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	
3. OBJETIVOS	11
3.1. GENERAL	11
3.2. ESPECIFICOS	11
4. JUSTIFICACION	
5. MARCO TEORICO	13
6. DISEÑO METODOLOGICO	25
6.1. TIPO DE INVESTIGACION	25
6.2. PROCESO	25
7. IMPLEMENTACION	
7.1. ANTECEDENTES	
7.2. MONTAJE	
8. PRESUPUESTO	80
8.1. Equipos y software	80
8.2. Costos de personal	
CONCLUSIONES Y RECOMENDACIONES	
BIBLIOGRAFIA	

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 3	39 Creación de usuario 2	43
Figura 4	0 Grupo de seguridad NAP	43
Figura 4	1 Método NAP	44
Figura 4	2 Servidores de Cumplimiento	44
Figura 4	I3 Ámbito DHCP en el NPS	45
Figura 4	14 Configurar Grupo	45
Figura 4	I5 Selección grupo NAP	46
Figura 4	l6 Servidores de remediación	46
Figura 4	17 Directivas de mantenimiento	47
Figura 4	l8 Resumen de configuración NAP en NPS	47
Figura 4	19 Validador de mantenimiento	48
Figura 5	50 Configuración de Validador de mantenimiento	48
Figura 5	51 Requisitos para equipos cliente	49
Figura 5	52 Propiedades ámbito DHCP	49
Figura 5	53 Ámbito DHCP para NAP	50
Figura 5	54 Dominio Restringido	50
Figura 5	55 Estado del Agente NAP	51
Figura 5	56 Firewall activado - Windows Update Automático	51
Figura 5	57 Antivirus/Antispyware Instalado y Activado	52
Figura 5	58 Desactivación de MSE	52
Figura 5	59 Estado de riesgo del Equipo	53
Figura 6	0 Dominio restringido.proyecto.local	53
Figura 6	31 Acceso a la red limitado	54
Figura 6	62 Activación de Seccurity Essentials	54
Figura 6	33 Acceso completo a la red	55
Figura 6	64 Dominio proyecto.local	55
Figura 6	65 Preparando Instalación de Actualizaciones	56
Figura 6	6 Actualizaciones Disponibles	56
Figura 6	37 Configurando Actualizaciones	57
Figura 6	88 Windows esta Actualizado	57
Figura 6	39 Instalar Actualizaciones Automáticamente	58
Figura 7	70 Usuarios y Equipos de AD	58
Figura 7	71 OU Administradores	59
Figura 7	2 OU Gerencia	59
Figura 7	73 OU Equipos NAP	60
Figura 7	74 OU Presidencia	60
Figura 7	75 OU Sistemas	61
Figura 7	76 OU Mercadeo	61
Figura 7	7 OU Gestión Humana	62
Figura 7	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	
Figura 87 Tipo de servicio NTP	67
Figura 88 Annouce Flags NTP	67
Figura 89 Activar NTP	
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	
Figura 94 Detención e iniciación de W32Time	
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	
Figura 106 Administración de Grupo Empresa	
Figura 107 GPO Proteger con contraseña	77
Figura 108 Activación del protector de pantalla	77
Figura 109 Tiempo de espera para bloquear equipo	
Figura 110 Cambio de Contraseña	
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?

¹Pablo Campos. NAP Con dhcp paso a paso. Disponible en:

http://pacampos.wordpress.com/2008/02/06/nap-con-dhcp-paso-a-paso/ EI 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/Servidor²

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

• VirtualBox³

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 2008⁴

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 Directory⁵

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 Unit⁶

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

⁶Ordenadores-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 Windows⁷

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.





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

• DNS⁸

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/usandosamba/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

• DHCP⁹

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.

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

⁹IETF. RFC 2131. Disponible en: http://www.ietf.org/rfc/rfc2131.txt EI 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/AAAAAAAAAAFo/lxb9ExTwNO8/s1600/servi dor-dhcp.png EI 15/05/12

5.2. Conceptos De Seguridad

• Firewall¹⁰

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.

• Antivirus¹¹

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 redes¹²

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

¹²Technet. Servidor de directivas de redes. Disponible en: http://technet.microsoft.com/eses/library/cc732912.aspx El 09/05/12

¹³ Technet. Introducción a NAP. Disponible en: http://technet.microsoft.com/eses/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 EXPLORATORIA¹⁴

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.

http://www.gestiopolis.com/canales7/mkt/investigacion-exploratoria-y-algunos-aportes-a-la-investigacion-demercados.htm El 27/05/12

¹⁴ Felipe Nieves Cruz. La Investigación Exploratoria. Disponible en:

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

TÉRM MICR	INOS DE LA LICENCIA DE LA VERSIÓN PRELIMINAR DEL SOFTWARE DE DSOFT	-
MICR	DSOFT WINDOWS SERVER 2008 RC	
Los té de dor Son di los so serán	rminos de esta licencia son un contrato entre Microsoft Corporation (o, en función ide viva, una de las sociedades del grupo) y usted. Sírvase leerlos detenidamente, a palicación a la versión preliminar del software arriba mencionado, el cual incluye portes en los que lo haya recibido, en su caso. Estos términos de licencia también de aplicación a los siguientes elementos de Microsoft:	
•	Actualizaciones.	
	Suplementos.	
	Servicios hasados en Internet	

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

Figura 8 Versión a Instalar

Sistema operativo	Arquitectura	Fecha de mo
Windows Server 2008 Standard (instalación completa)	X86	19/01/2008
Windows Server 2008 Enterprise (instalación completa)	X86	19/01/2008
Vindows Server 2008 Datacenter (instalación completa)	X86	19/01/2008
Windows Server 2008 Standard (instalación Server Core)	X86	19/01/2008
Windows Server 2008 Enterprise (instalación Server Core)	X86	19/01/2008
escripción: ita opción ejecuta la instalación completa de Windows Serve e usuario en su totalidad y admite todas las funciones del ser	er. Esta instalación rvidor.	incluye la interfaz

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

Insta	alling Windows	
That's install	s all the information we need right now. Your computer will restart several times during ation.	
J C	opying Windows files xpanding Windows files	
In	stalling features stalling updates	
G	ompleting installation .	



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



Figura 12 Primer Inicio de Sesión



Administration de servider (SKH MARCI) Administration de servider (SKH MARCI) De concert De concert <th>Administrador del servidor</th> <th></th> <th></th> <th>د</th>	Administrador del servidor			د
Notice is interested at distance (RNNAND) Anisotradia de servidor (SNNAND) Concretivitas is production (RNNAND) Configuration (RNNAND)	rdzivo Acción Ver Ayuda			
Aministrative del servider (SRV4491) Cariga información general del servidor (SRV4491) Cariga informacin general del servidor (SRV4491) Cariga información ge				
Resumes de servidores	Administrador del servidor (SRV-NAPO1) Características Dispróstico Configuración Almacenamiento	Administrador del servidor (SRV-IAP01) Cotenga información general del estado del servidor, n	aakce tareas principales de administración y agregue o quite funciones y características d	e servidor.
Información del equipo III Contrar propeidade or superior de equipo: SEV 44011 Gues de trabajo: UICXXXXX.02 IIII COXXXXX.02 Concersin de feas local: SEX 44001 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		🔿 Resumen de servidores		Ayuda de resumen de servidores
Grand et handen: III/CR002/E Carevanis de lans back: 1925 1832 100, 1944 habitado Excitario remoto: Derhabitado Excitario remoto: Derhabitado Id. del producto: 9.5577 CGH-752055-27517 Il. go contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar assoln Image: Contrar esta carevalo el incar esta carevalo el incarexitar esta carevalo el incar esta carevalo el incar esta		 Información del equipo Nombre completo de equipo: 	SRV444P01	 Cambiar propiedades del sistema Ver conexiones de red Configurar Escritorio remoto
Bottmin remde: Derkallabab Id. del producti: 9:5373-059-755295 Imformación de segundad Imformación de segundad Freeval de Vindone: Activado Actualizaciones de Vindone: São de casagor actualizaciones, mediante Vindones Lipítante Ultimas actualizaciones interibuirade: 3004/201210-273 a.m. Orninguar ECC de Internet: Activado para actualizaciones interibuiradores interibuirador		Grupo de trabajo: Conexión de área local:	WORKGROUP 192. 168.92.100, IPv6 habilitado	
☐ Igs mother ends cannols di hidar sessin Imformación de seguridad Imformación de seguridad Pressil de Vindous: Activado Actuatización de seguridad Imformación de seguridad Unne actuatización de seguridad Imformación de seguridad Unne actuatización de seguridad 30/4/2012 201-27 a.m. Configura de Indoue Activado para administratores Activado para subministo Configura de la EXIC de Internet Explore: Activado para subministo		Escritario remoto: Id. del producto:	Deshabiltada 92573-0EM-7502905-27517	
Información de segundad Fresul de Vindous: Activado Fresul de Vindous: Activado Acti		🗌 No mostrar esta consola al iniciar sesión		
Presa de introloci: Actualaciones de l'intoloci: Stote desarror actualizaciones, mediante l'inclueus Lipitate Configurationes instalaciones Configurationes instalaciones Configurationes instalaciones Configurationes instalaciones Configurationes instalaciones Configurationes instalaciones Configurationes Configurati		Información de seguridad		🔐 Ir a Firewall de Windows
Ultimes actualizaciones buscudas: 30)44/2012 01-07 a.m. Configurado de regar Ultimes actualizaciones instaladas: 30)44/2012 10-07 a.m. Configurado de regar Configurado de segunidad regionale (SIC) de Internet Activade para susminos Resument de funcciones Activado para susminos Activado para susminos		Actualizaciones de Windows:	Activado Solo descargar actualizaciones, mediante Windows Update	fg Buscar nuevas funciones Ejecutar Asistente para
Utime actualizatione refaisales: 30(4/2022 0x3 a.m. Configuración de seguridad nejorada (ESC) de Internet: Activada para administradores Explorer: Activada para susarrios Or Resamen de funciones: I Avuda de Resamen de		Últimas actualizaciones buscadas:	30/04/2012 01:47 a.m.	configuración de seguridad
🙃 Resumen de funciones 🔢 Ayuda de Resumen de		Ultimas actualizadones instaladas: Configuración de seguridad mejorada (ESC) de Internet Explorer:	30/04/2012 10:23 a.m. Activada para administradores Activada para usuarios	
		C Resumen de funciones		Ayuda de Resumen de funciones
⑦ Funciones: Receptor do datos		💮 Funciones: Recoplando datos		Ir a Fundones

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.





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

Comp L la	Datibilidad de sistema operativo Las mejoras en la configuración de seguridad en Windows Server 2008 afectan a las versiones anteriores de Windows
4	Los controladores de dominio de Windows Server 2008 tienen un diseño predeterminar más seguro para la configuración de seguridad llamada "Permitir algontmos de cifrado de Windows NT 4.0." Esto impide que los "clientes" de Microsoft Windows y los de no- Microsoft SMB usen estilos más vulnerables de algontmos de cifrado de NT 4.0 al establecer las sesiones del canal de seguridad con los controladores de dominio de Windows Server 2008. Como resultado, es posible que haya problemas en algunas operaciones o aplicaciones que necesiten un canal de seguridad atendido por los controladores de dominio de Windows Server 2008. Este cambio afecta a las plataformas de "clientes" de Windows NT 4.0, también las de no-Microsoft SMB y los dispositivos de red de almacenamiento conectado directamente (NAS) que no son compatibles con algontmos de cifrado menos vulnerables. Algunas operaciones en los clientes que ejecuten versiones anteriores a Windows Service Paci 1, se verá nafectadas, incluyendo operaciones de unión a un dominio que ejecute la Herramienta de migración para Active Directory o los Servicios de implementación de Windows . Para más información, lea el artículo 942564 en Knowledge Base
	< <u>Atrás</u> Squiente > Cancela

Figura 17 Configuración de Implementación

C Bosq	ue existente
C	Agregar un co <u>n</u> trolador de dominio a un dominio existente
C	Cr <u>e</u> ar un dominio nuevo en un bosque existente
	Este servidor se convertirá en el primer controlador de dominio del nuevo dominio.
G Coor	
Más infor	mación acerca de las posibles configuraciones de implementación

Figura 18 Nombre del Dominio

igne un nombre al dominio raíz del bosque	113
El primer dominio del bosque es el dominio raíz del bosque. Su nombre también es el nombre del bosque.	
Escriba el nombre de dominio completo (FQDN) del nuevo dominio raíz del bosque.	
EQDN del dominio raíz del bosque:	
proyecto.local	

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.

Antes de comenzar Funciones de servidor	Seleccore una o más funciones para instalar en este servidor. Bundones:	Descripción:
Erisore de conexión de red Configuración CRG IPv4 Configuración WENS IPv4 Ámbitos DHCP Modo en estado DHCPv6 Configuración CRS IPv6 Configuración CRS IPv6 Configuración CRS IPv6 Configuración CRS IPv6 Configuración	Active Directory Kighta Management Services Services de acceso y directivas de refeis Services de Certificate Server de Active Directory Services de directorio ligen de Active Directory Services de directorio ligen de Active Directory Services de forteración de Active Directory Services de Inglementación de Windows (WDS) Services (DDC) Services de Inglementación de Windows (WDS) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Services (DDC) Windows Server Update Services. Misinformación acerca de las funciones de sensitor	optioursooth disense de large prospontane de forma centralizada directiones Ptempontes e información relacionada para equipos cliente.

Figura 19 Selección de Servicios

Se seleccionan las características DHCP para su posterior instalación.

Figura 20 Introducción DHCP

Asistente para agregar funciones	5
Servidor DHCP	
Antes de comenzar Funciones de servidor Servidor DHCP Enlaces de conexión de red Configuración DNS IPv4	Introducción al servidor DHCP El Protocolo de configuración dinámica de host permite a los servidores asignar, o conceder, direcciones IP a equipos y otros dispositivos que están habilitados como clientes DHCP. La implementación de un servidor DHCP en la red proporciona a los equipos y otros dispositivos de red basados en TOP/IP directones IP válidas así como los parámetros de configuración adicionales que estos dispositivos necesitan, denominados opciones de DHCP. Esto permite a los equipos y dispositivos conectarse a otros recursos de red, como servidores DNS, servidores WINS y enrutadores.
Configuración WINS IPv4	Cosas que hay que tener en cuenta
Ámbitos DHCP	Debe configurar al menos una dirección IP estática en este equipo.
Modo sin estado DHCPv6 Configuración DNS IPv6 Confirmación Progreso Resultado	Antes de instalar el servidor DHCP, debe planear las subredes, los ámbitos y las exclusiones. Guarde un registro del plan en un lugar seguro para poder consultarlo en el futuro. Información adicional Introducción al servidor DHCP. Definición de ámbitos DHCP Integración de DHCP con DNS
	< Agterior Siguiente > Instalar Cancelar



Figura 21 Enlaces de conexión de red

Figura 22 Configuración servidor DHCP

_ 🗆 🗵 Papelera de recidaje Especificar la configuración del servidor DNS IPv4 Cuando los clientes obtienen como las direcciones IP de los especifique aquí se aplicará a proporcionarseles opciones i iario. La configuración que Funciones de servido s DNS y el r Servidor DHCP Enlaces de co Especifique el nombre del dominio p se usará para todos los ámbitos qu lominio primari de unic m yecto.local Ámbitos DHCP Modo sin estado DHCPv6 Configuración DNS IPv6 Autorización del servidor DHC Especifique las direcciones IP de los servidores DNS que usarán los clientes para la reso Estos servidores DNS se usarán para todos los ámbitos que cree en este servidor DHCP Dirección IPv4 10.0.2.15 Validar izar la Dirección IPv4 del servidor DNS alternativo ación acerca de la configuración del servidor DNS < Anterior Siguiente > Installer Canceler 🖉 Inicio 🛛 🚠 🗮 🔯 🌈 🛛 🚠 Administrador del ser... | ES 🐧 🕄 🏠 03:41 p.m.

Figura 23 Ámbito DHCP

1	🔒 Administrador del	servidor		
<u> (</u>	Archivo Acción Ve	Asistente para agregar fu	ciones X	
Papelera de recidaje		🧗 Agregar o	editar ámbitos DHCP	
	Servicio di Servicio	Antes de comenzar Fundames de servidor Servidor DHCP Enlaces de conesión de r Configuración DNS IPv4 Configuración DNS IPv6 Antotos DHCPv6 Configuración DNS IPv6 Autorización DNS IPv6 Autorización del servidor	Un dirible se intervisi de posibles directores IP pars van et 5. Servidor XHC no puede distribuir Agregar antibuir Un dirible se un intervisi de posibles directores IP pars van et 6. Servidor CHC no puede distribuir directores IP also cleates hata quese orieu antibuis. Northere de infetite: Part IVP Directorin IP modi: Directorin IP mod	
		Confirmación	Prestar a de subrec: 20020.200	
		Resultado	Tipo de subred: Cableado (la duración de la concesión ser 💆 arantzar la	
			V Active sets anoto Active sets anoto Canceler	
	<u>.</u>		Mis nformadin acera (e la aktiri de inibite ktirition.org https://www.contention.org <a <="" a="" href="https://www.contention.org"> <a href="https://www.conten</th><th></th>	
灯 Inicio 🛛 🚠 💻 🖥	🛙 🏉 🕌 Administr	ador del ser		ES 😚 👼 🏠 03:42 p.m.

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



Servicios de Servicios de Antes de comenzar Servidor DN Funciones de servidor Servidor weight de servidor	Para instalar las siguientes funciones, servicios de función o características, haga dic en Instalar. (i) I menage informativo a continuación	
a de constances a service unu d'activation de red configuración molto de la configuración molto de la configuración molto de la configuración molto de la configuración de la configuración molto de la configuración d	Configuration (Configuration (C	stores



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

12	🚡 Administrador del	servidor		_ 🗆 🗙
	Archivo Acción Ve	Asistente para agregar funciones		
Papelera de reciclaje	♦ ♦ I Administrader del si P P Funcones	Progreso de la ins	talación	
	□ Duccone: □ □	Antes de corretaria Par Luiar es de sen vido Servicios de acceso y or estivas d Servicios de fancián Confirmado Program Resultado	Se están instalando ao siguientes funciones, servidos de función o canacterísticae: Servicios de acceso y directivos de nedes	fundanes fundanes y bacquedas ko de Active
Vince in = (Administra	ader del ser.	Disatando la instalación	rdán ján ES Spor (5 0435 p.m.

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

.00	🖉 🗭 🕨 Panel de control 🔸 Sistema y seguridad 🕨 Sistem	na	
Ve ce @ Ac @ re @ Pr @ Cc sis	Propiedades del sistema Cambios en el dominio o el nombre del equipo Puede cambiar el nombre y la petenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red. <u>Más</u> rfomación Nombre de equipo: CLIENTE-NAP Nombre completo de equipo: CLIENTE-NAP Más Membro del © Dominio:	equipo o	quipo Reservados todos los del sistema no está disponible mV2 DualCore OL-66 - 210 GHz
Ve Ce W Int ren	Aceptar Cancelar Aceptar Cancelar dimiento Grupo de trabajo:	Aplicar WORKGROUP	tivo de 32 bits til o manuscrita no está disponible para esta pantalla e trabajo del equipo Cambiar configuración

\bigcirc	0-	😰 🕨 Panel de control 🔸 Sistema y seguridad 🕨 Sistema	→ 4y Buscar en el Panel de control P
	Ventar contro	Propiedades del sistema Cambios en el dominio o el nombre del equipo	po po
8 9 9 9	Admin Config remote Protec Config	Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red. <u>Más</u> información Nombre de equipo: CLIENTE-NAP	Seguridad de Windows Cambios en el dominio o el nombre del equipo Escriba el nombre y la contraseña de una cuenta con permiso para unirse al dominio.
	sistem	Nombre completo de equipo: CLIENTE-NAP Més Membro del © Dominio: proyecto Jocal © Grupo de trabajo: WORKGROUP	jramirez Dominio: proyecto.local Aceptar Cancelar de 32 bits manuscrita no está disponible para esta pantalla ria del anciez
	Vea tar Centro Window Informa rendimie	Aceptar Cancelar Aceptar Cancelar s opuate ción y herramientas de ento Activación de Windows	Aplicar NORKGROUP
6	•	🥖 🚞 🖸 🐖 🖬	ES 🔺 📭 🞲 01:26 a.m. 27/05/2012

Figura 31 Usuario Valido en el Dominio

Figura 32 Acceso Correcto al dominio

-		De la control e Sistema y seguridad e Sistema e fe Burcor en el Ponel de control
9		Panel de control + sistema y segundad + sistema
	Ventar contro	Propiedades del sistema Cambios en el dominio o el nombre del equipo bo remeto po po
۲	Admin	Puede cambiar el nombre y la pertenencia de este equipo. Los
۲	Config remote	cambios podrian afectar a acceso a los recursos de red. Mas información vados todos los derechos.
۲	Protec	Nombre de equipo:
۲	Config	CLIENTE-NAP 0
	sistem	Nombre completo de equipo: CLIENTE-NAP Cambios en el dominio o el nombre del equipo
		Miembro del
		Ciupo de trabajo: WORKGROUP
		Aceptar Cancelar pajo del equipo
		Combian Combian
	Vea tar	Acentar Cancelar Acelor
	Centro	
	Informa	sción y herramientas de Grupo de trabajo: WORKGROUP
	-chuirri	Activación de Windows
C	2)	🙆 🚆 💽 🐖 💐 🕵 ES 🔺 🖻 🗑 01.29 am.

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.

	- 6 3
	6_>
Directions NAP Arbite [Despecie] Viscolar Mostar viscolar en ella adicazión Gropesta local Ubscarán ^ Englisty Viscolar en ella dicazión Igrepenta local No Si propesto local	
Filtrado de seguridad La configuación en elle GPO tolo te puede aplicar a los grupos, susaios y equipos siguientes: Notates = & Equipos NAP (PROYECTO/Equipos NAP)	
AproxQutar Projekte	
	Directives NAP Aribia [Detach] Vincular Wincular Kota vincipation of a disaction Organization of the disaction Organization of the space basic Exception Respective of the space values a bits grapes: strutters y explore rajuenters: Noterial Respective Respective Appropr. Datase Properiodice

Figura 33 Directiva NAP

Figura 34 Agente NAP



Interve Actor Market Actor Balance Actor _ 6 × Clientes de cumplimiento Nombre Cliente de oplicación de cuaerriena de DHCP S Gente de cumprimerio de cuaerriena pas el acceso re Juliusió de confarca de l'Prec S Gente de cumprimerio de cuaerriena de Gateway TS S Cliente de aplicación de cuaerriena de EAP Estado Cliente de aplicación de cu x General Al habilitar el cliente, Protección de acceso a redes se puede aplicar desde este dispositivo. 🗵 Habilitar este cliente de cumplimiento S Cliente de aplicación de cuarentena de DHCP ld: 79617 Nombre: Cliente de aplicación de cuarenter Descripción Proporciona una aplicación basac 1.0 Versión Proveedor: Microsoft Corporation Aceptar Cancelar Estado: Habilitado × 灯 Trinicio 📔 🚋 📃 📓 Administración de directi... 📴 Usuarios y equipos de Ac... 📑 Editor de administraci... 💽 Sn thulo - Bloc de notas) ES 🔮 🕄 🏠 01:01 a.m.

Figura 35 Cliente de Cumplimiento DHCP

Figura 36 Centro de Seguridad

📕 Editor de administración de directivas de grupo					_ 5
Archivo Acción Ver Ayuda					
♦ ♦ <u>2</u> • • • • • • • •					
Directiva Directivas NAP [SRV-NAP.proyecto.local]	📑 Centro de senuridad				
🖻 👰 Configuración del equipo					
🗄 🧮 Directivas	Activat el Centro de comuidad (cólo	Configuración		Estado	Comentario
🗄 📃 Configuración de software	equipos de dominio)	Activar el Centro de seguridad (sólo equipos	de dominio)	and the second second	
🗉 🚞 Configuración de Windows			P	ropiedades de Ad	ctivar el Centro de segundad (solo equipos d] : 👗
🖂 📔 Plantillas administrativas: definiciones de directiva (archiv	Mostrar propiedades			Configuración Fy	nicación Comentario
🖃 🚞 Componentes de Windows					present conclusion
Administración de derechos digitales de Windows	Regustos: Almenos Missocit Windows VD			👼 Ashira d Car	the de constitued (sells are inter all continues of maintain
🗉 🧮 Administración remota de Windows (WinRM)	Professional o la familia de servidores			C Hosval el Cel	nito de segundad (solo equipos de dominio)
Administrador de recursos del sistema de Window	de Windows Server 2003				
🗉 🧮 Administrador de ventanas del escritorio				C No configurar	da
Área de encuentro de Windows	Descripción:			Habiltada	
Asistencia en línea	especifica si el Centro de securidad se			C Derhahiltada	
Buscar	activa o desactiva en los equipos			- Deshabikada	
Calendario de Windows	unidos a un dominio de Active				
Centro de movilidad de Windows	Directory. Cuando está activado, el				
Centro de seguridad	Centro de segundad supervisa la				
Cifrado de unidad BitLocker	informa al usuario si el ecuipo está				
Compatibilidad de aplicación	expuesto a algún peligro. La vista por				
Configuración de presentación	categorías Centro de seguridad del				
Control parental	Panel de control también contiene una				
🗉 🧾 Copia de seguridad	puede obtener recomendaciones para				
Directivas de Reproducción automática	ayudar a incrementar la seguridad del				
Explorador de juegos	equipo. Si el Centro de seguridad no				
🗉 🎬 Explorador de Windows	esta habilitado en el dominio, no se				
Fuentes RSS	serrión de estado del Centro de			Compatible com i	All manue Microsoft Windows VD Perferences a la franci
Grabadora de sonidos	seguridad.			compatible cont y	Anne increase in come in Protectional oral family.
Importar video	· · ·			Valor anterio	or Velor siguiente
🗉 🪞 Informe de errores de Windows	Tenga en cuenta que el Centro de			_	
Interfaz de usuario de credenciales	segundad solo se puede desactivar en equinos unidos a un dominio de				Anative Canadre Articar
🗉 🚞 Internet Explorer	Windows, Si un equipo no está unido				Acopia Calical Apros
Internet Information Services	a un dominio de Windows, la				
i NetMeeting	📘 configuración de directiva no tendrá 🔄				
	Extendido / Estándar /				
valores					
🚺 Tinicio 🛛 🚋 📃 🖉 📓 Administración de directi 📑 U	suarios y equipos de Ac 🧾 Editor de ar	dministraci 📃 Sin título - Bloc de notas			ES 👸 🛃 👍 01:02 a.m

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.

Usuarios y equipos de Active Director			_ <u>8</u> ×		
Archivo Acción Ver Ayuda					
🗢 🔿 🔰 📅 🤞 🗎 🗶 🖻 🙆	🔒 🛛 🖬 🔧 😒	11 🔻 🗾 🕱			
Usuarios y equipos de Active Directory [SR	Nombre	Tipo	Descripción		
💽 📋 Consultas guardadas	Nuevo objeto - Usuario	x	Cuenta integrada para la administración del equipo o dominio		
E 🚔 proyecto.local			cal Membros que tienen acceso administrativo al servicio DHCP		
🗄 🛄 Bultin	3		Administradores designados de la empresa		
Computers	Crearen: j	proyecto.local/Users	Administradores designados del esquema		
Dunian Controlers			Administratores designados del dominio		
Citicars Contractor			Todos los controladores de dominio del dominio		
	Nombre: D	Janiel Iniciales:	Los miembros de este grupo son controladores de dominio de sólo lectura en el dominio.		
	Apelidos:	Sanka	Let us be the second		
			Carl Grupp de administraciónes de LNC: Clastica DNE que lísense esemine e sua efecto de actualizaciones de feires en esemine de abora diseñas (habra como eseminiares TARTA)		
	Nombre completo:	Daniel Santa	Los miembros de aste remon em controlladoras de deminio de célo lastina en lombro de conces (calos calho so mais os prios).		
			Todas los servidores y estariones de trabaio unidos al dominio		
	Nombre de inicio de sesi	ión de usuario:			
	deanta @proyecto.loca	@proyecto.local	cal Los miembros de este grupo no pueden replicar las contraseñas a ningún controlador de dominio de sólo lectura en el dominio.		
		ión de unumin factorior a Mindows 2000)	cal Los miembros de este grupo pueden replicar las contraseñas a todos los controladores de dominio de sólo lectura en el dominio.		
	Inclusion of the sea	an de usualo (aneno e vindorio 2000).	Cuenta integrada para el acceso como invitado al equipo o dominio		
	PHUTECIUN	csana	Todos los invitados del dominio		
			Los membros de este grupo pueden modificar la directiva de grupo del domino		
		<atrás siguiente=""> Cancelar</atrás>	ical. Los memoros de este grupo pueden publicar certinicados en el directiono.		
			cal i tos ser noves de este grupo paeden obtener propodades de acceso reminito de los cabanos nal Membros que tienen armeso de sólo vista nara el servicio DHCP		
	& Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios del dominio		
<u></u>	1				
hulla - In .					
ଟ 🗍 👘 📰 🔤 🔤 🗍 🚺 Sin titu	io - Bloc de notas	Usuarios y equipos de) ES 🔰 🕄 🔥 09:45 a.m.		

Figura 38 Creación de usuario 1

Figura 39 Creación de usuario 2

📴 Usuarios y equipos de Active Directo	ory		_6×
Archivo Acción Ver Ayuda			
🗢 🔿 🙍 🖬 🥉 🗎 🗴	1 B 🛛 🛪 🛠 🗙 🐨 🏹 🖉 🗞		
Usurios y espaco de Active Directory (5 © Consulte guardode © Segli projectio Local © Segli projectio Local © Conputes © Conputes © Conputes © Conputes © Deter	Nordre Too Vere dijeto - Usuaris Too 3 Dear en: projecta local Uters Nordre: Juan Apdidat: Ramiez Nordre: Juan Ramiez Nordre: Juan Ramiez		Description Cuent rank pairs is a derivativation of equipo o domino ou Membra que forme acceso administration al derivato PKPP Administrationes desgrades de la grenzes Administrationes desgrades de deriven Administrationes desgrades de deriven Administrationes desgrades de deriven Losse deriventationes desgrades de deriven Losse deriver de deriven de derivende derivende deriven de deriven de derivende deriven de deriven d
	Norbe de ricio de sectión de susato: partinet Barrysetto local T Norber de ricio de sectión de susado (person a Vindowa 2000) PRO/ECTOV parties (24756 Siguentes) Carec	lo lo selar k	Los mientos de teta grupo por sol activados el anticamina de premientes. Todos las senderos - de teta grupo por paradem regionar a contratar de a manafera. Naci las mientos de teta grupo por paradem regionar las contratar de las contratadores de damino de silo lectura en el damino. Naci las mientos de teta grupo por parte regionar las de las de las contratadores de damino de silo lectura en el damino. Casa las mentos de teta grupo por parte mante a las de
K A	Buserio de domino Gupo de seguridad	- Global	Todes to sources de danne ESI 🖗 🖉 (h. 1994) Todes To

Figura 40 Grupo de seguridad NAP

Usuarios y equipos de Active Director;	Y		X
Archivo Acción Ver Ayuda			
🗢 🔿 🙍 🖬 🥉 🖬 🔀 🖻 🖄	a 🛛 🗃 🖏 🛬 🗑 🍸 💆 象		
📔 Usuarios y equipos de Active Directory (SR	Nonbre Tipo		Descripción
🗄 📋 Consultas guardadas	<u>λ</u> Δdministrador	Halarin	Cuenta integrada para la administración del equipo o dominio
proyecto.local	§ Nuevo objeto - Grupo	×	Membros que tienen acceso administrativo al servicio DHCP
🗈 🧾 Bultin	٤		Administradores designados de la empresa
Computers	1 Ga		Administradores designados del esquema
Doman Controllers	Crearen: proyecto.ocajusers		Administradores designados del dominio
licere	£		Todos los controladores de dominio del dominio
	Nombre de crupo:		Los miembros de este grupo son controladores de dominio de sólo lectura en el dominio.
	Factor MR		
	5 Indotrovina		Grupo de administradores de DNS
	Nombre de como (acterior a Wordows 2000):		Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de obros clientes (tales como servidores DHCP).
	En incr MIO		Los miembros de este grupo son controladores de dominio de solo lectura en la empresa.
	1 replosing		Todas los servidores y estaciones de trabajo unidos al dominio
	č debito de ce po		
		, gapo	Los membros de este grupo no pueden replicar las contraserias a ningun controlador de dominio de solo lectura en el dominio.
	C Dominio local C Se	guridad	Los membros de este grupo pueden replicar las contrasenas a todos los controladores de dominio de solo lectura en el dominio.
	Global C Dis	tribución	Cuenta integrada para el acceso como invitado al equipo o dominio
	C Universal		Touus its Invitatus del dutilitio
			Los minutures de actos no un moder modifiero la disaritiva de numa del dominia
			Los mientanos de este grupo pueden mounican a unecuna de grupo del cominico. Los mientanos de este asume suados sublicas contribucidos en el disertanio.
			Los recharios de este grupo pueden planical cerciticados en el aneccanio.
	Aceptar Can		tos ser nueles de este gropo pueden docente proposados de acceso remon de los asianos. Manhore que Namen arcano de cólo viste nare al canción DMCD.
			Traine los que denten acceso de Selo Hate para el Sel Hate Dirico.
		ande of selander ander	
<u>к</u>			
🎦 Inicio 🛛 🚋 📃 🖉 Sin titul	lo - Bloc de notas 🛛 📴 Usuarios y equipos de		ES 🐧 🐧 (b) 99:50 am.

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.

👶 Servidor de	Configurar NAP	× _ IX	
Archivo Accid	Seleccionar método de conexión de red para su uso con NAP		S • @ •
Directive Directive	Método de conexión de red: Seleccione el método de conexión de red que deses implementar en la red para equipos cliente compatibles con NAP. Las directivas creadas funcionarán sólo con este tipo de conexión de red. Para crear directivas para otros métodos de conexión de red, puede ejecutar el asistente de nuavo.	o a redes licitudes de	
	Protocolo de configuración dinámica de host (DHCP)	abrir el Asistente	
	Nombre de directiva: Este texto predeterminado se usa como parte del nombre de cada una de las directivas creadas con este asistente. Puede usar el texto predeterminado o modificarlo.	. 🗉	
	Requisitos adicionales: Debe realizar acciones adicionales para configurar NAP. Para ver los requisitos adicionales de NAP, haga cie en el vínculo siguierte. Requisitos adicionales	o que permiten a onecten a la red. restringida y	
	Avitarior Siguiente Final zar Cancelar		
/	E A Microsoft Manage		12:13 a.m.

Figura 41 Método NAP

Figura 42 Servidores de Cumplimiento



Figura 43 Ámbito DHCP en el NPS

🌖 Servidor de	Configurar NAP		
Archivo Acció	Especificar ámbitos DHCP		s • @•
Directiva Direc Direc Direc Direc Direc Direc	Si específica uno o más ámbitos habilitados para NAP, NPS evalúa el mantenimiento del sistema y realiza la autorización para los equipos cliente que solicitan una dirección (P a los ámbitos designados.	o a redes licitudes de	
E Proteccio	Si no especialca inigui ambito, la unectiva se aplica a todos los ambitos habilitados para inver en los servidores DHCP seleccianados. Si sepecífica un ámbito que no está habilitado para NAP, debe habilitar NAP para el ámbito después de completar el asistente.	•	
	Para especificar uno o más ámbitos, haga clic en Agregar.	i abrir el Asistente	
	Ambitos DHCP:		
	Agregar Editar Quitar	p que permiten a onecten a la red. restringida y	
		-	
	Anterior Sigurence Finalizar Cancelar		▶ 0% ▼

Figura 44 Configurar Grupo



Figura 45 Selección grupo NAP

Sele	ccionar Grupos		<u>? ×</u>	
Sel	eccionar este tipo de objeto:			
Gru	upos o Principios de seguridad integr	ados	Tipos de objetos	
Des	sde esta ubicación:			
pre	yecto.local		Ubicaciones	
Esc	riba los nombres de objeto que dese	a seleccionar (ejemplos):		
Eq	uipos		Comprobar nombres	
Nomi	bres múltiples encontrados			2 ×
Má: nom	s de un objeto coincide con el nombr Ibres de esta lista o vuelva a escribir	e "Equipos". Seleccione uno o r el nombre.	más	
	Nombres coincidentes:	Deservicesián	En la annata	
	Province (RDN)	Todas los soruidares y estacion	En la carpeta	
			provecto.local/Users	
	_			
	I			
			Aceptar	Cancelar

Figura 46 Servidores de remediación



Figura 47 Directivas de mantenimiento



Figura 48 Resumen de configuración NAP en NPS



Figura 49 Validador de mantenimiento

Servidor de directivas de rede				_ <u>- 8 ×</u>
Archivo Acción Ver Ayuda				P -
🗢 🔿 💋 📅 🛛 🖬				
NPS (.ocal) Cientes y servidores RADIUS J Directivas Directivas de solicitud de	Los Validadores de mantenimiento del sistema (SHV) la necesaria en los equipos cliente compatibles con NAF o más SHV a directivas de mantenimiento.	e permiten especificar 2. Para usar SHV, conf	la configuración igúrelos y agregue uno	s • @ •
Directivas de red	Nombre	Estado		
 Directivas de mantennier Processo de acesso a redes Validadores de mantenini Grupos de servidores de a Cuentas 	1월 Validador de manteninjento de segundad de Windows	Configurado		
	Estado: configurado			
	Configuraciones de códigos de error:			
1		J		_0% -

灯 Inicio 🛛 🚠 📰 🔗 🚱 🛛 🏈 Demostración NAP con D... 🛛 🚱 Servidor de directiva... 🛛 🗧 S 🔍 🐼 🗐 🏠 12:17 a.m.



Figura 50 Configuración de Validador de mantenimiento

Windows Vista Windows XP	
Con estos valores podrá especificar una directiva de validador de manterimiento de seguridad de Windows. Estas opciones definen los re	equisitos
Más información	
Firewall	
✓ Firewall habilitado para todas las conexiones de red	
Protección contra virus	
Aplicación antivirus activada Antivirus actualizado	
Protección contra spyware	
Aplicación anti spyware activada	
Protección de actualizaciones de segundad Restringir el acceso de dientes que no tengan instaladas todas las actualizaciones de segundad disponibles Importante Y	
Número mínimo de horas que deben transcurrir para que el cliente busque nuevas actualizaciones de 22 2	
De manera predeteminada, los dientes pueden recibir actualizaciones de seguridad de Microsoft Update. Si son necesarios orígene adicionales para la implementación, seleccione uno de los siguientes orígenes (o ambos).	iS
Windows Server Update Services 🖬 Windows Update	
Acept	Aplic

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.

Фриср	
Archivo Acción Ver Ayuda	
Propiedades de Ámbito [10.02.0] red nap Ambito Concessiones de dre Ambito Nombre de Ambito Nombre de Ambito Dirección IP Insiat 10.0.2.9 Bitoria Dirección IP Insiat 0.2.9 Bitor	
	_
istración de directi 🔁 Usuarios y equipos de Ac 😰 DHCP	

Figura 52 Propiedades ámbito DHCP

💂 Administración de directivas de gru	90	_ 8 ×
🗟 Archivo Acción Ver Ventana A	, yuda	_ # ×
	La x	
Administración de directives de grupo Administración de directives de grupo		
	<u>s</u>	
🐉 Inicio 🛛 🚠 📃 🖉 Adm	nistración de drest 📃 Usuarios y equipos de Ac 😰 DHCP] ES 🐧 🗟 🏠 12:59 a.m.

Figura 53 Ámbito DHCP para NAP

Figura 54 Dominio Restringido

📕 Administración de directivas de gru	po		_ _ _ _ _ ×
🚊 Archivo Acción Ver Ventana A	yuda		_8×
🗢 🔿 🔰 🖬 🙆 🖬	<u>Ф</u> рнср	<u>X</u>	
📓 Administración de directivas de grupo	Archivo Acción Ver Ayuda		
Bosque: proyecto.local	🗢 🔿 🔰 🖬 🖉 🖬	8	
E 🚔 commos	Фонсе	Dpciones Ámbito	
🚽 Default Domain Policy	E Sv-nap.proyecto.local	Caused Optimer susmate	
Directivas NAP	E 1919 F Ambto [10.0.2.0] red p.		-
Doman Concroiers P Doman Concroiers	💼 Conjunto de direccio	Upciones estandar de DHLP	
🗄 🎽 Filtros WMD	Concesiones de dire	Lase de protección de acceso a red prede ho	
🖻 🧊 GPO de ínicio	e 🔄 Reservas	Opciones disponibles	
 ± ± 100s Modelado de directivas de grupo 	Opciones de servidor	O15 Nombre de dominio DNS	
🥻 Resultados de directivas de grup	E ∰ IPv6	R17Byta da acceso de la raío	
		X Y	
		Entrada de datos	
		Valor de la nestrivoido provecto, local	
		cadena:	
		Analy Panaly Johny	
		Huspitel Lanceal Huspitel	
	x >		
🎝 Inicio 🛛 🚠 📃 🔍 Adm	inistración de directi 🛛 📴 Usuarios y eq	pos de Ac D DHCP	ES 🛐 🗟 🍙 12:58 a.m.
			, n= 0 v

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

	vs Update da	👻 🔛 Buscar	<u></u>
<mark>yrchivo Edición <u>V</u>er <u>H</u>erramientas Ayy Suscar actualizaciones</mark>	da		
Buscar actualizaciones			
	Windows Undate		0
Cambiar configuración	windows opuace		
Ver historial de actualizaciones			12
Restaurar actualizaciones ocultas	Preparando la instalación		
Actualizaciones: preguntas más frecuentes			
		Detener la instalación	
	Búsqueda más reciente de actualizaciones:	Hoy a las 01:47 a.m.	
	Se instalaron las actualizaciones: Recibe actualizaciones:	Hoy a las 10:23 a.m Ver historial de actualizaciones Sólo para Windows	
	Obtener actualizaciones para otros produ	ictos de Microsoft. Más información	
	10		

Consulte también			
Actualizaciones instaladas			

Figura 66 Actualizaciones Disponibles



Consulte también Actualizaciones instaladas

Figura 67 Configurando Actualizaciones



Figura 68 Windows esta Actualizado

🖉 Windows Update		_6 ×
💽 🚱 🖉 • Panel de control • Wind	lows Update	💌 📴 Buscar 🙋
Archivo Edición Ver Herramientas A	yuda	
dg Buscar actualizaciones	Windows Update	0
Cambiar configuración		
Ver historial de actualizaciones	Windows actá schustinada	
Restaurar actualizaciones ocultas	No hay actualizationes disponibles para su equipo.	
Actualizaciones: preguntas más frecuentes		
	Búsqueda más reciente de actualizaciones: Hoy a las (35:50 p.m. Se instalaron les actualizaciones: 14/05/2012 a las 10:38 a.m., Ver historial de actualizaciones Recibe actualizaciones: Sólo para Windows	
	Obtener actualizaciones para otros productos de Microsoft. Más información	
Consulte también		
Actualizaciones instaladas		
🐉 Inicio 🛛 🚋 📰 🖉 Windo	ows Update	ES 👰 😴 🌘 03:50 p.m.
		🎯 😳 🖉 🖶 🚺 🚺 🚺 CTRL DERECHA

Configuración de Windows update

Figura 69 Instalar Actualizaciones Automáticamente

Sambiar configuración	
🚱 🕞 🖉 • Panel de control • Windows Update • Cambiar configuración	👻 🔛 Buscar 🗾 🙋
Archivo Edicón Ver Herranientas Ayuda	
Elija la forma en que Windows puede instalar las actualizaciones	
Cuando el equipo está conectado, Windows puede comprobar automáticamente las actualizaciones e instalarlas usando esta configuración. Cuando estén disponibles nuevas actualizaciones, puede instalarlas antes de apagar el equipo	
¿Cómo me puede ayudar la actualización automática?	
Actualizaciones importantes	
🔮 Instaler actualizaciones automáticamente (recomendado) 🗾	
Instalar nuevas actualizaciones: Todos los dias 💌 a las 10:00 a.m. 💌	
Actualizaciones recomendades	
Cofrecerne actualizaciones recomendadas de la misma forma que recibo las actualizaciones importantes	
Quién puede instalar actualizaciones	
Permitir que todos los usuarios instalen actualizaciones en este equipo	
Nota: es posible que Windows Lipótels es actualize automáticamente antes de que busque otros actualizaciones. Lea nuestra <u>declaración de crivitacidad en línea.</u>	
Aceptar Cancelar	
👔 Inicio 🛛 🚡 📃 🖉 Cambiar configuración	ES 👰 🗟 🌘 03:50 p.m.

Segmentación de permisos por unidades organizacionales Figura 70 Usuarios y Equipos de AD

🚽 Usuarios y equipos de Active Directo	ry		<u>_8×</u>
Archivo Acción Ver Ayuda			
(= => 2 📰 🎸 🗀 🗶 💷 🧔	📑 🛛 🖬 😤 🐮 🝸 💆 🐍		
Usuarios y equipos de Active Directory [SF	Nombre	Tipo	Descripción
🗉 🧮 Consultas guardadas	& Administrador	Usuario	Cuenta integrada para la administr
proyecto.local	Administradores de DHCP	Grupo de seguridad - Dominio local	Miembros que tienen acceso admin
🗄 🚞 Builtin	Administradores de empresas	Grupo de seguridad - Universal	Administradores designados de la e
Computers	Administradores de esquema	Grupo de seguridad - Universal	Administradores designados del es
Domain Controllers	Admins. del dominio	Grupo de seguridad - Global	Administradores designados del do
ForeignSecurityPrincipals	Secontroladores de dominio	Grupo de seguridad - Global	Todos los controladores de dominio
Users	Controladores de dominio de sólo lectura	Grupo de seguridad - Global	Los miembros de este grupo son co
	👗 Daniel santa	Usuario	
	2 DnsAdmins	Grupo de seguridad - Dominio local	Grupo de administradores de DNS
	A DnsUpdateProxy	Grupo de seguridad - Global	Clientes DNS que tienen permiso pa
	Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de este grupo son co
	Sequipos del dominio	Grupo de seguridad - Global	Todas los servidores y estaciones o
	& Equipos NAP	Grupo de seguridad - Global	
	Rupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local	Los miembros de este grupo no pue
	Ropo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local	Los miembros de este grupo puede
	1. Invitado	Usuario	Cuenta integrada para el acceso co
	A Invitados de dominio	Grupo de seguridad - Global	Todos los invitados del dominio
	Juan Carlos Ramirez	Usuario	
	Repropietarios del creador de directivas de grupo	Grupo de seguridad - Global	Los miembros de este grupo puede
	Rublicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de este grupo puede
	Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de este grupo pued
	St Usuarios de DHCP	Grupo de seguridad - Dominio local	Miembros que tienen acceso de sóli
	St Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios del dominio
			Þ
🖓 Inicio 🛛 🚠 📰 👘 📴 Usua	rios y equipos de		ES 🛐 🛃 🏠 10:04 a.m.

Figura 71 OU Administradores

Nuevo objeto -	iinos de Active Directory Unidad organizativa	×		_ <u>_8 ×</u>
🧧 🗾 o	rear en: proyecto.local/		Tipo	Descripción
E Nombre: Administrad I Proteger	red contenedor contra eliminación accidental Aceptar Cancelar	Ayuda	bulitnDomain Contenedor Unidad organizativa Contenedor Contenedor	Default container for upgraded com Default container for donain contro Default container for security identi Default container for upgraded user
4				

Figura 72 OU Gerencia

<u>_</u>	suarios y equinos de Active Directory		1		_ 8 ×
2 80	evo objeto - Unidad organizativa	×			
	Crear en: proyecto.local/		Tipo	Descripción	
E -	Nombre:		o hay elementos disponibles en esta vista.		
	Gerencia				
	Proteger contenedor contra eliminación accidental				
	Aceptar Cancelar Ayuda				
•					Þ
🛛 🎝 Ir	nicio 🛛 🚠 📃 👘 📴 Usuarios y equipos de			ES 🛐 💽 🏠 10	:05 a.m.

Figura 73 OU Equipos NAP

📴 Usuarios y equipos de Active Dire	ctory	×
Archivo Acción Ver Ayuda		
🗢 🔿 🙋 📷 📋 📖 💁 🗟	Nuevo objeto - Unidad organizativa	×
Usuarios exclusos de Active Directos Usuarios exclusos de Active Directos E Bultin B Dultin B Computers ForeignSecurityPrincipals Users Administradores Gerencia	Varevo objeto - Unidad organizativa Image: Crear en: proyecto.local/ Nombre: [Equipo: NAF] Image: Proteger contenedor contra eliminación accidental Image: Concelar (Acceptar) Acceptar (Acceptar)	Descripción Default container for upgraded com Default container for domain contro Default container for security identi Default container for upgraded user
▼		
🥂 Inicio 📑 📰 🖂 🖂	suarios y equipos de	ES 🕺 🔂 🏠 10:05 a.m.

Figura 74 OU Presidencia

Isuarins v equinas de Active Directory		_6×
Crear en: proyecto.local/ Nombre: Presidencia Proteger contenedor contra eliminación accidental Acceptar Acceptar Cancelar Ayuda	Topo bullthDomain Contenedor Unided organizativa Contenedor Contenedor Unided organizativa Unided organizativa Unided organizativa	Descripción Default container for upgraded com Default container for dismain contro Default container for security identi Default container for upgraded use
<		ES 🔗 📢 10:07 a.m.

Figura 75 OU Sistemas

Usuarios y equipos de Active Directory		_18 ×
Nuevo objeto - Unidad organizativa		
Crear en: proyecto.local/	Tipo	Decerinción
	builtipDomain	Description
E Nombre:	Contenedor	Default container for upgraded com
Sistemas	Unidad organizativa	Default container for domain contro
	Contenedor	Default container for security identil
Proteger contenedor contra eliminación accidental	Contenedor	Default container for upgraded user
	Unidad organizativa	
	Unidad organizativa	
	Unidad organizativa	
Aceptar Cancelar Ayuda		
		<u> </u>
🎦 Inicio 🛛 🚠 📃 🛛 🧧 Usuarios y equipos de		ES 🛐 📢 🕞 10:07 a.m.

Figura 76 OU Mercadeo

E	115	uarios y equinos de Active Directory				_ 8 ×
	Nu	evo objeto - Unidad organizativa	×			
4		Crear en: provecto local/Mercadeo				
				Tipo	Descripción	
				o hay elementos disponibles en esta vista.		
Ľ		Nombre:				
		Mercadeo				
		Proteger contenedor contra eliminación accidental				
		Aceptar Cancelar Ayuda				
				-		
L						
L						
L						
L						
L						
L						
L						
4						Þ
2	In	icio 📑 🔲 🧧 Usuarios x equipos de			ES 😽	🔁 👍 10:10 a.m.

Figura 77 OU Gestión Humana

	Usuarios y equinos de Active Directory		_ 8 ×
	luevo objeto - Unidad organizativa 🔀		
	Crear en: proyecto.local/	Тіро	Descripción
E	Nombre: Gestion Humana IV Photeger contenedor contra eliminación accidental	bulithDomain Contenedor Unidad organizativa Contenedor Unidad organizativa Unidad organizativa Unidad organizativa Unidad organizativa Unidad organizativa Unidad organizativa	Default container for upgraded com Default container for domain contro Default container for security identif Default container for upgraded user
ī	Aceptar Cancelar Ayuda		1
		J	
1.47	Inicio 🔄 🐜 📃 🛛 🖓 Usuarios y equipos de		ES M 🔂 📩 10:10 a.m.

Figura 78 Segmentación Por OU

Usuarios y equipos de Active Director	y		_ B ×
Archivo Acción Ver Ayuda			
🗢 🔿 🙋 💼 🗈 🖬 🙆 😽	🖬 🗏 📚 🛅 🔻 🖸 🗞		
Usuarios y equipos de Active Directory [SR	Nombre	Tipo	Descripción 👻
🗉 🧮 Consultas guardadas	Contract Con	Contenedor	Default container for upgraded user account
proyecto.local	Computers	Contenedor	Default container for upgraded computer ac
🗉 📴 Builtin	ForeignSecurityPrincipals	Contenedor	Default container for security identifiers (SIC
Computers	Domain Controllers	Unidad organizativa	Default container for domain controllers
Earcian Controllers Earcian Seg with Originals	🚞 Builtin	builtinDomain	
PoreignoecuntyPrincipals	Administradores	Unidad organizativa	
Administradores	💼 Gerencia	Unidad organizativa	
Gerencia	Equipos NAP	Unidad organizativa	
Equipos NAP	Presidencia	Unidad organizativa	
Presidencia	Sistemas	Unidad organizativa	
🛅 Sistemas	Mercadeo	Unidad organizativa	
🗂 Mercadeo	Gestion Humana	Unidad organizativa	
💼 Gestion Humana	Grupos de Seguridad	Unidad organizativa	
📔 Grupos de Seguridad	Clientes NAP	Unidad organizativa	
Clientes NAP			
			N
	1.1		<u> </u>
🎦 Inicia 🛛 🔍 🔲	ios y equipos de		ES 🗿 🗐 (b. 10:18 a.m.

Configuración de Directivas de Grupo

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

😹 Administración de directivas de grupo				_ 5 X		
🗟 Archivo Acción Ver Ventana Ayuda				X		
Americania de dectas de grupo Actives Maria Descar protectulos de Descar protec	Prohibir modificaciones de red Jadaio (Detate: Corrigatolio (Delegacion) Prohibir modificaciones de red Dato exception e 2/55/2012/35/20 a.s. Configuración del equipo (hubitada) Deceivas Petallas administrativas Definiones de descrito (activos ADMO) ecopendes del Red/Consciones de decisio efensos e las conexiones LAN Capadado pas halitar o denholitar una conexio LAN Pohibir el acceso a la propeder de una conexio LAN	quan local Configuración Deshalikado Habilado	Caestaio	e del allaca state state state state state state		
				z		
]					
Minicia 🔒 🗖 🎯 🖉 Administración	a de de			ES 🗿 🗐 (n 1257 am		

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+

s (locales)	🔍 Servicios (locales)		Aplicación del sistem	a COM+ Propiedades (Equipo local)	X		
	Aplicación del sistema COM+	Nombre +	General Iniciar sesór	Recuperación Dependencias	scripción pilta el acceso .	Iniciar sesió	
	Inidar el servicio	Adaptador de rendmient	Nombre de servicio:	COMSysApp	porciona infor	. Sistema local	
	Descripción:	Administración de aplica: Administración de certific	Nombre para mostrar:	Aplicación del sistema COM+	cesa las solicit porciona servi	. Sistema local . Sistema local	
	Administra la configuración y el seguimiento de los componentes del Modelo de objetos componentes del	Administración remota de Administrador de conexio	Descripción:	Administra la configuración y el seguimiento de los componentes del Modelo de objetos	 servicio Adminis. sa una conexió 	Servicio de red Sistema local	
	(COM+). Si se detiene el servicio, la mayoría de los componentes COM+ no funcionarán correctamente. Si se	Administrador de conexic Administrador de cuenta Administrador de sesión	Ruta de acceso al eje C:\Windows\system3	ecutable: 2'dihost.exe /Processid:(02D4B3F1-FD88-11D1	ninistra conexi nicio de este se. porciona sent	Sistema local Sistema local Sistema local	
	deshabilita este servicio, no se podrá iniciar ningún servicio que dependa especificamente de él.	Agente de directiva IPse Agente de Protección de	Tipo de inicio:	Deshabiltado	rotocolo de se. pilta la funcion	Servicio de red Servicio de red	
		Alsamiento de claves CN Almacenamiento protegic Aplicación auxiliar de Net	Avudarme a configura	rlas opciones de ínicio de senvicios.	tervido Aislami tece almacena ixporciona comp.	 Sistema local Sistema local Servicio local 	
		Aplicación auxiliar IP Aplicación del sistema CC	hicar	Deere Pausa Rearud	porciona cone	Sistema local Sistema local	
		Archivos sin conexión Asignador de detección « Audio de Windows	Puede especificar los el servicio desde aqu	parámetros de inicio que se aplican cuando se ir I.	icia sa un mapa de . ministra el aud	Sistema local Servicio local Servicio local	
		Ayuda del Panel de conti Ayudante especial de la	Parámetros de inicio:		e servicio prop. mite que los a	Sistema local . Sistema local	
		G Captura SIMP Centro de distribución de			controladores	Servicio local Sistema local Setema local	
		Cliente de seguimiento d		Aceptar Cancelar	Aplicar ntene los vinc	 Sistema local Servicio local 	
		Cliente DNS		Iniciado Automático	El servicio de Clie	. Servicio de red	

Figura 83 Deshabilitar RPC

Q, Servicios			_ <u>5</u> ×
Archivo Acción Ver	Ayuda		
🔍 Servicios (locales)	Q Servicios (locales)		
	Ubicador de llamada a	a Ubicador de Ramada a procedimiento remoto (RPC) Propiedades (🔀 de inicio Descripción Iniciar sesió	
	procedimiento remoto (RPC)	General Inicar sestin Recuperación Dependencias ul lua Administra las sesi Sistema local tual Exige el cumplimie Sistema local	
	Iniciar el servicio	Nombre de servicio: RpoLocator permite informar Sistema local	
	Descripción: Administra la base de dator del escuito	Nombre para mostrar: Ubicador de llamada a procedimiento remoto (RPC) val Registra la plataf Servicio local	
	de nombres RPC.	Descripción: Administra la base de datos del servicio de mático (nicio re Permite el acceso Servicio local omático Proporciona cuatr Servicio de red	
		mático Servicio Controlad Sistema local prédico Oficre controlhi Sistema local	
		Puta de acceso a ejecutade: C:Windows'system32/locator exe omático (nicio re Administra la aute Sistema local	
		Topo de Inicio: Destrabilitado	
		Audame a confauer las opciones de inicio de servicios. Val El servicio WcsPlu Servicio local	
		Peter del servicio Servicio local	
		hidar Deterer Pasar Remote hal Administra el acce Servicio local	
		Puede executional in a second and a mich ou e second and a mich ou execution and a mich ou execution of the mich outer	
		el servicio desde aquí. Indico Permite a los usua	
		Parámetros de inicio: como de	
		a habita la creació Sistema local lual Administra proces Sistema local	
		ual Aprega, modifica Sistema local	
		Abertar Lancear Apicar omátos (nicio re Habilta la detecci Sistema local	-
	Extendido / Estándar /		
💐 🛄 📜 🥼	i 🔮 🕼 🛔 📑 📢 🚊 🔤 🛛 🍳 Se	vicios	ES 🚭 🕉 🗐 🛞 11:40 p.m.

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

😰 Editor del Registro					
Archivo Edición Ver Favoritos Ayuda					
Berneters Berneters	Pondere Pordeterminado) Description Descripti Description Descripti Description Description	Tipo REG_52 REG_52 REG_52 REG_DWORD REG_BINARY REG_STRARY REG_STRARY REG_WORD REG_WORD REG_WORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Datos (vidir no establecido) @%%5ystemRodt%isystem32[w32tme.dl],-201 @%%5ystemRodt%isystem32[w32tme.dl],-201 0x0000001 (1) 80 51 10 00 00 00 00 00 00 00 00 00 00 00 00		
.quipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentContr	rolSet\Services\W32Time				
🍹 Inicio 📄 🚠 💻 🏉 👘 🚮 Editor del R	Registro		ES 🕺 🛃 🌘	12:19 p.m	

Figura 87 Tipo de servicio NTP

	usbprint 🔺	Nombre	Тіро	Datos
	USBSTOR	(Predeterminado)	REG_SZ	(valor no establecido)
	usbuhci	ab NtpServer	REG_SZ	time.windows.com,0x9
÷	UxSms	ab ServiceDII	REG EXPAND SZ	%systemroot%\system32\w32time.dll
÷-)}	VBoxGuest	ServiceDllUnload	REG DWORD	0×00000001 (1)
÷- 🏄 '	VBoxMouse	ab ServiceMain	REG SZ	SychostEntry W32Time
	VBoxService	ab Type	REG SZ	NTSDS
÷ 🕌	VBoxSF			
÷.	VBo×Video			
÷ 🦊	vds			
🕀 🕌 -	vga			
🕀 🦛 🖌	VgaSave			
- 🖊 -	viaagp			
- i i i i i i i i i i i i i i i i i i i	ViaC7			
- 🖊 -	viaide			
	vmbus			
• • • • • • • • • • • • • • • • • • •	volmgr		Editar cadena	X
••••••••••••••••••••••••••••••••••••••	volmgrx	•	cultar cauena	
±	volsnap		Nombre de valor:	
1 - <u>-</u>	vsmraid		Tupe	
1	V55		1,360	
	W321me		Información del valor:	
	Conrig		NTP	
	Parameters			
				Aceptar Cancelar
	WacomBon			
	Waparp			
	Waparpy6			
÷	WcsPlugInService			
1.	wd			
÷	wdfo1000			
÷	WdiServiceHost			
÷	WdiSystemHost			
	→			

Figura 88 Annouce Flags NTP

🖬 Editor del Registro				_ 8 ×
Archivo Edición Ver Favoritos Ayuda				
	Nombre	Tipo	Datos	
	(Predeterminado)	REG_SZ	(valor no establecido)	
	3 AnnounceFlags	REG_DWORD	0×0000000a (10)	
🗷 🍑 UxSms	38 EventLogFlags	REG DWORD	0×00000002 (2)	
🗷 🎍 VBoxGuest	FrequencyCorrec	REG DWORD	0x00000004 (4)	
😟 🍌 VBoxMouse	HoldPeriod			Dec 1
	WI argePhaseOffset	Editar valor de DWUR	(D (32 bits)	
🕀 🎍 VBoxSF	i ocalClockDispers	Nombre de valor:		
🕀 🎍 VBoxVideo	MaxAllowedDbac	Annes man Flame		-
🕀 🎍 vds	MaxNegPhaceCo	pannouncertags		
🕀 🎍 vga	MaxDellTeters val	Información del valor:	Base	
🕀 🎍 VgaSave	MaxPoint iterval	R	C Hexadecimal	
	maxPosPhaseCor	19	G D	
ViaC7			 Decimal 	
- 🕌 viaide	PhaseCorrectRate			
- wnbus	PollAdjustFactor		Aceptar Cancelar	
🕀 🕌 volmgr	SpikeWatchPeriod			
🕀 🎍 volmgr×	TimeJumpAuditOf	REG_DWORD	0X00007080 (28800)	
🖽 🦊 voisnap	🐯 UpdateInterval	REG_DWORD	0×00000064 (100)	
🖽 🕌 vsmraid				
🖭 🕌 VSS				
E W321me				
Config				
Parameters				
1 ImeProviders				
H W35VC				
wacomPen				
H e wanarp				
H wanarpvb				
wcsPlugInservice				
wd witer ooo				
Wdr01000				
WdiSystemHost				
A A A A A A A A A A A A A A A A A A A				
Equipo\HKEY LOCAL MACHINE\SYSTEM\CurrentContro	/ lSet\Services\W32Time\C	onfig		
🍠 Inicio 📔 🚠 💻 🏉 🔢 🎯 Editor del Re	egistro			ES 🛐 📆 🎝 12:21 p.m.

Figura 89 Activar NTP



Figura 90 Dirección NTP Server



Figura 91 Special Poll Interval

	1		*	
	usbprint A	Nombre	Tipo	Datos
	USBSTOR	(Predeterminado)	REG_SZ	(valor no establecido)
-	usbunci	AllowNonstandardModeCombinations	REG_DWORD	0×00000001 (1)
1 1	UX5ms	CompatibilityFlags	REG_DWORD	0×80000000 (2147483648)
별	VBoxGuest	20 CrossSiteSyncFlags	REG_DWORD	0×00000002 (2)
±	VBoxmouse	ab) DilName	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
	VBoxService	80 Enabled	REG_DWORD	0×00000001 (1)
<u>+</u>	VBOXSH	8 EventLogFlags	REG_DWORD	0×00000001 (1)
±	vBoxvideo	310 InputProvider	REG DWORD	0x00000001 (1)
±	🖕 vds	W LargeSampleSkew	REG DWORD	0×00000003 (3)
±	🖉 vga	BesolvePeerBackoffMaxTimes	REG DWORD	0×00000007 (7)
±	Vgabave	BecolvePeerBackoffMiputes	REG DWORD	0×0000000 (15)
	viaagp	SpecialPollInterval	REC DWORD	0×00000+10 (2600)
	ViaC7	ab Special Politice Paraising	DEC MULTI ST	0,00000010 (3000)
	🖕 viaide	speciaiPoiri imekemaining	REG_MULTI_52	
	vmbus			
뽀	🖕 volmgr			
뽀	🖕 volmgr×			
	🖕 volsnap	Editor unlos de	DWODD (22 bits)	×1
±	🖕 vsmraid	Eulcar valor ut	2 DWORD (32 DICS)	
±	VSS 🐘	Nombre de val	or:	
	W32Time	Special Pollute	an and	
	Config	[opecial-olime	a vai	
	Parameters	Información de	I valor: 🛛 🗖 Base 💳	
	ImeProviders	lan	CHe	wadecimal
	NtpClient	134		
	NtpServer		• De	ecimal
Ū.	📙 W35VC			
	📙 WacomPen		Acep	tar Cancelar
Ū-	📙 Wanarp	11		
÷	📙 Wanarpv6 🛛 🗕			
÷.	📙 WcsPlugInService			
	🎍 wd			
<u>, i i i i i i i i i i i i i i i i i i i</u>	🕌 wdf01000 🖉	1.		
	•	•		

Figura 92 Max Pos Phase Correction

	uchprint •	Nombro	Tino	Dates
	USBSTOR	(Predeterminado)	DEG SZ	(valor no establecido)
	usbuhci	(incoccontando)	REG_DWORD	0×0000000E (E)
÷	UxSms	W Eventi odElago	REG_DWORD	0×0000003 (3)
÷.	VBoxGuest	21 Exemune ConnectDate	REG_DWORD	0+00000004 (4)
÷-	VBoxMouse	en indencycorrectivate	REG_DWORD	0.00000000 (7)
	VBoxService	en la seconda de	REG_DWORD	0x00000005(5)
÷	VBoxSF	angerhaseonset	REG_DWORD	0x021a1080 (50000000)
	🚹 VBo×Video		REG_DWORD	0x0000000a (10)
	🚹 vds	MaxAllowedPhaseOrrset	REG_DWORD	uxuuuuuuze (300)
	🚹 vga	MaxNegPhaseCorrection	REG_DWORD	UXUUU2A3UU (1728UU)
	🚹 VgaSave	MaxPolIInterval	REG_DWORD	0×0000000a (10)
	🍌 viaagp	MaxPosPhaseCorrection	REG_DWORD	0x0002a300 (172800)
	🍌 ViaC7	MinPollInterval	REG_DWORD	0×00000006 (6)
	🍌 viaide	PhaseCorrectRate	REG_DWORD	0x00000007 (7)
-	🎍 vmbus	PollAdjustFactor	REG_DWORD	0x00000005 (5)
÷	📙 volmgr	SpikeWatchPeriod	REG_DWORD	0×00000384 (900)
	📙 volmgr×	👯 TimeJumpAuditOffset	REG_DWORD	0×00007080 (28800)
	🖕 volsnap	👪 UpdateInterval	REG_DWORD	0x00000064 (100)
	🖕 vsmraid			
œ	VSS VSS			
8	W32Time		Editar valor d	e DWORD (32 bits)
	Parameters		Nombre de va	lor:
	ImeProviders		MaxPosPhase	Correction
	NtpClient		المراجعة والمراجع	dualan D
	Intpoerver		Información de	Base Carl
*	W35VC		30	 Hexadecimal
	Wacomen			 Decimal
	Wanarp			
	Washingto Service			Aceptar Cancelar
	wcshidginbervice			
-	wdf01000			
1		1		
uido)HKEY LOCAL MA	CHINE'SYSTEM'CurrentContr	J olSet\Services\W32Time\Config		
haboh wer Trocke Tub	contractor or control renecories			

Figura 93 Max Neg Phase Correction

🙀 Editor del R	Registro									_ 8
Archivo Edició	on Ver Fav	oritos Ayuda								
		usbprint		Nombre		Tipo	Datos			
		JSBSTOR		(Predeterminado)		REG_SZ	(valor no establecido)			
	- 👘 L	usbuhci		🔀 AnnounceFlags		REG_DWORD	0×00000005 (5)			
	🕐 👘 👘 U	JxSms		88 EventLogFlags		REG_DWORD	0×00000002 (2)			
	- 🖭 👘 👘	/BoxGuest		B FrequencyCorrect	Rate	REG_DWORD	0×00000004 (4)			
	🗉 🖷 🦛 V	/BoxMouse		👪 HoldPeriod		REG_DWORD	0×00000005 (5)			
	*	BoxService		🔀 LargePhaseOffset		REG_DWORD	0×02faf080 (500000	0)		
		/BOX5F		30 LocalClockDispersio	n	REG_DWORD	0×0000000a (10)			
		/buxvideu		30 MaxAllowedPhase	Offset	REG_DWORD	0×0000012c (300)			
		/G5		MaxNegPhaseCorr	ection	REG_DWORD	0×0002a300 (172800)		
		rga IgaSave		88 MaxPollInterval		REG_DWORD	0×0000000a (10)			
	1.1	/jaann		100 MaxPosPhaseCorr	ection	REG_DWORD	0×0000001e (30)			
	i	/iaC7		職 MinPollInterval		REG_DWORD	0×00000006 (6)			
		riaide		200 PhaseCorrectRate		REG_DWORD	0×00000007 (7)			
		/mbus		8 PollAdjustFactor		REG_DWORD	0×00000005 (5)			
	👘 🚠 🗸	/olmgr		88 SpikeWatchPeriod		REG_DWORD	0x00000384 (900)			
	👘 🗓 v	/olmgr×		3 TimeJumpAuditOff	set	REG_DWORD	0x00007080 (28800)			
	😐 🕀 🚺 v	/olsnap		30 UpdateInterval		REG_DWORD	0x00000064 (100)			
	🔅 🕀 👘	/smraid		1 ·						
	🔅 🕀 🖗 🕻	/55							_	
	🔅 🦊 🔁	W32Time			Edita	r valor de DW	ORD (32 bits)		×	
		Config			Nom	bre de valor:				
	6	TimeProviders			Max	NegPhaseCorre	ection		-	
		- 📔 NtpClient			1		. D			
					mo	macion dei valo	Base C			
	😐 🕀 🖊 V	W35VC	_		30		U Hexade	scimal		
		VacomPen					Decima	l		
	💷 🕂 🦊 👌	Wanarp							_	
	E 🖷 🕌 👌	Wanarpv6	_				Aceptar	Cancelar	1	
		wcselugInService								
		WU Wdf01000	-1		_					
	(T) - 10 V	0001000	<u>بن</u>							
Equipo\HKEY LO	CAL MACHIN	WE\SYSTEM\Curren	LContro	ו Set\Services\W32Time\	Confia					
	h 📰 🍊	Contraction and the second sec	del De	aistro					ES 🙀	🗐 👍 12:28 p.m
		- Cuicos		2						with the second

Figura 94 Detención e iniciación de W32Time



Deshabilitar protocolos inseguros Figura 95 Bloqueo puerto FTP datos

🔔 🌔	Firewall de Windows	
Equipo Servidor de directivas de redes	Activar o desactivar Firewall de Firewall de Windows	
—	Windows Pemitir un proge "Configuration de Turceuil de Vindows XII de fineal de Xin Agregar un puerto XI	
Papelera de Simbolo del sistema	Les esta configuración por a abrur un puerto a través de Frevail de Windows. Para executora el número y protociós del parter, consulte la documentación del rograma o servo que desea usar.	
reddaje	Nombre: FTP debs payetdas.	
<u>,</u>	Numero de puerto: 20	
inistración de Usuarios y equipos ctivas de grupo de Active Directory	тишин н цр С цор	
and and a second	40x8 responses al later un puerte? Centre al responses to al later un puerte? Listoritorio restorial de administración de Nindous (NMI) Directorial de administración de Administración de Nindous (NMI) Directorial de administración de Nindous (NMI) Directorial de administración de Administración de Nindous (NMI) Directorial de administración de Administración de Administración de Administración de Administración de Administración de	
C III	Vea también Centro de redes	
'Inicio 📃 🚠 🖑 🔐 🕜 🙏 🗔 🚱 🛤 📼	🔐 Frend de Windows 🖉 Configuración de Fre	ES 🖉 🎽 🔂 12:5

Figura 96 Bloqueo puerto FTP control

👰 👂	Frewall de Windows
Equipo Servidor de directivas de redes	Activar o desactivar Firewall de Firewall de Windows Windows
Parcée de Sintono del interne recider	Permitri un porgo Configuración de Firenald de Vinadous X > coñver malintencionado del Finesal de Vina Agregar un poerto X >
Administración de - Usardos y equipos deschiras de grupo de Active Directory	Número de parto: [2]
10 40	Contrast and the adverter adverter of the adve
Cite Cite	Ves también Centro de redes
🎝 Inicio 📃 🚠 🔮 🔐 🗿 🐍 📃 😝 📓 💷	🔐 Firewall de Windows 🛛 🔐 Configuración de Fire

Figura 97 Bloqueo puerto Telnet

🔊	Firewall de Windows	
Equipo Servidor de directivas de redes	Activar o desactivar Firewall de Eirewall de Windows	
	Windows FICHUR CHINAGWS Permitir un progra Configuración de Firenall de Vindows 🗶 o software malintencionado	
Fapelera de Sintolo del estema	del Freual de linn Agregar an puerta Use esta configurados para abrir un puerta a través de Freual de Il títodos. Fara e configurados paratos de puerto, consulte la documentos de forgargonas e serios que de seu sor.	
reddaje	Ventre: Teinet of de guesdes.	
"	Numer de puerter 23	
Administración de Usuarios y equipos directivas de grupo de Active Directory	C UP	
fin and the second seco	Cardor setota di di run porta? Cardor setota Cardor s	
	Vez también Centro de tedes	
🐉 Inicio 📃 🚠 🖓 🔐 👔 🦓 👗 🔟	Preval de Windows	ES 🛃 👸 🎒 12:58

Activar log de eventos

Visor de eventos					_ 6 ×			
Archivo Acción Ver Ayuda								
🛃 Visor de eventos (local)	Visor de eventos (local)	Acciones						
E 😽 Vistas personalizadas	Introducción y resumen	Visor de eventos (local)						
Eventos administrativos Esperimer de republica	in outcom presumen		Ultima actualización: 20/05/201	2 10:51:56 a.m.	🧟 Abrir registro quardado			
Servicios de dominio de Active Directo	Introducción							
Servidor DHCP	~			_	Y Crear vista personalizada			
T Servidor DNS	Para ver los eventos que se produjeron en	el equipo, seleccione el nodo	adecuado de vista personalizada, registro u o	igen en	Importar vista personalizada			
Servicios de acceso y directivas de re	el arboi de la consola. La vista personalizat independientemente del prinen à continua	da Eventos administrativos co Inción, se muestra una vista ad	ntiene todos los eventos administrativos, regada de todos los registros		Conectarse a otro equipo			
Registros de Windows Ankrastin	magana anna an angan maana	and to involve and note by						
Sequidad	Recomen de aventes administrations				ler /			
Setup	Tresenten de overnes doministratives				Actualizar			
🚺 Sistema	Tipo de evento Id. del e Origen	Registro Última ho	24 horas 7 dias Total		🛿 Ayuda 🕨 🕨			
Eventos reenviados	Crítico	- 0	0 0 0					
Registros de aplicaciones y servicios Supportes de bandurase	Error	- 0	0 3 10	_				
Toternet Explorer	⊞ Advertencia	- 0	1 1.828 2.083					
Key Management Service	🗄 Información	- 2	12 24.438 28.707	-				
🖂 🎽 Microsoft								
E 🔛 Windows	Nordica visitas encientemente •							
Replication DFS								
Servidor DNS	Nombre	Descripción	Modificado Creado					
Suscripciones	Registros de aplicaciones y servicios Unternet Expl	lorer No disponible	12/05/2012 0 12/05/2012 03:25:45 p					
-	Registros de aplicaciones y servicios Eventos de H	hardware No disponible	12/05/2012 0 12/05/2012 03:25:45 p					
	Registros de Windows\Eventos reenviados	No disponible		- 11 -]			
	Registros de Windows\Sistema	No disponible	17/05/2012 0 12/05/2012 03:25:45 p					
	Registros de Windows\Setup	No disponible	17/05/2012 1 12/05/2012 03:29:48 p					
	Registros de Windows\Seguridad	No disponible	17/05/2012 0 12/05/2012 03:25:45 p	_				
	1			<u> </u>				
				_				
x <u> </u>	Resumen de registro							
🐉 Inicio 🛛 🚠 💻 🛛 🚺 Visor de ev	ntos				ES 😚 👼 🌀 10:53 a.m.			

Figura 98 Visor de Eventos
Figura 99 Sucesos servicios instalados

🖁 Visor de eventos		_62
Archivo Acción Ver Ayuda		
🗢 🔿 💈 🖬 🞴 🖬		
🛃 Visor de eventos (local)	Servicios de dominio de Active Directory 129 eventos	Acciones
E 📑 Vistas personalizadas	✓ 12 sector	Servicios de dominio de Active Directory
Eventos administrativos	2 123 evenus	🧟 Abrir renistra querdado
Servicios de dominin de Artive Directo	Nivel Fecha y hora Origen Id. del ev Categoría de la tarea	
Servidor DHCP	Dinformación 17/05/2012 03:58:12 p.m. NTDS ISAM 701 Desfragmentación con conexión	Y Crear vista personalizada
Y Servidor DNS	Información 17/05/2012 03:58:06 p.m. ActiveDirectory_DomainService 1869 Catálogo global	Importar vista personalizada
🝸 Servicios de acceso y directivas de re	Diformación 17/05/2012 03:58:06 p.m. NTDS 15441 700 Desfragmentación con conexión	Thur its secondards stud
👔 Registros de Windows	Diformación 17/05/2012 03:58:06 p.m. NTDS IS4M 102 General	 Pitrar vista personaizada actual
🛃 Aplicación	Información 17/05/2012 03:43:31 p.m. ActiveDirectory_DomainService 1394 Control de servicios	Propiedades
📔 Seguridad	Información 17/05/2012 03:43:01 p.m. ActiveDirectory_DomainService 1000 Control de servicios	AD BACK
Setup	Advertencia 17/05/2012 03:43:01 p.m. ActiveDirectory_DomainService 2886 Interfaz LDAP	
Sistema	Información 17/05/2012 12:09:24 a.m. ActiveDirectory_DomainService 1004 Control de servicios	Guardar los eventos en la vista personalizada c
Eventos reenviados	Diformación 17/05/2012 12:09:24 a.m. NTDS ISAM 103 General	Exportar vista personalizada
Registros de aplicaciones y servicios	Unformación 14/05/2012 12:29:46 p.m. NTDS ISAM 701 Desfragmentación con conexión	Canine sida navenakada
Evenus de l'arunare	Unformación 14/05/2012 12:29:40 p.m. ActiveDirectory_DomainService 1869 Catálogo global	Cupidi visia personalizatia
Key Management Service	Unformación 14/05/2012 12:29:41 p.m. NTDS ISAM 700 Desfragmentación con conexión	Adjuntar tarea a esta vista personalizada
F Microsoft	Unformación 14/05/2012 12:29:41 p.m. NTDS ISAM 102 General	Ver
Windows	Unformación 14/05/2012 12:15:04 p.m. ActiveDirectory_DomainService 1394 Control de servicios	-
Replicación DPS	🕕 Información 14/05/2012 12:14:34 p.m. ActiveDirectory_DomainService 1000 Control de servicios	G Actualizar
🧱 Servicio de directorio	Evento 701, NTDSISAM X	👔 Ayuda
Suscripciones	General [Turbuller]	Evento 701, NTDS ISAM
	The second s	Propiedades de evento
	NTDS (580) NTDSA: La desfragmentación con conexión completó un recorrido completo en la base de datos "C-\Windows\NTDS 🚑	Adjuntar tarea a este evento
	Redenier Andrea - Andrea Andrea	E Copiar
	Nombre de registro: Servicio de directorio	Guardar eventos seleccionados
	Origen: NTDSISAM Registrado: 17/05/2012 03:50:12 p.m.	R sautos
	1d. del evento: 701 Categoría de tarea: Desfragmentación con conexión	
[]]	Minde Televerside Televers Olicies	👔 Ayuda
		1
Tairia 📑 📰 📑 Wissa da au	nhae	EC 🕅 🗐 🖒 10-53 at

Figura 100 Sucesos de Seguridad

🚦 Visor de eventos						_ 8 ×
Archivo Acción Yer Ayuda						
(= =) 🙎 🖬 👔						
Usor de eventos (local)	Seguridad 8.081 eventos					Acciones
🗉 🚔 Vistas personalizadas	Debayedara Catharitan	Aim	Tel del sussis	Columnia da la terrar		Seguridad
T Eventos administrativos	Palabras dave Fecha y nora	Urigen Manaach Utadamanaacha audhtar	LO. DEI EVENDO	Categoria de la carea		
E Funciones de servidor	Auditoria correcta: 20/06/2012 10:52:19 a.m	 Microsoft Windows security auditing. 	4031	Cerrar sesion		Abrir registro guardado
Y Servicos de dominio de Active Directi	Auditoria carrecta 20/05/2012 10:52:11 8.	 Microsoft Windows security addicing. 	4624	Cerrar sesion		🔻 Crear vista personalizada
T Service DHS	Auditoria carrecta 20/05/2012 10:52:00 a m	Manacht Windows security addeing.	4624	Cerrar sestion		Terrortar virta narronalizada
Servicio de arreso y directivas de ra	Autoria correcta 20/05/2012 10:52:09 a.m.	Menorit Windows security ducking.	4624	Cerrer sesuir		
E Retistros de Windows	Audiona carrecta 20/06/2012 10:52:09 a.m.	Microsoft Windows security additing.	4672	Inicia de cesión emeriel		Vaciar registro
Apicación	 Auditoria correcta: 20/05/2012 10:52:09 a.m. Auditoria correcta: 20/05/2012 10:52:09 a.m. 	Microsoft Windows security auditing.	4674	Inicia de sestán especiel Inicia de ceción		Fibrar registro actual
Seguridad	Auditoria correcta 20/05/2012 10:52:09 a m	Microsoft Windows security audition	4672	Inicia de sesión especial		
Setup	Auditoría correcta 20/05/2012 10:52:09 a m	Microsoft Windows security auditing	4674	Inicia de seción		Propedades
🛃 Sistema	Auditoria correcta 20/05/2012 10:52:09 a.m.	Microsoft Windows security auditing.	4572	Inicia de sesión esnecial		Buscar
Eventos reenviados	Q Auditoría correcta 20/05/2012 10:52:09 a.m	Microsoft Windows security auditing.	4624	Inicio de sesión		Guardar eventos romo
E Registros de aplicaciones y servicios	Auditoria correcta 20/05/2012 10:52:09 a.m.	Microsoft Windows security audition.	4672	Inicia de sesión especial		ICI CONTRACTORISTICS
Eventos de hardware	Q Auditoría correcta 20/05/2012 10:51:15 a.m	Microsoft Windows security auditing.	4634	Cerrar sesión		Adjuntar tarea a este registro
Internet Explorer	Q Auditoría correcta 20/05/2012 10:51:15 a.m	Microsoft Windows security auditing.	4672	Inicio de sesión especial		Ver >
key Management Service	Auditoría correcta 20/05/2012 10:51:15 a.m	Microsoft Windows security auditing.	4624	Inicia de sesión		But
E Hurdson	Q Auditoría correcta 20/05/2012 10:51:15 a.m	Microsoft Windows security auditing.	4648	Inicia de sesión		Q Actualizar
Replicación DPS	Q Auditoria correcta 20/05/2012 10:51:15 a.m	Microsoft Windows security auditing.	4769	Operaciones de vale	-	🛛 🕜 Ayuda 🔹 🔸
Servicio de directorio	Evento 4634, Microsoft Windows security au	liting.			x	Evento 4634, Microsoft Windows security audi *
Suscripciones	General Detalles					Propiedades de evento
					-	Afjurtar tarea a este evento
	Ca camó cación an una cuanta				÷	
	pe certo sesion en una cuerta.					ta Copiar +
	Nombre de registro: Seguridad					Guardar eventos seleccionados
	Origen: Microsoft Wind	ows security auditing. Registra	do: 20/1	05/2012 10:52:19 a.m.	_	Actualizar
	ld, del evento: 4634	Catenor	a de tarea: Cen	rar sesión		🛛 Ayuda 🔶 🕨
		Calego			•	
	Manh Tafannarian	Relident	Albento Base	latenia semasta		
🕅 Tricio 🛛 🚡 🔳 🖉 Yisor de eventos 🖉 🗟 🙆 10.53 a.m.						

Configuración del Firewall

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

Papelera de reciclaje	Firewall de Windows Activar o desactivar Firewall de Windows Permitir un programa a través del Firewall de Windows	Firewall de Windows Firewall de Windows puede ayudar a prevenir que piratas informat acceso al equipo a través de Internet o la red. FComo me ayuda un firewall a proteger el equipo?	icos o software malintencionado	Cerra
		Firewali de Vindows esta atyldando a proteger el equipo Firewali de Windows esta activado. Las conexiones de entrada que no tienen ninguna excepción esta Mostrar una notificación cuando un programa esté bloqueado: Ubicación de red: 20ué son las ubicaciones de red?	Cambiar la configuración n bloqueadas. No Red de dominio	
	Vea también Centro de redes			
😂 Inicio 📋 🚠	📃 🛛 📓 🔐 Firewall de Wind	ows] ES 👸 🔞	👌 11:06 a.m.

Figura 101 Firewall de Windows



<text></text>	🖥 Firewall de W	indows		X
Ves tambe Centro de tedes Tende : De Franci de Workey Providence state de Tana	Percendi de Velocita		maticos o software malintenoconado obtengan acceso al equipo a traves de Internet o la red.	K (1.
	Inicio	E Freval de Windows		FS 🕺 🗐 (h 08:04 p.m.

Figura 103 Firewall Activado

Firewall de Windows		_ _ 8
Activar o desactivar Firewall de Windowr	Firewall de Windows	•
Permitir un programa a través del Firewall de Windows	Firewall de Windows puede ayudar a prevenir que piratas info o la red.	ormáticos o software malintencionado obtengan acceso al equipo a través de Internet
	¿Cómo me ayuda un firewall a proteger el equipo?	General Excepciones Opciones avanzadas
	Firewall de Windows está ayudando a proteger el equip	Firewall de Windows está ayudando a proteger el equipo
	Las conexiones de entrada que no tienen ninguna excepció Mortrar una notificación cuando un programa esté bloque	Firewall de Windows ayuda a proteger su equipo al impedir que usuarios sin autorización o software malintencionado obtengan acceso al equipo a través de Internet o de una red.
	Ubicación de red:	🕑 🧿 Activado
	2001e son las unicaciones de red:	Esta configuración no permite que ningún origen externo se conecte al equipo, excepto aquéllos desbloqueados en la ficha Excepciones.
		Bloquear todas la conexiones entrantes Seleccione esta opción cuando se conecte a una red en ubicaciones menos seguras. Se emitién todas las exceptiones y no recibrá ningún aviso cuando Firewall de Windows bloque los programias.
		😢 C Desactivado
		Evite usar esta configuración. Si desactiva hirawall de Vindowis, este equipo será más vulherable a accesos no autorizados o a software maintencionado.
		Más información acerca de esta configuración
Vea también		Aceptar Cancelar Aplicar
Centro de redes		
Inicio 🛛 🚠 📰 🖉	Firewall de Windows	ES 🚳 🛃 🏠 08:05 p.m

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

📔 Usuarios y equipos de Active Director			_[8] ×
Archivo Acción Ver Ayuda			
🍬 🔿 🖄 📅 🥉 🖬 🗶 🖻 🖄	2 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
📴 Usuarios y equipos de Active Directory [SR	Nombre	Tipo	Descripción -
Constance productions and an entropy of the second s	Juncte Bergenstein der Gennino Bennetzeis der dernino Besteins der Gennino Besteins der Gennino Besteins der Genning Besteins der Genning Besteins der Genning Besteins der Genning der Genning Besteins der Besteins Besteins der Besteins der Genning der Besteins der Besteins der Genning der Besteins der Besteins der Genning der Besteins der Besteins der Besteins der Besteins der Besteins der Besteins der Besteins der Besteins der Besteins der Bestein Besteins der Bestein der Besteins der Bestein Besteinstein der Besteinstein der Bestein Besteinstein der Besteinstein der Besteinstein Besteinstein der Besteinstein der Besteinstein der Besteinstein Besteinstein der Besteinstein der Besteinstein der Besteinstein Besteinstein der Besteinstein der Besteinstein der Besteinstein Bestein der Besteinstein der Bestein der Bestein der Besteinstein der Bestein der Besteinstein der Besteinstein der Besteinstein der Besteinstein der Besteinstein der Bestein	Concerte seguride - C Grape te seguride - C	Longenter L
🐉 Inicio 🛛 🚠 📃 👘 🗍 📴 Usuar	rios y equipos de		ES 👰 🗐 🕼 10:59 am.

Figura 104 Administración Grupo Esquema

Figura 105 Administración Grupo del Dominio

Figura 106 Administración de Grupo Empresa

📴 Usuarios y equipos de Active Director	1			_ 8 ×		
Archivo Acción Ver Ayuda						
🗢 🔿 🙍 🖬 🥉 🖬 🗶 🖻 🙆	8 🛛 🖬 🕇 🔌 😫 🍸 💆 🕭					
Usuarios y equipos de Active Directory [SR	Nombre	Tipo	Descripción +			
Louiser, reapond & Athen Einstony (SP Constant and the Timestony (SP Constant and the Timestony (SP Constant and the Timestony (SP Longenter SP Longent	Janzies de Comino S. Usaarios de Comino S. Cratolocitores de comino S. Cratolocitores de comino S. Lapiose de dorino S. Lapiose de dorino S. Lapiose de dorino S. Laboratores de HCP S. Sendores 24,5 e LAS C. Cratolocitores de comino de solo lectura S. Cratolocitores de comino de solo lectura S. Projektica de comino de solo lectura S. Diractoristar de cominador de dectores de grupo S. Diractoristar de comissión de cominador de solo de dectores S. Diractoristar de seguenta S. Antonicolatores de seguenta S. Antonicolatores de seguenta S. Esupon Nale	Teo Grapo de segurida - C Grapo de segurida - C	Bergroße + odes & Administrationes de empresas	de los usuanos a engresa. el domino. el domino. o produto de domino de siño lectura en el domino. ambre de otros dentes (bales cano servidores DHCP).		
<u> </u>						
				, , ,		
🖉 Inicio 🛛 🚋 📃 🔤 🗍 📴 Usuar	🚺 Inicio 🛛 🚡 📕 🔰 🔁 Usuarios y equipos de 🛛 ES 👰 🔞 👔 11:00 a.m.					

Bloqueo automático de sesión activada (a 5 minutos)

) 2 🖬 🛛 🛓 🛛	27			
irectiva Bloqueo de equipos (SR 🖟 Configuración del equipo	🦉 🧧 Pantalia	-		Propiedades de Proteger el protector de pantalla mediante co
Incretaria I	Proteger of protector de pantala mediatic contracella I Nestrar gracefades I Nestrar gracefades I Personality I Personality	Configuración Tesma de control (2) Quitor el demento Partalia en Parela de control 2) Quitor la ficia Apartencia y tesma 2) Dutaría ficia Sentore 2) Dutaría ficia Sentore 2) Dutaría ficia Sentore 2) Dutaría ficia Sentore 2) Dutaría de Sentore 2) Dutaría de Sentore 2) Dutaría de Sentore 2) Dutaría de Sentore 2) Entore de articipación 2) Tespo de capos de doractor de partalia 2) Tespo de capos de doractor de partalia	Etiské No orfigurála No orfigurála No orfigurála No orfigurála No orfigurála No orfigurála No orfigurála	Configuración Espicación Conertano Pologra el pratector de partala mediante contraveña No configurada Abitada Deshabitada Compañía con Rimenos Microsoft Windows 2000 Service Pack 1 Viáor anterior Viáor aparteci Respire Cancolar Acester Cancolar Acester Cancolar Acester Acester Cancolar Acester Acester Acester Acester Aces
	Extendido (Estándar /			

Figura 107 GPO Proteger con contraseña

Figura 108 Activación del protector de pantalla

ectiva Bloqueo de equipos [SRV	📫 Pantalla				
Configuración del equipo	-	-		Propiedades de Protector de pantalia	1
Directivas Preferencias	Protector de pantalla	Configuración	Estado Cr	Configuración Explicación Comentario	
Configuración de usuario	Mostrar <u>propiedades</u>	Quitar el elemento Pantalla en Panel de control Cultar la ficha Apariencia y temas	No configurada No configurada	Protector de paritalia	
Configuración de Softix Configuración de Windi Pantillas administrativa	Al menos Microsoft Windows 2000 Service Pack 1	El Ocultar la ficha Escritorio El Ocultar la ficha Protector de pantalla	No configurada No configurada	C No configurada	
Carpetas compartir Componentes de V	Descripción: Habilita los protectores de pantalla del	El Ocultar la ficha Configuración Protector de pantalla	No configurada Habilitada	C Deshabiltada	
Elistotrio Elistotrio Mexi Julio y barrel Ared & control Areade & control Configuración Transa del Transa del Portenia Red Stema Configuración del Portenia Red Stema Configuración del Portenia Totos los valores Performas	Sections. Sectionalise sets applies the sets epicotan to protectives de partala- section Protectives de partala de la section Protectives de partalàs de la section Protectives de partalàs de la contra La nomesiones a los usareses protector de partalas. Si la holtas, se ejecuta un protector te partala, este quanta de la partala, se partala, este quanta un protector la partala, este quanta un protector la partala, este quanta un protector de partala, este quanta un partector de charada esteraria de aporta de anterio de oponh Nomes de entro equadado in realista	■ indirect de atomo escudade de protector de partala Photoper optication de partala neadra tombeñ ■ Tempo de espara de partactor de partala ■ Impedir cambos en el pagel taoz	na ongurata Habilada Habilada Na onfyrada	Compatible con: A mence Moscott Windows 2000 Service Red Valor anterior Valor arguiente Aceptar Cancelar Cancelar	k 1
_	ciente; como segunda condición, el tiempo de espera del protector de pantalla se establece en un valor diferente de cero mediante la opción				

Figur. _8× <u>?</u>× Propiedades de Tiempo de espera del p Tiempo de espera del protector de Configuración pantalla Estado Ct Configuración Explicación Comentario Comparadio
 Comparadio
 Term de econtrol
 Term de econtrol
 Coultre la deventra Paralialis en Areal de control
 Coultre la de Acoreccia y terms
 Coultr No configurada No configurada No configurada No configurada Habilitada No configurada Habilitada Tiempo de espera del protector de partalia C No configurada Habilitada C Deshabilitada Número de segundos de espera hasta que se active el protector de pant Habilitada Habilitada Segundos: 300 🗼 No configurada Cuando se configura, este tiempo de inactividad se puede establecer desde un mínimo de 1 segundo hasta un máximo de 86.400 segundos o 24 horas. Si se establece en cero, no se iniciará el protector de pantalla. 📔 Programas Esta opción no surte efecto en cualquiera de las siguientes circunstancias: E Sistema 4 • Compatible con: Al menos Microsoft Windows 2000 Service Pack 1 a 18 -La opción está deshabilitada o no e ha configurado. Valor anterior Valor siguiente El tiempo de espera está istablecido en cero. Aceptar Cancelar - Se ha habilitado la opción "Sin rotector de pantalla". -Ni la opción "Nontre del archivo ejecutable del protector de pantalla" Extendido / Estándar / 🚺 Thicio 📃 🚠 🖞 🔐 🗿 🙏 📴 🚱 🚊 🚾 🖉 Windows Update 🛛 🚊 Administración de directi... 📑 Editor de admi ES 🛃 🕄 🌖 12:52 p.m. nistraci_

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-lainvestigacion-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/AAAAAAAAAAFo/lxb9ExTwNO8/s1600/ servidor-dhcp.png EI 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/usandosamba/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/eses/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/eses/library/cc732912.aspx El 09/05/12