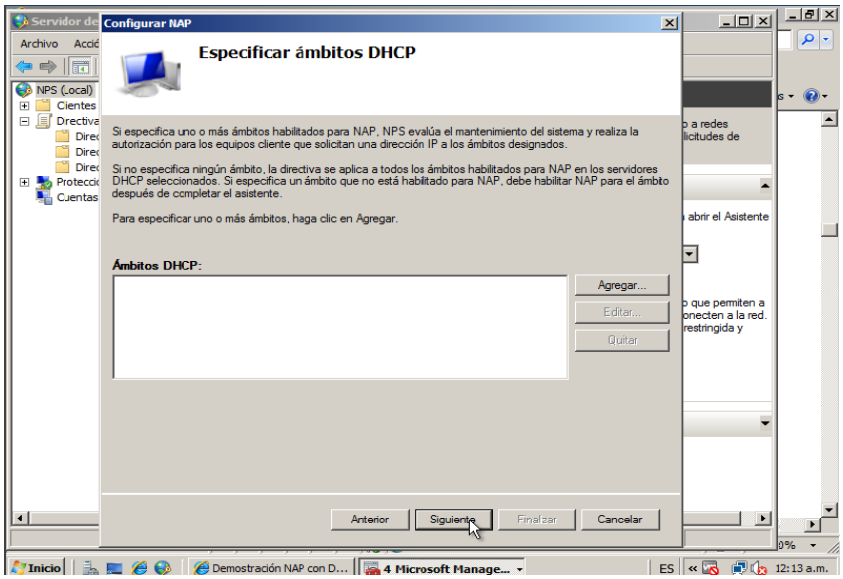


Figura 44 Configurar Grupo

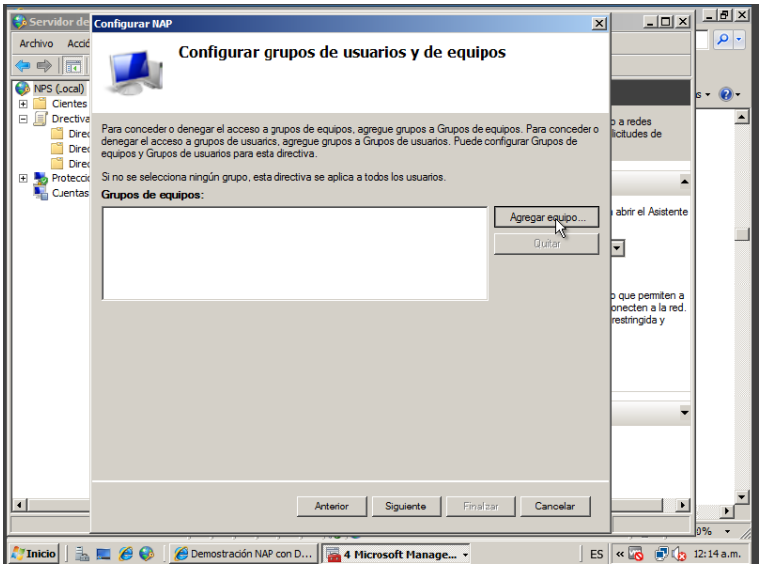


Figura 45 Selección grupo NAP

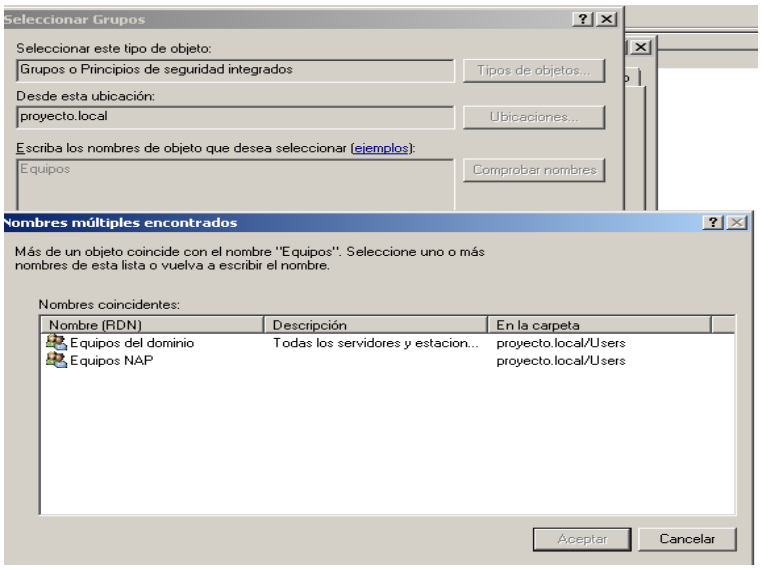


Figura 46 Servidores de remediación

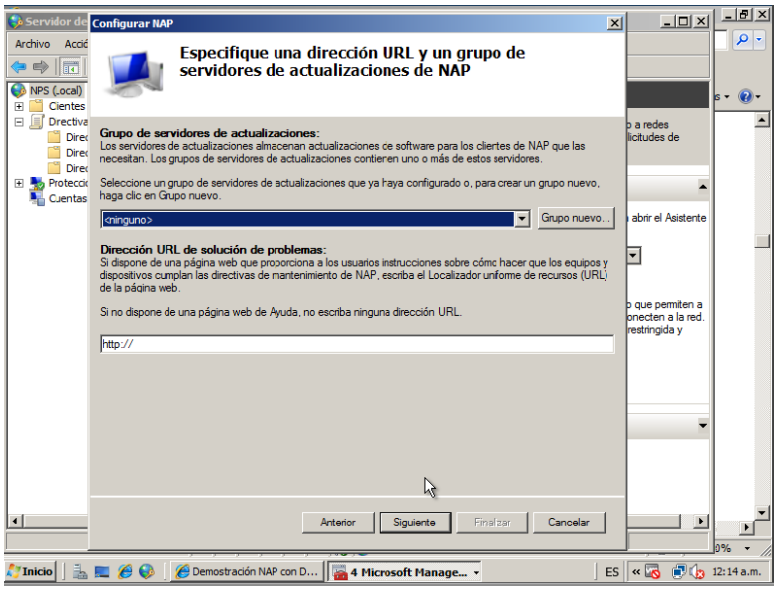


Figura 47 Directivas de mantenimiento

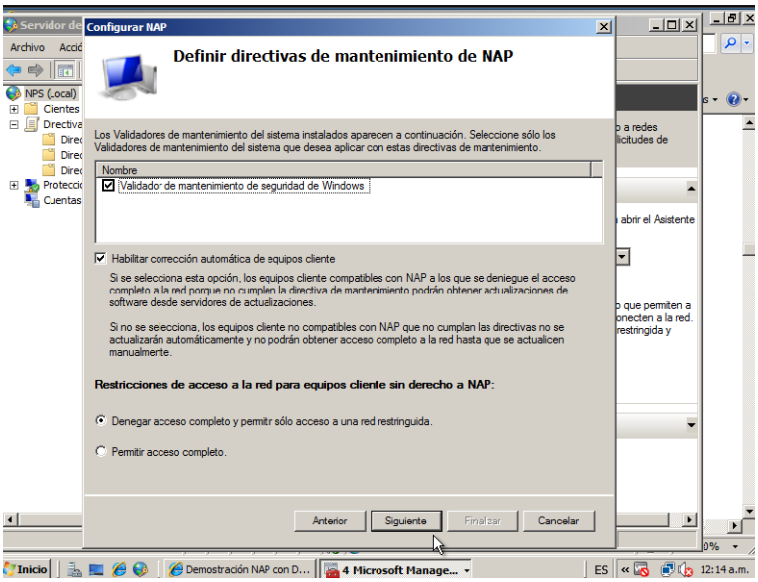


Figura 48 Resumen de configuración NAP en NPS

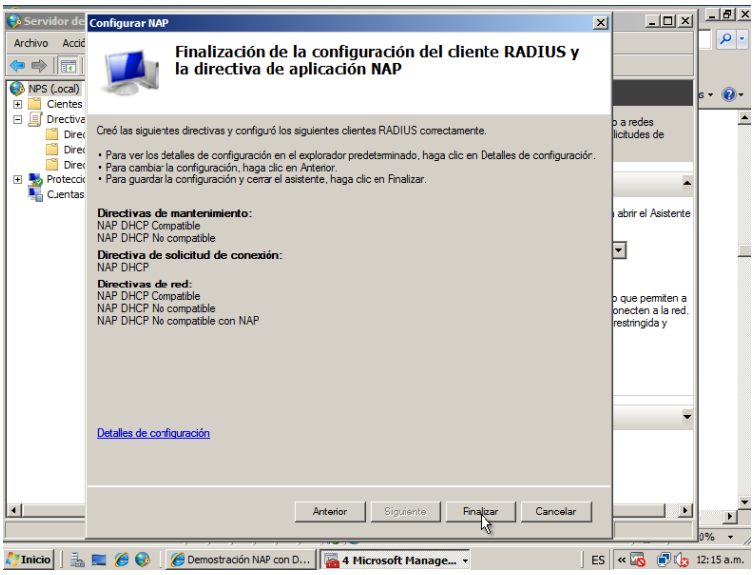


Figura 49 Validador de mantenimiento

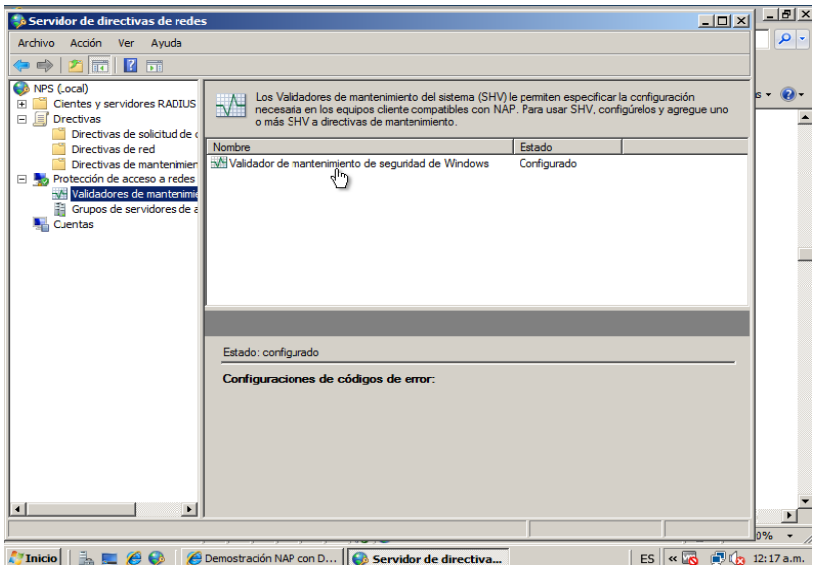


Figura 50 Configuración de Validador de mantenimiento

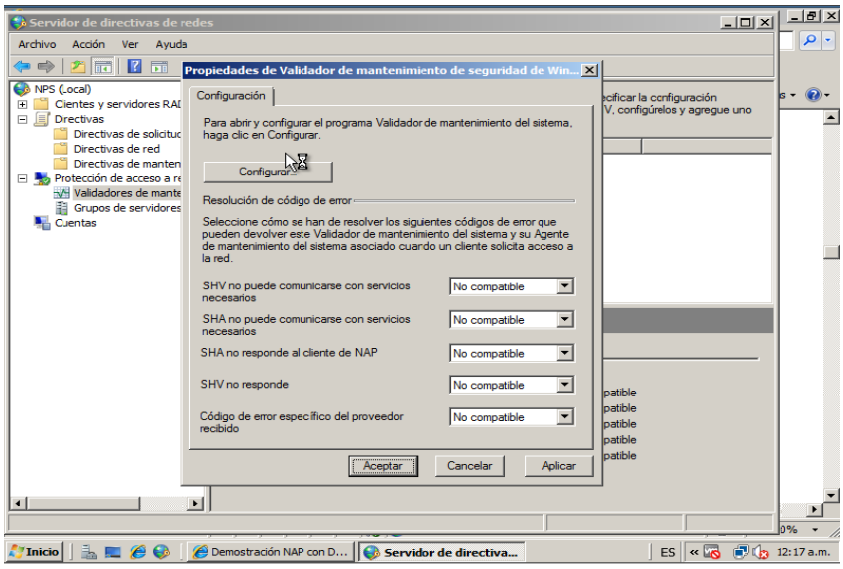
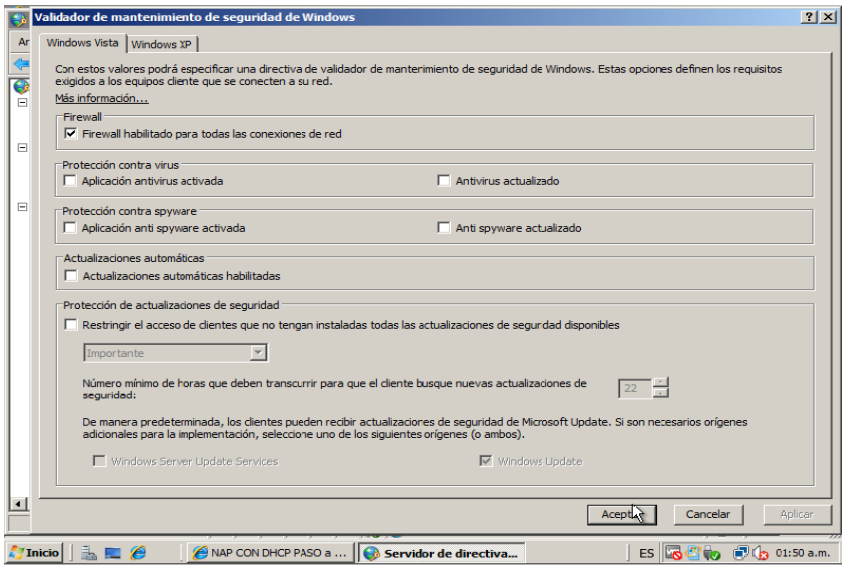


Figura 51 Requisitos para equipos cliente



7.2.8. Configuración del servidor DHCP para NAP

En las siguientes figuras se muestran las configuraciones para que el ámbito configurado en el servidor DHCP sea controlado desde el NPS y proteja el acceso a la red entregando parámetros de red ya sea restringido o con acceso total.

Figura 52 Propiedades ámbito DHCP

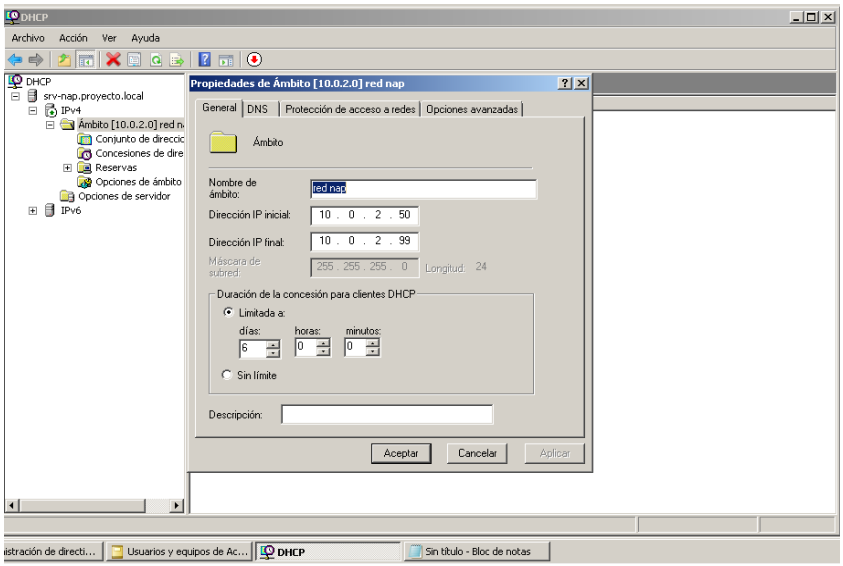


Figura 53 Ámbito DHCP para NAP

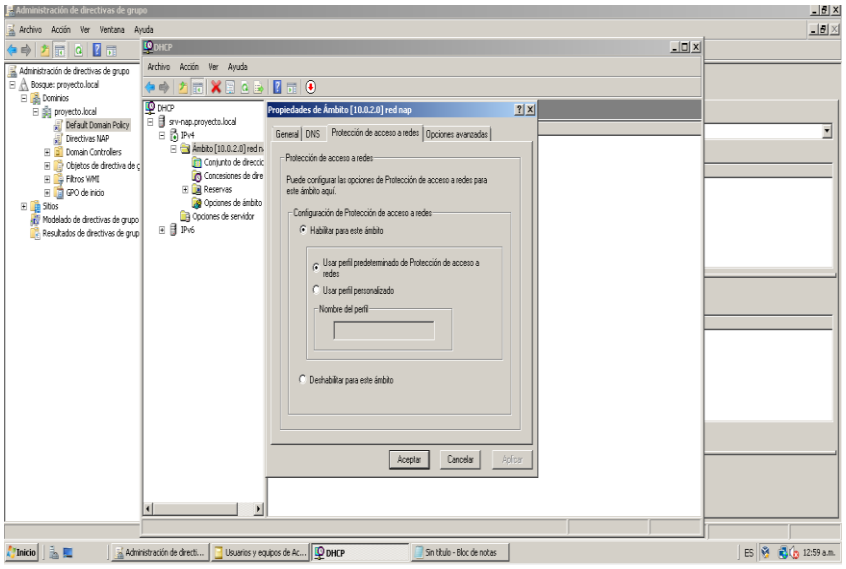
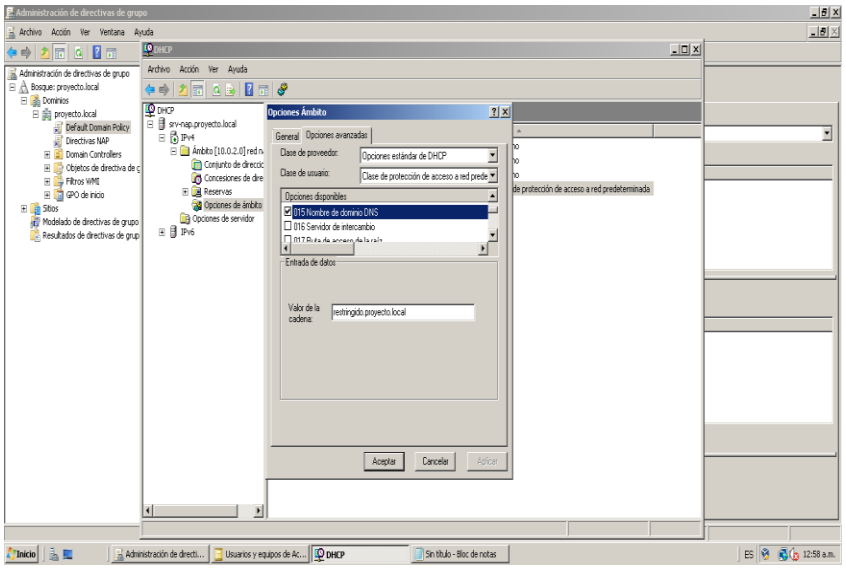


Figura 54 Dominio Restringido



7.2.9. Demostración de cumplimiento NAP

En las siguientes figuras de pantalla se evidencia el proceso de cumplimiento NAP en DHCP, cuando el quipo cumple con todos los requerimientos definidos en el validador de mantenimiento del sistema que en esta caso son Firewall activado, actualización e instalación de Windows Update automáticas, software antivirus y antispyware instalado. Con estos parámetros se prueba el Software Microsoft Security Essentials que tiene las funcionalidades de antivirus y antispyware, se activa y desactiva para evidencias el paso de estado acceso completo a la red a

un acceso limitado o restringido. Debido a que la auto remediación de equipos clientes esta activada si el Firewall y Windows Update no esta configurados correctamente al paso de unos segundos estos se reconfiguran automáticamente para cumplir con las directivas NAP.

Figura 55 Estado del Agente NAP

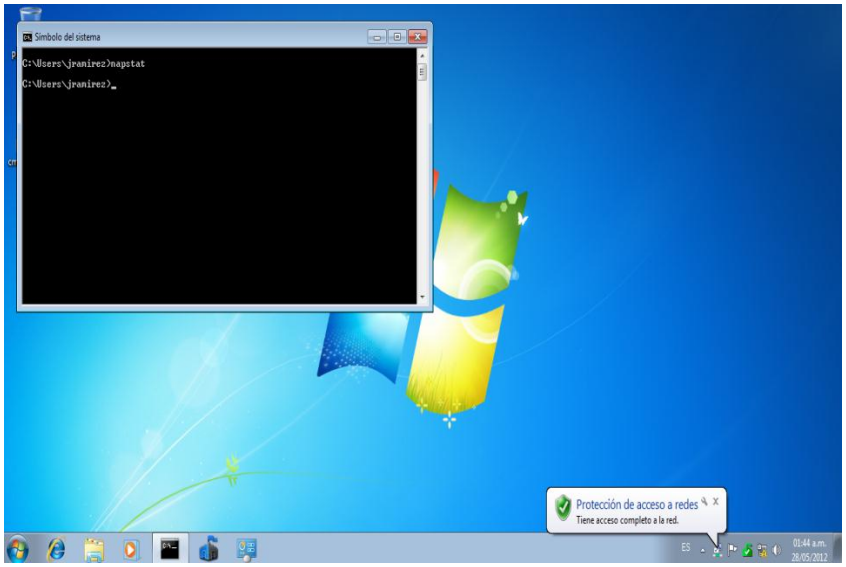


Figura 56 Firewall activado - Windows Update Automático

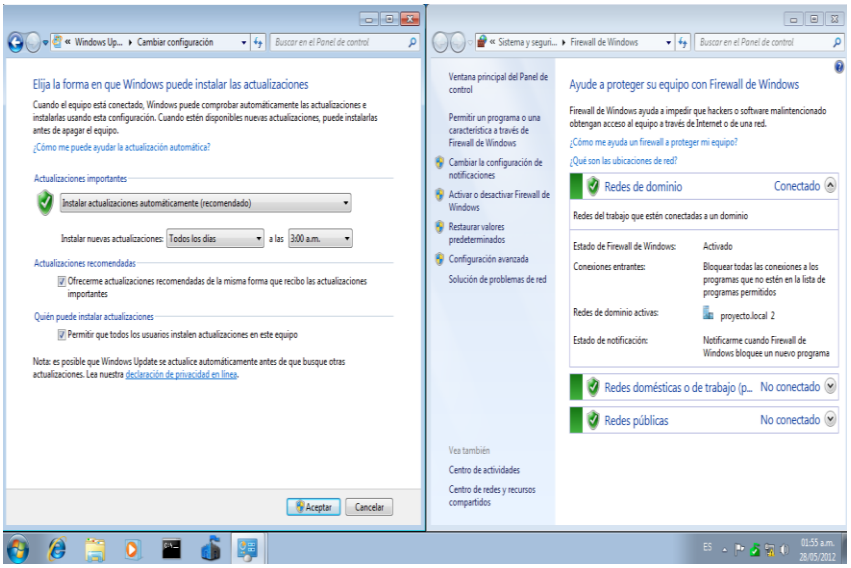


Figura 57 Antivirus/Antispyware Instalado y Activado

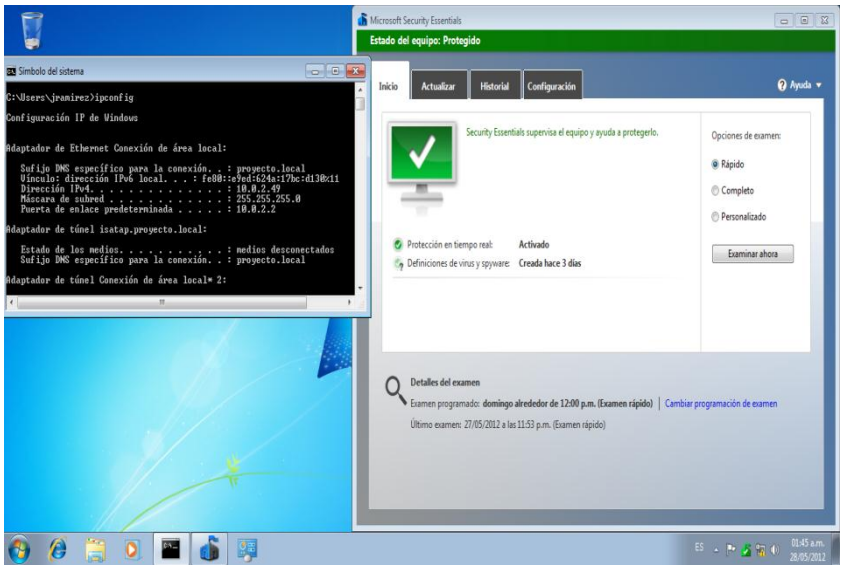


Figura 58 Desactivación de MSE

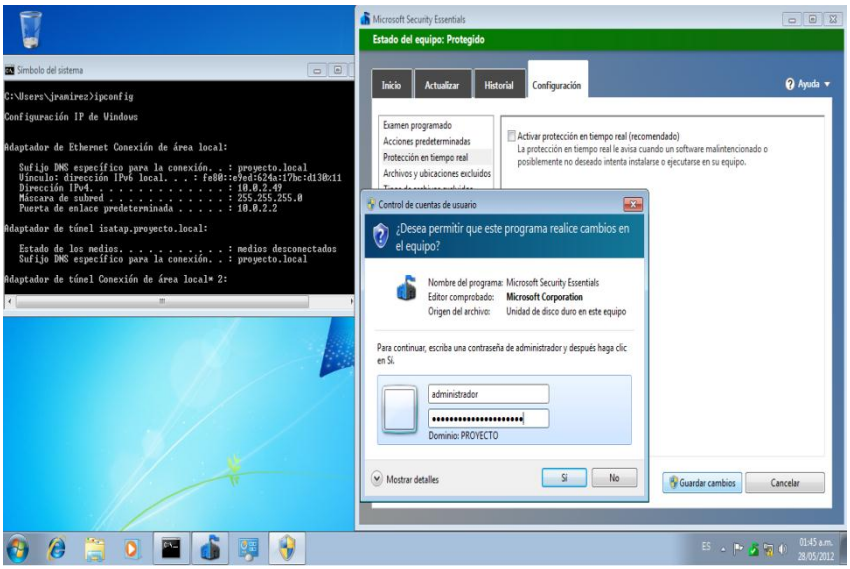


Figura 59 Estado de riesgo del Equipo

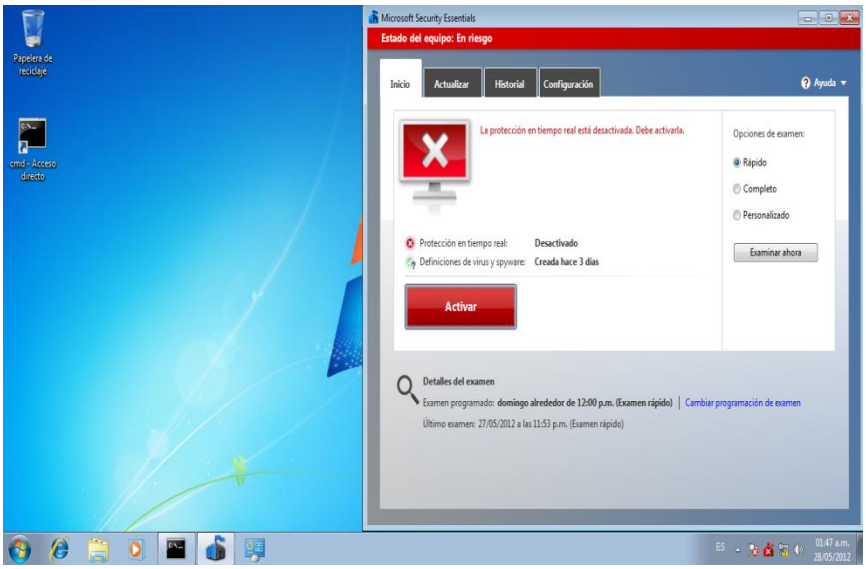


Figura 60 Dominio restringido.proyecto.local

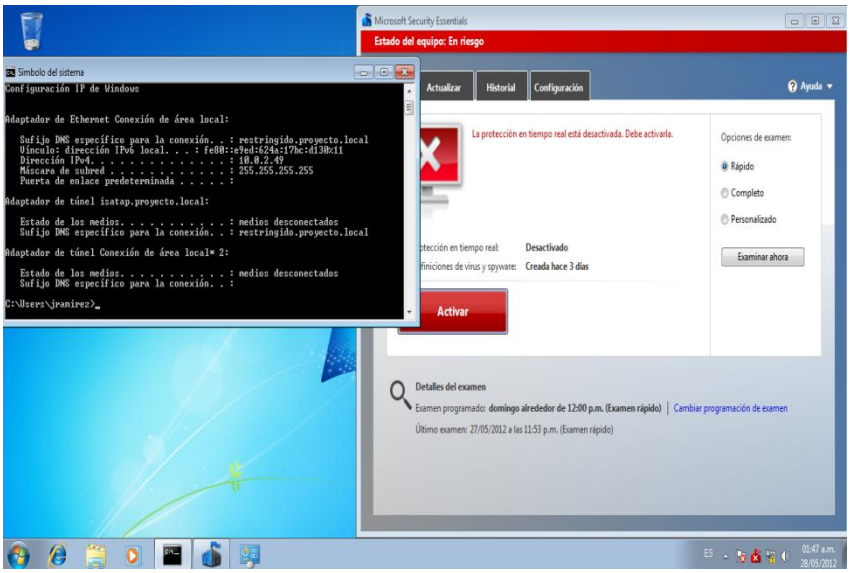


Figura 61 Acceso a la red limitado

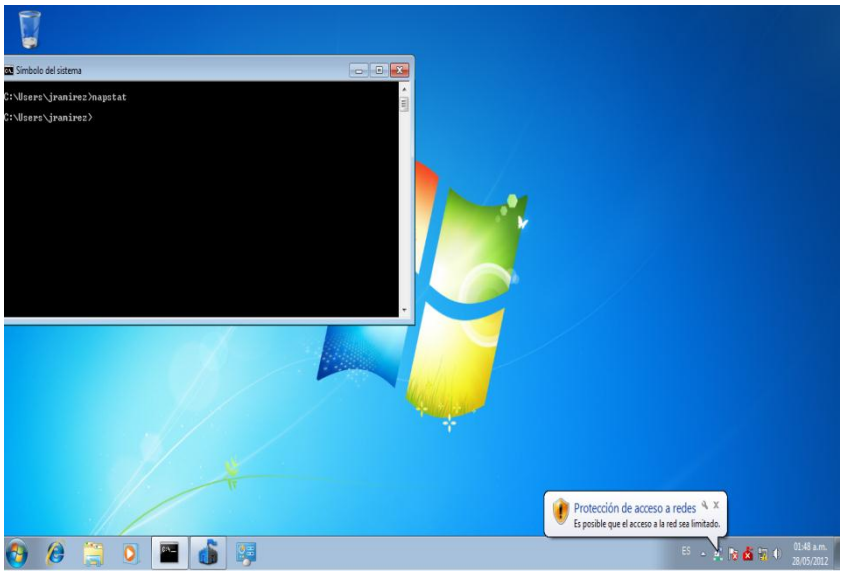


Figura 62 Activación de Seccurity Essentials

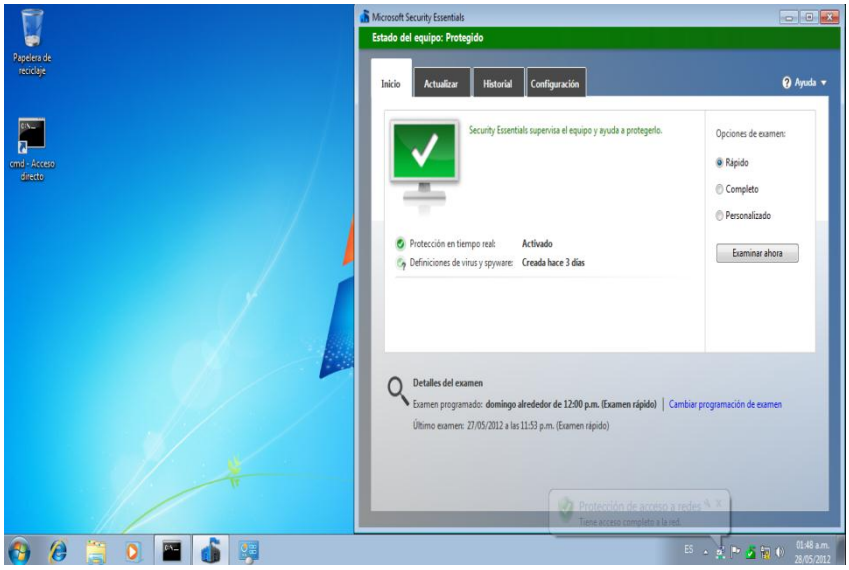


Figura 63 Acceso completo a la red

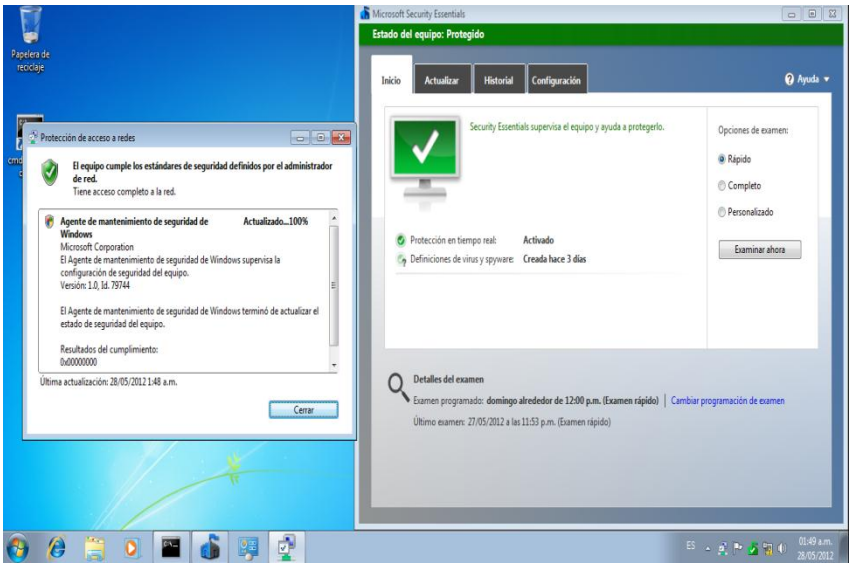
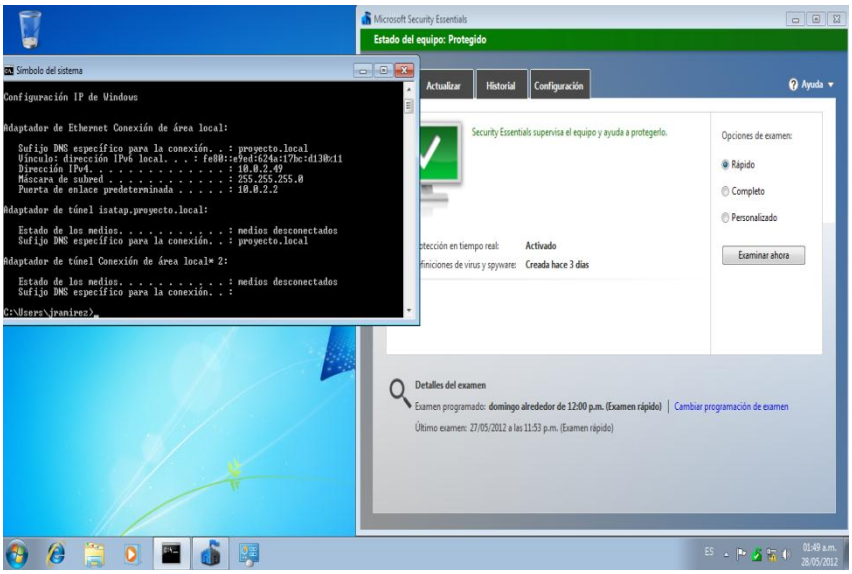


Figura 64 Dominio proyecto.local



7.2.10. Parámetros Técnicos de Seguridad

Todas las figuras restantes evidencian procedimientos de configuración que brindaran parámetros técnicos de seguridad a la implementación del proyecto NAP incluyen configuraciones en el sistema operativo, reglas de firewall, actualizaciones automáticas, servicio de hora en red NTP, permisos y políticas de grupo en el Active Directory

- ***Instalación de los últimos parches y actualizaciones***

Figura 65 Preparando Instalación de Actualizaciones

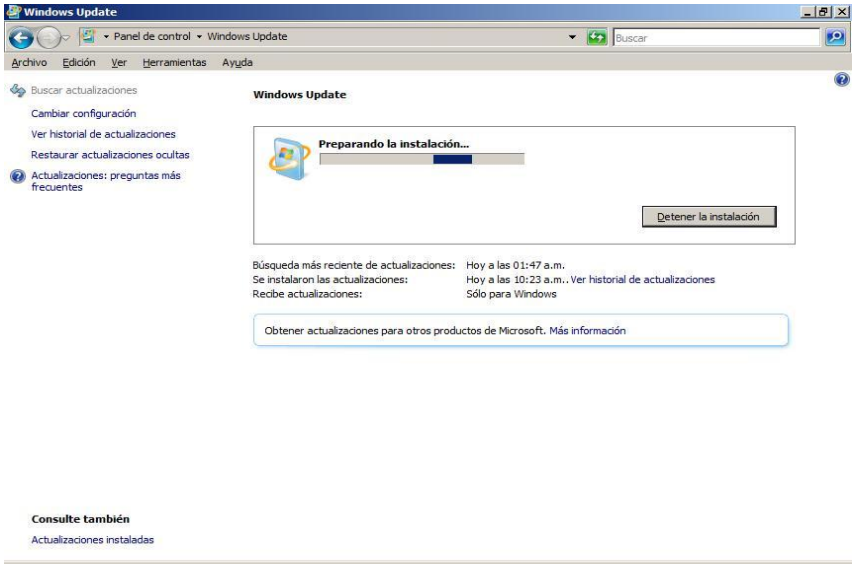


Figura 66 Actualizaciones Disponibles

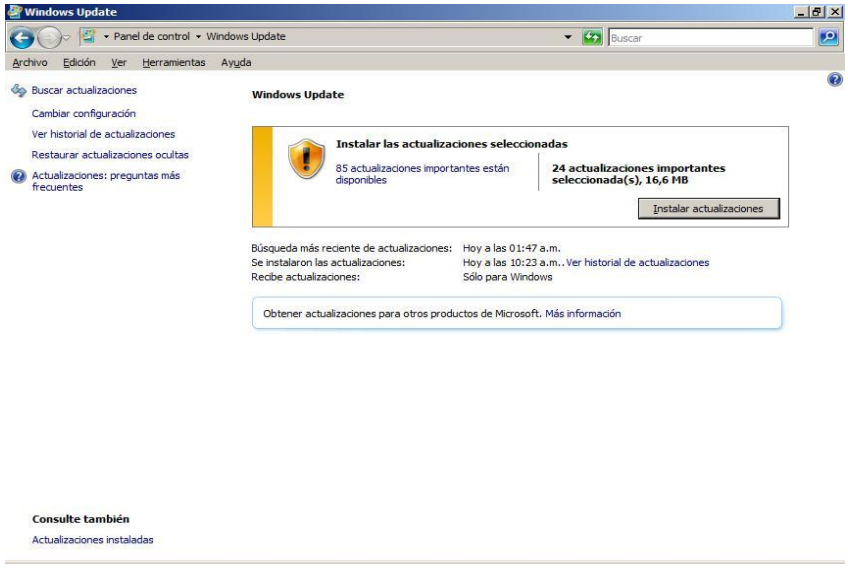
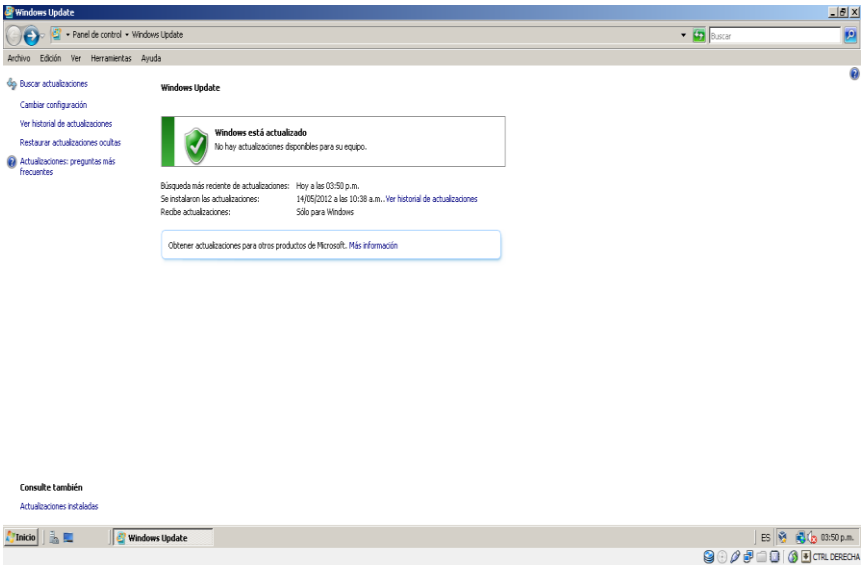


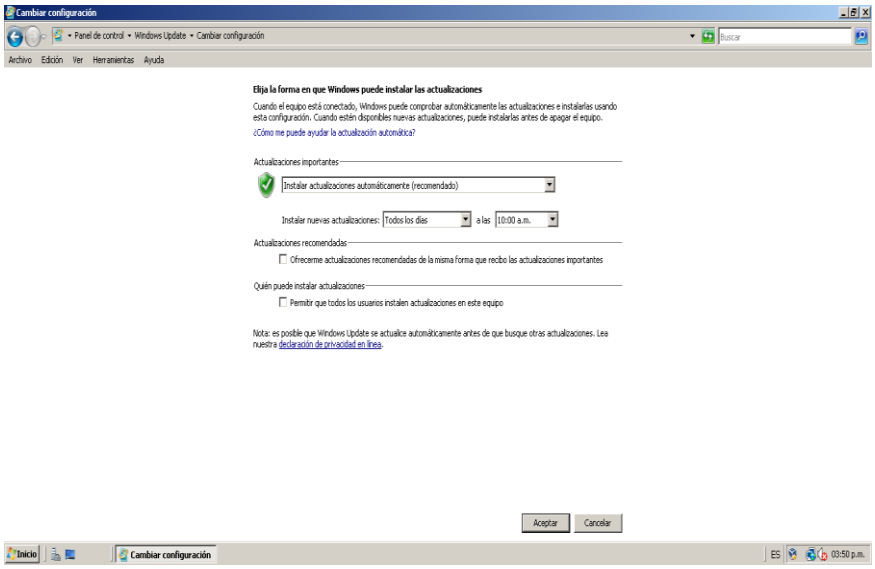
Figura 67 Configurando Actualizaciones

Figura 68 Windows esta Actualizado



- ***Configuración de Windows update***

Figura 69 Instalar Actualizaciones Automáticamente



- ***Segmentación de permisos por unidades organizacionales***

Figura 70 Usuarios y Equipos de AD

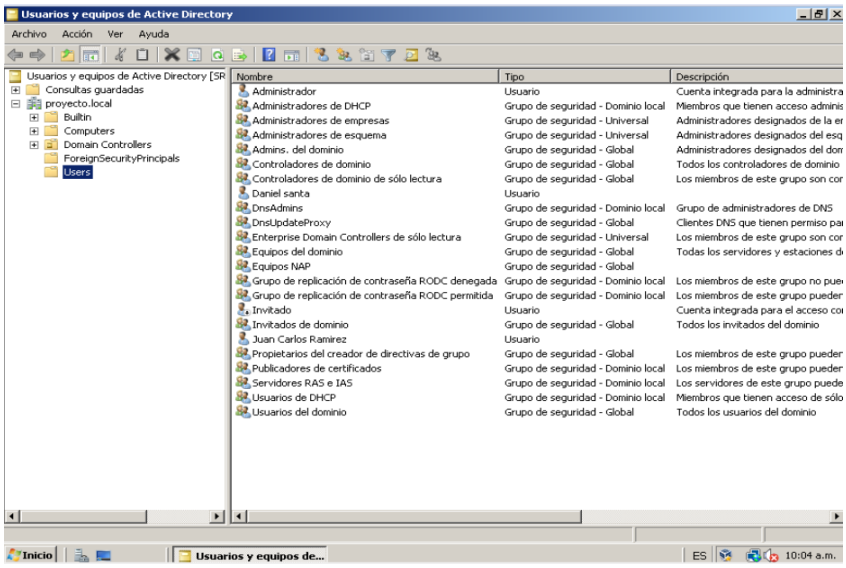


Figura 71 OU Administradores

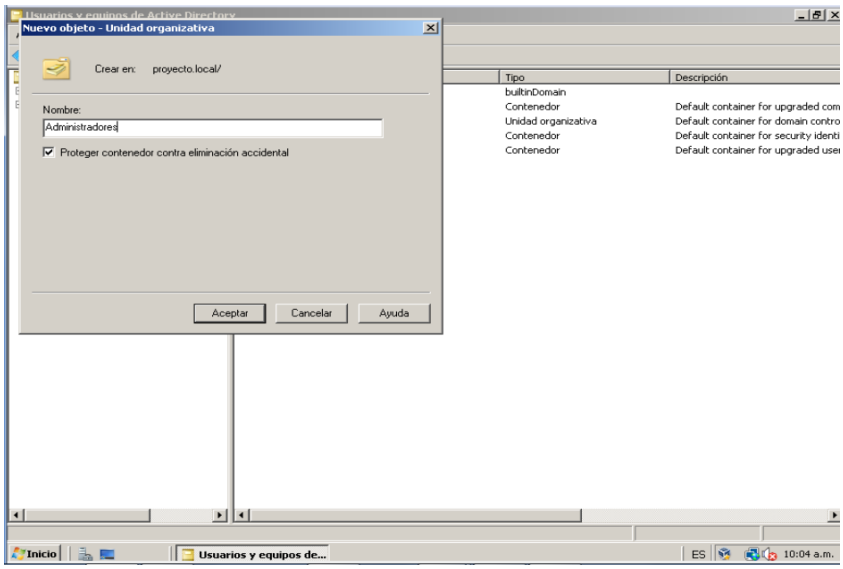


Figura 72 OU Gerencia

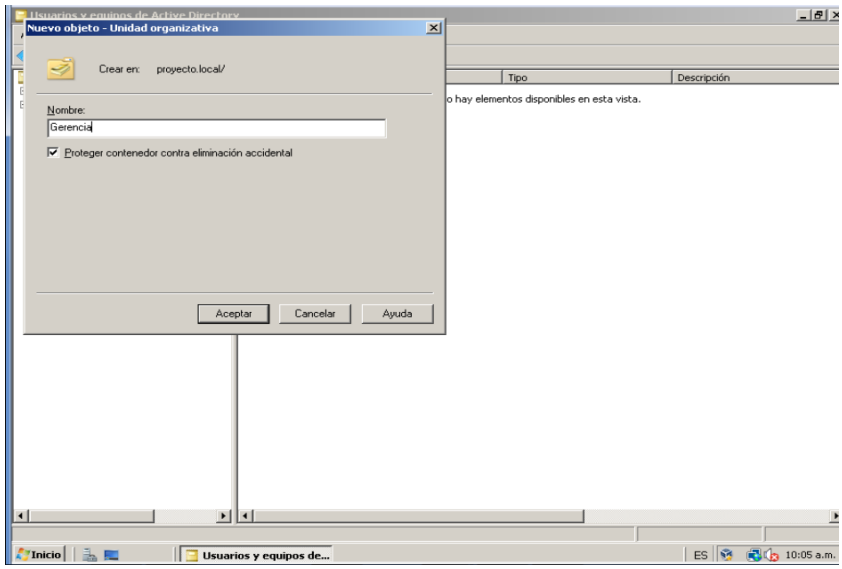


Figura 73 OU Equipos NAP

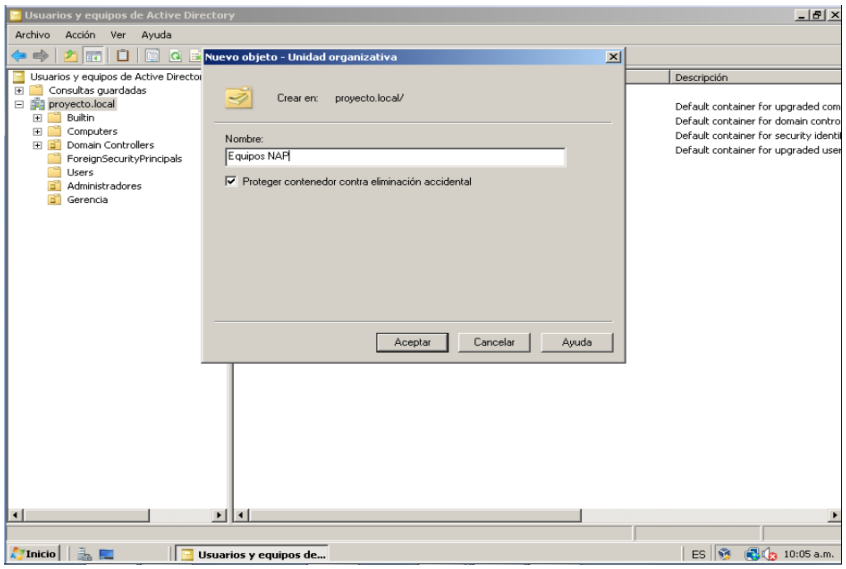


Figura 74 OU Presidencia

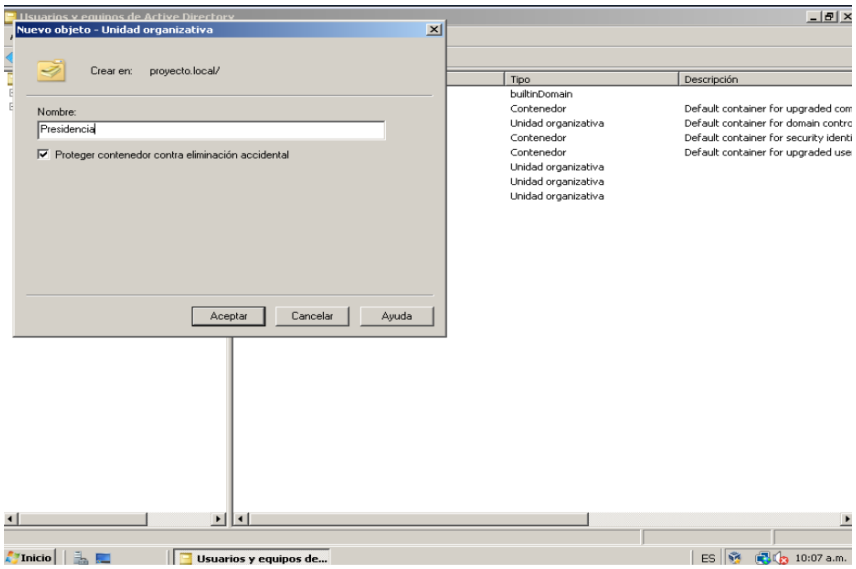


Figura 75 OU Sistemas

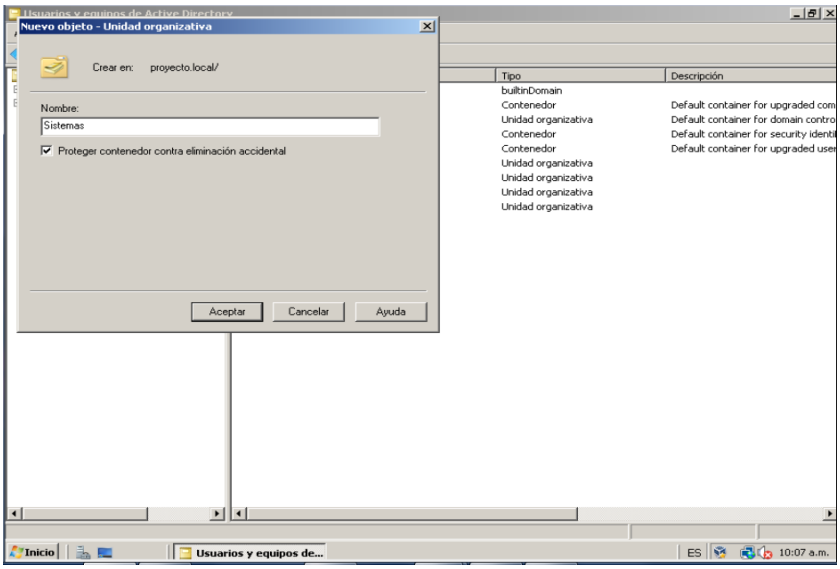


Figura 76 OU Mercadeo

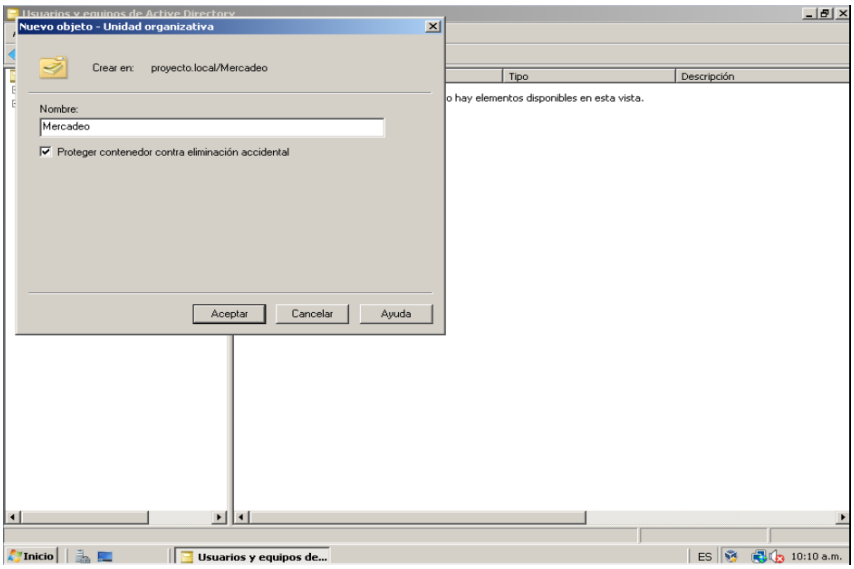


Figura 77 OU Gestión Humana

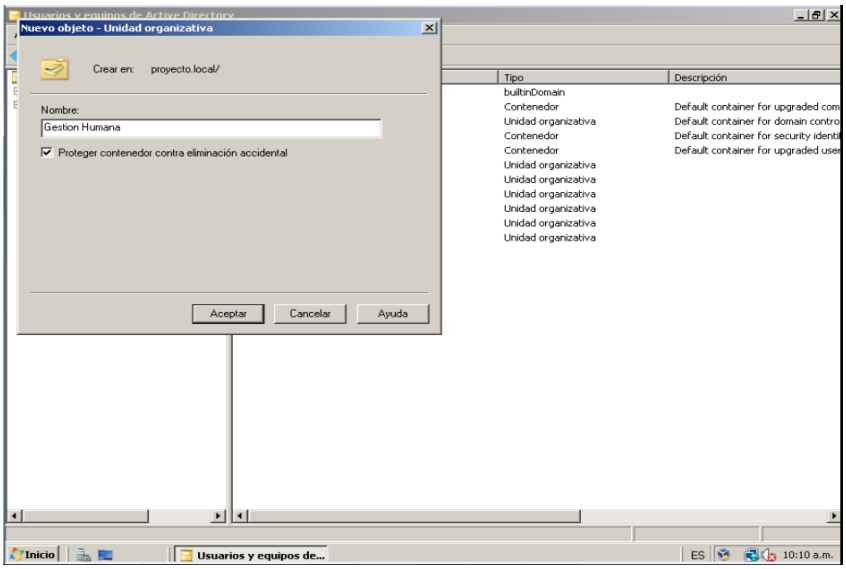
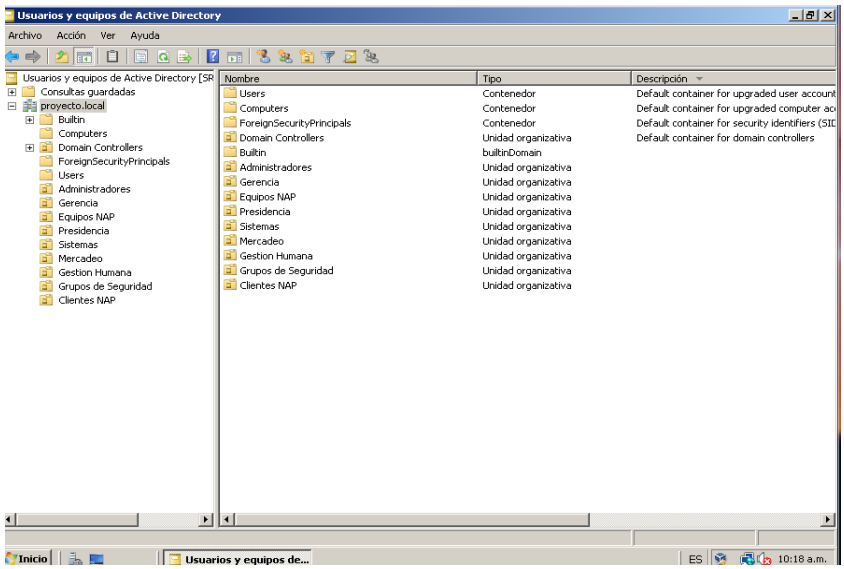


Figura 78 Segmentación Por OU



- ***Configuración de Directivas de Grupo***

Estas directivas permiten establecer reglas para controlar a los usuarios y maquinas as clientes que ingresan a la red.

Figura 79 GPO Prohibir propiedades de LAN

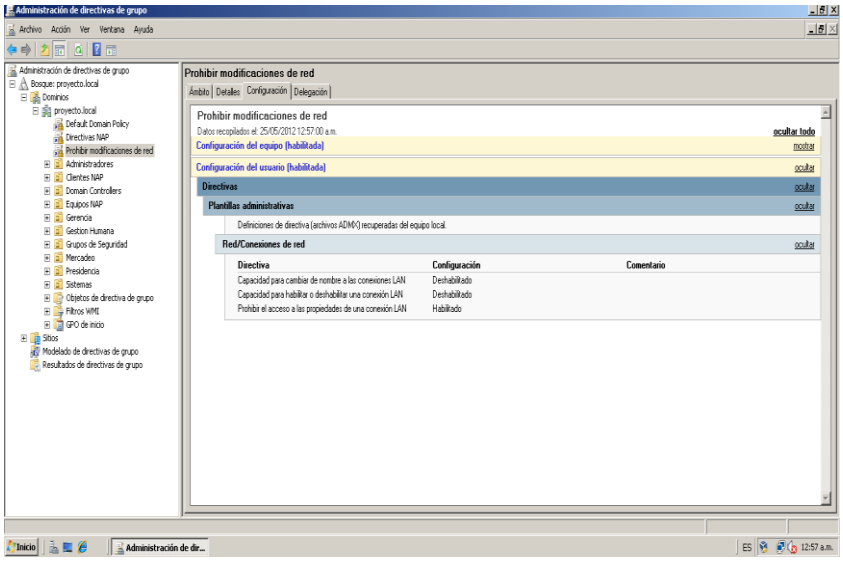
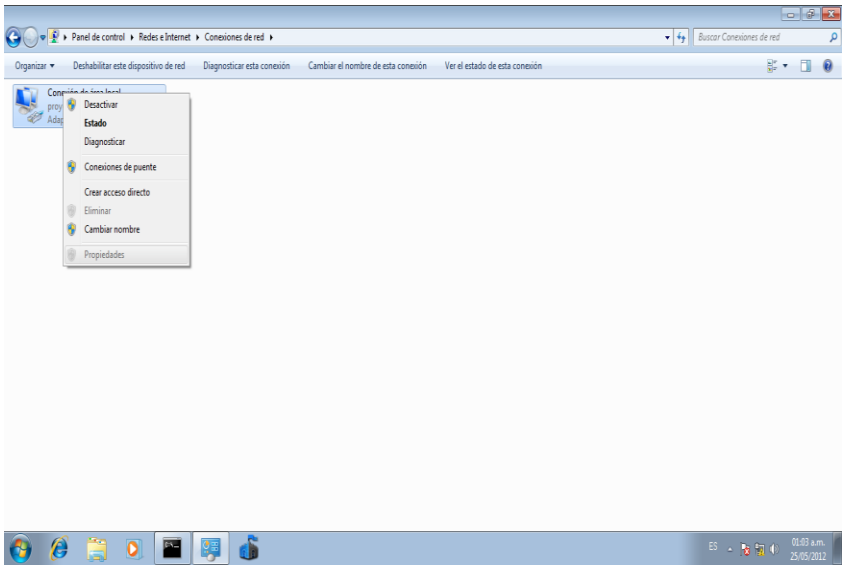
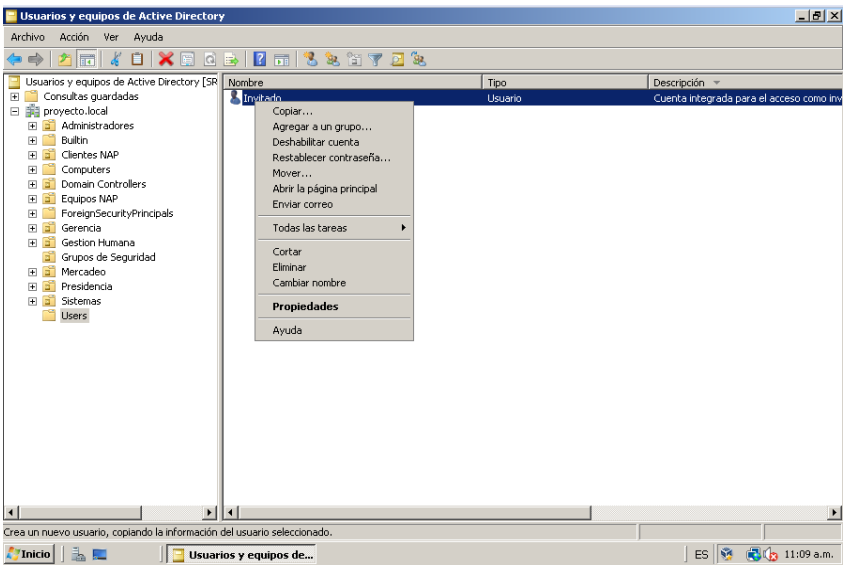


Figura 80 Propiedades de conexión LAN Prohibidas



- ***Desactivar las cuentas default o que no se usen***

Figura 81 Desactivación Cuenta Invitado



- ***Desactivar los servicios que no se usen (como DNS, COM+, etc.).***

Figura 82 Deshabilitar COM+

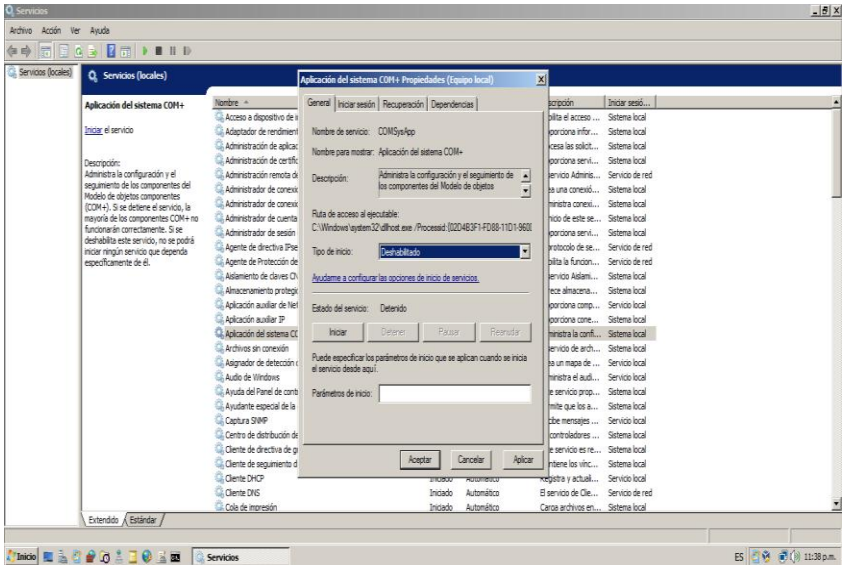
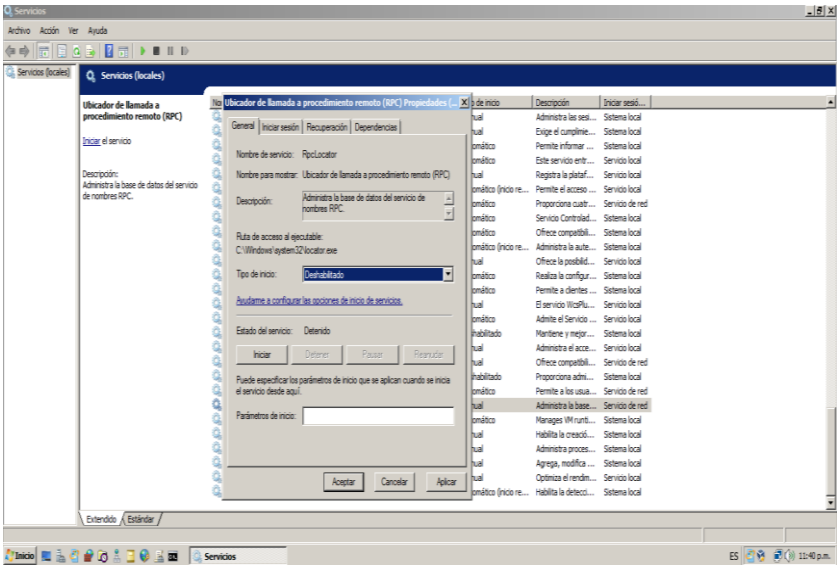


Figura 83 Deshabilitar RPC



- ***Activar NTP***

Este protocolo permite coordinar en la red la hora y fecha de los equipos para una correcta comunicación. Las siguientes figurasen el numeral Activar NTP muestran el proceso de configuración.

Figura 84 Ejecutar regedit

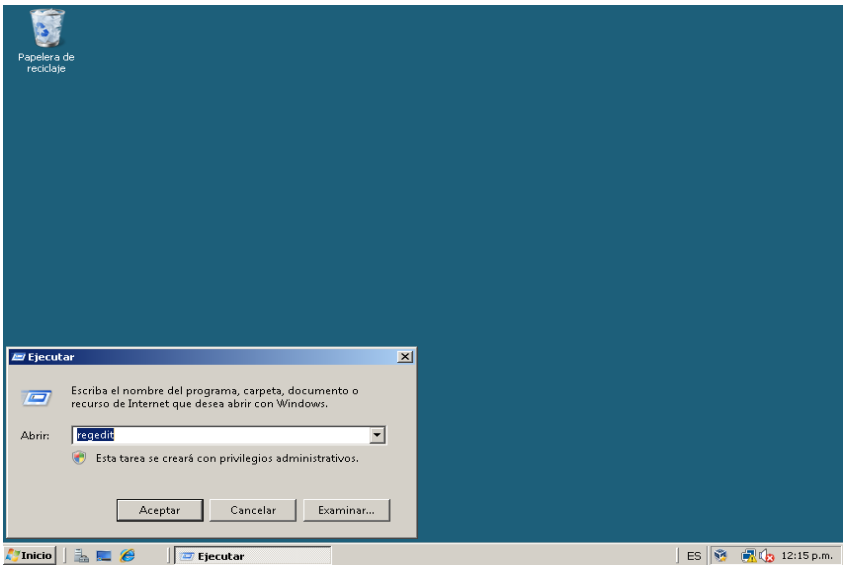


Figura 85 Editor de registro

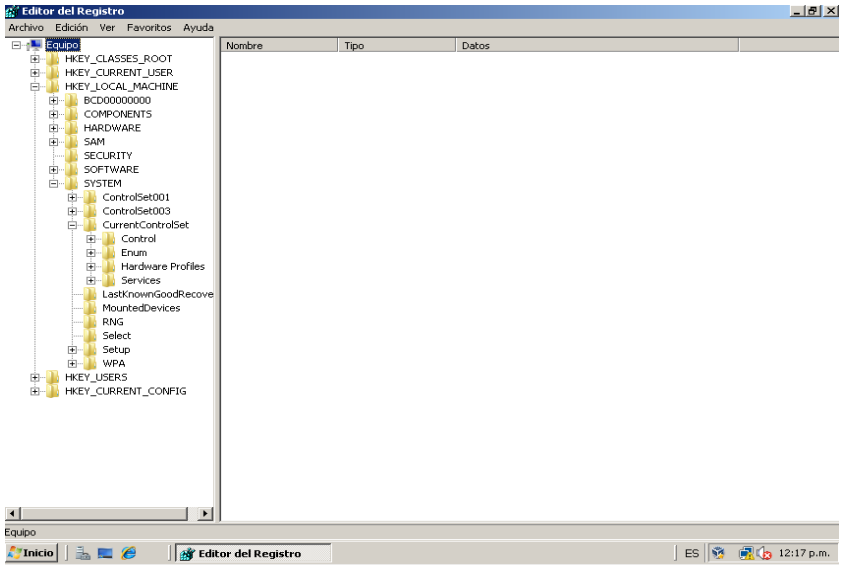


Figura 86 Servicio W32TIME

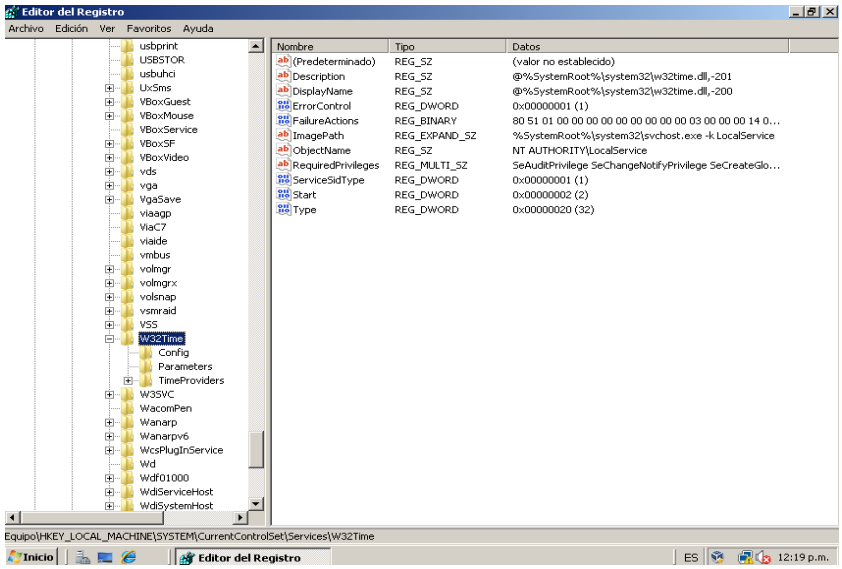


Figura 87 Tipo de servicio NTP

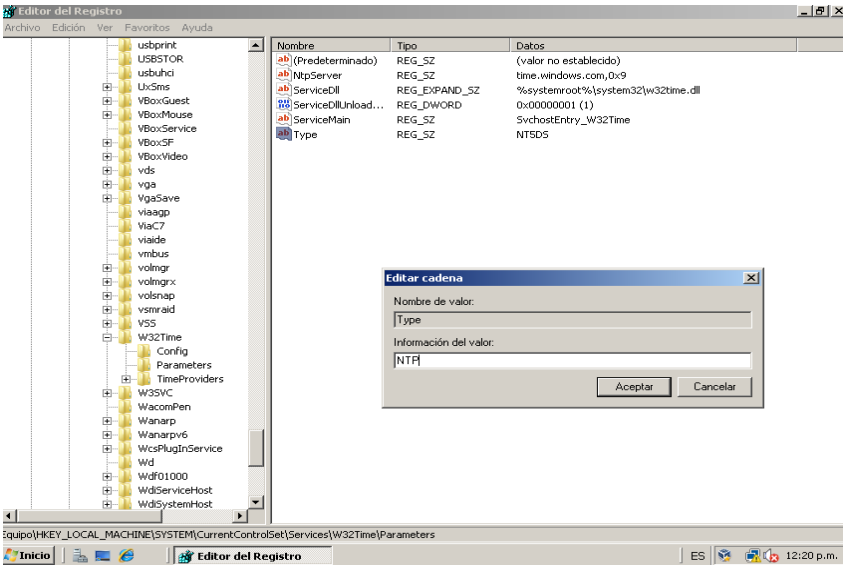


Figura 88 Annouce Flags NTP

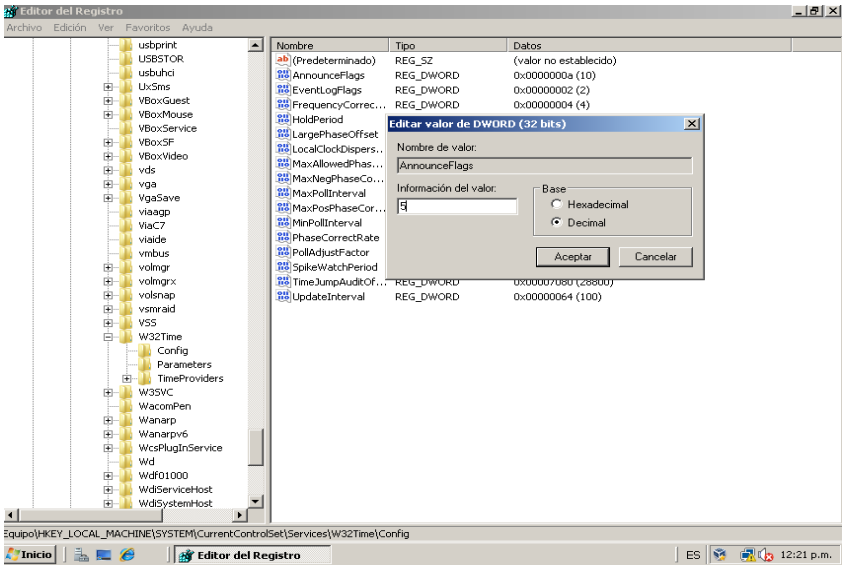


Figura 89 Activar NTP

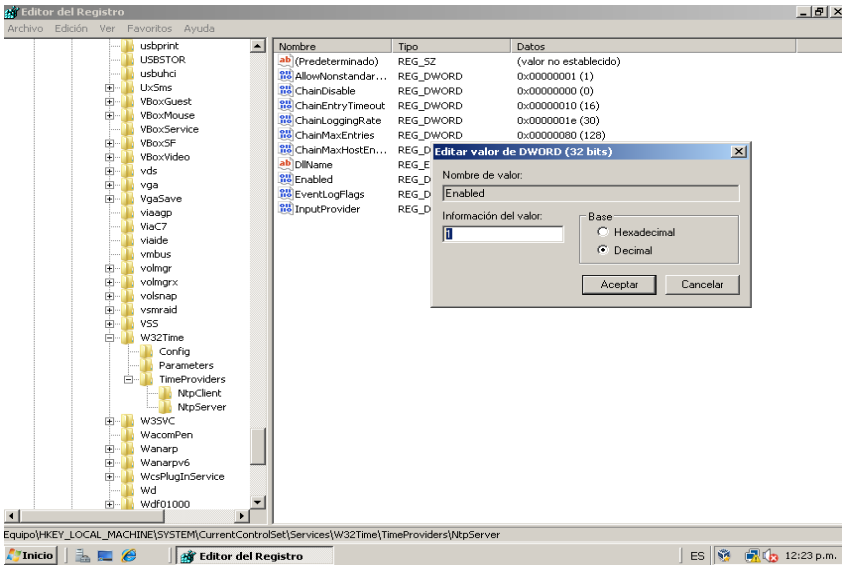


Figura 90 Dirección NTP Server

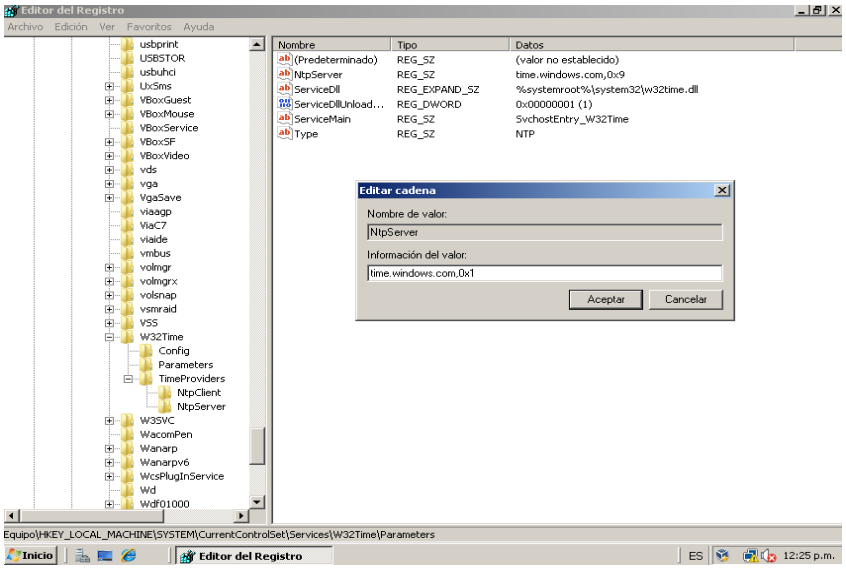


Figura 91 Special Poll Interval

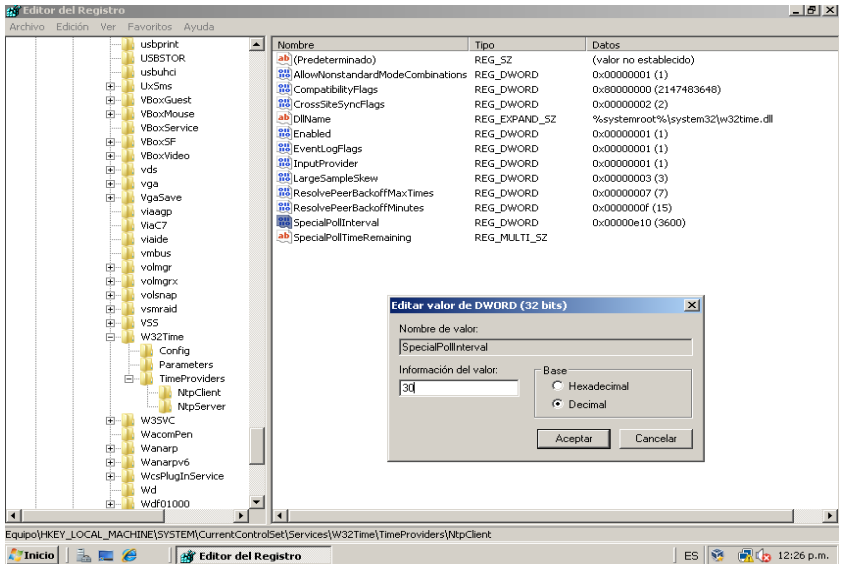


Figura 92 Max Pos Phase Correction

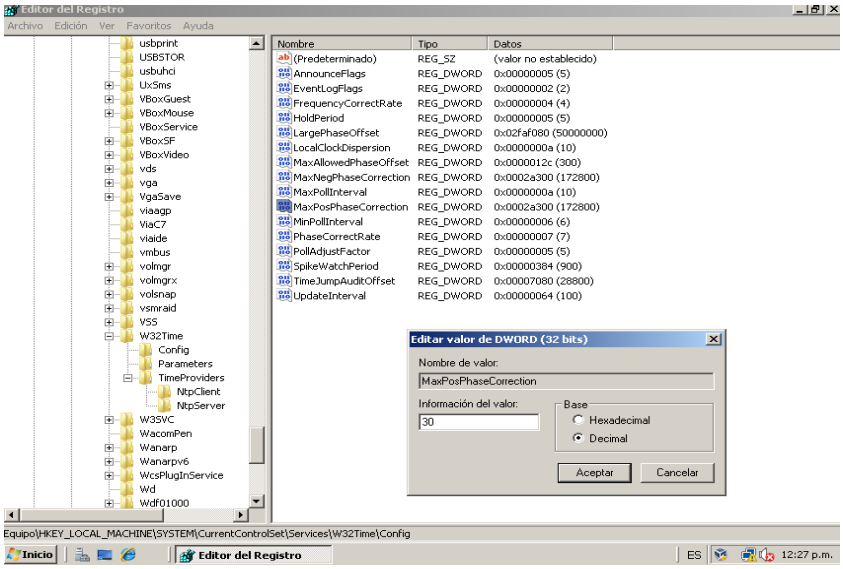


Figura 93 Max Neg Phase Correction

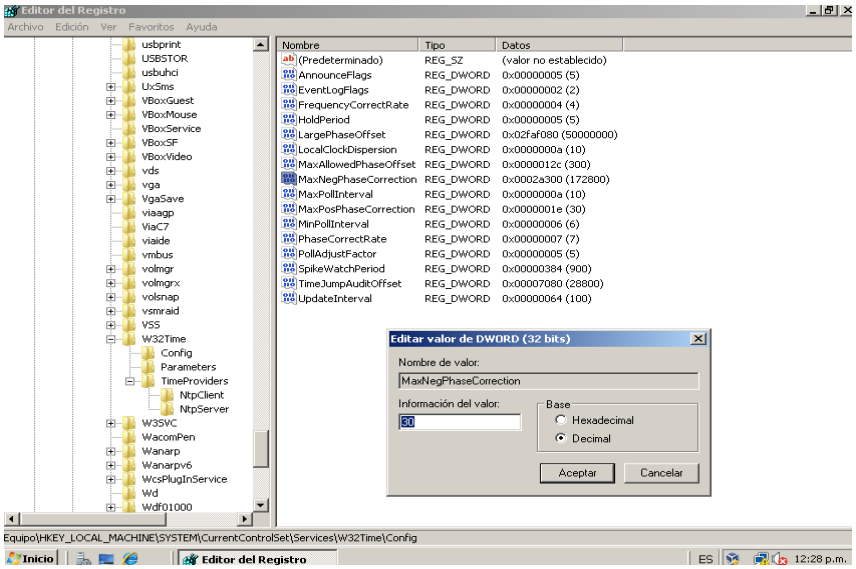
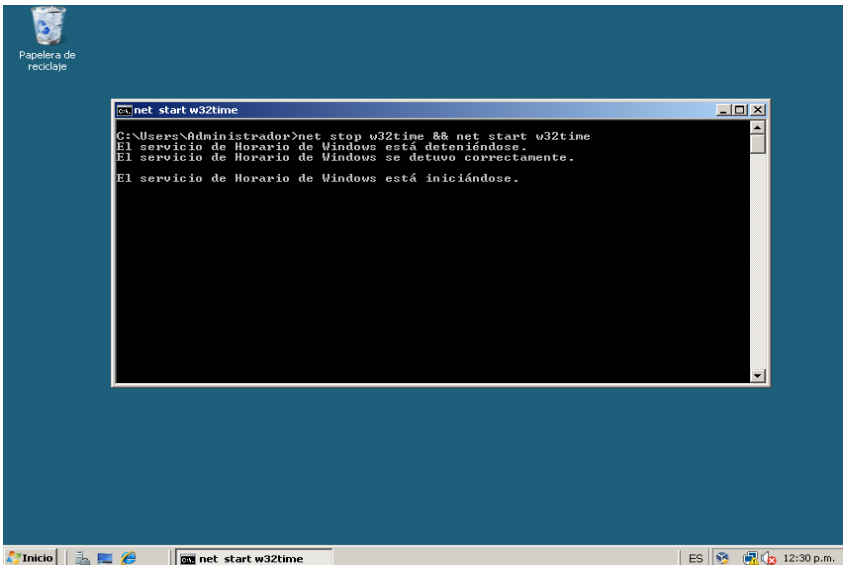


Figura 94 Detención e iniciación de W32Time



- ***Deshabilitar protocolos inseguros***

Figura 95 Bloqueo puerto FTP datos

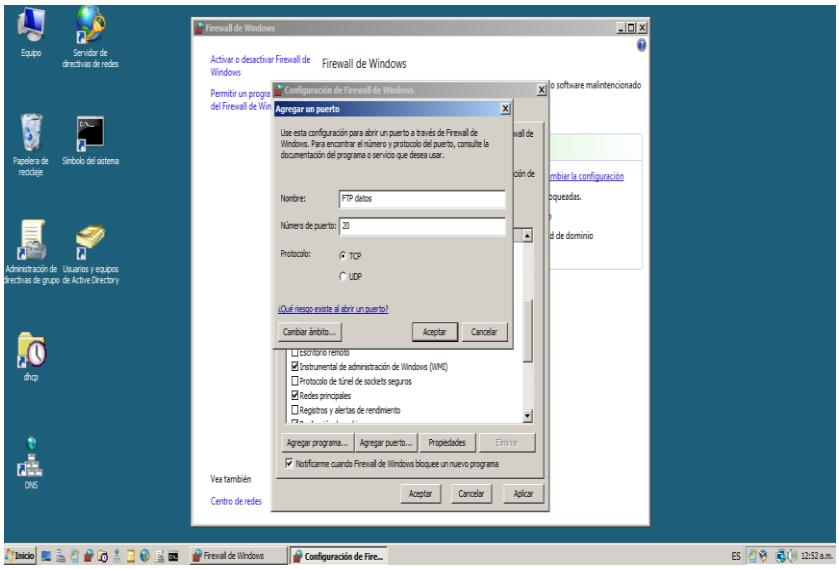


Figura 96 Bloqueo puerto FTP control

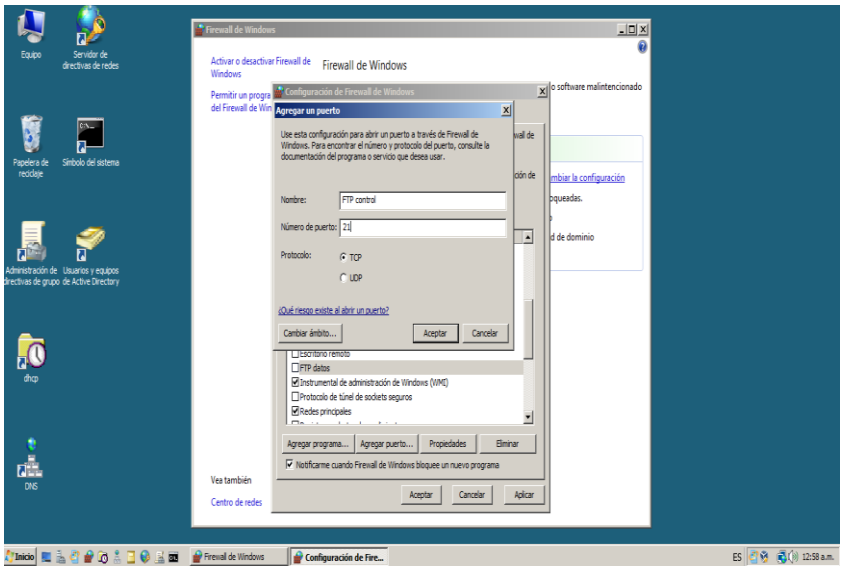
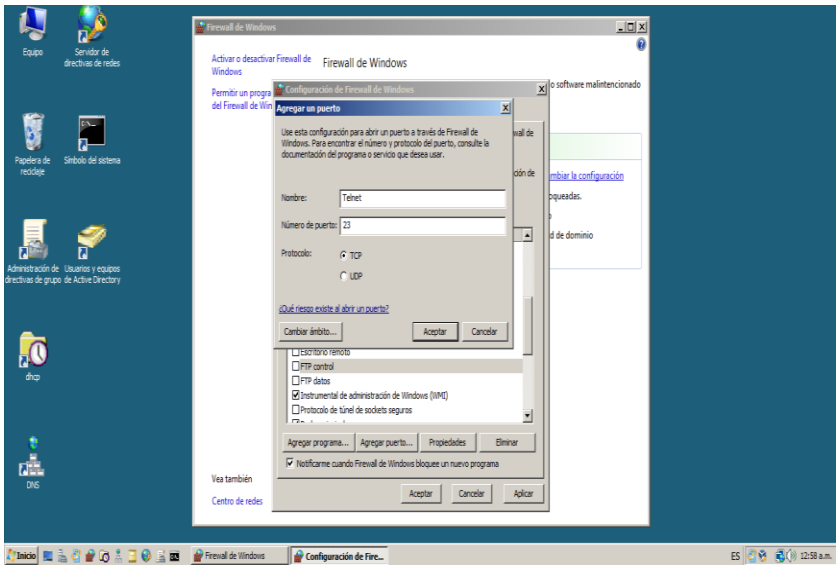


Figura 97 Bloqueo puerto Telnet



- ***Activar log de eventos***

Figura 98 Visor de Eventos

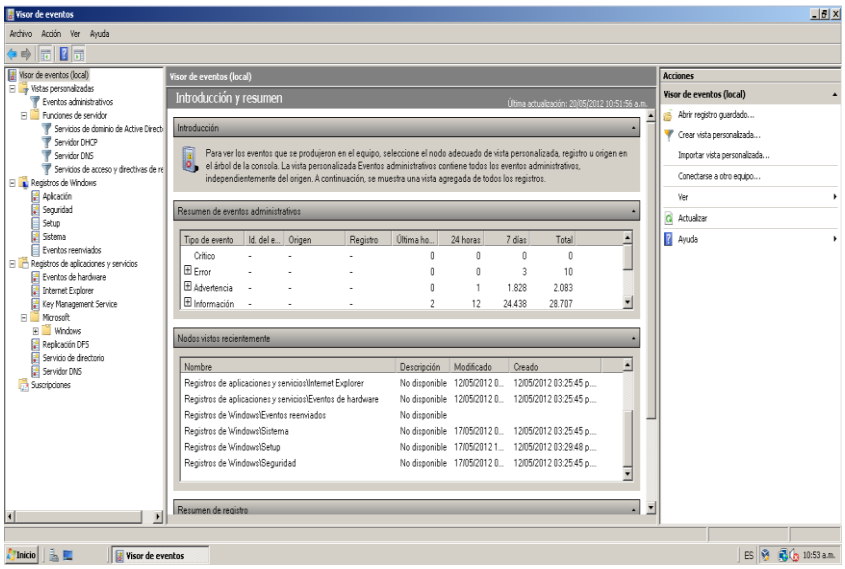


Figura 99 Sucesos servicios instalados

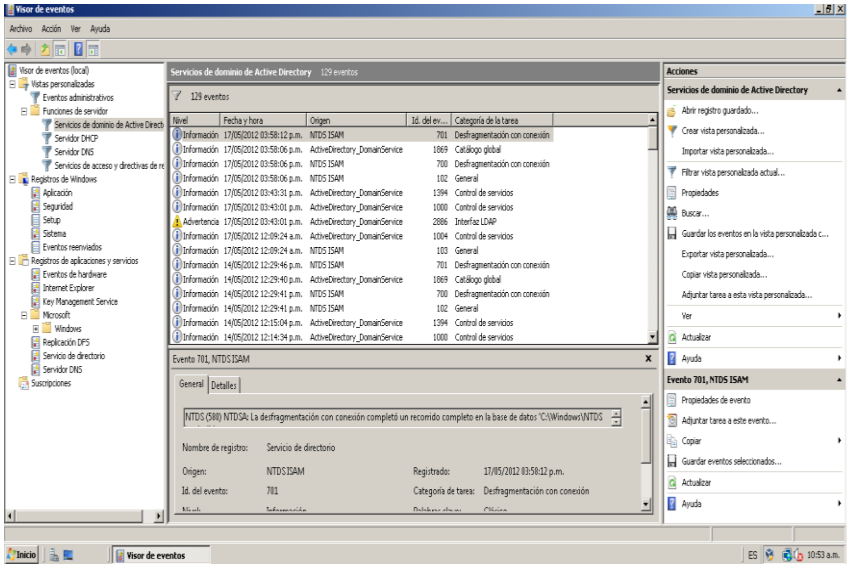
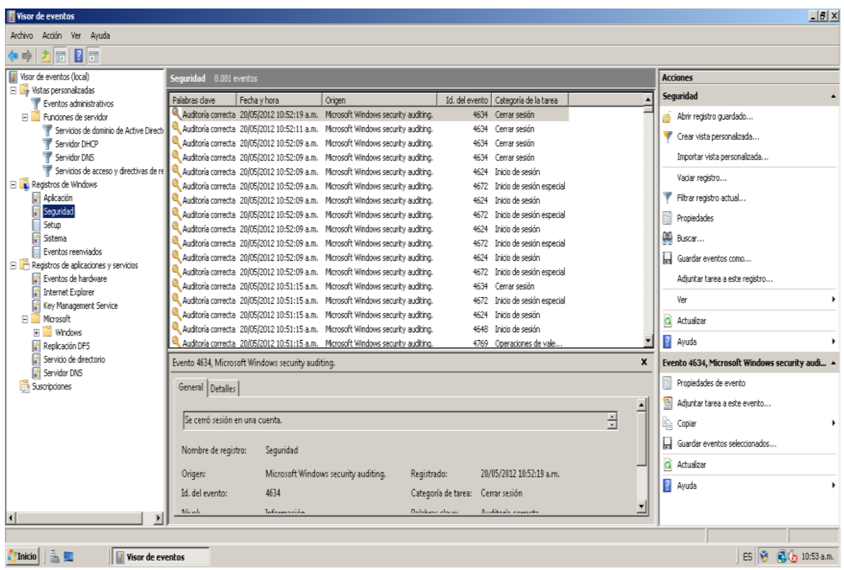


Figura 100 Sucesos de Seguridad



- ***Configuración del Firewall***

En las siguientes figuras se evidencia la configuración del firewall para que solo permita conexiones al servidor en los puertos permitidos.

Figura 101 Firewall de Windows

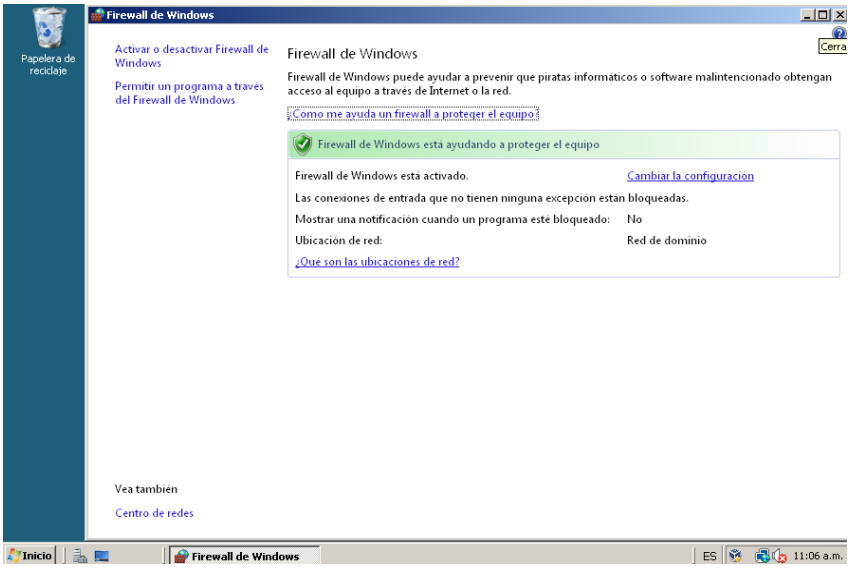


Figura 102 Excepciones en el Firewall

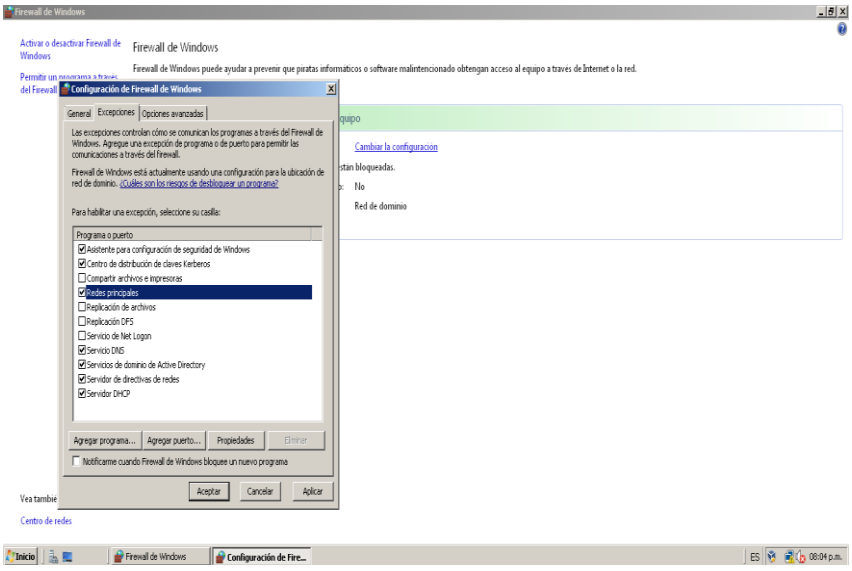
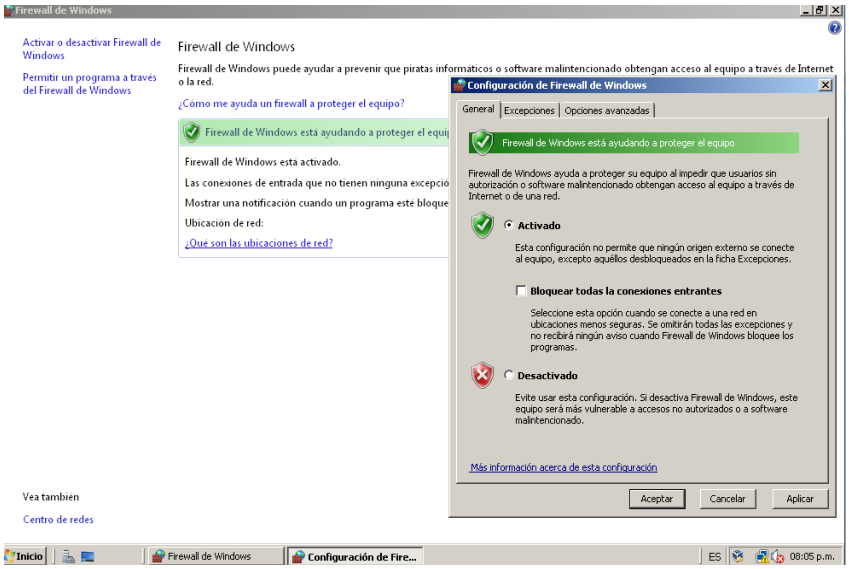


Figura 103 Firewall Activado



- ***Restringir el uso de los grupos Domain Admin, Enterprise Admin y Schema solo a personas autorizadas***

Figura 104 Administración Grupo Esquema

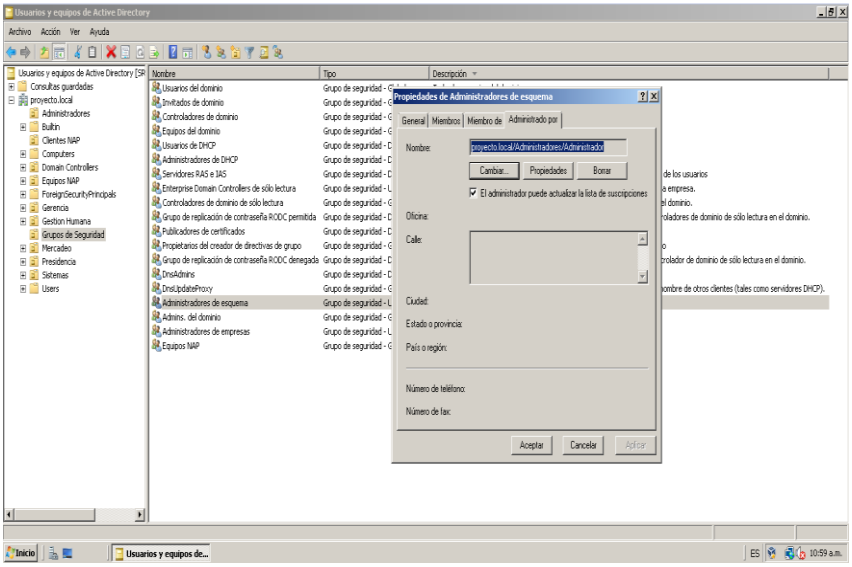


Figura 105 Administración Grupo del Dominio

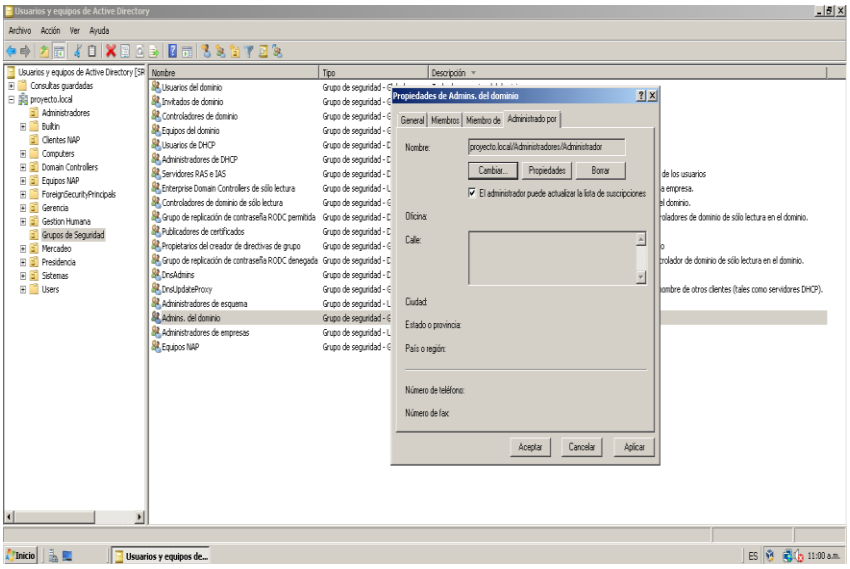
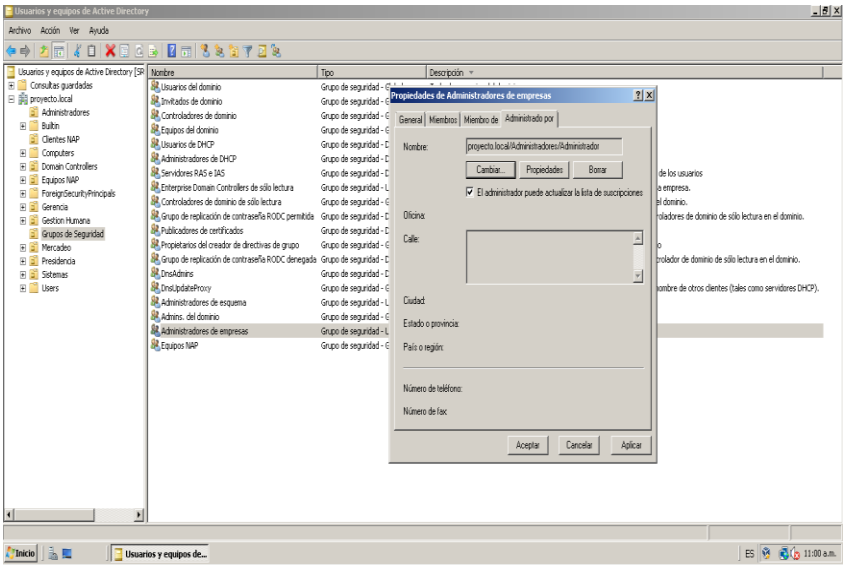


Figura 106 Administración de Grupo Empresa



- ***Bloqueo automático de sesión activada (a 5 minutos)***

Figura 107 GPO Proteger con contraseña

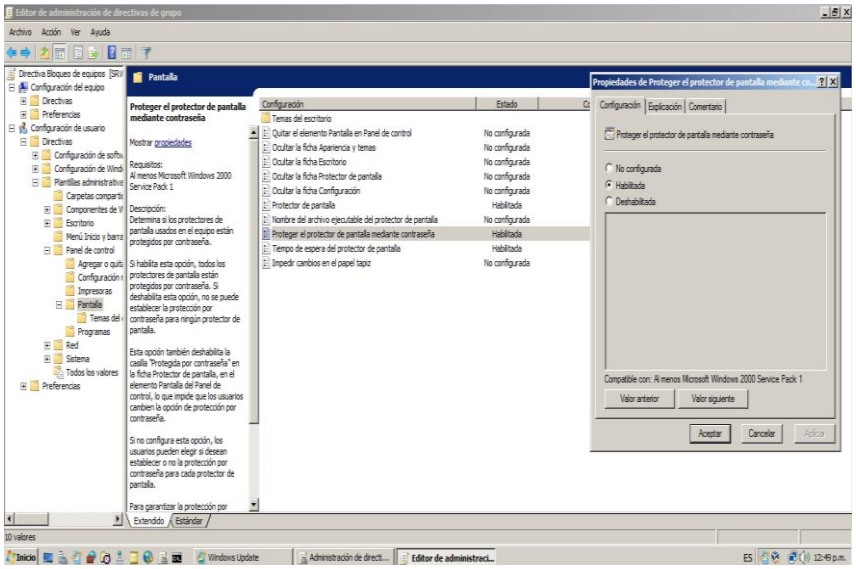


Figura 108 Activación del protector de pantalla

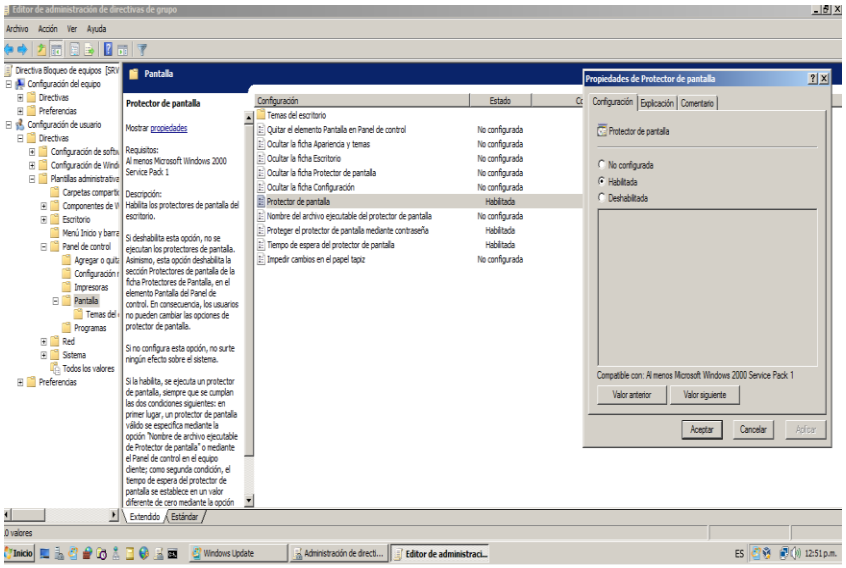
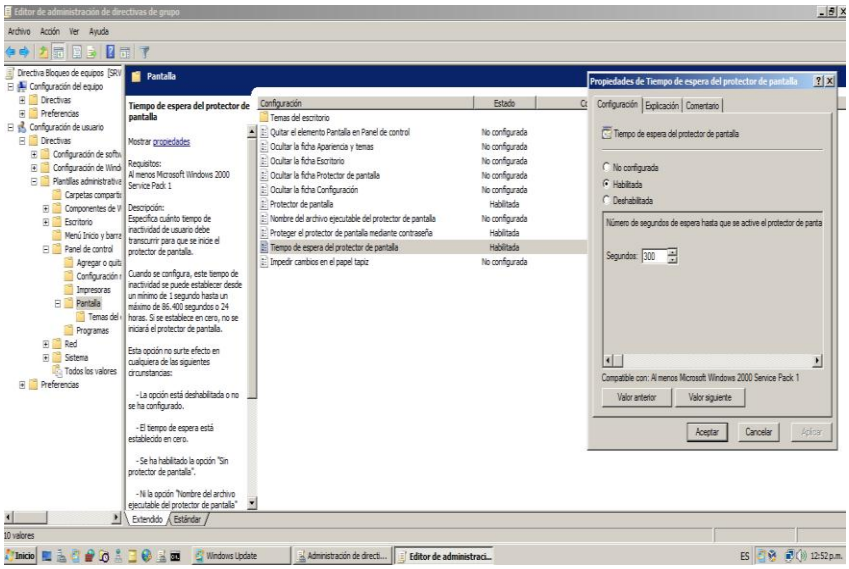


Figura 109 Tiempo de espera para bloquear equipo



- ***Configuración de password fuerte (mínimo 14 caracteres)***

Figura 110 Cambio de Contraseña

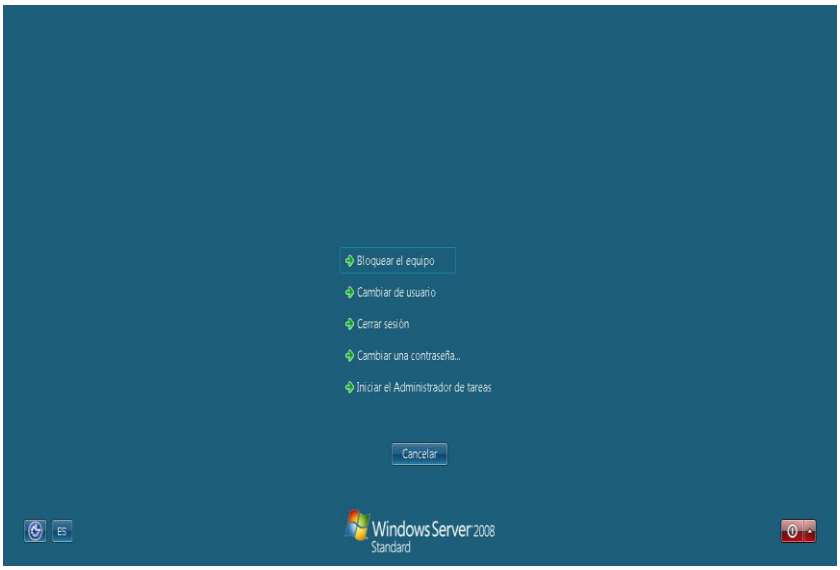
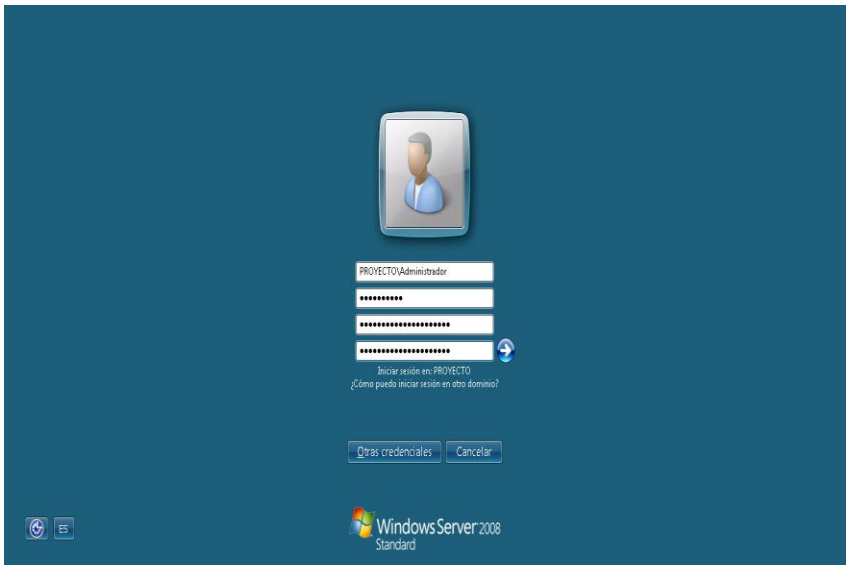


Figura 111 Nueva contraseña de administrador



8. PRESUPUESTO

8.1. Equipos y software

En este ítem se deben tener en cuenta los costos de licenciamiento del sistema operativo Windows server 2008 y los equipos que son requeridos.

DESCRIPCION	PRECIO COP
Windows Server 2008 Standard con 5 licencias cliente	1.807.770
Equipo de computo 8 GB de RAM, HDD 120 GB, Intel Corei7	1.700.000

- Tener en cuenta infraestructura de red ya implementada.

8.2. Costos de personal

- Este ítem involucra los procesos de instalación, configuración y puesta en marcha de la plataforma NAP y las configuraciones requeridas en los demás servicios de los cuales depende.
- Costo de personal: 700.000 COP

CONCLUSIONES Y RECOMENDACIONES

Network Access Protection provee formas de asegurar que cualquier equipo de computo que se conecte al dominio ya sea de forma cableada o inalámbrica y que reciba parámetros a través de DHCP, se acomode a las políticas definidas en el agente validador del sistema de seguridad de Windows, a través del servicio del agente NAP los equipos clientes estarán siendo monitoreados inclusive luego de obtener acceso a la red, lo que es una gran ventaja ya que esto permite mantener igual el nivel de seguridad en todo el transcurso de tiempo que los equipos se encuentren conectados a la red corporativa.

Con la implementación de Network Access Protection se obtiene poderosas herramientas para una compañía u organización que posea infraestructura de red y dominios basados en Windows, estas herramientas controlaran el acceso a la red, mitigaran en gran medida los contagios de virus u otro malware, también dificultaran el ingreso de intrusos o atacantes a los sistemas informáticos, además debido a que pueden existir servidores de remediación los clientes tendrán a su disposición actualizaciones y software que les permitirá solucionar su situación de no acceso a la red y luego de cumplir con los parámetros NAP el acceso será permitido nuevamente.

Es muy importante tener en cuenta a la hora de implementar las funciones de NAP las reglas que se configurase basan en tres estados posibles de los equipos clientes entre ellos están que el cliente no reconozca o no tenga instalado el cliente NAP por lo que no se le concederá acceso a la red ya que no hay manera de verificar si cumple con los requisitos de acceso a la red, por otro lado esta el cliente que reconoce NAP, y cumple los requerimientos por lo que tiene conectividad completa y por ultimo esta el cliente que reconoce NAP, y no cumple los requerimientos, si se puede remediar, pasaría a cumplir requerimientos y tendría acceso a la red, si no se puede remediar, queda restringido.

BIBLIOGRAFIA

- Miguel Ángel Álvarez. Que es un firewall. Disponible en: http://www.desarrolloweb.com/articulos/513.php El 17/05/12
- Definiciones ABC. Definición de antivirus. Disponible en: http://www.definicionabc.com/tecnologia/antivirus.php El 17/05/12
- Felipe Nieves Cruz. La Investigación Exploratoria. Disponible en: http://www.gestiopolis.com/canales7/mkt/investigacion-exploratoria-y-algunos-aportes-a-la-investigacion-de-mercados.htm El 27/05/12
- IETF. RFC 2131. Disponible en: http://www.ietf.org/rfc/rfc2131.txt El 27/05/12
- José M. Piquer. El DNS. Disponible en: http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html El 08/05/12
- Juanlu991. Como crear un servidor DHCP. Disponible en: http://2.bp.blogspot.com/_xpi2MxMdjek/TUcAYWIYOeI/AAAAAAAAAFo/lxb9ExTwNO8/s1600/servidor-dhcp.png El 15/05/12
- Juansa. Introducción a redes, Arquitectura Cliente/Servidor. Disponible en: http://www.juansa.net/Admin2003/cliser.htm El 08/05/12
- Linux-cd. Dominio Windows. Disponible en: http://linux-cd.com.ar/manuales/usando-samba/node17.html El 05/05/12
- Microsoft. Introducción técnica a Windows Server 2008. Disponible en: http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx El 14/05/12
- NewDevices. Protocolo DNS. Disponible en: http://www.newdevices.com/tutoriales/dns/images/1d.png El 15/05/12
- Oracle. VirtualBox. Disponible en: https://www.virtualbox.org/ El 14/05/12
- Ordenadores-y-Portátiles. ¿Qué es el *directorio activo* de Windows?. Disponible en: http://www.ordenadores-y-portatiles.com/directorio-activo.html El 08/05/12
- Scrib. Implementación de la estructura de una unidad organizativa. Disponible en: http://es.scribd.com/doc/86009669/11-Implementacion-de-La-Estructura-de-Una-Unidad-Organizativa El 15/05/12
- Technet. Introducción a NAP. Disponible en: http://technet.microsoft.com/es-es/library/dd759127.aspx El 10/03/12
- Technet. Protección de Acceso a redes. Disponible en: http://i.technet.microsoft.com/dynimg/IC233149.gif El 17/05/12
- Technet. Servidor de directivas de redes. Disponible en: http://technet.microsoft.com/es-es/library/cc732912.aspx El 09/05/12