Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Administración de Directivas de Grupo para la configuración segura de Sistemas Corporativos basados en Windows Server 2012

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Manuel López Pérez

Tutores: Juan Luis Posadas Yagüe

Juan Carlos Cano Escribá

2014/2015

Resumen

En el presente documento se explican las bases de administración de la seguridad de *Windows Server 2012* con directivas de grupo, partiendo de cero, instalando en primer lugar el sistema operativo, diseñando la estructura del dominio e implementando el mismo, se detalla la creación del bosque, así como la administración de los elementos más importantes que lo componen, el establecimiento y configuración correctamente de *Active Directory* y de las unidades organizativas y usuarios con sus correspondientes roles utilizando un caso de estudio de una empresa real. El proyecto se centra en el tema de la configuración segura del sistema *Windows Server* 2012 mediante directivas de grupo.

Palabras clave: Sistema operativo, directivas de grupo, directorio activo, seguridad, *Windows Server 2012*.

Abstract

This document security management bases of Windows Server 2012 with Group are explained, from scratch, installing the operating system, the domain structure designing and implementing of it, creating is detailed forest as well as administration of the most important elements that compose it, the establishment and configuration of Active Directory correctly and organizational units and users with corresponding roles using a case study of a real company. The project will focus more on the issue of securitization of Windows Server 2012 system through Group Policies.

Keywords: Operating system, group policy object, Active Directory, security, Windows Server 2012.

Índice de contenidos

Índice de capturas

Índice de figuras

Índice de tablas

1. Introducción

1.1. Motivación

Los sistemas de información en las empresas tienen un gran impacto al ir trabajando con grandes volúmenes de información, conforme va pasando el tiempo y evolucionando la tecnología. Para organizar y gestionar esta gran cantidad de información se necesita un sistema que garantice la disponibilidad, el acceso y la seguridad de la misma, al menor coste posible.

Planificar y gestionar la infraestructura de TIC de una organización es un trabajo difícil y complejo que requiere una base muy sólida en la aplicación de los conceptos fundamentales en áreas como la informática, así como de gestión y habilidades del personal. En sistemas de información hay importantes preocupaciones de software como la fiabilidad, seguridad, facilidad de uso y la eficacia y eficiencia para los fines previstos, todas estas preocupaciones son vitales para cualquier tipo de organización.

Los sistemas corporativos basados en red permiten a las empresas gestionar estos recursos, posibilitando su uso compartido, ofreciendo herramientas que garanticen la seguridad y la disponibilidad de los mismos. En estos sistemas se puede gestionar el acceso a los recursos, dividir la empresa en sus distintos departamentos (con sus respectivos empleados) organizarlos en unidades organizativas, compartir tanto escáneres e impresoras en red (normalmente suelen ser unidades multifunción), etc.

Los sistemas operativos de Microsoft van cogiendo cada vez más importancia y aceptación en el mundo empresarial, debido a que ofrece una solución estable y fiable para los sistemas de información de cualquier empresa, debido a que son los más utilizados por los usuarios. La última versión de sistema operativo de Microsoft para este propósito es *Windows Server (*en adelante WS*) 2012*, tiene diferentes versiones para cada empresa y son las siguientes:

- ***Datacenter*:** Para entornos de nube privada con un alto grado de virtualización.
- ***Standard*:** Para entornos con hasta 2 instancias de virtualización.
- ***Essentials*:** Para pequeñas y medianas empresas (hasta 25 usuarios), esa versión no permite la virtualización.
- ***Foundation*:** Para pequeñas empresas (hasta 15 usuarios) instalado en servidores monoprocesador, esa versión no permite la virtualización.

El sistema operativo está diseñado para trabajar de forma óptima con *Windows* 8, 8.1 y próximamente con *Windows* 10, al igual que con su predecesor *Windows* 7. Existe además la posibilidad de trabajar directamente sobre el servidor, bien para administrar el mismo o bien para ejecutar aplicaciones instaladas allí, como su antecesor *Windows Server 2008*.

1.2. Objetivo

El objetivo fundamental que persigue este Trabajo de Final de Grado (en adelante TFG) es establecer una guía que pueda dotar al futuro graduado en Ingeniería Informática de los conocimientos necesarios para diseñar, implementar, configurar y evaluar la seguridad de los sistemas WS 2012 utilizando directivas de grupo, intentado que se ajuste al máximo a la realidad que se encontrará al incorporarse al mercado laboral. Para ese fin se utilizará un caso de estudio de una empresa real en la cual se implementará. La figura 1 muestra una pequeña distribución de la topología de red de la empresa, la cual se verá afectada cuando se implemente el estudio realizado en este TFG.

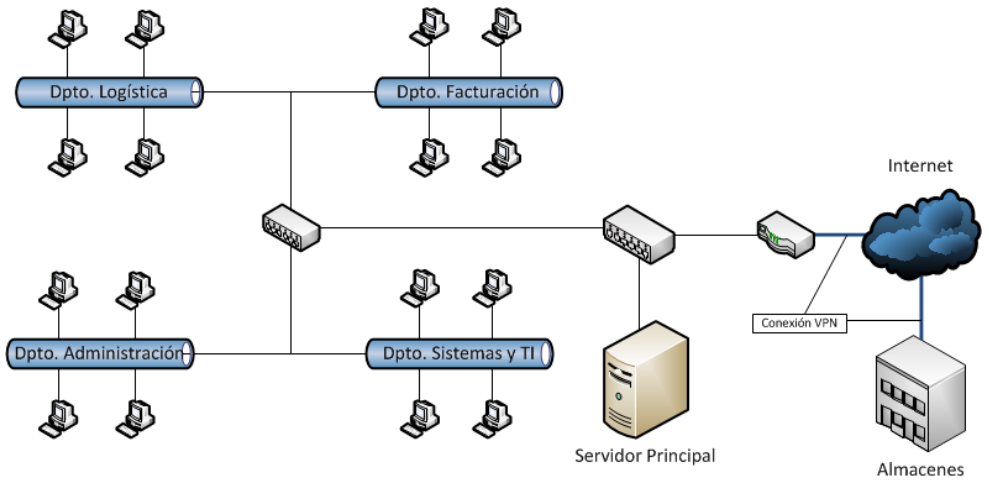


Figura 1 Topología de la red de la empresa

Para la realización de las pruebas, antes de ponerlo en funcionamiento en la empresa, se definirá un entorno ficticio (el entorno contará con un gran parecido con la realidad de la empresa) con varios departamentos con sus respectivos trabajadores y con sus limitaciones a la hora de acceder a los recursos. Para ello utilizaremos el siguiente caso de estudio:

CASO DE ESTUDIO

Dentro de la compañía Car Volum S.L., los usuarios, ordenadores y recursos generales se quiere mejorar la organización de ellos en los diferentes departamentos: Logística, Facturación, Administración e Sistemas y TI.

Departamento de Logística:

Este departamento está formado por los ordenadores y usuarios que se encargan de todo lo relacionado con la administración de las mercancías que se deben distribuir a sus correspondientes destinos. En particular, el departamento consiste en los siguientes ordenadores, usuarios, roles y recursos:

- **Ordenadores:** Este departamento contiene el acceso local a los ordenadores del departamento de logística (pclogX) y por escritorio remoto a sus respectivos escritorios.
- **Usuarios:** Este departamento está formado por los usuarios que realizan diferentes tareas administrativas de este departamento: Carla de Vries, Amine Ben, Silvia Sarrion e Irene Asencio.

- **Roles:** Todos ellos desempeñan el mismo rol en el departamento, teniendo acceso al directorio de Logística.

Departamento de Facturación:

Este departamento está formado por los ordenadores y usuarios que se encargan de elaborar las facturas emitidas desde los departamentos Operadores TTE y Logística. En particular, el departamento consiste en los siguientes ordenadores, usuarios, roles y recursos:

- **Ordenadores:** Contiene el acceso a los ordenadores del departamento de facturación (pcfacX) y por escritorio remoto a sus respectivos escritorios.
- **Usuarios:** Este departamento está formado por los usuarios que realizan diferentes tareas administrativas de este departamento: Marisa Pérez e Silvia Martínez.
- **Roles:** Todos ellos desempeñan el mismo rol en el departamento, teniendo acceso al directorio de Facturación.

Departamento de Administración:

Este departamento está formado por los ordenadores y usuarios que se encargan de administrar las facturas emitidas a los clientes como a los acreedores. Las funciones generales son: contabiliza las facturas emitidas y recibidas, cobra a los clientes, pagar a los proveedores y a los empleados, y liquida los impuestos en las fechas correspondientes. En particular, el departamento consiste en los siguientes ordenadores, usuarios, roles y recursos:

- **Ordenadores:** Contiene el acceso a los ordenadores del departamento de administración de facturas (pcadmX) y por escritorio remoto a sus respectivos escritorios.
- **Usuarios:** Este departamento está formado por los usuarios que realizan diferentes tareas administrativas en el dominio de este departamento: Patricia García e María José Salvador.
- **Roles:** Todos ellos desempeñan el mismo rol en el departamento, teniendo acceso al directorio de Administración y al de Facturación.

Departamento de Sistemas y TI:

Este departamento está formado por los ordenadores y usuarios que participan en la administración del dominio. En particular, el departamento consiste en los siguientes ordenadores, usuarios, roles y recursos:

- **Ordenadores:** Este departamento contiene los servidores de la compañía y los ordenadores del departamento (pcsisX).
- **Usuarios:** Este departamento está formado por los usuarios que realizan diferentes tareas administrativas en el dominio: Fede de Luna e Manuel López.
- **Roles:** Todos ellos desempeñan el mismo rol de administradores del sistema.
- **Recursos:** Este departamento tiene varias carpetas que contienen la información de usuario que debe estar disponible para los usuarios del dominio. Tales carpetas están almacenadas en los servidores y se ofrecen al resto de ordenadores del dominio como carpetas compartidas. Las carpetas que están definidas actualmente son las siguientes: Logística, Facturación, Administración y Sistemas y TI.

Acerca de los recursos a los que pueden acceder:

Esta sección detalla los diferentes niveles de acceso que deben definirse para cada uno de los recursos (carpetas, archivos, etc.) de la compañía. Para cada recurso, sus niveles de acceso deben cumplirse independientemente del ordenador desde donde el recurso vaya a ser accedido. Cada nivel de acceso se asocia con uno o más roles previamente definidos en este documento, de tal forma que solo los usuarios que desempeñan tales roles deben tener concedido dicho nivel.

- **Niveles de acceso a la carpeta Logística:**

NIVEL DE ACCESO	ROLES RELACIONADOS	DESCRIPCIÓN
Completo	*Domain Admins*	Este nivel contempla todos los permisos posibles; esto incluye crear, modificar, borrar, cambio de permisos y toma de posesión de cualquier fichero y subcarpeta del proyecto.
Modificación	Logística	Este nivel incluye permisos para crear, borrar, leer y modificar cualquier fichero o subcarpeta; sin embargo, no incluye el cambio de atributos de protección de ficheros o subcarpetas.
Lectura	*Domain Users*	Este nivel incluye acceso de lectura para todo fichero y carpeta existente en la carpeta; sin embargo, crear, modificar o borrar ficheros o subcarpetas no está permitido.

Tabla 1 Roles de la carpeta Logística

- **Niveles de acceso a la carpeta Facturación:**

NIVEL DE ACCESO	ROLES RELACIONADOS	DESCRIPCIÓN
Completo	*Domain Admins*	Este nivel contempla todos los permisos posibles; esto incluye crear, modificar, borrar, cambio de permisos y toma de posesión de cualquier fichero y subcarpeta del proyecto.
Modificación	Facturación Administración	Este nivel incluye permisos para crear, borrar, leer y modificar cualquier fichero o subcarpeta; sin embargo, no incluye el cambio de atributos de protección de ficheros o subcarpetas.
Lectura	*Domain Users*	Este nivel incluye acceso de lectura para todo fichero y carpeta existente en la carpeta; sin embargo, crear, modificar o borrar ficheros o subcarpetas no está permitido.

Tabla 2 Roles de la carpeta Facturación

- **Niveles de acceso a la carpeta Administración:**

NIVEL DE ACCESO	ROLES RELACIONADOS	DESCRIPCIÓN
Completo	*Domain Admins*	Este nivel contempla todos los permisos posibles; esto incluye crear, modificar, borrar, cambio de permisos y toma de posesión de cualquier fichero y subcarpeta del proyecto.
Modificación	Administración	Este nivel incluye permisos para crear, borrar, leer y modificar cualquier fichero o subcarpeta; sin embargo, no incluye el cambio de atributos de protección de ficheros o subcarpetas.
Lectura	*Domain Users*	Este nivel incluye acceso de lectura para todo fichero y carpeta existente en la carpeta; sin embargo, crear, modificar o borrar ficheros o subcarpetas no está permitido.

Tabla 3 Roles de la carpeta Administración

1.3. Materiales utilizados

Con el fin de que este proyecto se asemeje lo máximo posible a la realidad se utilizará un equipo como servidor. El equipo utilizado para las pruebas será proporcionado por la universidad en el laboratorio de TFG en el cual se instalará un sistema operativo servidor y todo el software necesario para la realización de este trabajo.

El sistema operativo usado para la instalación de los servidores que aparecen en este trabajo será de la familia WS 2012, en concreto, se instalará *Microsoft Windows Server 2012 R2 Standard*, instalado bajo licencia obtenida en el marco del programa "*Microsoft Dream Spark*", que facilita a los estudiantes de la Universidad Politécnica de Valencia la descarga de software de Microsoft.

Se manejará la versión del sistema *Standard* debido a que en la empresa, donde se realizará en un futuro la implementación de este TFG, contiene varias máquinas virtuales y el número de empleados es superior a 30 en la sede central más otros tantos distribuidos por los diferentes almacenes y sucursales en varias comunidades, dichos usuarios se conectarán por vía VPN a la sede principal de la empresa.

2. Instalación del sistema

En esta sección del TFG procederemos a instalar el sistema operativo *WS 2012 Standard* donde realizaremos la pruebas de seguridad, dicho servidor estará formado por roles que desempeña en la empresa como por ejemplo DHPC, DNS, etc.

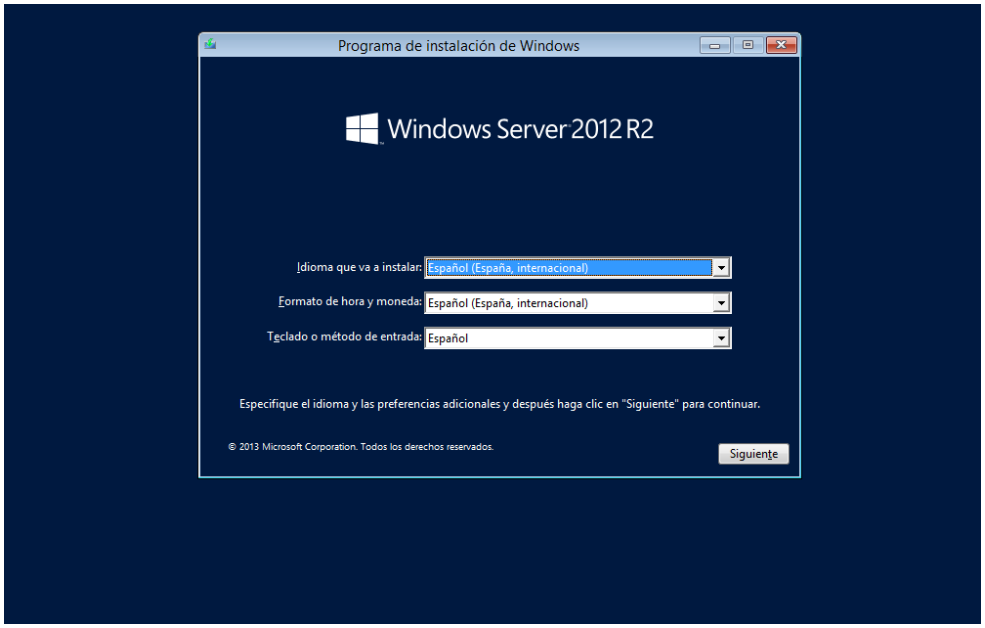
El servidor de prueba que se utilizará en el laboratorio de TFG de la Universidad Politécnica de Valencia tiene recursos limitados, dichos recursos son los siguientes:

- **Procesador:** Intel Core I5-760 a 2.80GHz
- **Memoria RAM:** 4GB
- **Disco Duro:** 320GB

Para la realización de pruebas dichos recursos nos bastan aunque en la empresa donde se pretende implementar la configuración documentada en este TFG el servidor dispone de los siguientes recursos:

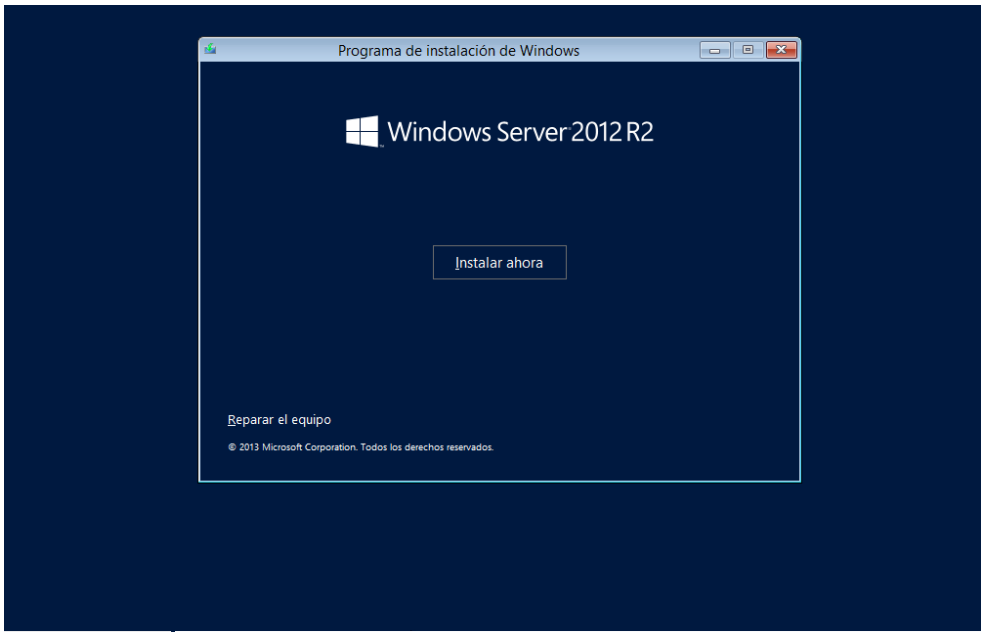
- **Procesador:** 2 procesadores Intel Xeon E5620 a 2.40GHz
- **Memoria RAM:** 40GB
- **Disco Duro:** Cabina de discos (500GB asignadas al sistema operativo)

El servidor del laboratorio cuenta con los requisitos para implementar el sistema operativo *WS 2012 R2*. Sabiendo las características del servidor se procederá con la instalación del sistema operativo, en la primera ventana de la instalación se configurará el idioma del sistema como también el formato de hora y moneda como se muestra en la captura 1.



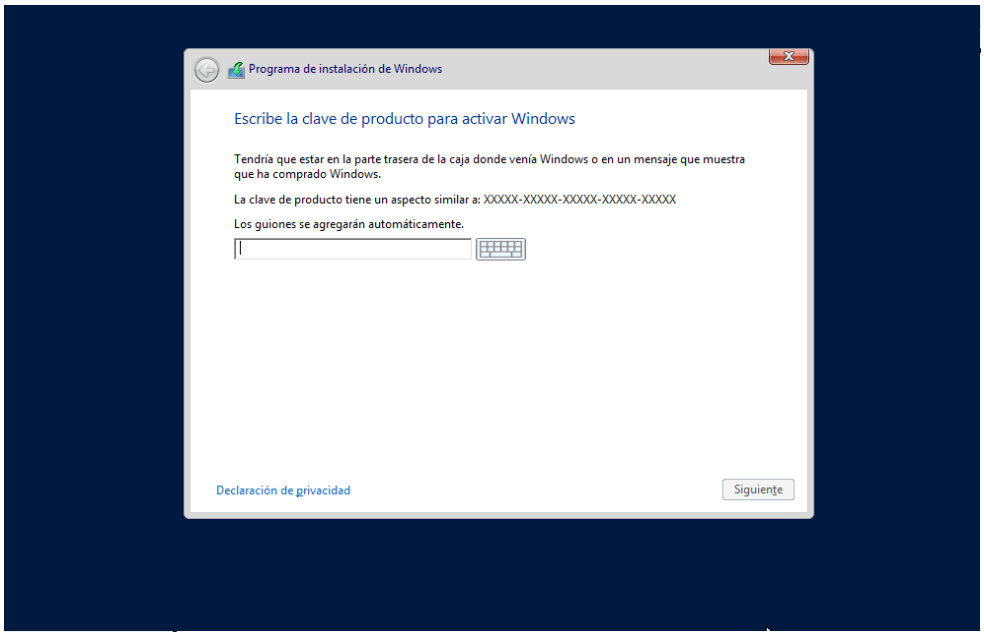
Captura 1 Elección del idioma y formato de hora y moneda

Una vez configurado se clicará en “Siguiente”. En la siguiente ventana se empezará con la instalación clicando en “Instalar ahora”.



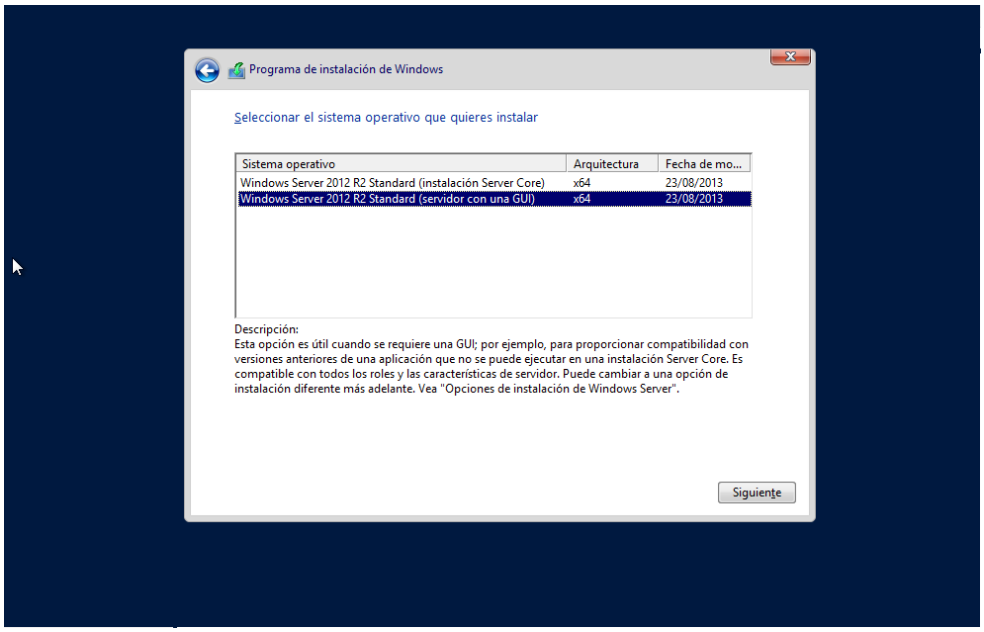
Captura 2 Inicio de la instalación del sistema

Seguidamente pedirá la clave de activación del sistema operativo, la clave que se utilizará será la proporcionada mediante el programa “*Microsoft Dream Spark*” para estudiantes, cuando se instale dicho sistema en la empresa se utilizará una clave comprada. Una vez introducida la clave se clicará en “Siguiente”.



Captura 3 Activación de Windows

En la siguiente ventana es de selección del tipo de sistema operativo que se va instalar.



Captura 4 Selección del sistema operativo a instalar

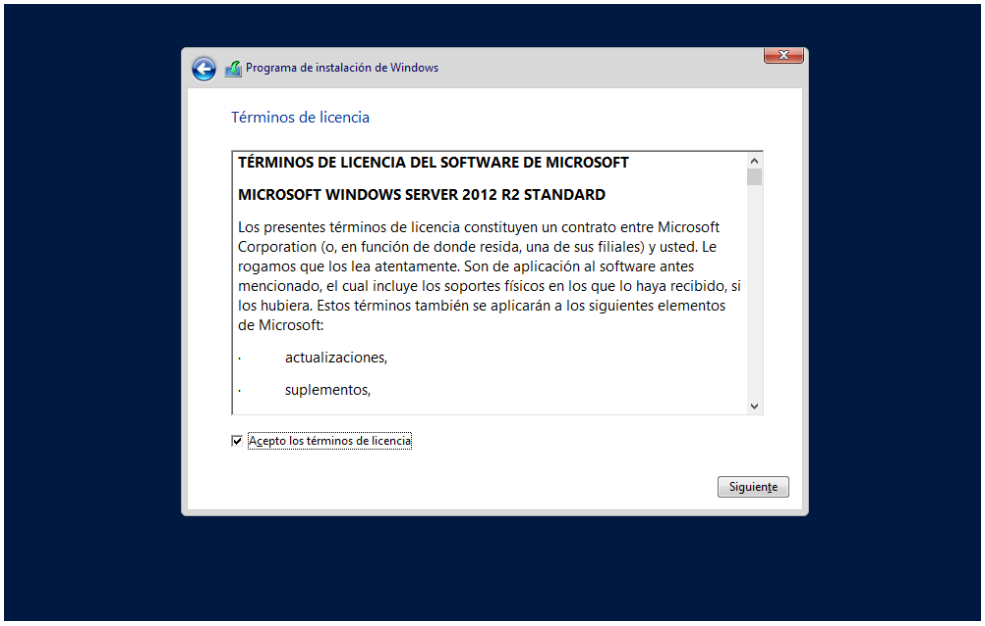
Como se observa en la captura 4, el programa de instalación permite elegir entre dos instalaciones:

- Server Core: instalación mínima, sin ninguna interfaz gráfica.
- Servidor con una GUI[1]: instalación con interfaz gráfica.

Para facilitar las tareas de administración del sistema a instalar se seleccionará la versión con GUI y se clicará en “Siguiente”.

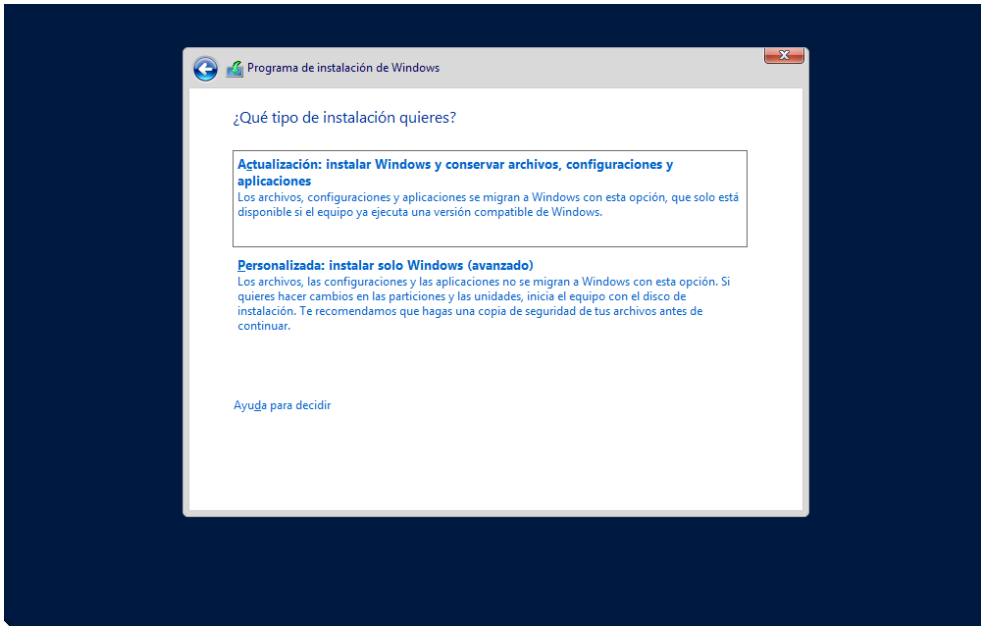
[1] GUI (*Graphic User Interface* o Interfaz Gráfica de Usuario): Es un conjunto de formas y métodos para que el usuario pueda interactuar con el sistema utilizando formas gráficas e imágenes.

Posteriormente, en la siguiente ventana, habiendo leído los términos de licencia del *software* de Microsoft, se aceptarán marcando la casilla "Acepto los términos de licencia" y se clicará en "Siguiente".



Captura 5 Términos de licencia del software de Microsoft

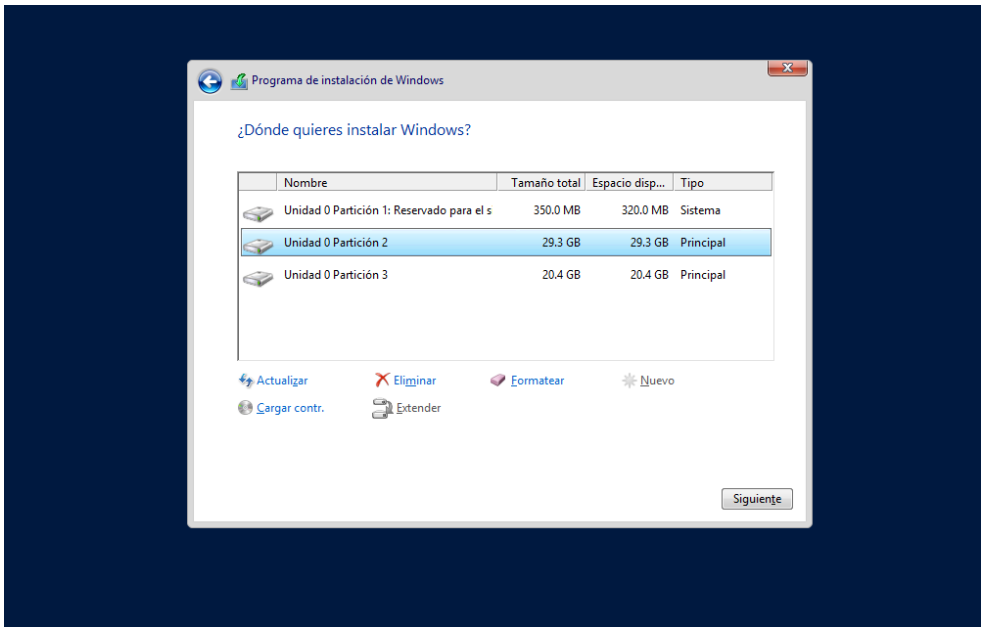
Después se procederá con la configuración de las particiones que tendrá el disco duro. Para tal fin y como es una instalación nueva se clicará en la opción "Personalizada: instalar solo *Windows* (avanzado)".



Captura 6 Selección de tipo de instalación

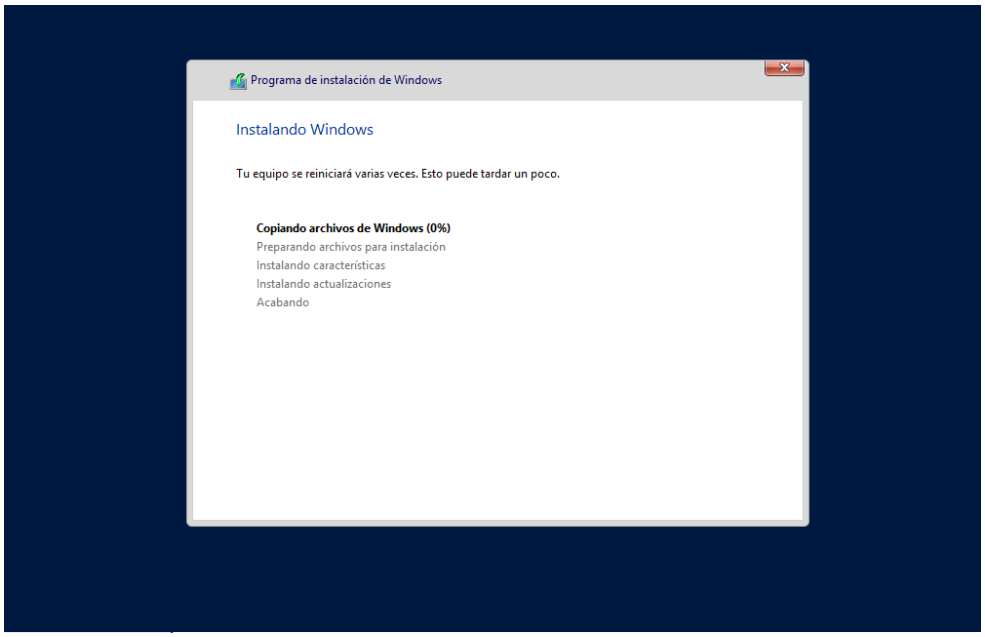
Se abrirá la ventana donde se crean las diferentes particiones. En la empresa donde se implementará la configuración se crearán dos particiones una para el sistema de 320GB y otro como *backup* de 180GB para la bases de datos, en este caso de estudio se crearán las mismas particiones, pero la de *backup* se utilizará para el almacenamiento de los usuarios.

Como en la empresa se utiliza una cabina de discos, la partición secundaria del disco duro del servidor de pruebas no será necesaria ya que el servidor trabaja con máquinas virtuales, con lo cual se le asignarán una cuota de disco a cada máquina y a cada usuario.



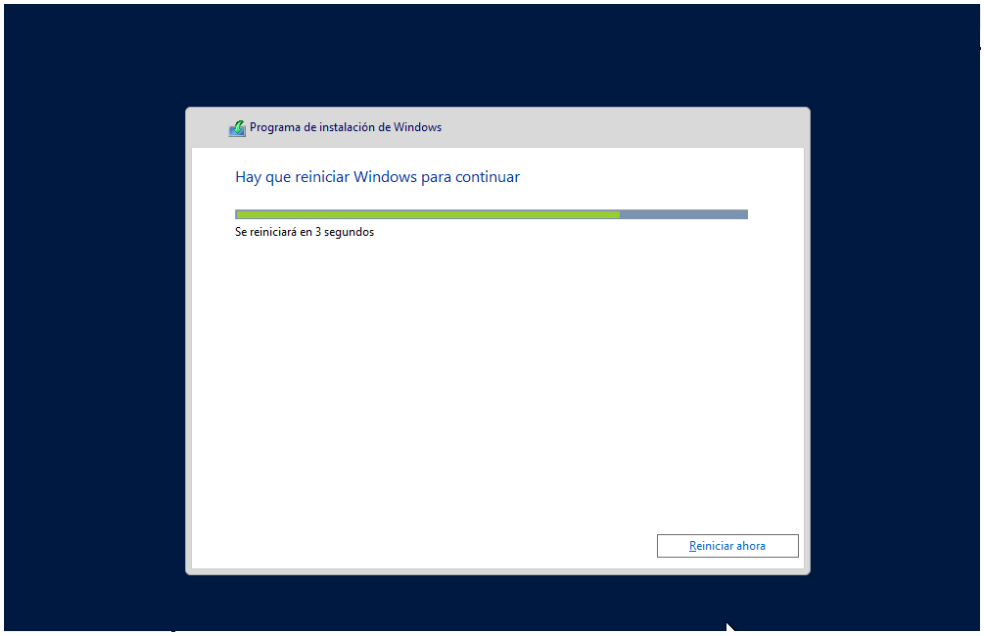
Captura 7 Particiones del disco duro

Una vez creadas las particiones se seleccionará la partición donde irá el sistema y se clicará en “Siguiente”. El sistema empezará con instalación como se observa en la captura 8.



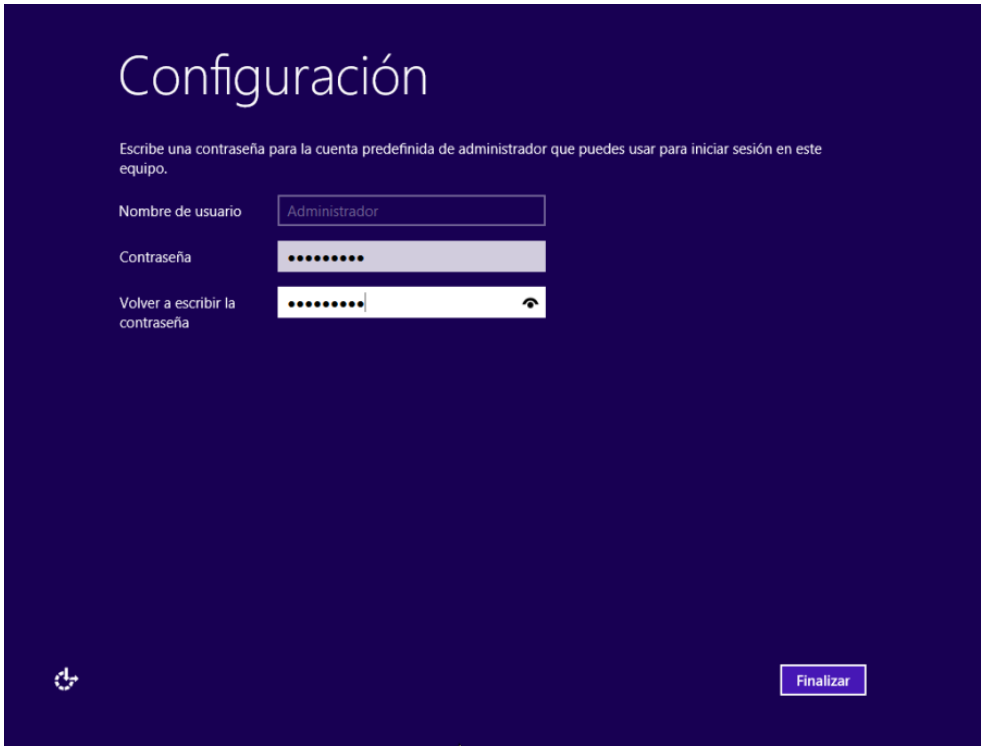
Captura 8 Instalación del sistema

Cuando acabe la instalación el servidor se reiniciará.



Captura 9 Reinicio del sistema para continuar la instalación

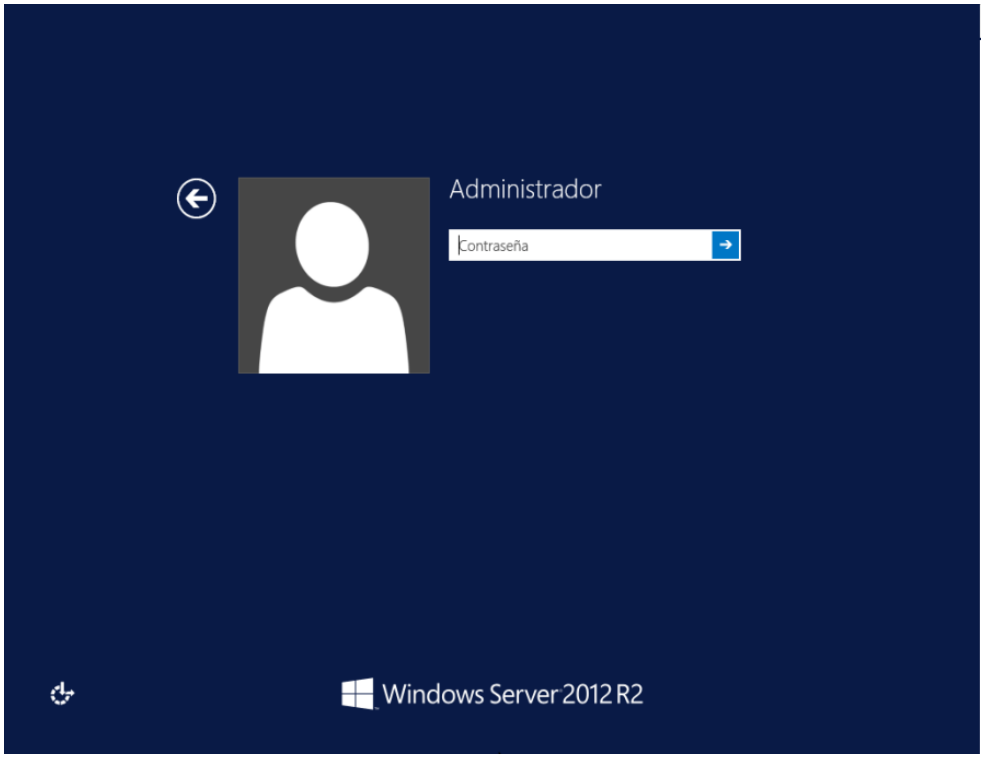
Una vez se reinicie el servidor en la primera ventana que aparece pedirá que se le asigne una contraseña al administrador, esta ventana solo aparecerá una vez. Se pondrá la contraseña y se finalizará la instalación clicando en "Finalizar".



Captura 10 Configuración del usuario Administrador del Sistema

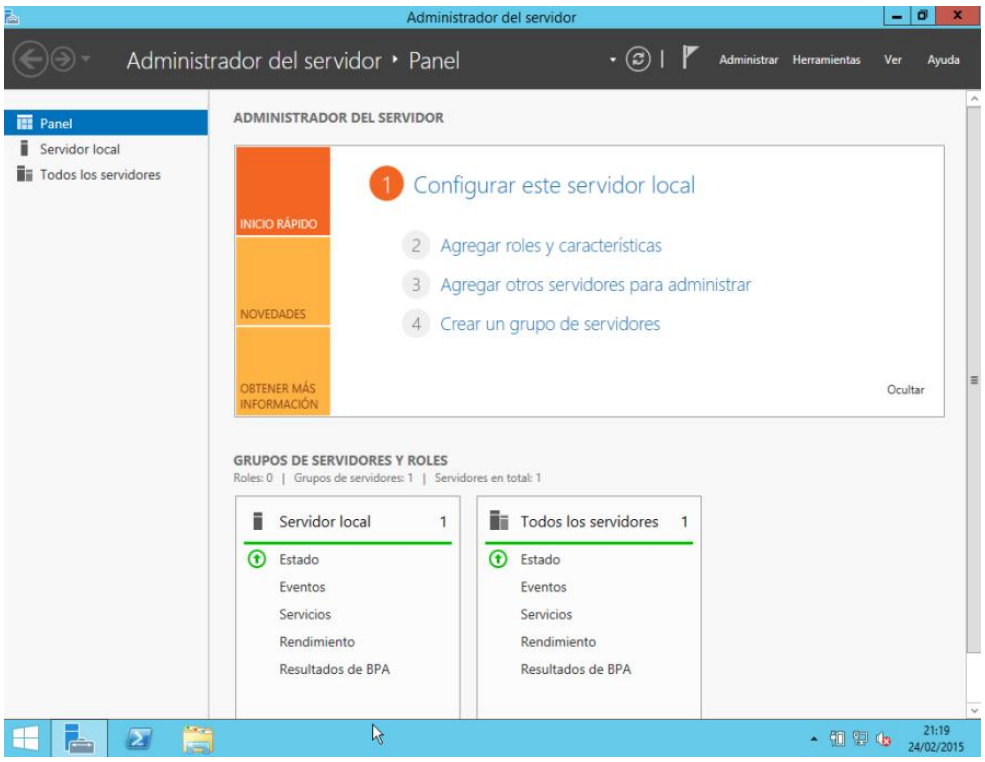
Las capturas 11 y 12 aparecen cada vez que se inicie el sistema. En la captura 11 se pulsará la combinación de teclas que aparece con lo que abrirá la ventana de acceso que se observa en la captura 12 donde se pondrá la contraseña, el usuario que aparezca siempre será el último que hubiera iniciado sesión en el sistema. Una vez puesta la contraseña se pulsará la tecla "Intro" o se clicará la flecha de azul al lado de la contraseña.

Captura 11 Inicio del sistema



Captura 12 Acceso al sistema

La primera ventana que se muestra al iniciar sesión con el usuario administrador será la del "Administrador del servidor", la cual siempre se abrirá a los administradores del sistema a no ser que se configure lo contrario.



Captura 13 Ventana del Administrador del servidor

En esta ventana aparecen todos los roles o configuraciones que están configurados en el sistema, como podemos observar en la captura 13 algunos roles ya vienen instalados por defecto.

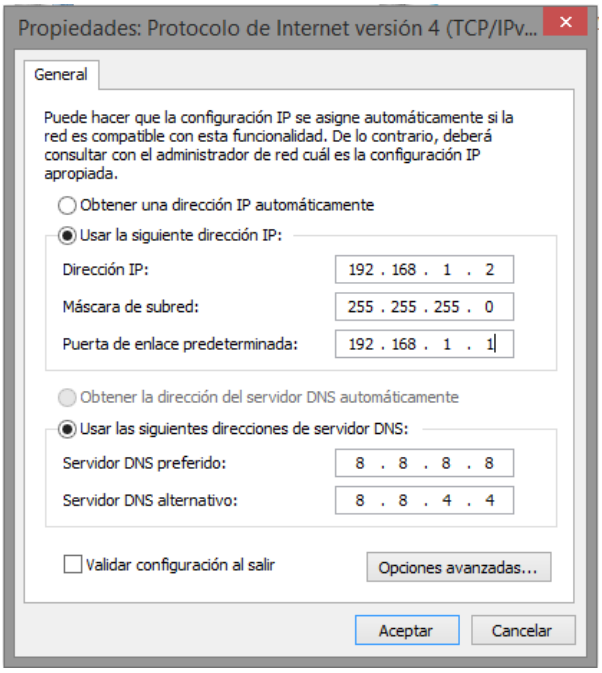
Antes de empezar con la instalación de los roles, configuración de las políticas de seguridad, etc. es necesario a tener en cuenta la estructura de la red de la empresa, dicha red está formada por cuatro subredes (en un futuro se crearán más redes) de hasta 254 ordenadores. Las redes se han distribuido de la siguiente manera:

Red: 192.168.0.0/22

- Subred sede principal Quart de Poblet, Valencia: 192.168.1.0/24
- Subred delegación Agoncillo, La Rioja: 192.168.2.0/24
- Subred delegación Dos Hermanas, Sevilla: 192.168.3.0/24
- Subred almacén Ribarroja, Valencia: 192.168.4.0/24

Como el servidor estará en la sede principal habrá que configurarle una IP estática (en la empresa dicho sistema será una máquina virtual) de la siguiente manera:

- IP: 192.168.1.2
- Mascara: 255.255.255.0
- Puerta de Enlace: 192.168.1.1
- DNS: 8.8.8.8 / 8.8.4.4 (Se pondrán los DNS de Google por ejemplo)



Captura 14 Configuración del adaptador de red del servidor

En un entorno real de la empresa resultaría necesario acometer la instalación de un sistema antivirus potente en el servidor junto algún sistema *firewall*, con el fin de protegerlo de las amenazas de internet, pero para realizar pruebas se instalará un antivirus gratuito (por ejemplo el antivirus *Microsoft Essential*) y el firewall que se utilizará será el de la Universidad Politécnica de Valencia.

Una vez terminado el proceso configuración e instalación del antivirus se dispondrá de un sistema server en funcionamiento en el cual se realizarán las pruebas.

3. *Active Directory*

Active Directory (en adelante AD) es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red. También permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

3.1. Diseño

La unidad principal de la estructura lógica de AD es el dominio. Un dominio es un conjunto de ordenadores, equipos, usuarios, recursos, etc., que comparten una base de datos de directorio común. Los distintos dominios seguirán una estructura de nombres basada en DNS, en el que cada subdominio se creará agregando un identificador a la izquierda del nombre del dominio padre. El uso de dominios permite conseguir los siguientes objetivos:

- Delimitar la seguridad.
- Replicar la información.
- Aplicar directivas de grupo.
- Delegar permisos administrativos.

Para que el dominio funcione debe estar dentro de un árbol, el cual está dentro de un bosque. Un bosque está formado por uno o varios árboles, estos árboles estarán formados por uno o varios dominios.

El primer domino que se crea en AD es el domino raíz del boque, al mismo tiempo se creará el árbol y el bosque que lo contienen, dicho bosque recibirá el mismo nombre del dominio raíz. Los siguientes dominios que se creen y se inserte en el árbol pasaran a ser un dominio secundario o hijo del principal. Toda la estructura antes mencionada está controlada por los controladores de domino, que son aquellos servidores que ejecutan software capaz de mantener la estructura del AD.

Tal y como se ha detallado en la introducción, este trabajo se desarrolla en el marco de una empresa real en cuya sede principal se encuentran los servidores y las oficinas. También cuenta con varios almacenes y sucursales repartidos por el país, los cuales se conectaran con la sede principal mediante conexión vía VPN. Para satisfacer las necesidades de información de la empresa, se ha diseñado el siguiente esquema:

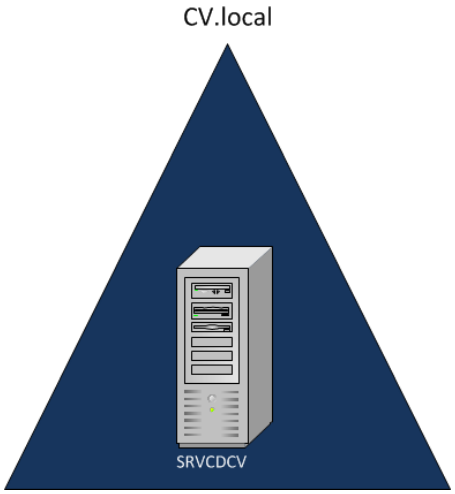
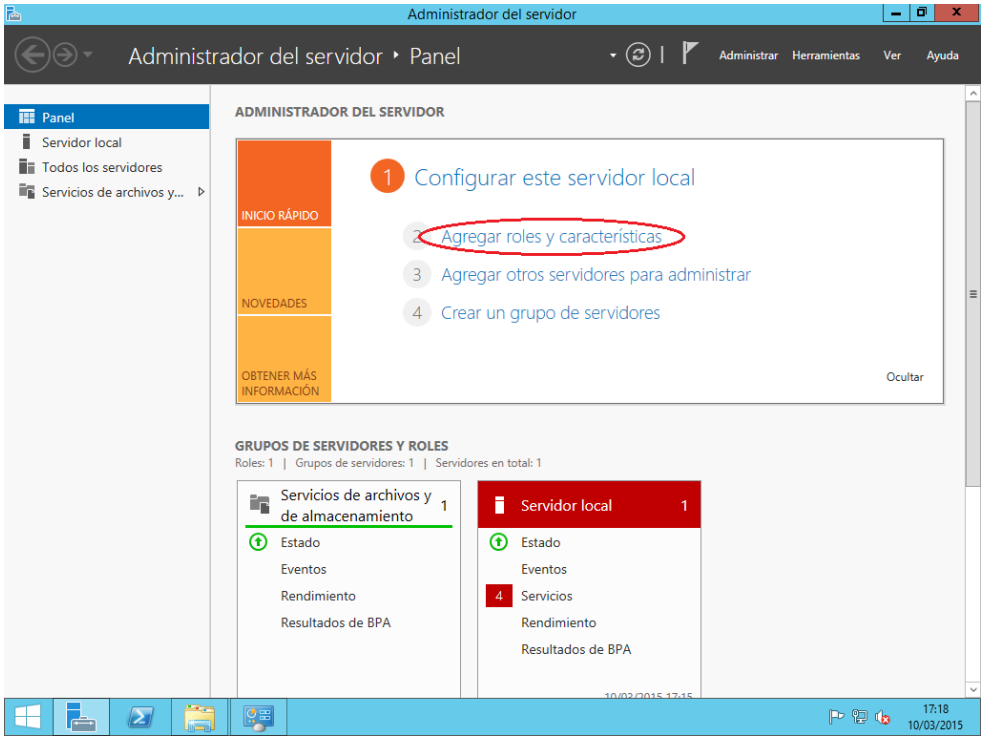


Figura 2 Bosque de la empresa

Como se observar en la Figura 2 la empresa solo contará con un bosque que contiene un árbol con un único domino.

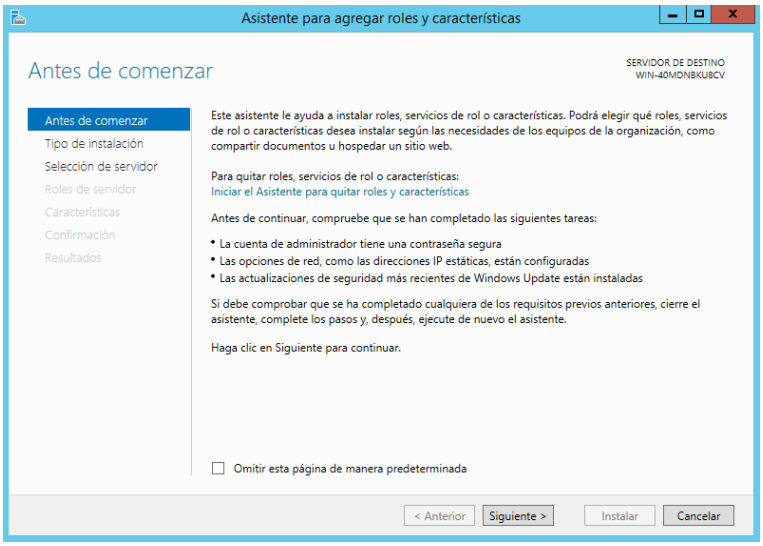
3.2. Creación bosque

El servidor ejercerá el rol de Servicios de dominio de *Active Directory* (AD DS) en el cual se encuentra el bosque del domino. Se procederá con la instalación de dicho rol, para ello se accede al "Administrador del servidor" en el cual se clicará en "Agregar roles y características".



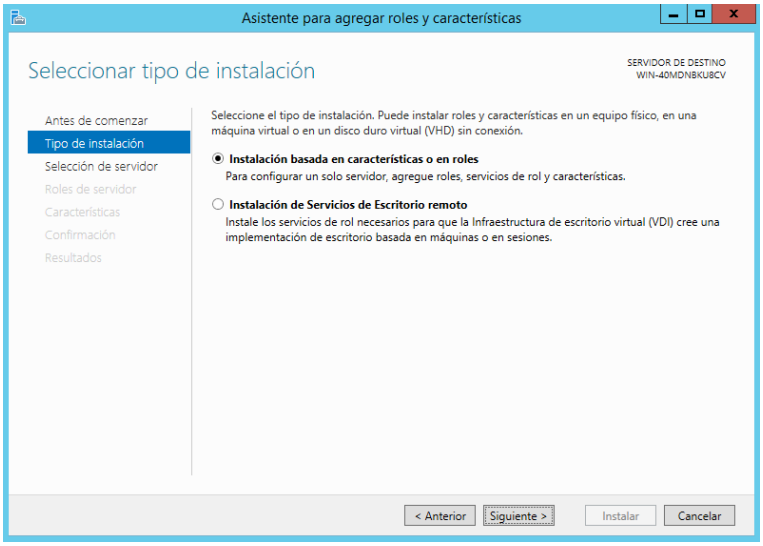
Captura 15 Administrador del servidor, "Agregar roles y características"

Se ejecutará el asistente para agregar roles y características. En dicha ventana se explica que hace el asistente, como buena práctica se debería leer y se marcar la casilla “Omitir esta página de manera predeterminada” para que no vuelva a parecer en otras instalaciones de roles o características y se clicará en “Siguiente” para proseguir con la instalación.



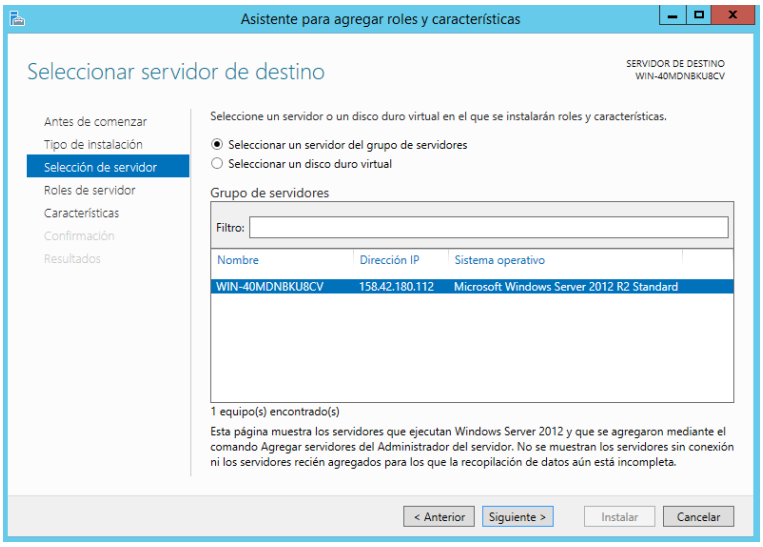
Captura 16 Descripción del asistente “Agregar roles y características”

En la siguiente ventana se seleccionará el tipo de instalación, en este caso como se instalará un rol en el servidor se seleccionará la primera opción “Instalación basada en características o en roles” y se clicará en “Siguiente”.



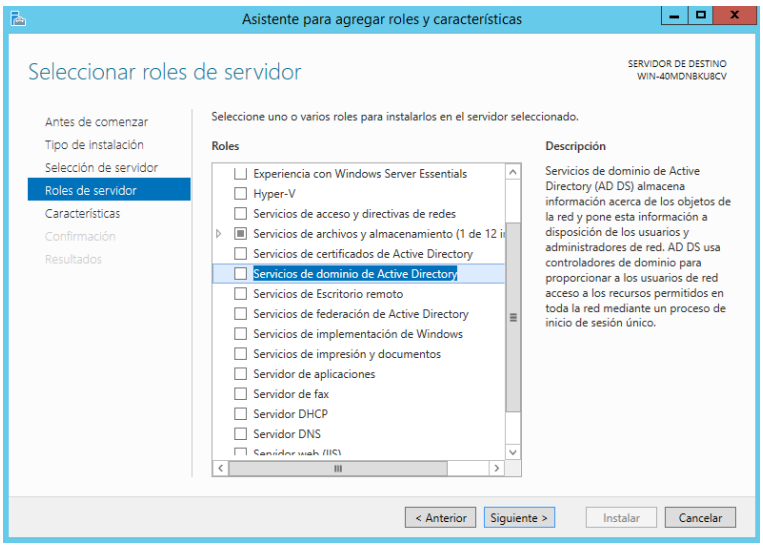
Captura 17 Asistente, “Selección del tipo de instalación”

A continuación, se elegirá que servidor ejercerá este rol, en este caso solo tenemos un servidor de pruebas, en la empresa donde se pondrá en funcionamiento este caso de estudio contará de varias máquinas virtuales. Se seleccionará el servidor y se clicará en "Siguiente".



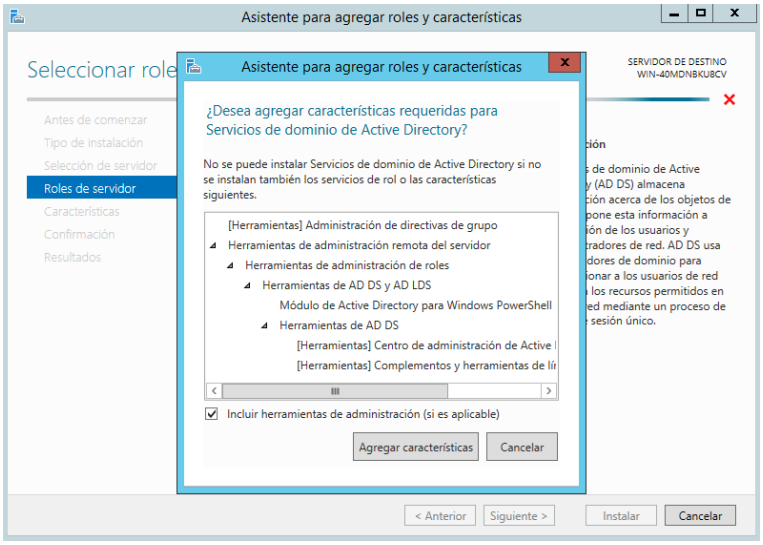
Captura 18 Asistente, "Seleccionar servidor de destino"

En la ventana de roles del servidor aparecerá una lista con todos los roles que se pueden instalar en nuestro servidor, por ahora solo se instalará un rol en el servidor más adelante se instalarán el resto de roles necesarios. Se seleccionará el rol "Servicios de dominio de *Active Directory*".



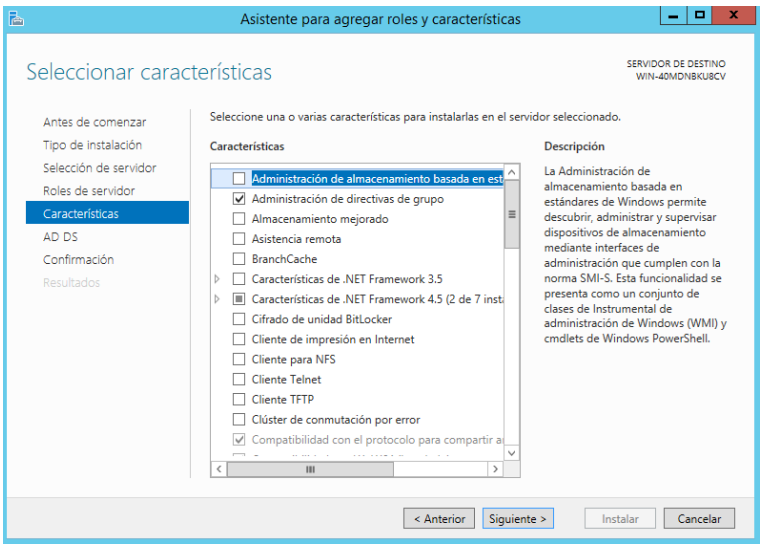
Captura 19 Asistente, "Selección de roles de servidor"

Al seleccionar este rol se abrirá una ventana en la cual preguntará si se quieren agregar las características necesarias para el funcionamiento este rol, se clicará en "Agregar características" para aceptar estas características.



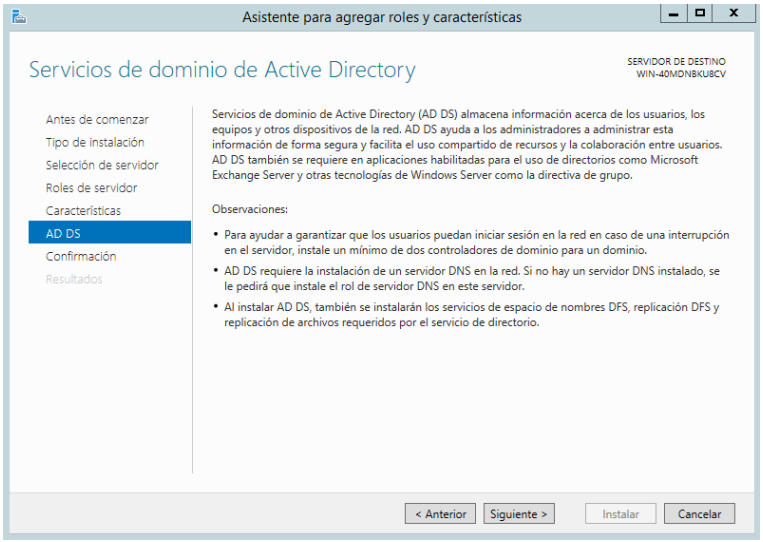
Captura 20 Agregar características al rol seleccionado

Se comprobará que el rol que se va instalar esta seleccionado marcado, comprobado esto se clicará en "Siguiente". En la ventana de característica no se marcará ninguna, debido a que dichas características se han aceptado antes para que se instalarán con el rol. Por consiguiente, se clicará en "Siguiente".



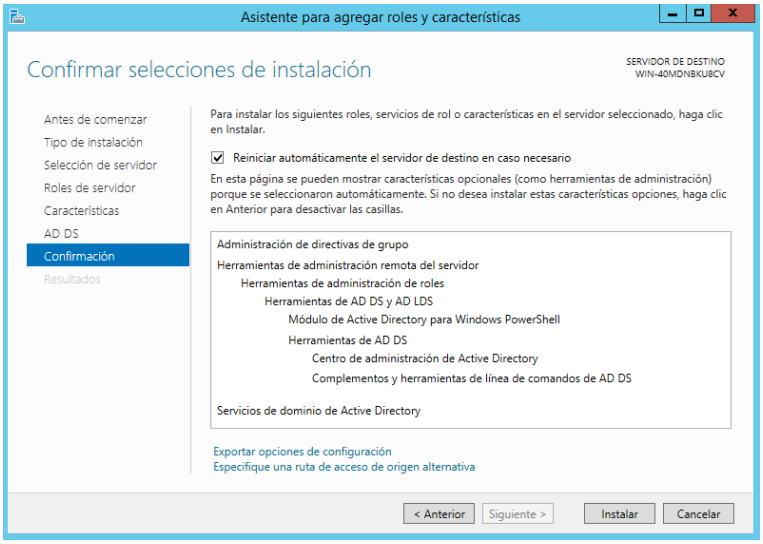
Captura 21 Asistente, "Seleccionar características"

En la siguiente ventana aparecerá una breve descripción del rol AD DS, se leerá y se clicará en “Siguiente”.



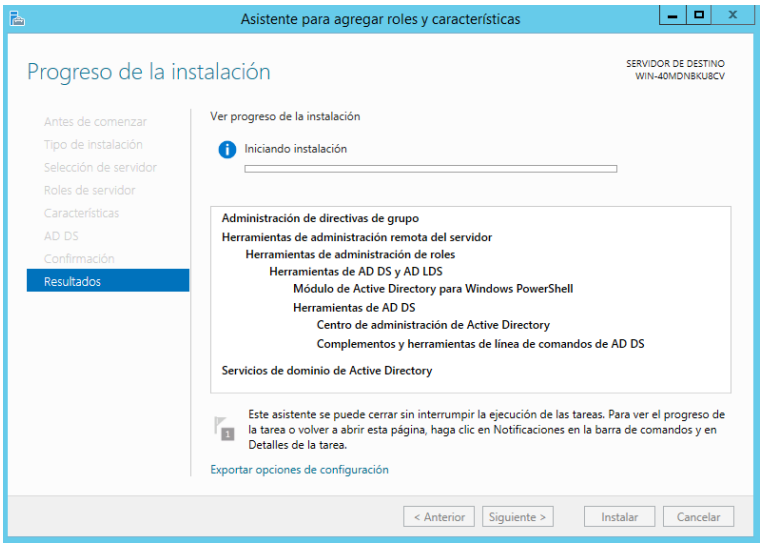
Captura 22 Descripción del rol AD DS

En la penúltima ventana del asistente se mostrará un listado de lo que se instalará, en dicha ventana se deberá comprobar que toda la configuración a instalar este correcta, en caso contrario se deberá volver atrás y realizar los cambios necesarios para su correcta configuración. Una vez comprobada se clicará en “Instalar”.



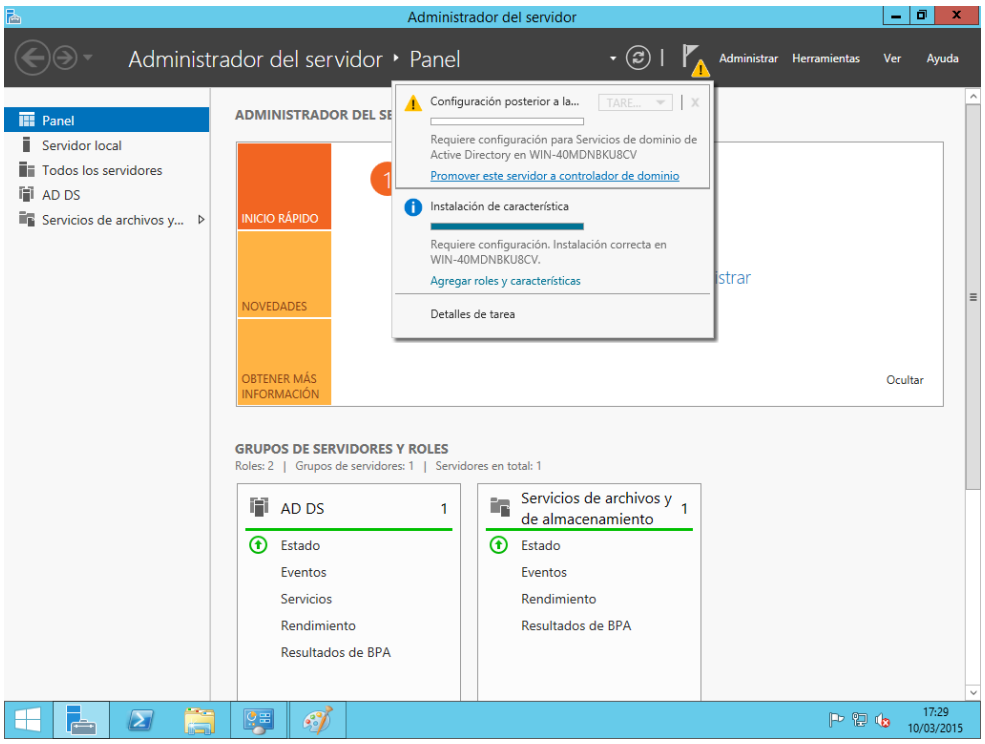
Captura 23 Listado de instalación del rol

Como recomendación se marcará la casilla “Reiniciar automáticamente el servidor de destino en caso necesario” para que se instale todo correctamente. En la última ventana del asistente empezará el proceso de instalación una vez terminado, en caso de ser necesario, se reiniciará el servidor.



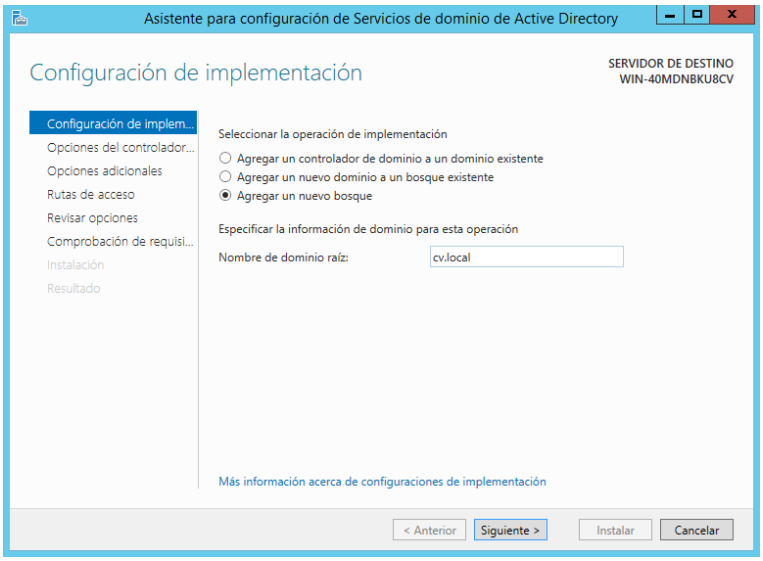
Captura 24 Proceso de instalación del rol

Una vez reinicie el servidor en la ventana de “Administración del servidor” en la parte de arriba aparecerá una advertencia en cual se le informa al administrador que falta configurar el rol instalado.



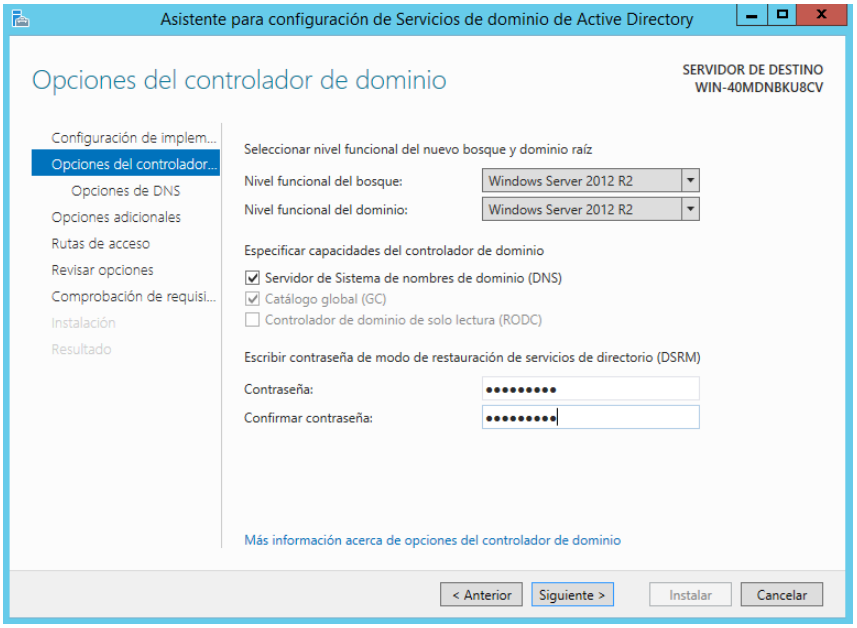
Captura 25 Advertencia del rol AD instalado

Para terminar de configurar el rol se clicará sobre la advertencia. En la primera ventana de configuración se marcará la opción “Agregar nuevo bosque”, se le asignará un nombre al dominio (en este caso “cv.loval” que el mismo que el de la empresa) y se clicará en “Siguiente”.



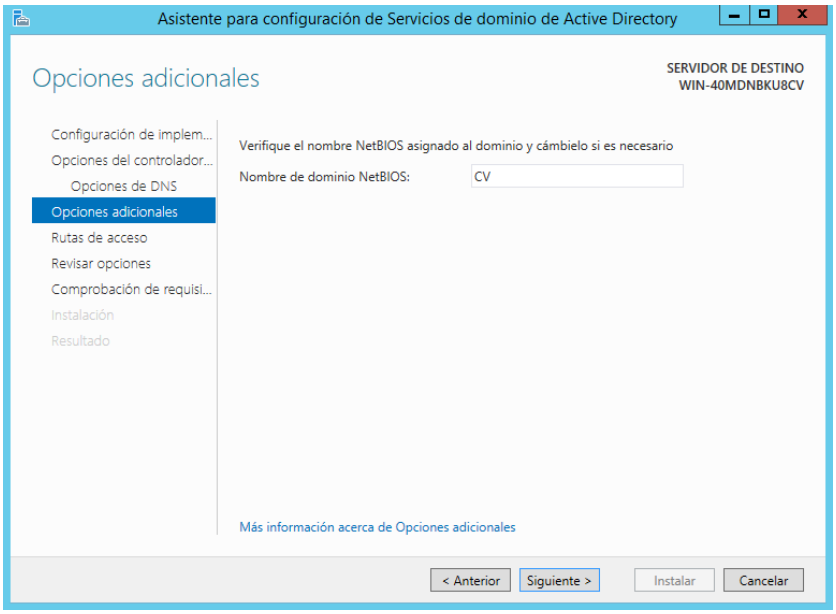
Captura 26 Asistente AD, “Configuración de implementación”

En la siguiente ventana se configurará el servidor como servidor de DNS marcando la casilla “Servidor de Sistema de nombres de dominio (DNS)”, se escribirá una contraseña para el modo de restauración de servicios de directorio (en adelante DSRM) y se clicará en “Siguiente”.



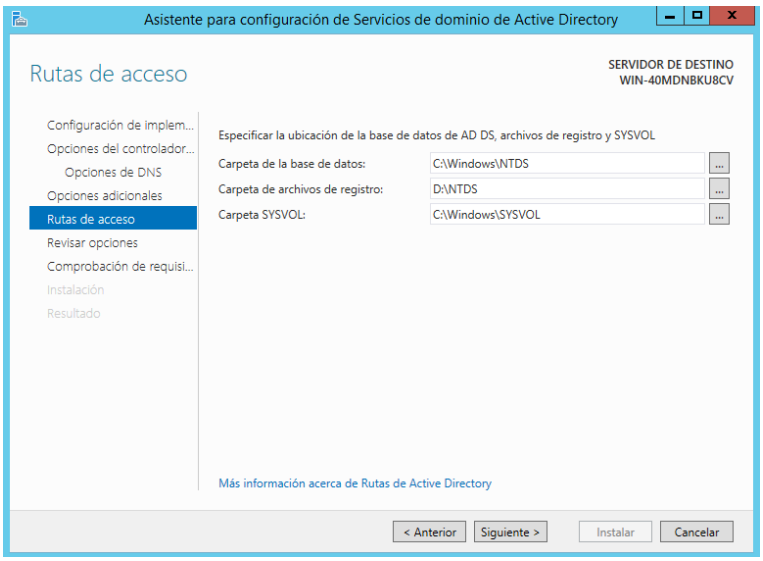
Captura 27 Asistente AD, “Servicio de DNS”

Siguiendo con el asistente se pondrá el nombre de dominio NetBIOS[2] que será "CV" como el del dominio AD DS y se clicará en "Siguiente".



Captura 28 Asistente AD, "NetBIOS"

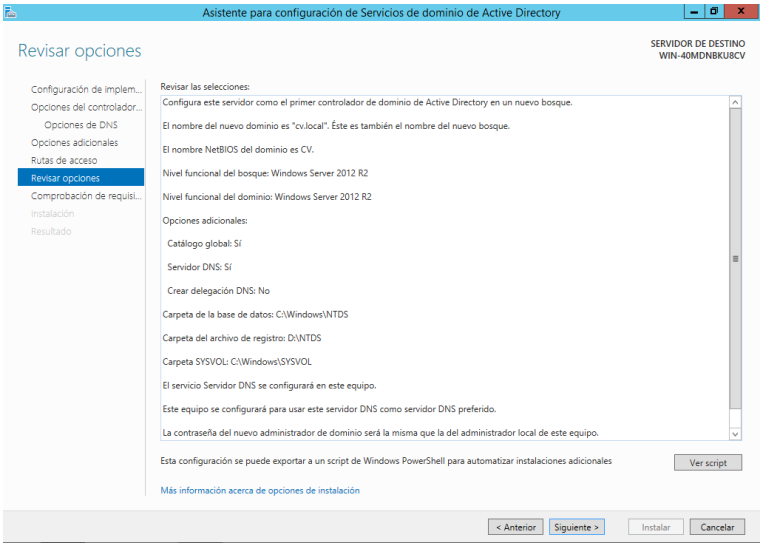
En la ventana de rutas de acceso de ubicaciones de la base de datos de AD DS, archivos de registro y SYSVOL es aconsejable que no todos los datos estén en la misma unidad, en este caso el disco duro está dividido en varias particiones. La partición "D" se utilizará para que se guarden los archivos de registro como para su función principal la de ofrecer cuotas de disco a los usuarios. Se cambiará la ubicación donde se guardan estos archivos y se clicará en "Siguiente".



Captura 29 Asistente AD, "Rutas de acceso"

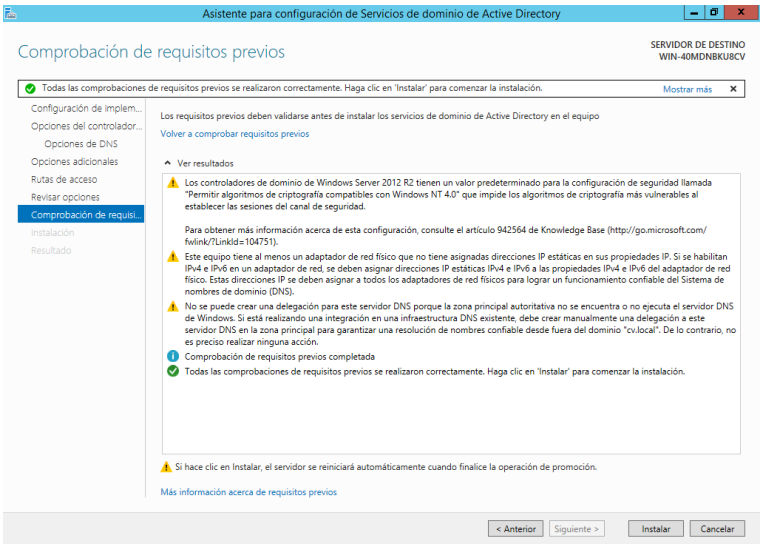
[2] NetBIOS (Network Basic Input/Output System): Es una especificación de interfaz para acceso a servicios de red.

En la siguiente ventana se revisará que la configuración para que sea la correcta, sino se volverá para atrás, y se clicará en “Siguiente”.



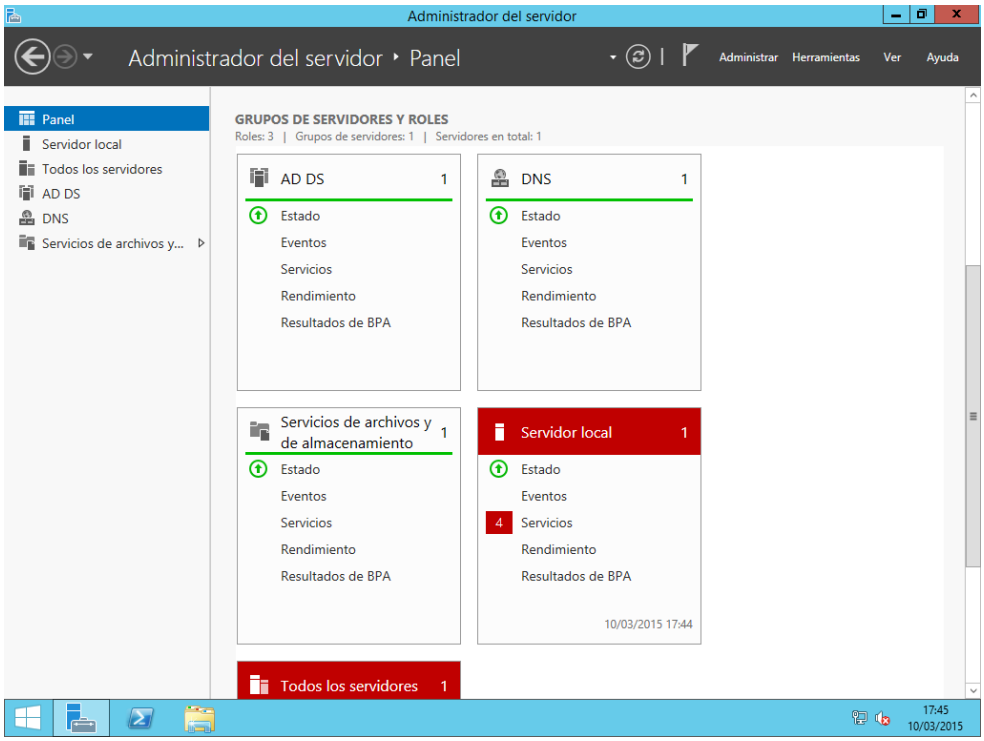
Captura 30 Asistente AD, “Listado de configuración”

En la ventana de instalación saldrá una lista de comprobación de requisitos, en ella aparecerán advertencias de cambios que se deberían hacer, algunos de ellos se harán posteriormente. Una vez comprobada la lista se clicará en “Instalar”.



Captura 31 Asistente AD, “Instalación”

Si se ha configurado bien el rol en la ventana de administración del servidor su cuadro estará en verde, con lo cual el rol AD DS estará en funcionando en el servidor.



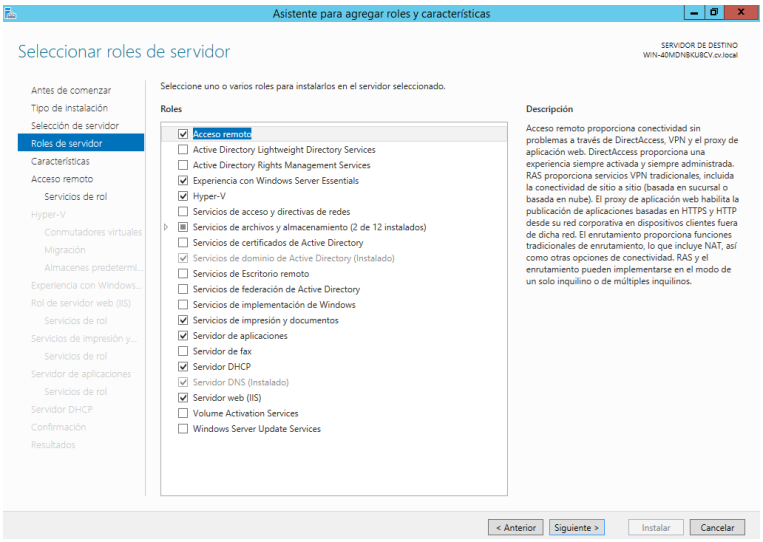
Captura 32 Administrador del servidor con los roles instalados

3.3. Instalación y configuración de roles que ejercerá el servidor

En esta sección del TFG se instalarán y configurarán otros roles con los que trabaja la empresa para acercarse lo más posible a un escenario real de funcionamiento. Se procederá con la instalación los siguientes roles:

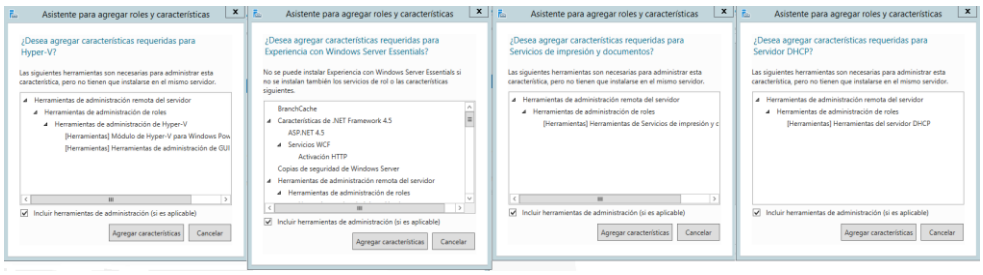
- **Rol Acceso Remoto**, para acceder remotamente al servidor.
- **Rol Hiper-V**, para la gestión de máquinas virtuales.
- **Rol Experiencia con *Windows Server Essentials***, para la protección de datos.
- **Rol Servidor Web (IIS)**, para páginas web y compartición de información vía web.
- **Rol Servicios de impresión y documentación**, para la gestión de impresoras, escáneres y multifuncionales compartidas en red.
- **Rol Servidor de aplicaciones**, para gestionar las aplicaciones que se ejecutan en red.
- **Rol Servidor DHCP**, para ofrecer direcciones IP a los equipos conectados a la red.

Se seleccionará los roles anteriormente mencionados de la lista de la ventana de "Roles del servidor" del asistente "Agregar roles y características" como se ha hecho en la instalación del rol AD DS.



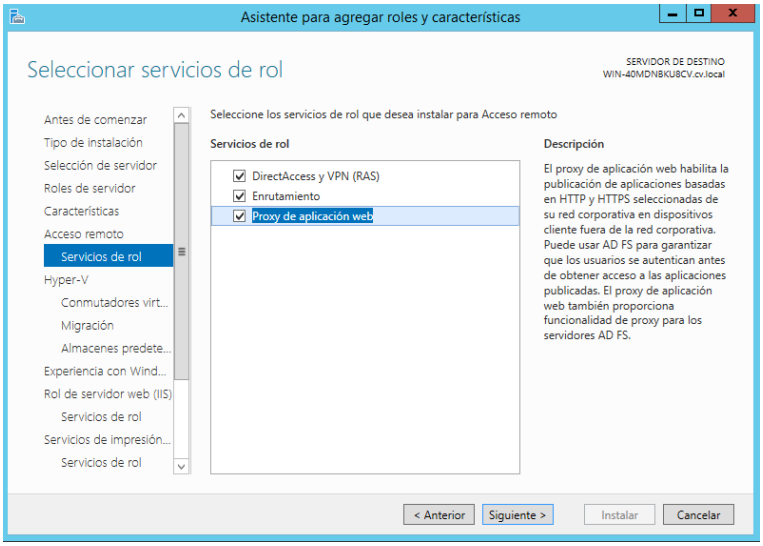
Captura 33 Listados de roles instalados y que se pueden instalar

Se procederá con la instalación de los roles como se ha hecho anteriormente, en la lista cuando se seleccionen los roles Hiper-V, experiencia con *WS Essentials*, servicios de impresión y documentación y servidor DHCP se agregarán características necesarias para su funcionamiento.



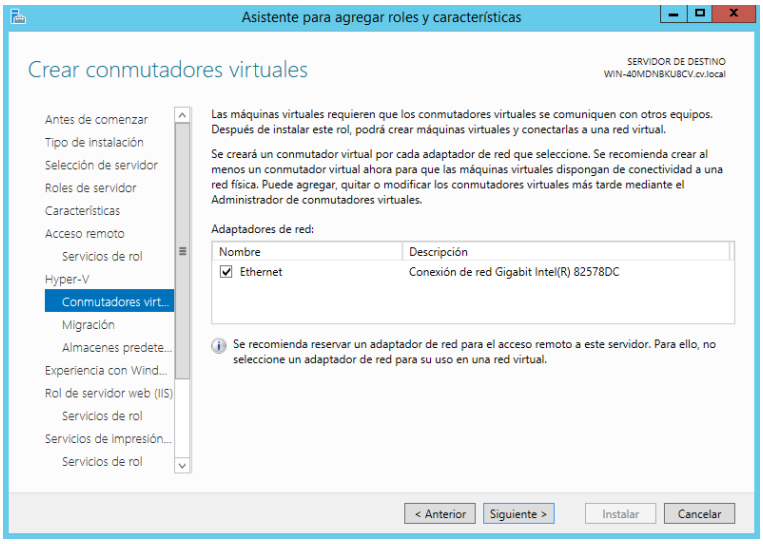
Captura 34 Agregar características a los roles

En la ventana de características se dejarán como está configuradas, a partir de esta ventana se empezará con la configuración de los servicios que se instalarán en cada rol. En el rol de Acceso remoto se seleccionará los tres servicios que aparecen, para ofrecer el mayor funcionamiento al acceso remoto. En el servicio de DirectAccess y VPN (RAS) se agregarán características necesarias para su funcionamiento.



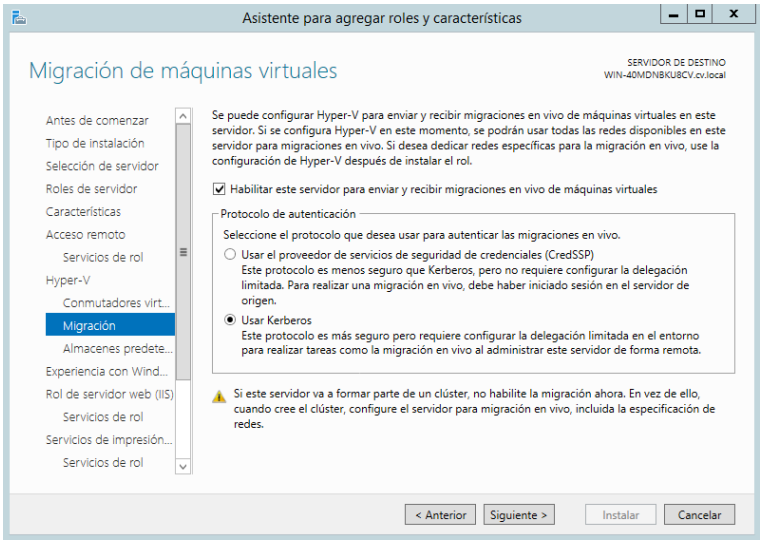
Captura 35 Servicios del rol Acceso remoto

En el rol Hyper-V primero se configurará la creación de conmutadores virtuales para las máquinas virtuales, en la lista se seleccionará la tarjeta de red del equipo (este equipo solo dispone de una pero un equipo servidor en un rack tiene alrededor de 4 tarjetas) y se clicará en "Siguiente".



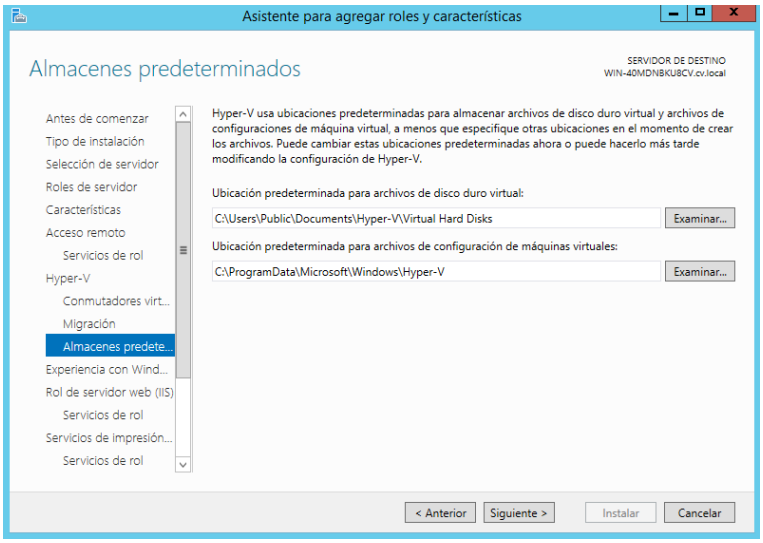
Captura 36 Rol Hyper-V, "Selección del conmutador"

Segundo se configurará la migración de las máquinas virtuales para así poder recibir o enviar máquinas virtuales a través de la red, esto se utilizará para copias de seguridad de las máquinas virtuales de la empresa. Se marcará la casilla "Habilitar este servidor para enviar y recibir migraciones en vivo de máquinas virtuales", se seleccionará el protocolo de autentificación Kerberos y se clicará en "Siguiente".



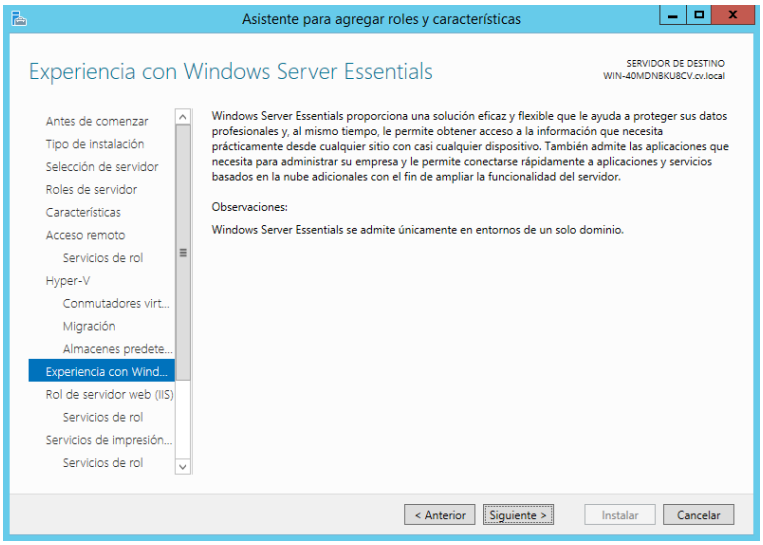
Captura 37 Rol Hyper-V, "Protocolo que se utilizará en la migración"

Por último, en la configuración "Almacenes predeterminados" se dejará por defecto, se proseguirá clicando en "Siguiente".



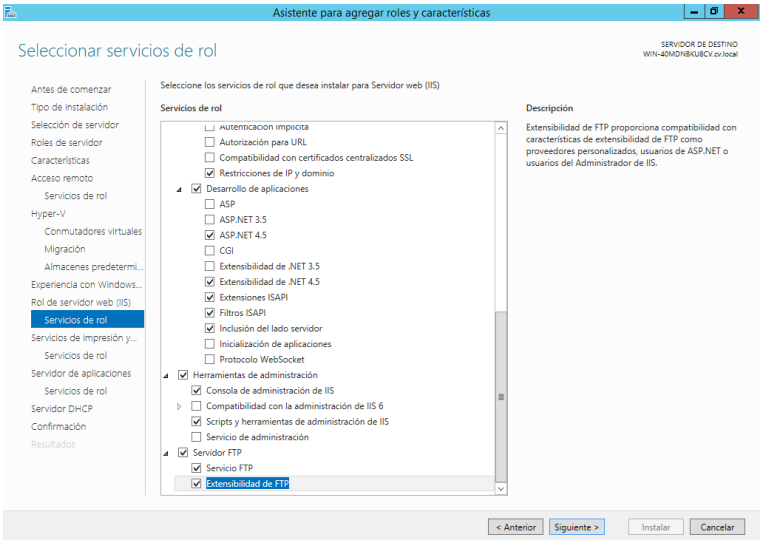
Captura 38 Rol Hyper-V, "Selección de los almacenes"

En el rol Experiencia con *Windows Server Essentials* aparecerá una breve descripción la cual se leerá y clicará en “Siguiente”.



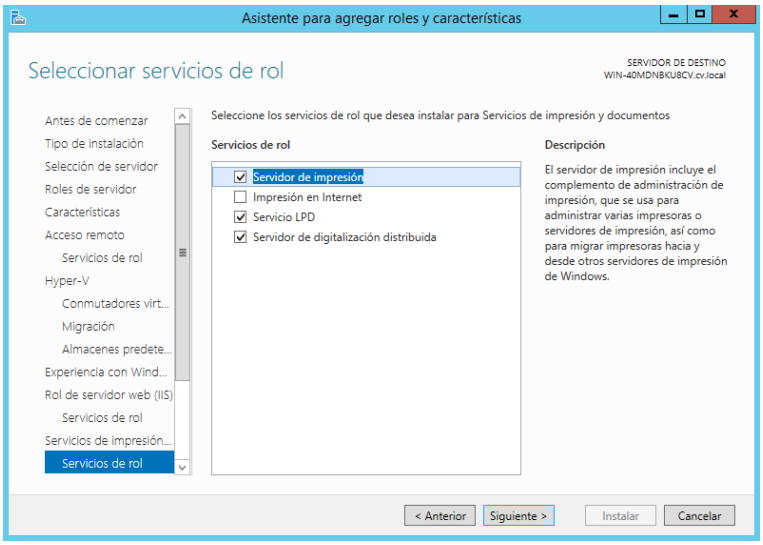
Captura 39 Descripción del rol Windows Server Essentials

En el rol IIS se marcará el servicio “Servidor FTP”, debido a que la empresa se utiliza para compartir archivos con sus lectores de códigos de barras. Una vez marcada la casilla se clicará en “Siguiente”.



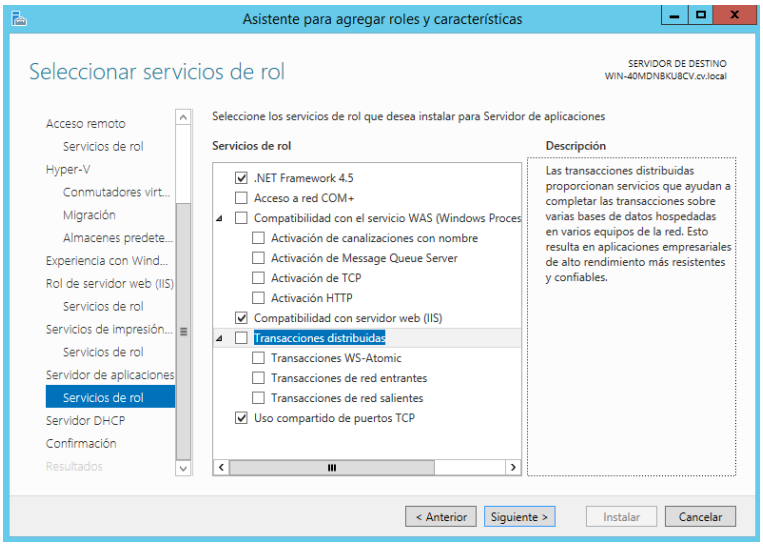
Captura 40 Características del rol IIS

En el rol Servicios de impresión y documentación se marcaran los servicios “Servidor de impresión” (para la gestión de impresoras), “Servicio LDP” (para que los sistemas UNIX puedan utilizar las impresoras y escáneres compartidor en red) y “Servidor de digitalización distribuida” (para gestión de los archivos escaneados). Una vez seleccionados se clicará en “Siguiente”.



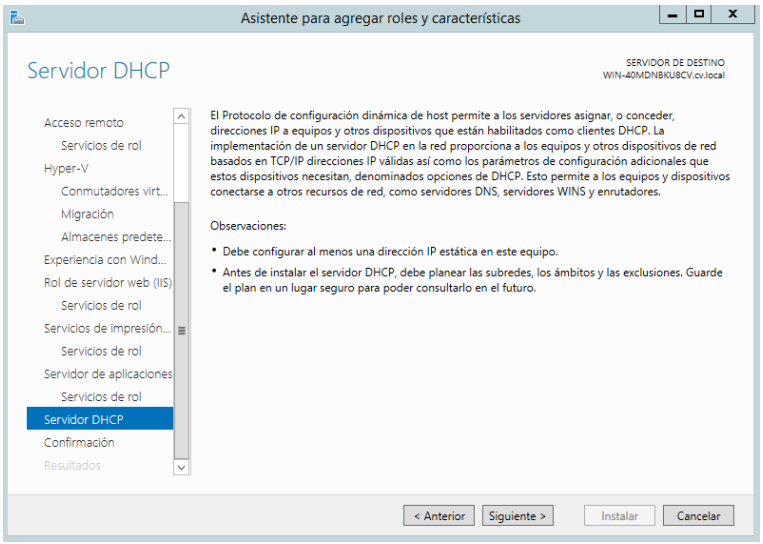
Captura 41 Rol de Servicios de impresión y documentación

En el rol Servidor de aplicaciones se marcará los servicios “Compatibilidad con servidor de web (IIS)” (para que pueda interactuar con el rol IIS) y “Uso compartido de puestos TCP” (para que puedan operar los distintos sistemas de la empresa). Una vez seleccionados se clicará en “Siguiente”



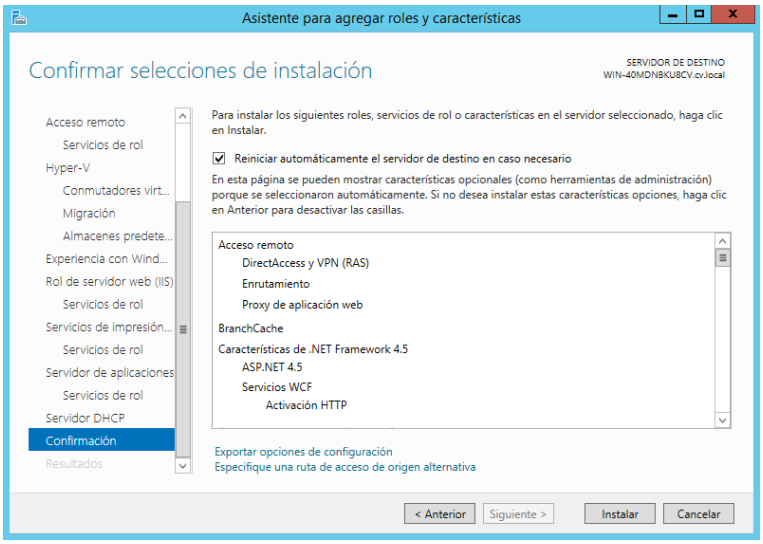
Captura 42 Agregar características al rol Servidor de aplicaciones

En el rol Servidor DHCP aparecerá una descripción del mismo la cual se leerá y se clicará en "Siguiente".



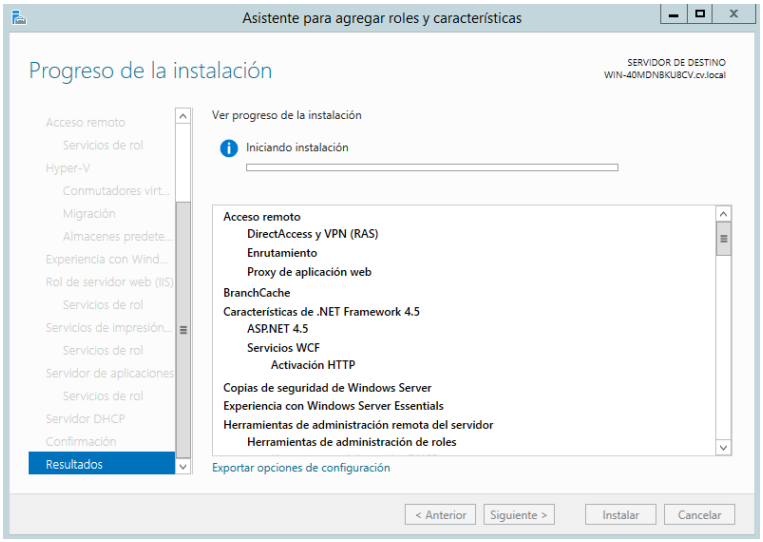
Captura 43 Descripción del rol servidor DHCP

En la ventana de confirmación se comprobará que todo este correcto en la lista, sino se volverá para atrás, y se clicará en "Instalar".



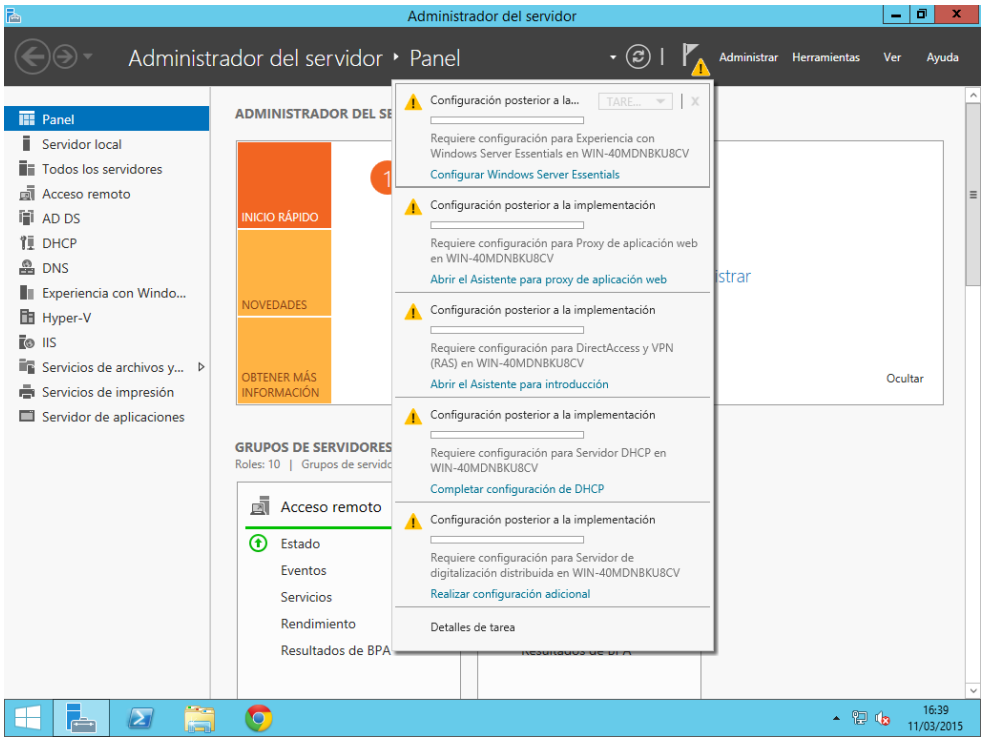
Captura 44 Instalación de los roles

Empezará el proceso de instalación de los roles y cuando termine se reiniciará de ser necesario.



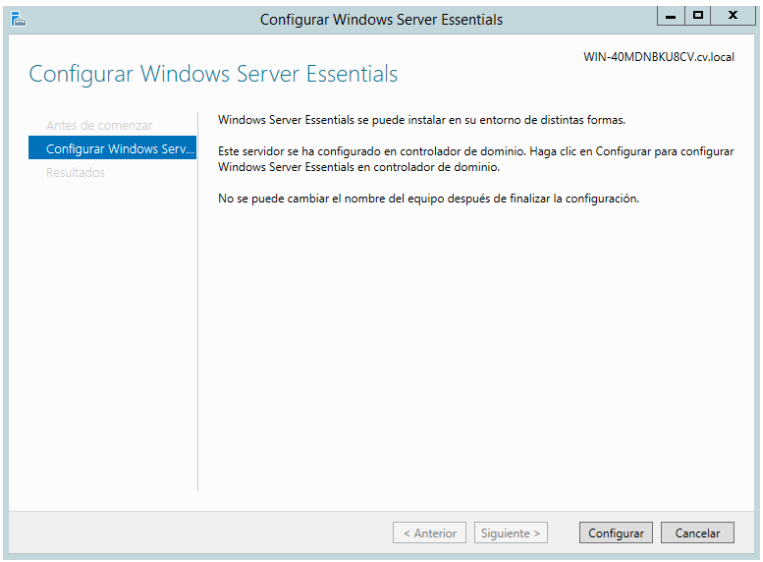
Captura 45 Proceso de instalación de los roles

Como pasó en la instalación del rol AD DS aparecerán advertencias para configurar algunos aspectos de los roles que se acaban de instalar.

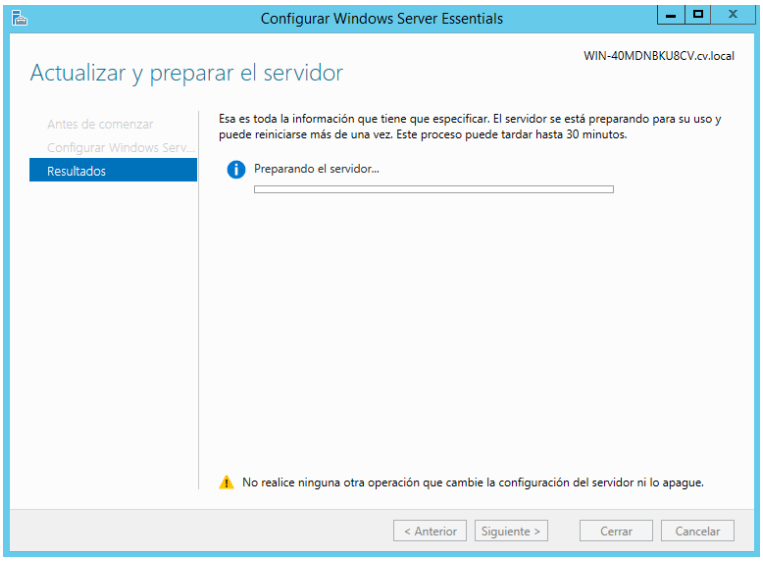


Captura 46 Advertencia de los roles instalados

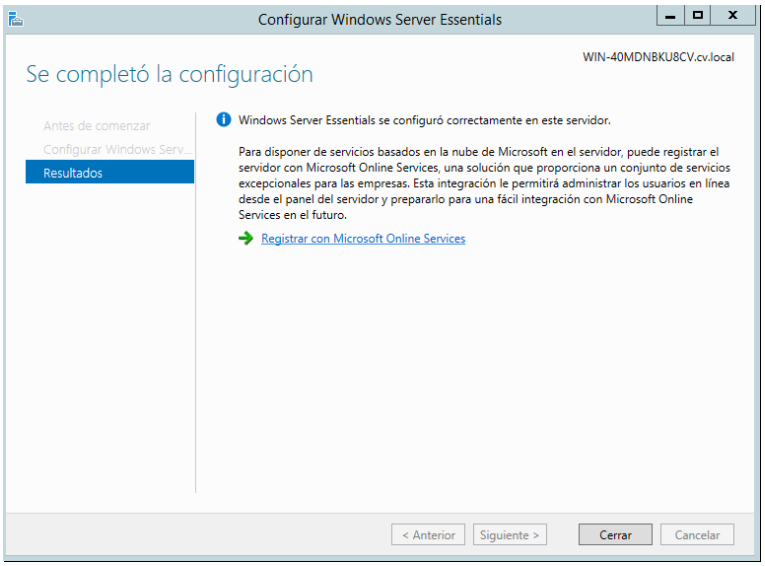
Después, se procederá con la configuración los roles instalados como se ha hecho anteriormente, se configurará el rol *WS Essential* clicando en "Configurar" y posteriormente en "Cerrar" cuando termine la configuración del rol.



Captura 47 Configuración del rol WS Essential

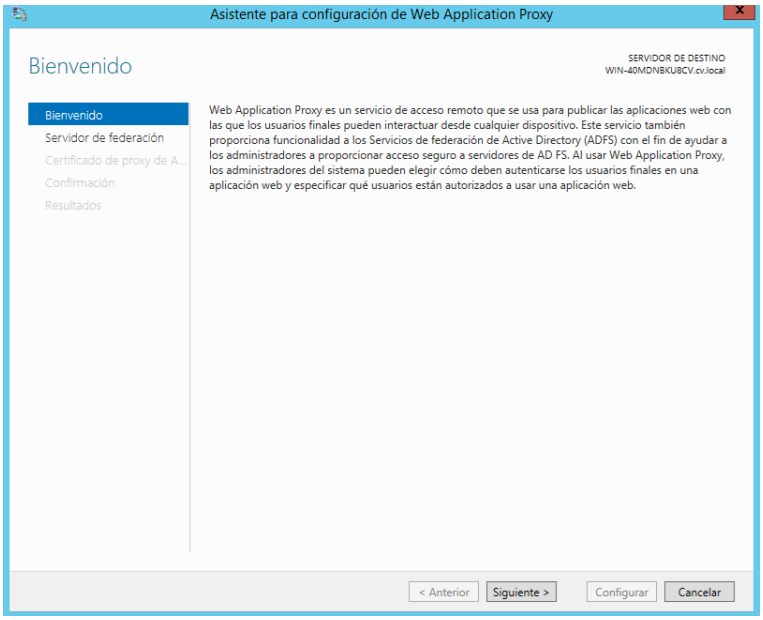


Captura 48 Proceso de configuración de WS Essential



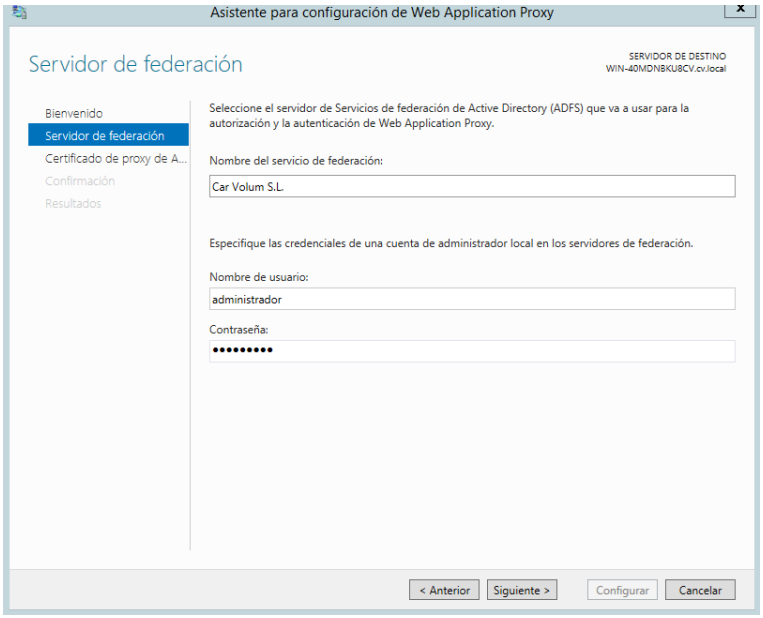
Captura 49 Finalización del rol WS Essential

El siguiente a configurar será el servicio *Web Application Proxy* del rol IIS, en la primera ventana de configuración nos aparece la descripción del servicio, se leerá y se clicará en "Siguiente".



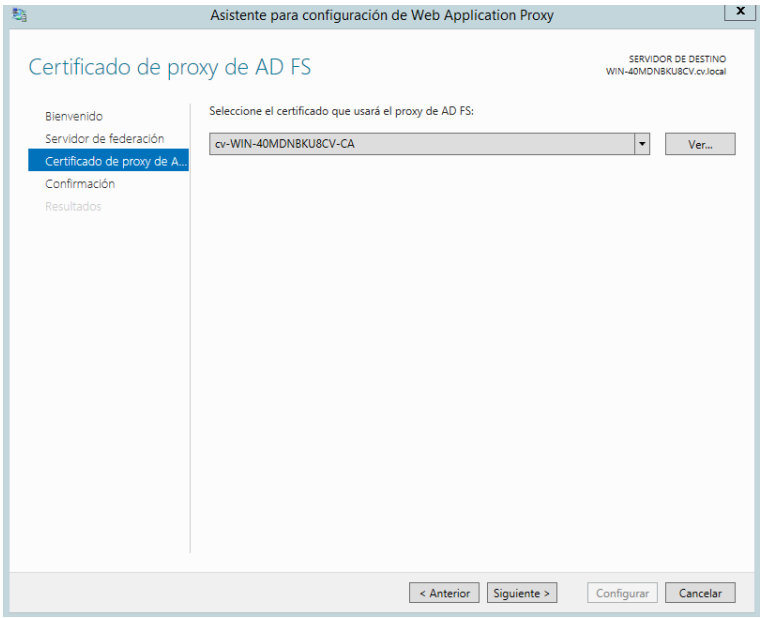
Captura 50 Descripción del servicio Web Application Proxy

En la segunda ventana se pondrá el nombre del servicio de federación y se clicará en "Siguiente".



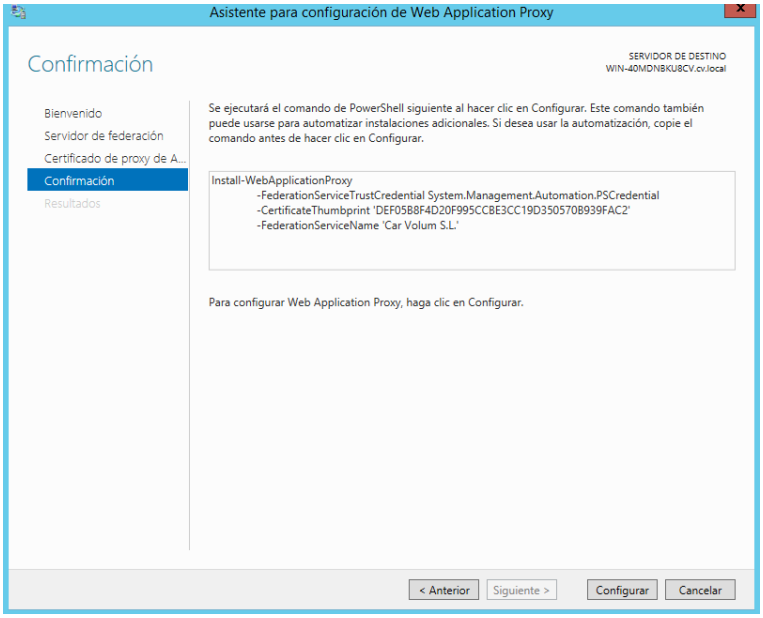
Captura 51 Configuración del servidor de federación

En la tercera ventana habrá que seleccionamos el certificado de federación que se utilizará en el proxy, el certificado que se utilizara es el de la empresa aunque se aparentará que se tiene, y se clicará en "Siguiente".



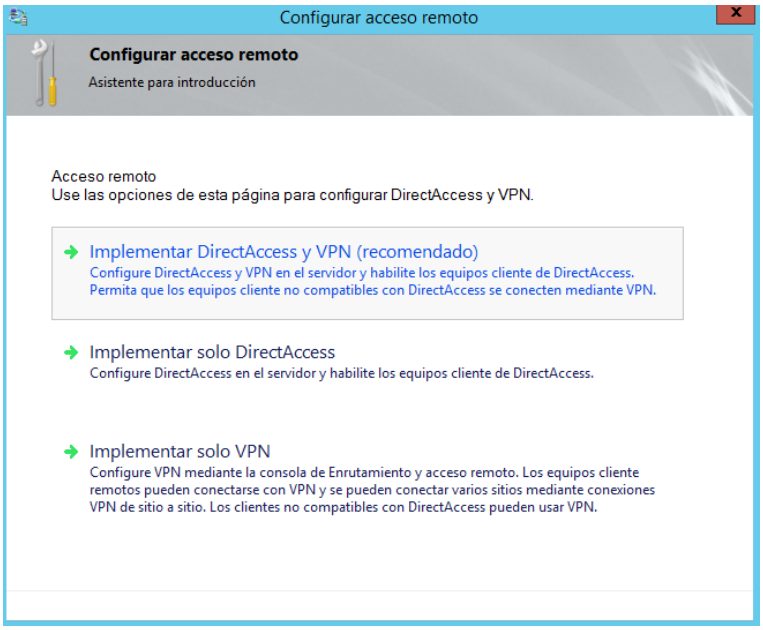
Captura 52 Selección del certificado de federación

En la cuarta ventana se leerá la información que se procederá a instalar en el proxy y se clicará en “Configurar” para terminar de configurarlo.



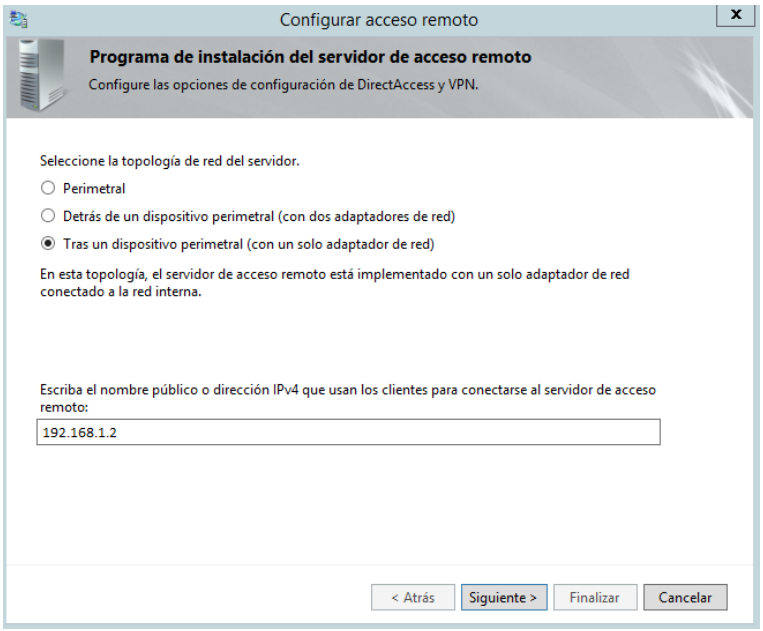
Captura 53 Listado de configuración del servicio Web Application Proxy

Una vez configurado el servicio de *Web Application Proxy* ahora se procederá con la configuración del rol de acceso remoto. En la primera ventana de configuración se seleccionará la primera opción “Implementar DirectAccess y VPN” que es la recomendada y es la que se necesita.



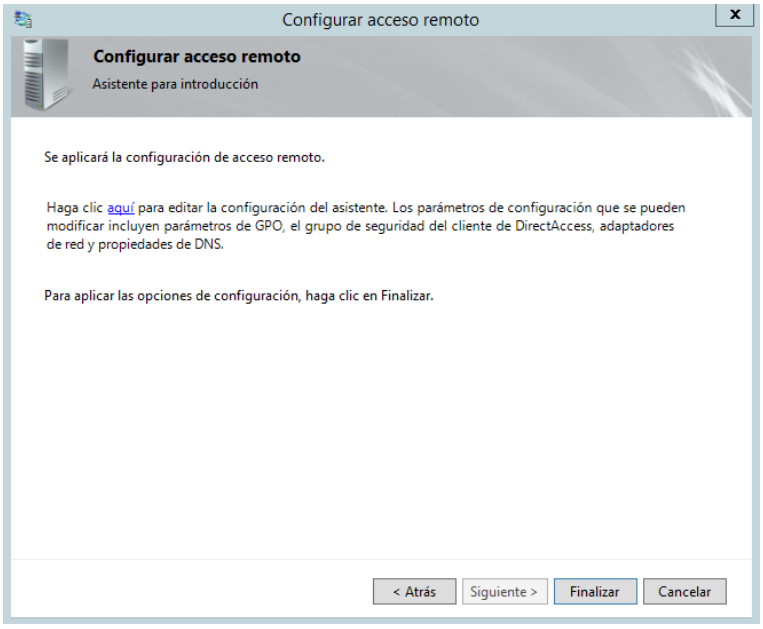
Captura 54 Configuración del rol Acceso remoto

En la segunda ventana se seleccionará la tercera opción “Tras un dispositivo perimetral”, debido a que en la empresa se utiliza un *firewall*. Se escribirá la IP del servidor donde accederán remotamente, en este caso la configurada en la tarjeta de red, y se clicará en “Siguiente”.



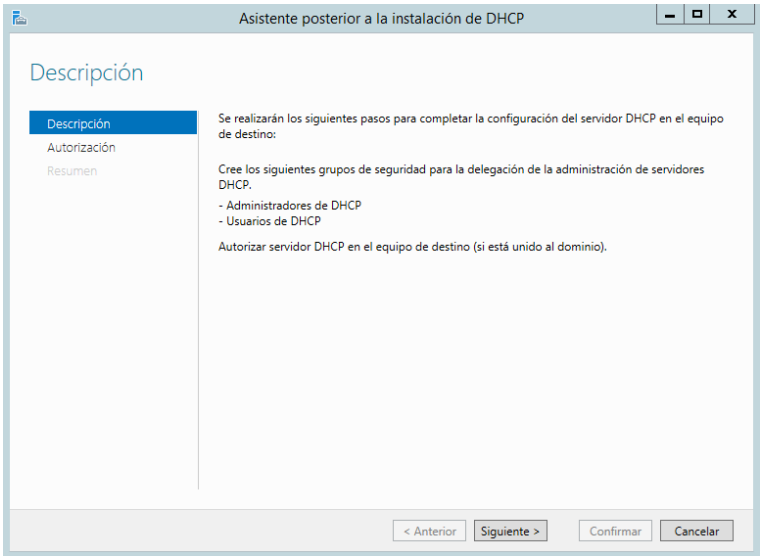
Captura 55 Configuración IP del acceso remoto

En la última ventana se clicará en “Finalizar” para aplicar la configuración realizada.



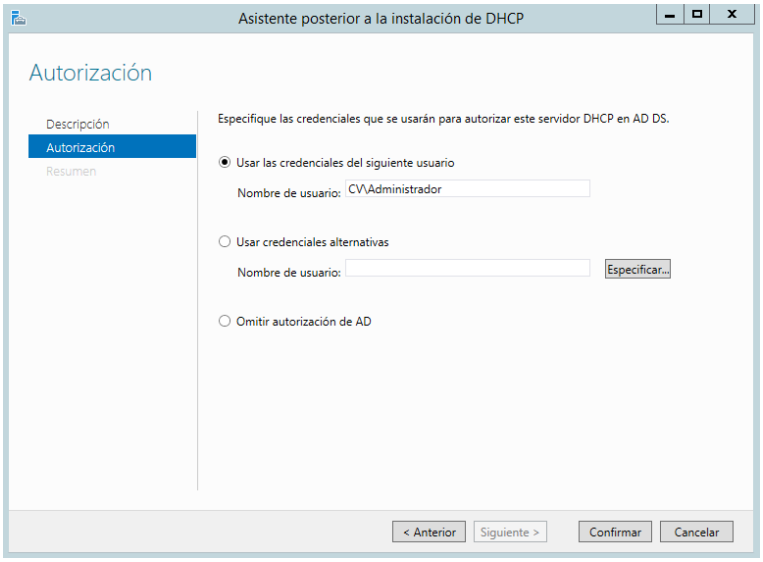
Captura 56 Finalización de la configuración del rol Acceso remoto

A continuación, se configurará el servidor DHCP. En la primera ventana del asistente del DHCP aparecerá un descripción del mismo, se leerá y se clicará en “Siguiente”.



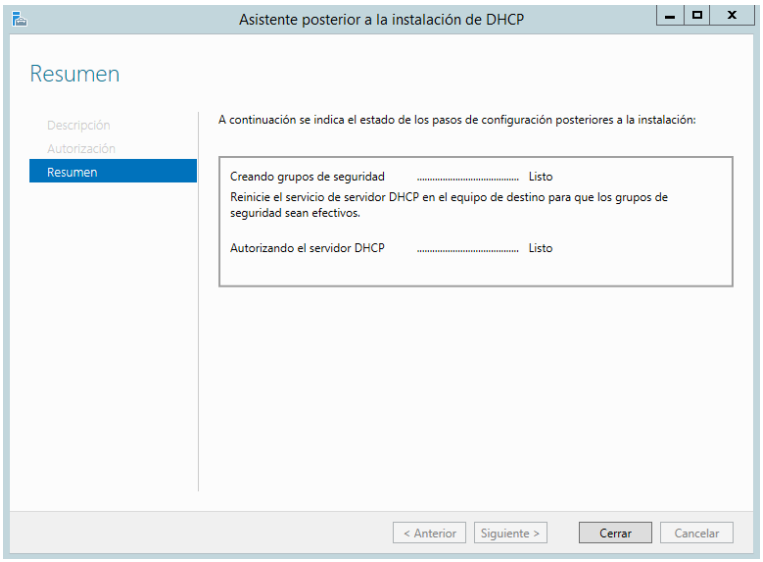
Captura 57 Descripción del servidor DHCP

En la segunda ventana se seleccionará la opción “Usar credenciales del siguiente usuario:” en la cual se escribirá el usuario con privilegios de administrador (por defecto se escribirá el usuario administrador que viene configurado con la instalación del sistema) y se clicará en “Confirmar”.



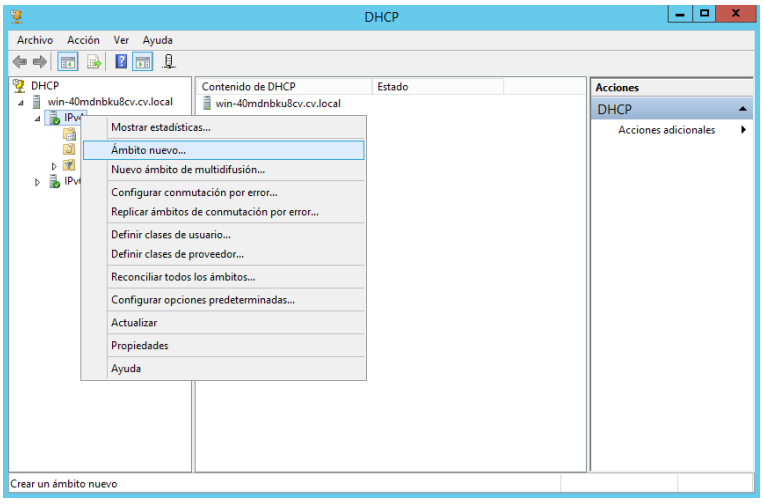
Captura 58 Configuración de la autentificación del servidor DHCP

En la última ventana aparecerá un resumen de la configuración, se leerá y se clicará en "Cerrar" para terminar con la configuración.



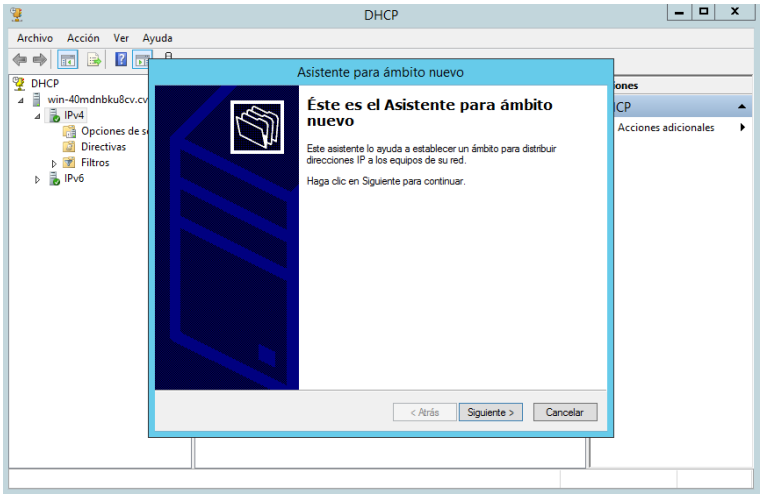
Captura 59 Resumen de la configuración del servidor DHCP

Una vez hecha a configuración básica del servidor DHCP se procederá con la creación de un nuevo ámbito en el cual se configurará el rango de IP que serán ofrecidas por el servidor a los equipos de la red. Para ello en la ventana de servidor DHCP se clicará con el botón derecho sobre "IPv4" y se accederá a "Ámbito nuevo…".



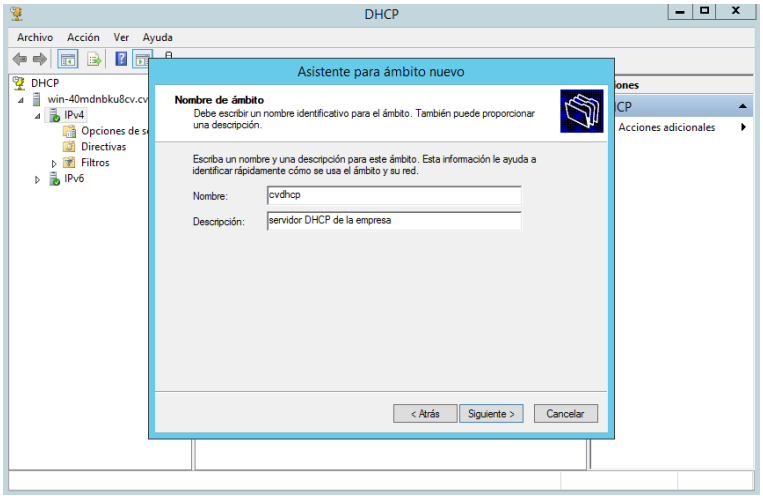
Captura 60 Creación del nuevo ámbito

Se abrirá la primera ventana del asistente del ámbito, la cual es descriptiva, en la que se clicará en “Siguiente” para empezar con el asistente.



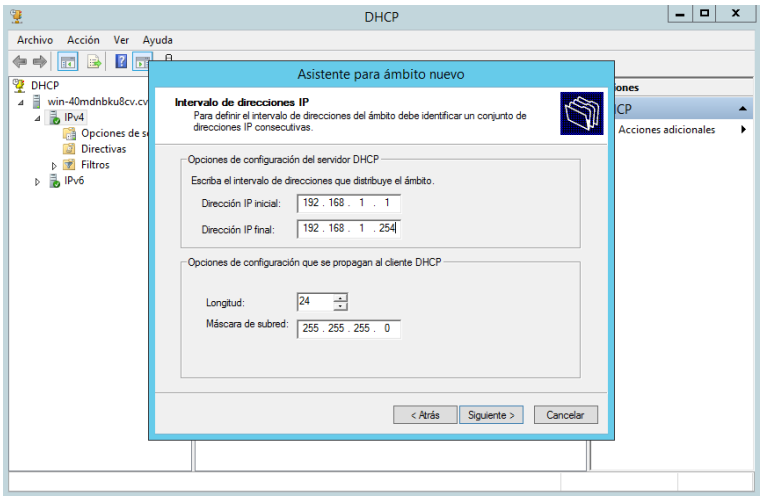
Captura 61 Inicio de creación del nuevo ámbito

En la segunda ventana se escribirá el nombre del ámbito, la descripción del mismo y se clicará en “Siguiente”.



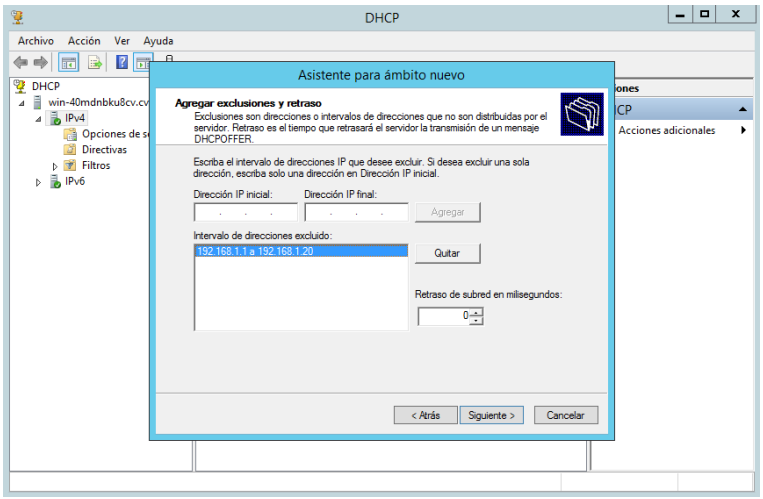
Captura 62 Asignación del nombre del ámbito

En la tercera ventana “Intervalo de direcciones IP” se escribirá el rango de direcciones IP, la máscara de red y se clicará en “Siguiente”.



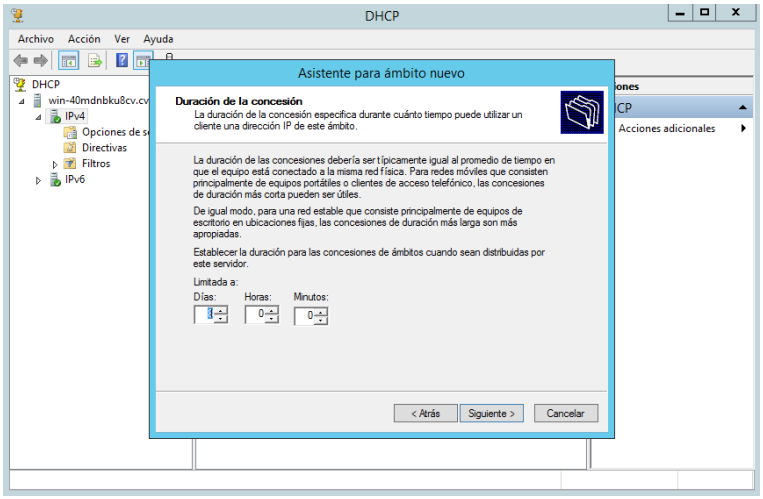
Captura 63 Asignación del rango de IP al ámbito

En la cuarta ventana “Agregar exclusiones y retraso” se añaden el rango de IP del 1 al 20, estas IP se utilizaran estáticamente para servidores, enrutadores y medios en red (impresoras, escáneres, unidades multifunción, etc.), y se clicará en “Siguiente”.



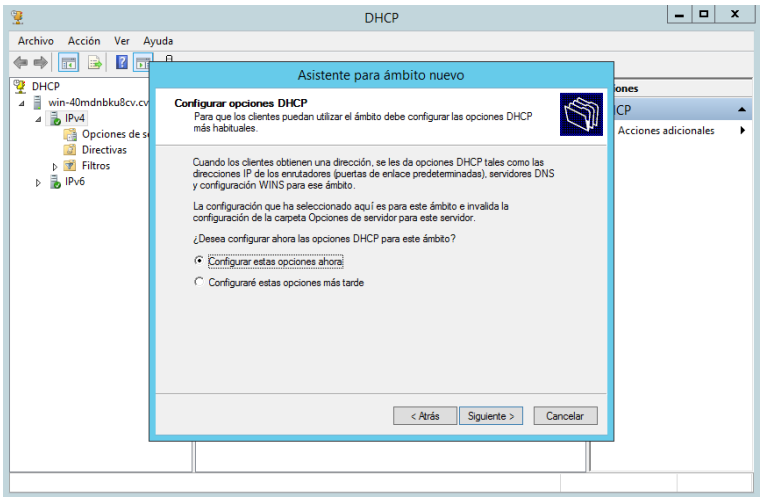
Captura 64 Asignación de rango exclusión del ámbito

En la quinta ventana “Duración de la concesión” se especificará que la IP expirará en los equipos a los 30 días y se clicará en “Siguiente”.



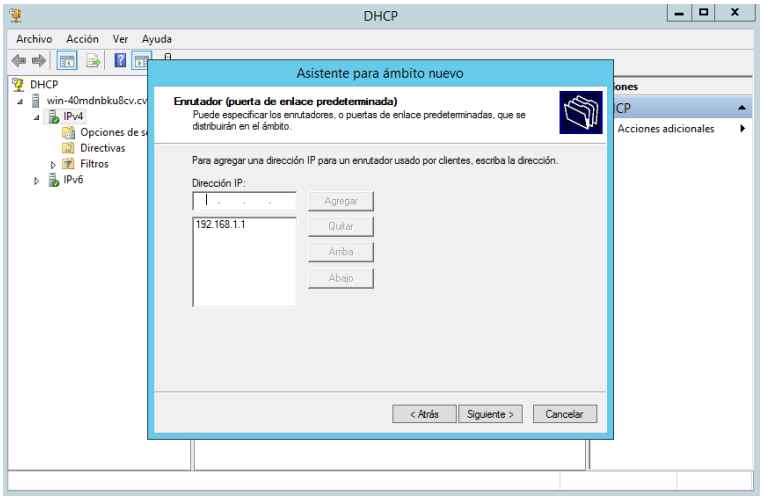
Captura 65 Asignación del tiempo de concesión

En la sexta ventana se seleccionará la opción “Configurar estas opciones ahora” para configurar las opciones que se les ofrece a los equipos cliente y se clicará en “Siguiente”.



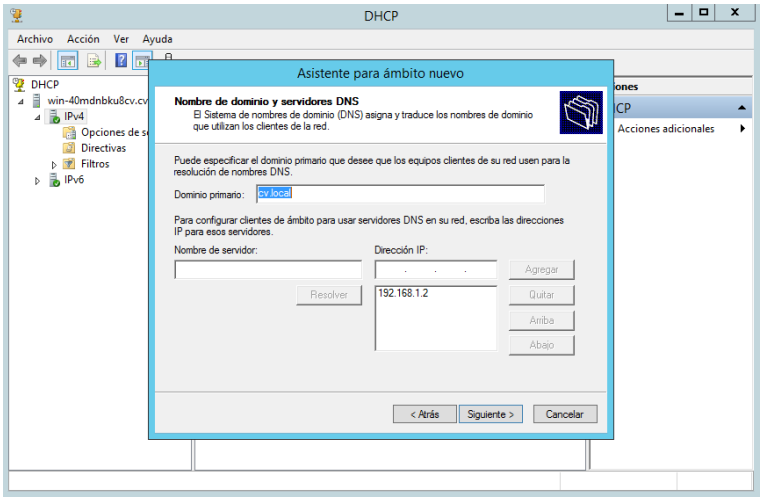
Captura 66 Configuración de opciones DHCP

En la séptima ventana se agregará la IP de nuestro enrutador y se clicará en “Siguiente”.



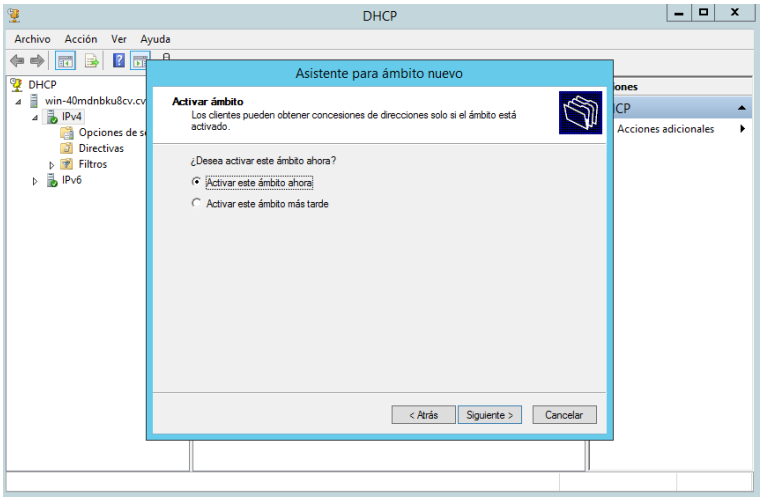
Captura 67 Asignar la IP del enrutador

En la octava ventana se escribirá el domino primario, se añadirá la IP del servidor DNS y se clicará en “Siguiente”.



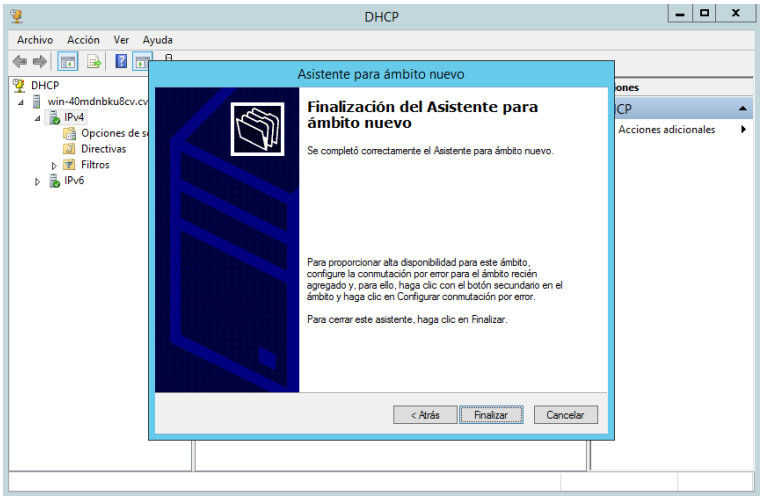
Captura 68 Asignar al servidor DNS

En la novena ventana se dejara por defecto, en la décima se seleccionará la opción "Activar este ámbito ahora" para que empiece a dar IP a los equipos y se clicará en "Siguiente".



Captura 69 Activación del servidor DHCP

En la última ventana, se clicará en "Finalizar" para acabar la creación del ámbito.



Captura 70 Finalización de la configuración del ámbito

Con este último rol se tendrán configurados todos los roles que tiene la empresa en el servidor de pruebas para asemejarse lo máximo posible al real.

3.4. Servicios de escritorio remoto

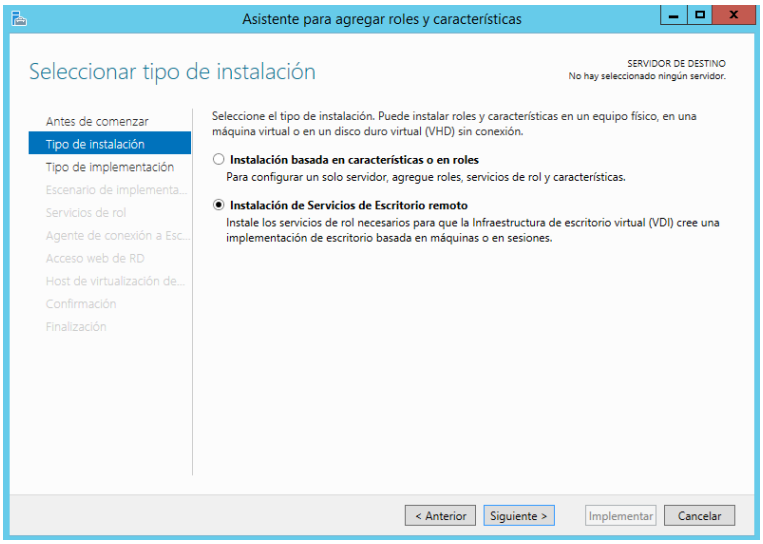
Los Servicios de Escritorio remoto de *Windows Server 2012* proporciona tecnologías que permiten a los usuarios conectarse a escritorios virtuales, programas *RemoteApp* y escritorios basados en sesión. Estas conexiones se pueden utilizar bien para disponer de un entorno completo de trabajo de usuario o bien para la ejecución de aplicaciones.

La comunicación entre los equipos clientes y el servidor se basa en el protocolo RDP (*Remote Desktop Protocol*), que se transmite a través de la red, encapsulado y cifrado en TCP. El protocolo RDP es un protocolo propietario de Microsoft, que apareció por primera vez en

Windows NT y que ha sufrido cambios a lo largo de sus distintas versiones. El servicio de escritorio remoto tiene compatibilidad mejorada para los escenarios siguientes:

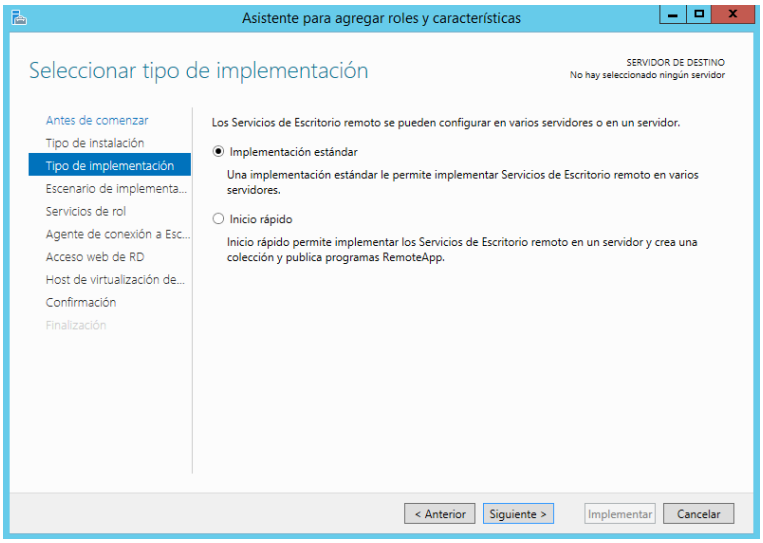
- Implementaciones de Infraestructura de escritorio virtual (VDI)
- Implementaciones de virtualización de sesión
- Publicación centralizada de recursos
- Experiencia del usuario enriquecida con el Protocolo de escritorio remoto (RDP)

En la empresa se utiliza mucho este servicio para trabajar con el software ERP que usa, por ello en este TFG se implementará. Se procederá instalando el rol de escritorio remoto tal y como se ha hecho con los roles anteriores, excepto que en la ventana de selección del tipo de instalación se elegirá la segunda opción la de "Instalación de Servicios de Escritorio remoto". Una vez seleccionada se clicarás en "Siguiente".



Captura 71 Instalación del rol Escritorio remoto

En la ventana de tipo de implementación se seleccionará la primera opción “Implementación estándar”, debido a que en la empresa se utiliza servidores implementados en máquinas virtuales, y se clicará en “Siguiente”.

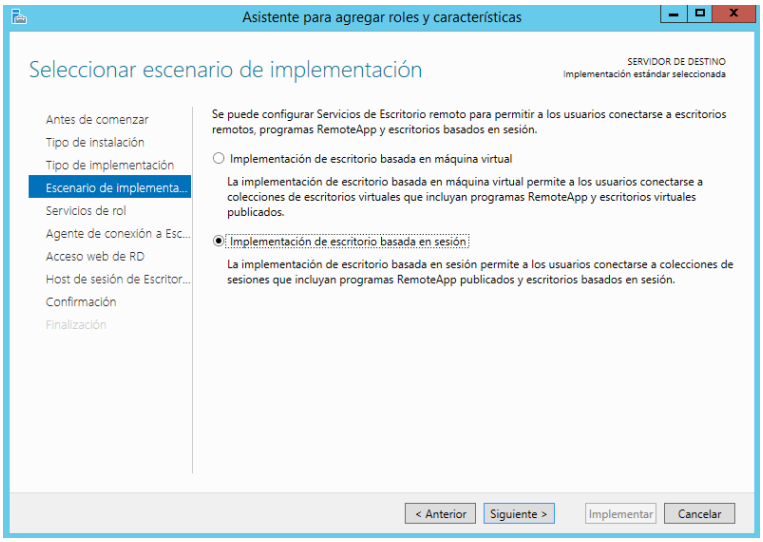


Captura 72 Tipo de implementación del Escritorio remoto

A continuación, se seleccionará el modo de escritorio que se iniciará en la sesión de los usuarios cuando accedan por este servicio. En el rol de escritorio remoto se puede elegir entre dos tipos implementación:

- **Basados en máquina virtual**, generan el escritorio del usuario a partir de una máquina virtual de “Hyper-V”
- **Basados en sesión,** lo hacen en base a una sesión de usuario en el servidor.

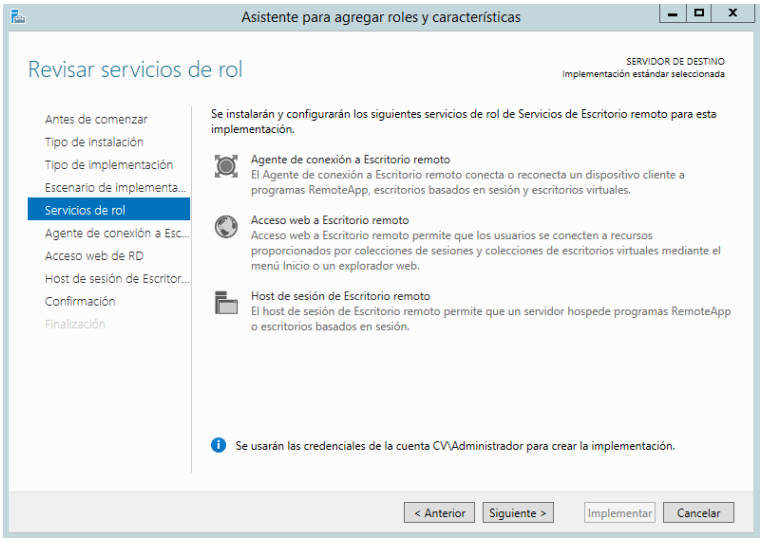
En este caso se seleccionará el segundo tipo, debido a que los empleados de la empresa utilizan este sistema, y se clicará en “Siguiente”.



Captura 73 Implementación de escritorios

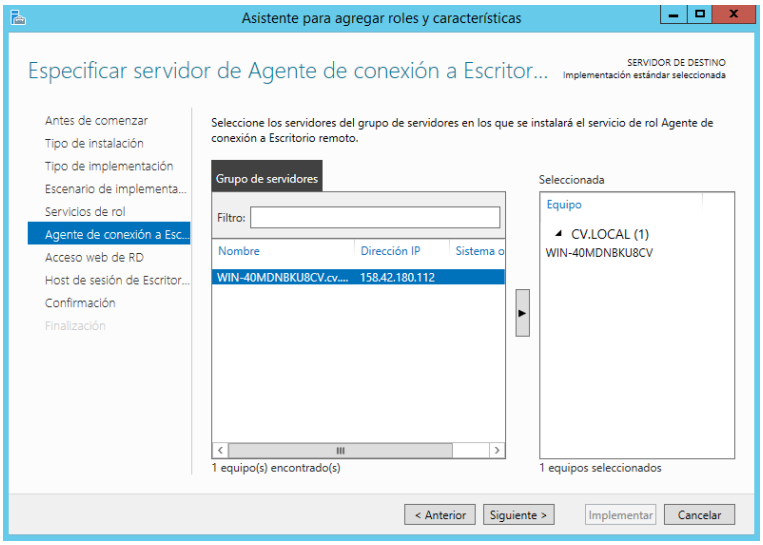
Con la selección del tipo de implementación del escritorio basado en sesión, se instalarán los siguientes roles:

- **Agente de conexión de escritorio remoto (*RD Connection Broker*):** Se encarga de la conexión de los dispositivos cliente a sesiones de escritorio o a aplicaciones remotas.
- **Acceso web a escritorio remoto (*RD Web Access*):** Proporciona acceso a las aplicaciones o a los escritorios remotos a través de un navegador web.
- **Host de sesión de escritorio remoto (*RD Host Session*):** Es el encargado de hospedar los escritorios remotos y los programas publicados.

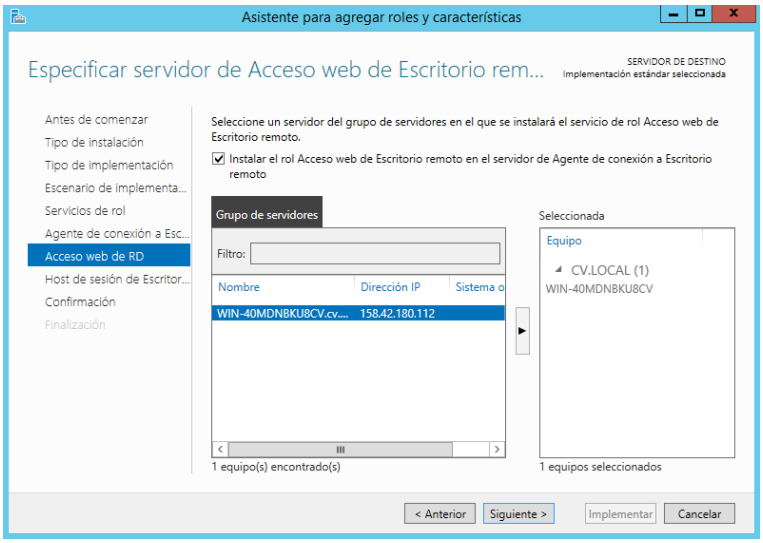


Captura 74 Servicios que se instalarán con el rol Escritorio remoto

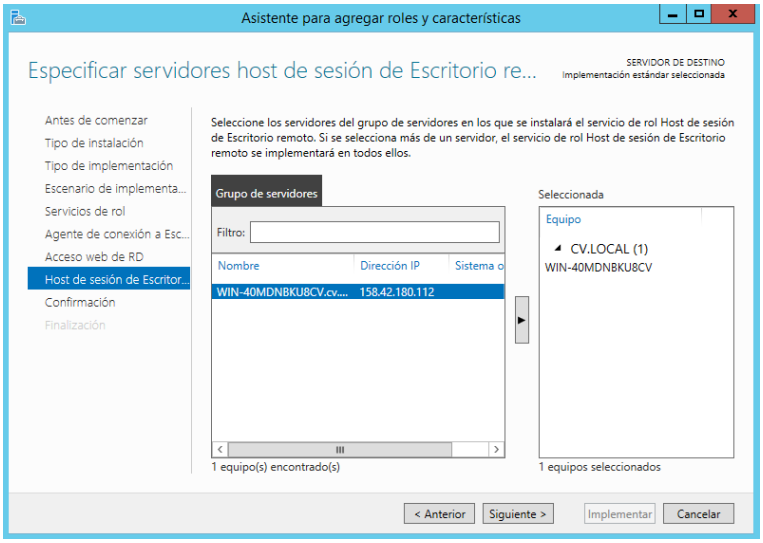
En las ventanas de Agente de conexión, Acceso Web y Host de sesión se seleccionará el servidor, en este caso en la lista solo aparece uno si hubieran más servidores podríamos elegir otro distinto. En la ventana de Acceso Web también se marcará la casilla “Instalar el rol de Acceso Web de Escritorio remoto en el servidor Agente de conexión a Escritorio remoto”.



Captura 75 Agente de conexión a Escritorio remoto

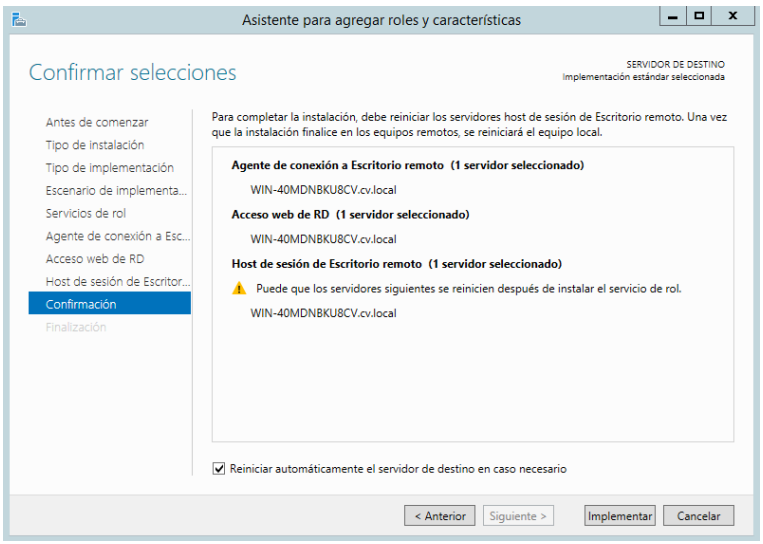


Captura 76 Acceso web de Escritorio remoto



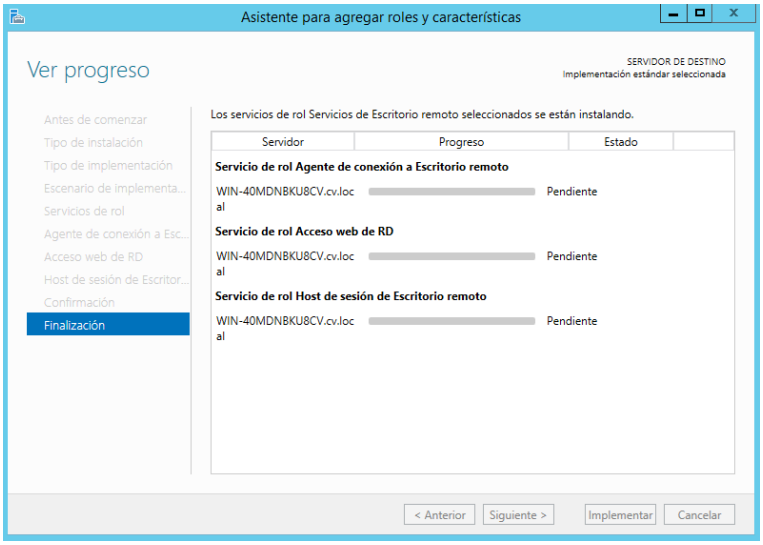
Captura 77 Host de sesión de Escritorio remoto

En la ventana de “Confirmación” aparecerá un listado de toda la configuración realizada en la cual se marcará la casilla “Reiniciar automáticamente el servidor de destino en caso necesario” y se clicará en “Implementar”.



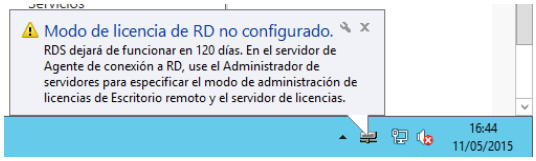
Captura 78 Confirmación de la instalación del rol Escritorio remoto

Empezará la instalación de los roles, cuando termine el proceso de estación el servidor se reiniciará.



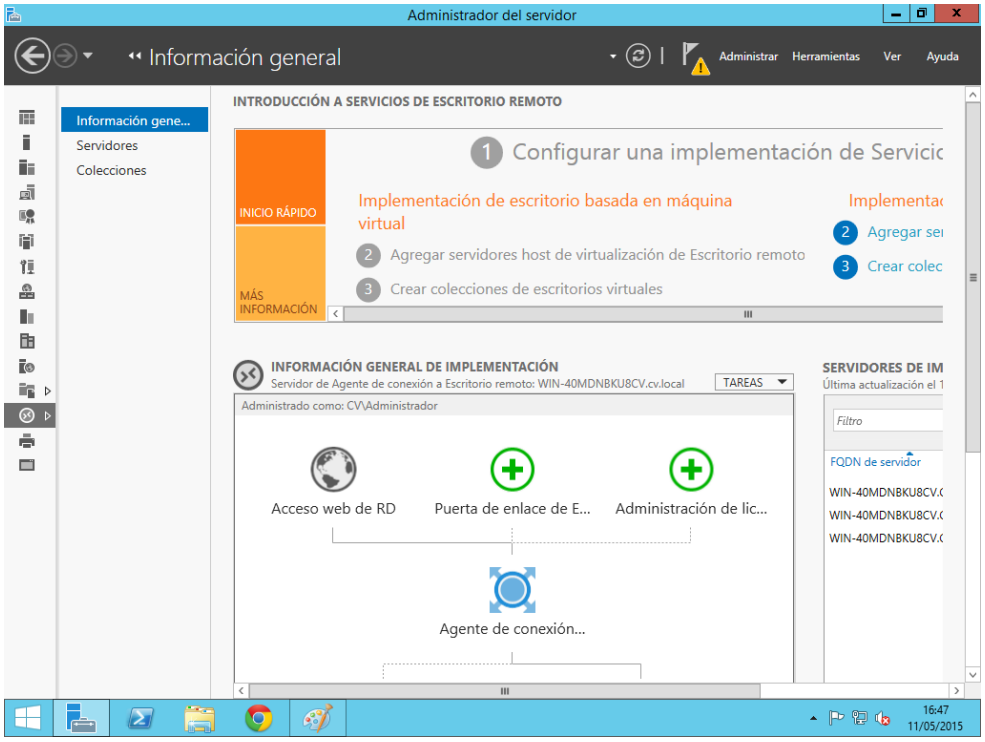
Captura 79 Proceso de instalación del rol Escritorio remoto

Una vez instalado el rol de escritorio remoto se procederá con la configuración del mismo. El sistema nos advertirá de que el servicio estará disponible durante 120 días, tras terminar este periodo se deshabilitar. La empresa dispone de un paquete de licencias aunque en esta caso se simularemos que se dispone de él.



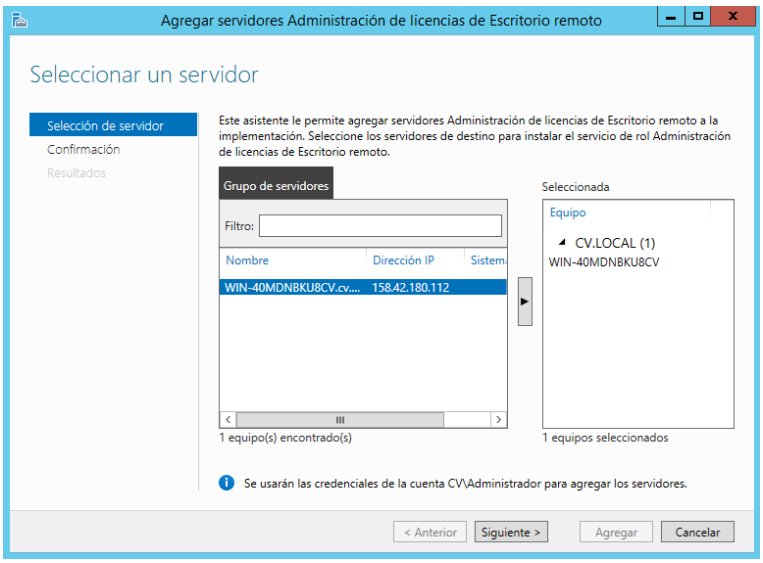
Captura 80 Advertencia licencias no configuradas

Para la activación del servicio, en la ventana del "Administrador del servidor", se accederá al "Servicios de Escritorio remoto". En susodicha ventana se clicará en "Administración de licencias".

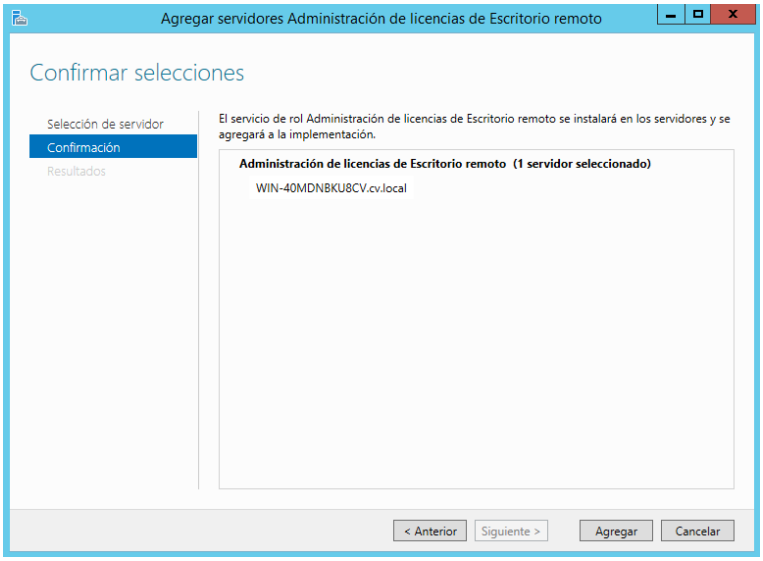


Captura 81 Administración de los servicios de Escritorio remoto

Se abrirá la ventana para agregar el servidor de administración de licencias, en la cual se seleccionará el servidor en la ventana "Selección del servidor" y en la siguiente ventana "Confirmación" se clicará en "Agregar". Con esto se agregará el servidor de licencias.

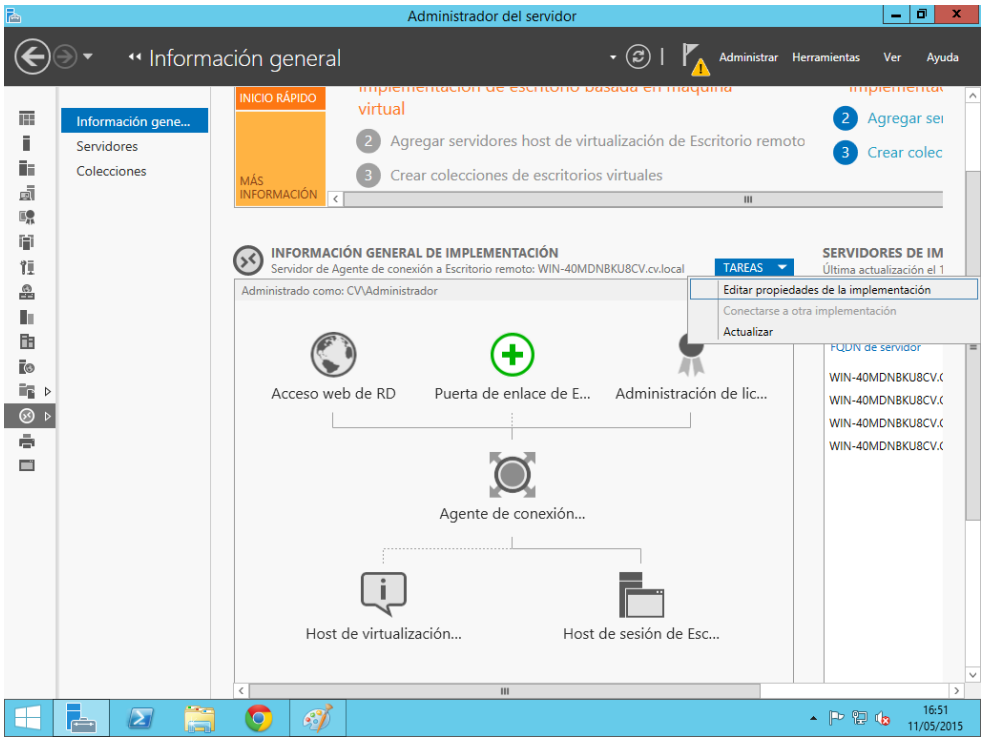


Captura 82 Selección del servidor de licencias



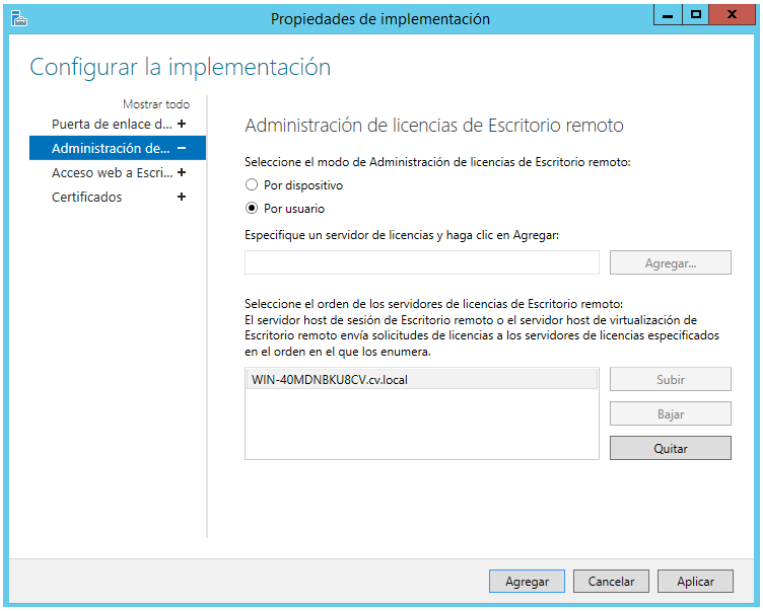
Captura 83 Confirmación del servidor de licencias

Una vez agregado el servidor de licencias habrá que configurar la distribución de las licencias. Para ello en la ventana de "Servicios de Escritorio remoto" se clicará en "TAREAS\Editar propiedades de la implementación".



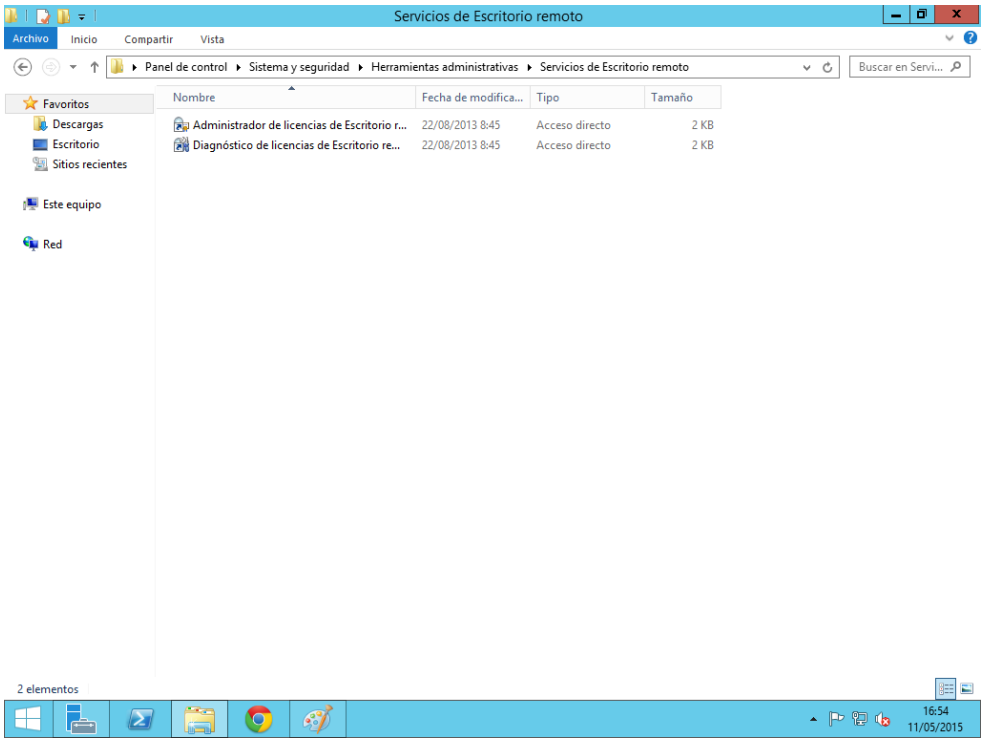
Captura 84 Editar propiedades de la implementación

En la ventana que se abrirá en la sección "Administración de licencias de Escritorio Remoto" se seleccionará la opción "Por usuario" para dar flexibilidad a la hora de iniciar sesión de escritorio remoto a los usuarios desde cualquier equipo.



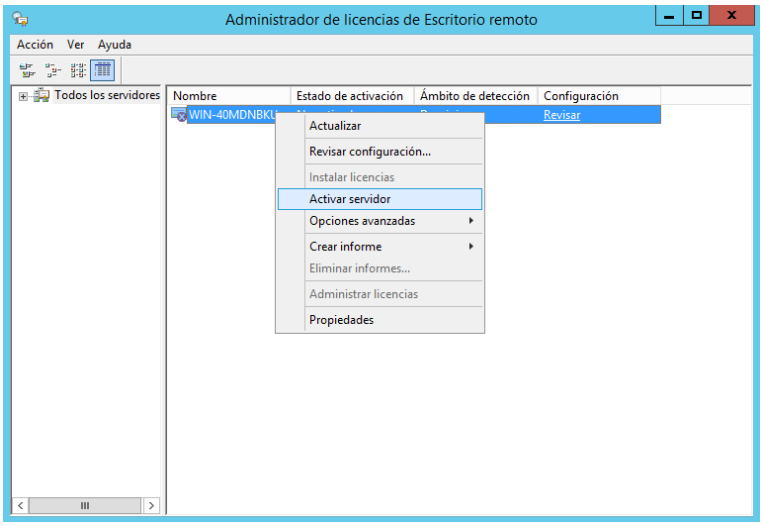
Captura 85 Administración de licencias de Escritorio Remoto

Una vez configurado el "Administrador de licencia" se accederá a las "Herramientas administrativas", en la cual se habrá generado la carpeta "Servicios de Escritorio remoto" con dos entradas para la configuración y la gestión de los mismos. Se accederá al "Administrador de licencias de Escritorio remoto".



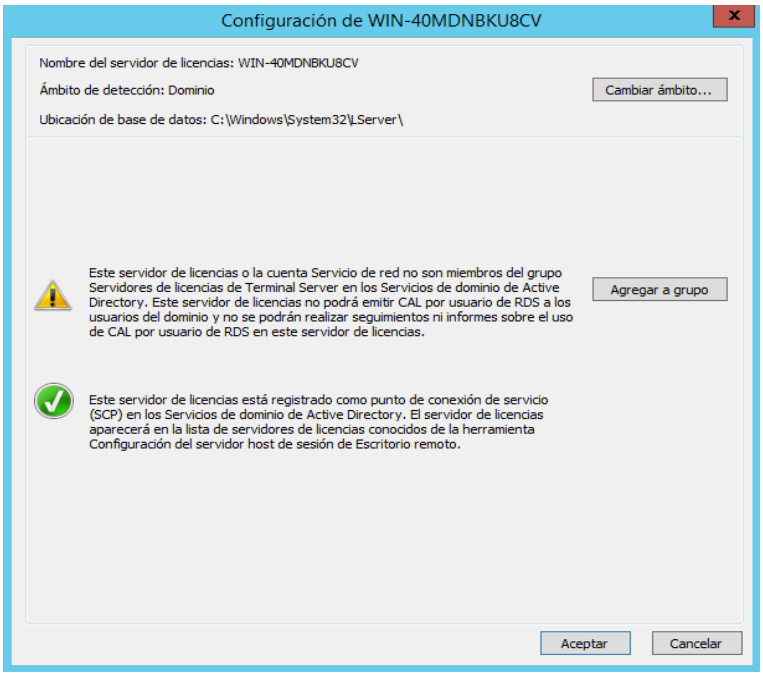
Captura 86 Directorio Servicios de Escritorio remoto

Se abrirá el "Administrado de licencias de Escritorio remoto" en la que se comprueba que el servidor de licencias esta desactivado. En este caso no se activará debido a que no se dispone del paquete de licencias pero habrá que revisar la configuración puesto que es necesario realizar ciertos cambios en la misma. Para ello se clicará con el botón derecho sobre el servidor y se seleccionará "Revisar configuración".



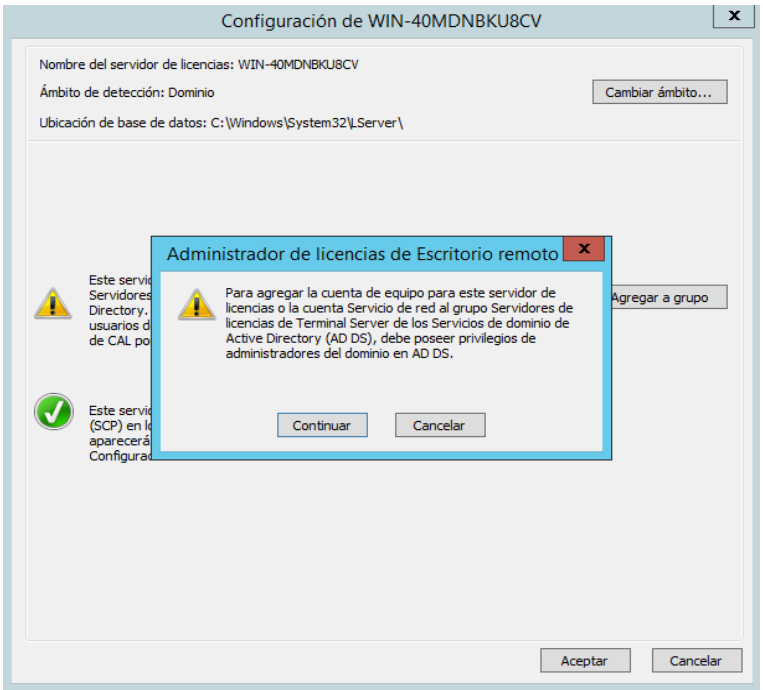
Captura 87 Servidor de licencias

En la ventana de configuración del servidor aparece una advertencia de que el servidor de licencias no está dentro del grupo "Servidores de licencias de *Terminal Server*". Se clicará en "Agregar a grupo" para añadirlo al grupo.



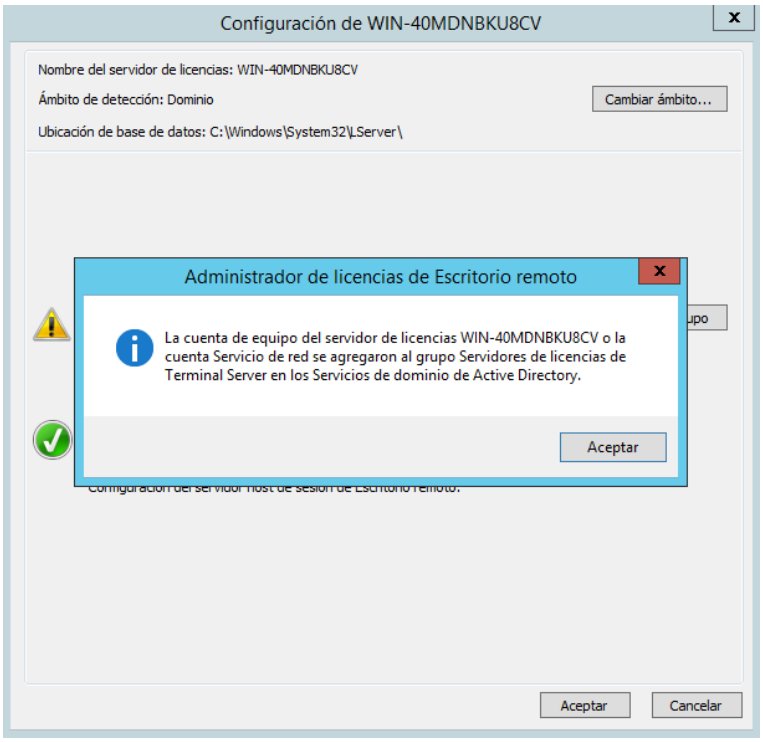
Captura 88 Configuración del servidor de licencias

El sistema advertirá de que se debe tener privilegios de administrador para añadir el servidor, en dicha ventana se clicará en "Continuar".



Captura 89 Agregar servidor al grupo Servidor de licencias de Terminal Server

Cuando termine informará de que se ha añadido el servidor al grupo, posteriormente se clicará en “Cerrar”.



Captura 90 Éxito añadiendo el servidor al grupo

Instalado y configurado el rol de “Escritorio remoto” estará funcionando durante 120 días que son suficientes para la realización de las pruebas.

3.5. Administración de AD DS

AD DS se utiliza para crear una infraestructura escalable, segura y administrable para la administración de usuarios, unidades organizativas y recursos, y proporcionar compatibilidad con aplicaciones habilitadas para el directorio.

También proporciona una base de datos distribuida que almacena y administra información acerca de los recursos de red y datos específicos de las aplicaciones habilitadas para el uso de directorios. La organización de los elementos de la red en una estructura de contención jerárquica ofrece las siguientes ventajas:

- El bosque actúa como un límite de seguridad para la organización y define el ámbito de autoridad de los administradores.
- Se pueden crear dominios adicionales en el bosque para facilitar la partición de los datos de AD DS, lo que permite a las organizaciones replicar datos solo si es necesario.
- Las unidades organizativas simplifican la delegación de autoridad para facilitar la administración de un gran número de objetos.

La seguridad se integra con AD DS a través de la autenticación de inicio de sesión y el control de acceso a los recursos del directorio. La administración basada en directiva facilita la administración de incluso las redes más complejas. Algunas características adicionales son:

- Un conjunto de reglas que define las clases de objetos y atributos incluidos en el directorio, las restricciones y límites de las instancias de estos objetos y el formato de sus nombres.
- Un catálogo global que contiene información acerca de todos los objetos del directorio.
- Un mecanismo de consulta e índice para poder publicar los objetos y sus propiedades.
- Un servicio de replicación que distribuye los datos de directorio en una red.
- Roles de maestro de operaciones o *Flexible Single Master Operations* (FSMO). Los controladores de dominio que contienen los roles de maestro de operaciones se designan para realizar tareas específicas para garantizar la coherencia y eliminar las entradas en conflicto del directorio.

3.5.1. Unidades organizativas, grupos de usuarios y usuarios

Para realización de las pruebas se procederá con la creación de las unidades organizativas (en adelante OU), los usuarios, grupos de trabajo y los directorios compartidos tal y como se ha mencionado en el caso de estudio.

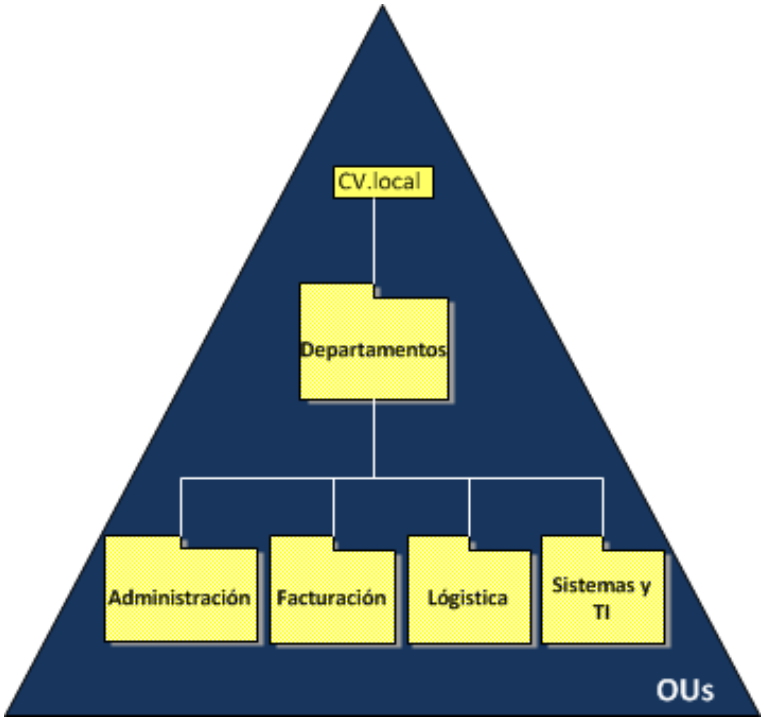
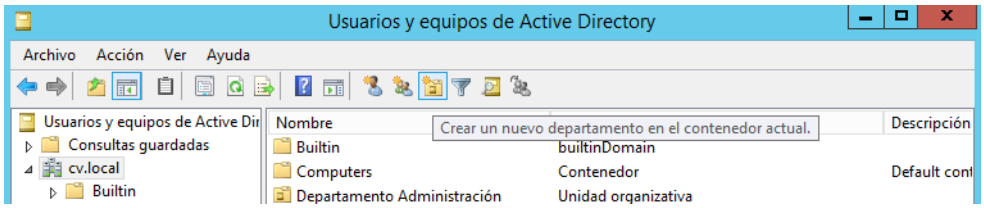


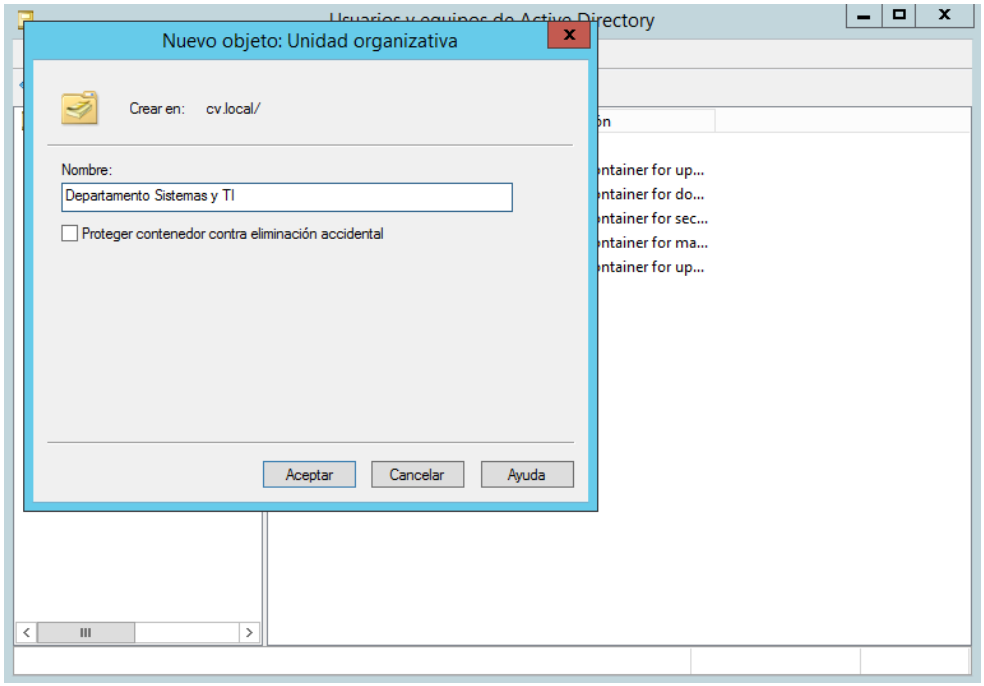
Figura 3 Unidades Organizativas

Primero, se crearán las OU. Las OU son contenedores administrativos dentro del AD que son usadas para coleccionar o agrupar objetos que comparten unos requerimientos comunes para la administración, configuración o visibilidad. Para crearlas se accederá a las herramientas administrativas y se clicará en "Usuarios y equipos de *Active Directory*". Se abrirá la ventana de usuarios y equipos en la que se seleccionará el dominio local "cv,local" y se clicarás en "Crear un nuevo departamento en el contenedor actual".



Captura 91 Crear nuevo departamento

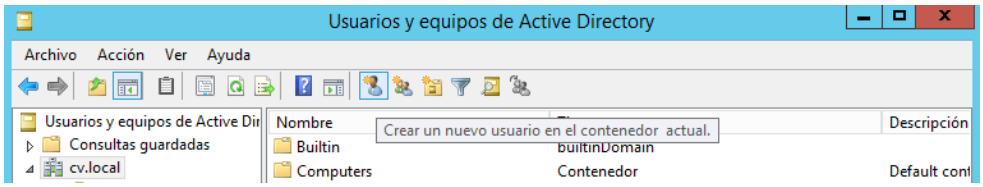
Se abrirá la ventana de "Nuevo objeto: Unidad Organizativa" en la cual se escribirá el nombre de la OU y se clicará en "Aceptar" para crearla.



Captura 92 Nuevo objeto: Unidad organizativa

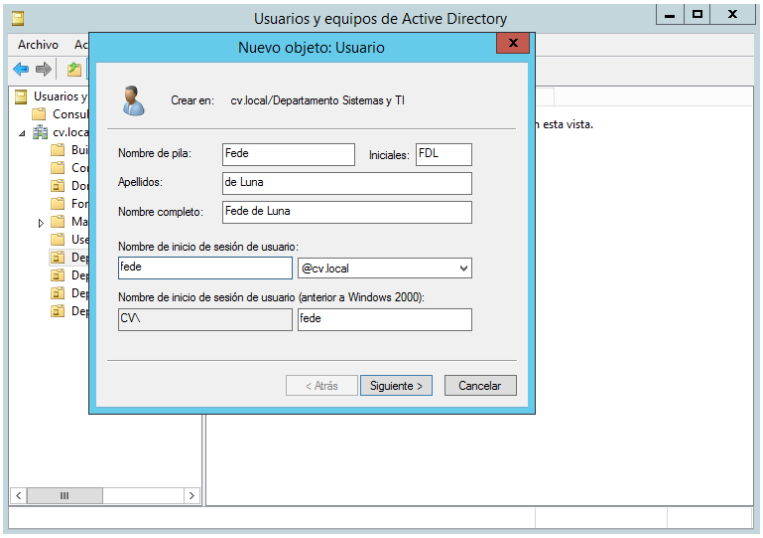
De este modo se crearán todas las OU del caso de estudio propuesto.

Segundo, se procederá con la creación de los usuarios que pertenecerán a cada departamento en el AD. Se accederá a la OU, a la pertenecerá el usuario, y se clicará en "Crear un nuevo usuario en el contenedor actual".



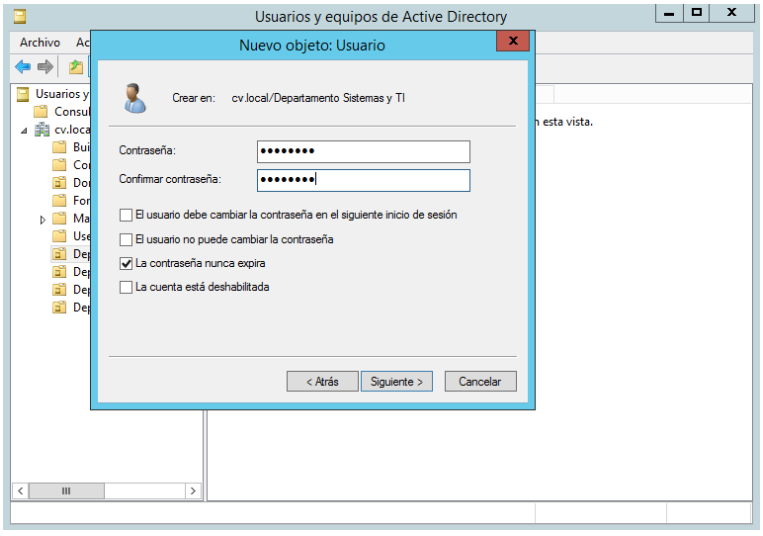
Captura 93 Crear nuevo usuario

Se abrirá la ventana de "Nuevo objeto: Usuario" en la que se escribirá el nombre, los apellidos y el usuarios con el cual accederá al dominio y se clicará en "Siguiente".



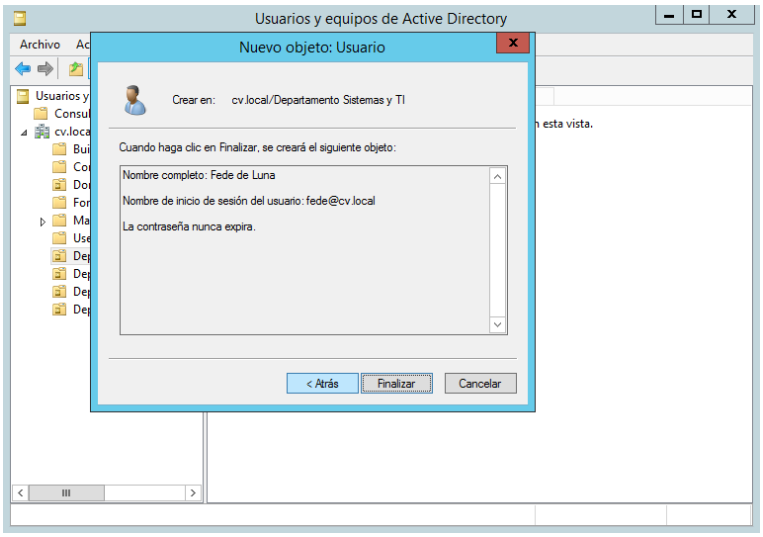
Captura 94 Nuevo objeto: Usuario, configurar nombre

En la siguiente ventana se escribirá la contraseña, entre las opciones a elegir la única opción que se marcará será "La contraseña nunca expira" y se clicará en "Siguiente".



Captura 95 Nuevo objeto: Usuario, configurar contraseña

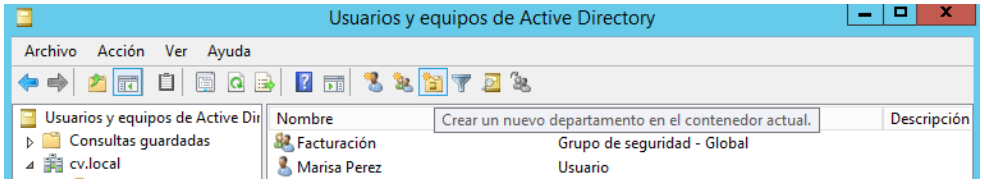
En la última ventana del objeto nos aparecerá la descripción del usuario y se procederá con la creación en la cual se clicará en “Finalizar” para crear al usuario.



Captura 96 Nuevo objeto: Usuario, descripción de la configuración

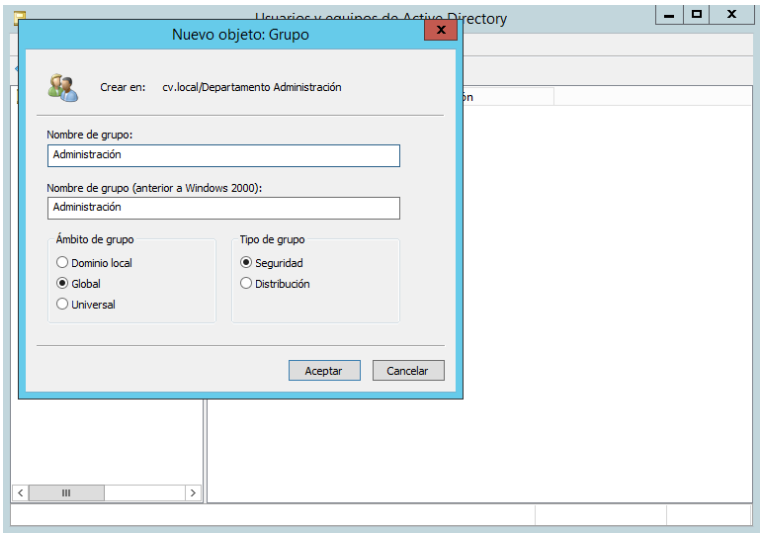
Así se crearán los demás usuarios en sus respectivas OU.

Tercero, se procederá con la creación de los grupos a los cuales pertenecerán cada usuario, al pertenecer a susodicho grupo se les otorgarán permisos y la capacidad de realizar diversas tareas en el equipo dentro del dominio. En cada OU se creará un grupo al que pertenecerán los usuarios de la misma unidad. Para crear el grupo se accederá a la OU y clicará en “Crear un nuevo grupo en el contenedor actual”.



Captura 97 Crear nuevo grupo

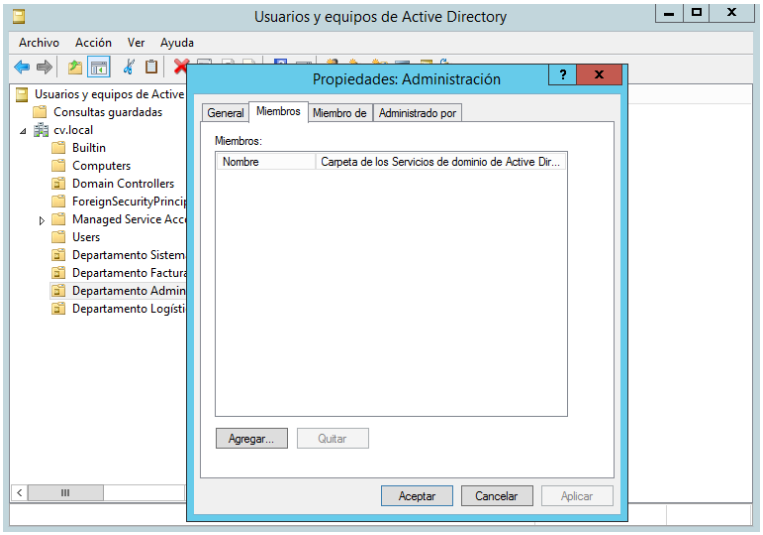
Se abrirá la ventana “Nuevo objeto: Grupo” en la que se escribirá el nombre del grupo, se elegirá el ámbito, en este caso se seleccionará el ámbito “Dominio local”, y se seleccionará la opción “Seguridad” en el tipo de grupo. Se clicar en “Aceptar” para crear el grupo.



Captura 98 Nuevo objeto: Grupo

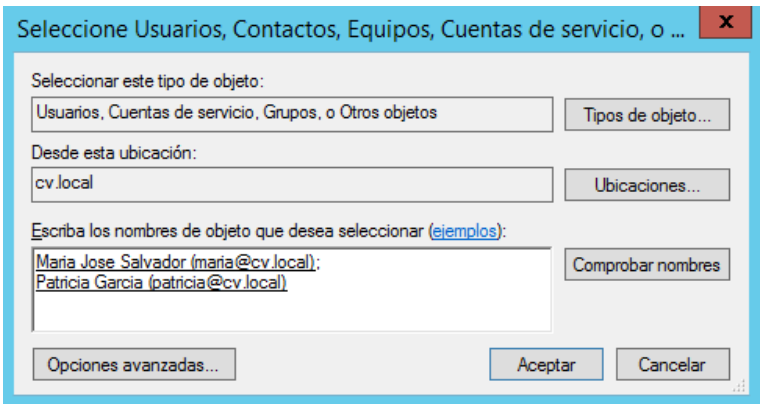
Así se crearán los demás grupos, el único grupo que no se creará es el de los administradores del sistema que pertenecen a la OU de “Sistemas y TI” los cuales sus miembros se añadirán al grupo de seguridad “Administradores” creado automáticamente en la instalación del sistema operativo.

Cuarto, se procederá añadiendo a los usuarios como miembros en sus respectivos grupos. Pare ello se hará doble clic sobre el grupo, se abrirá la ventana de propiedades del grupo en la que se accederá a la pestaña “Miembros” y allí se clicará en “Agregar…”.



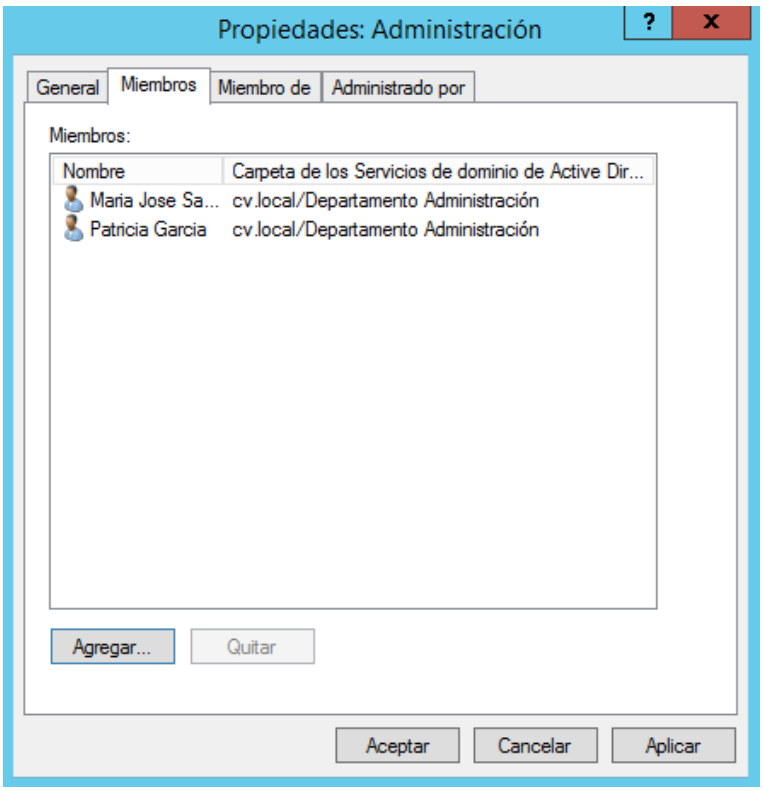
Captura 99 Pestaña “Miembros” del grupo seleccionado

Se abrirá la ventana de "Selección de usuarios, grupos,..." en la cual en el recuadro de abajo se escribirán los nombres de los usuarios, una vez escritos se clicará en "Comprobar nombre" para comprobar que dichos nombres están bien escritos, y se clicará en "Aceptar".



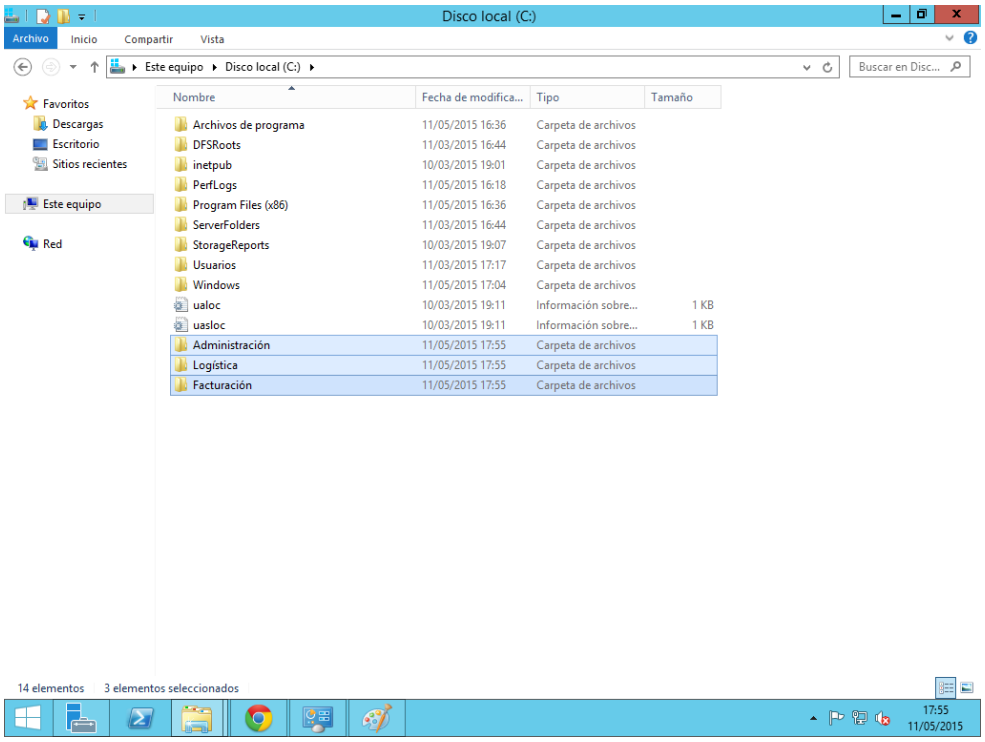
Captura 100 Selección de miembro del grupo

Con esto los usuarios estarán agregados al grupo, así se procederá con los demás grupos.



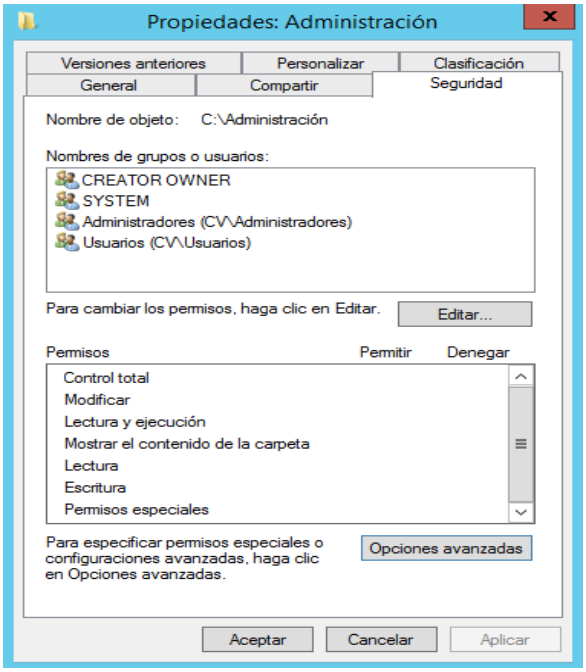
Captura 101 Miembros añadidos al grupo

Quinto, se crearán los directorios compartidos donde tendrán acceso los usuarios, añadiendo los grupos con sus permisos en los respectivos directorios. Los directorios se crearán, en el caso del servidor de pruebas, en la unidad “C:/”.



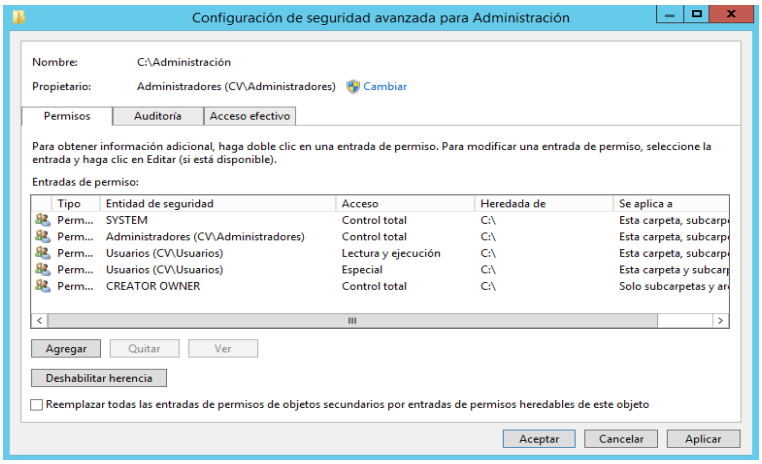
Captura 102 Unidad C:/

Una vez creados los directorios se procederá agregando los grupos a los que pertenecen los usuarios, para ello se accederá a las propiedades del directorio en la pestaña “Seguridad” y se clicará en “Opciones avanzadas”.



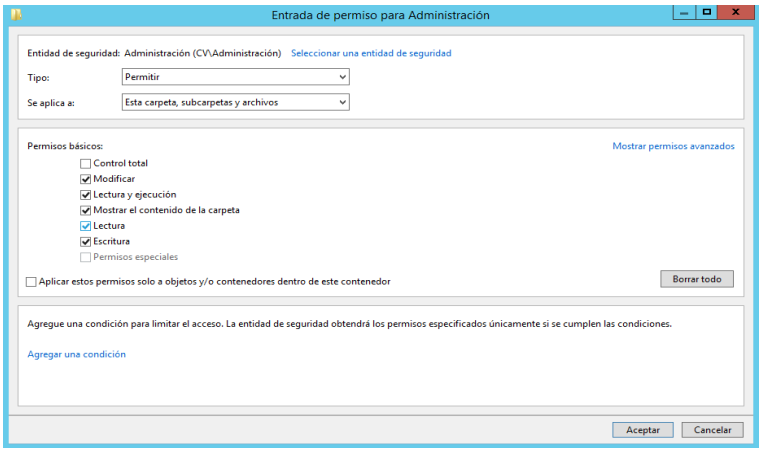
Captura 103 Propiedades del directorio seleccionado

Se abrirá la ventana de "Configuración de seguridad avanzada" en la que se clicará en "Agregar" para añadir al grupo.



Captura 104 Configuración de la seguridad del directorio

En la ventana que se abrirá se seleccionará al grupo que tendrá más permisos sobre directorio. Se seleccionaran que permisos tendrá, según explicados en el caso de estudio, y se clicará en "Aceptar".

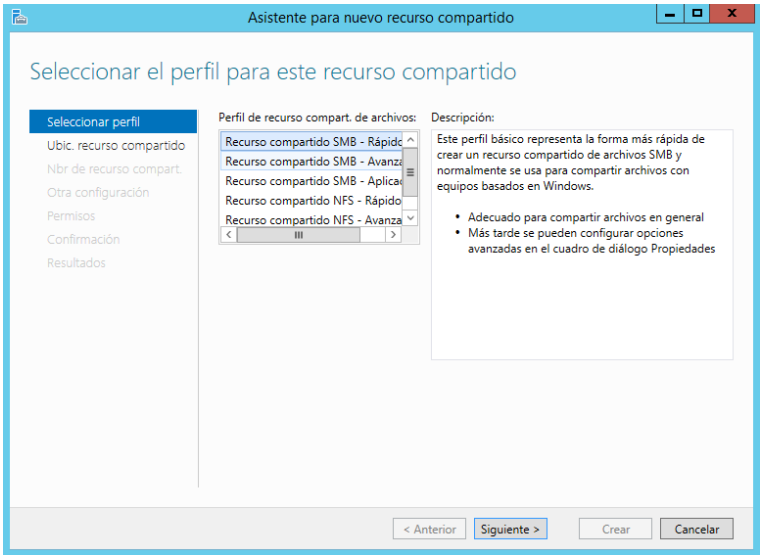


Captura 105 Permisos asignados al grupo seleccionado

Por último, Una vez añadidos los grupos con sus respectivos permisos en los directorios se compartirán los directorios creados. Para ello se accederá al "Administrador del servidor" a la sección "Servicios de archivos y almacenamiento". En esa ventana se accederá a "Recursos compartidos" en la cual se clicará en "TAREA/Nuevo recurso compartido…".

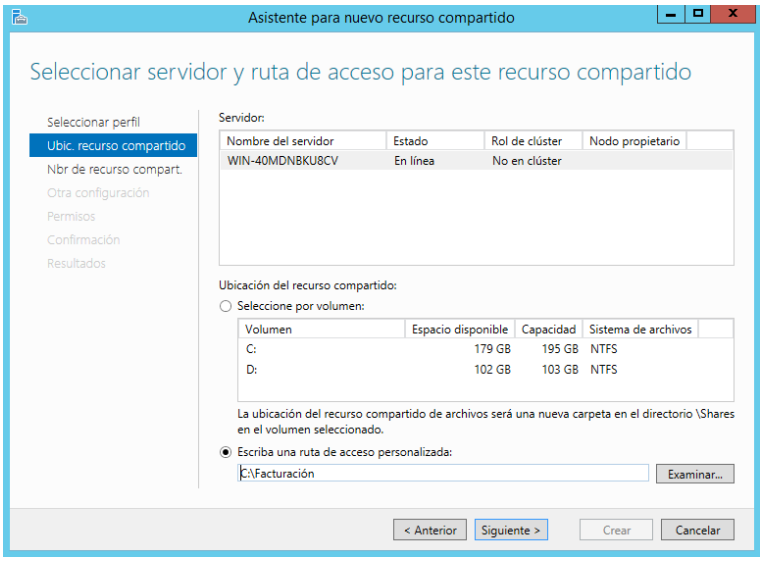
Captura 106 Recursos compartidos

Se ejecutará el asistente del recurso compartido en el que en su primera ventana se seleccionará "Recurso compartido SMB – Rápido" de la lista y se clicará en "Siguiente".



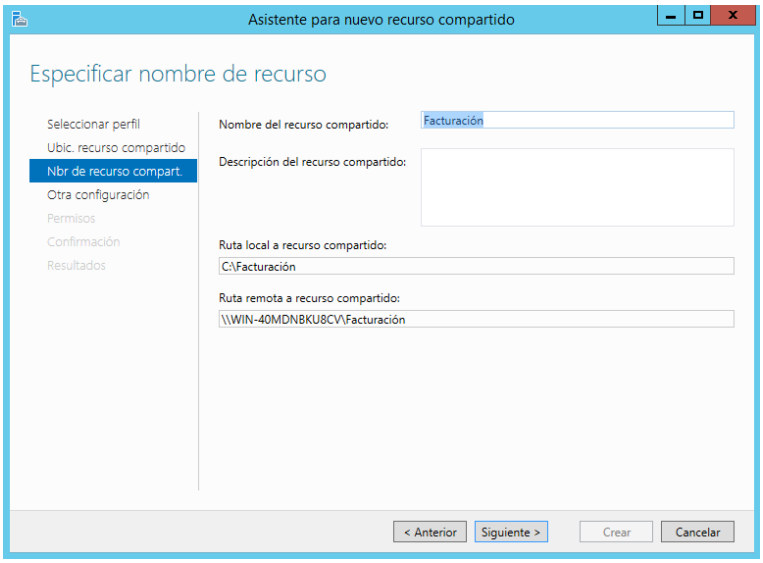
Captura 107 Selección del perfil del recurso compartido

En la segunda ventana se seleccionará "Escriba una ruta de acceso personaliza" en la que se clicará en "Examinar", se seleccionará uno de los directorios anteriormente creados y se clicará en "Siguiente".



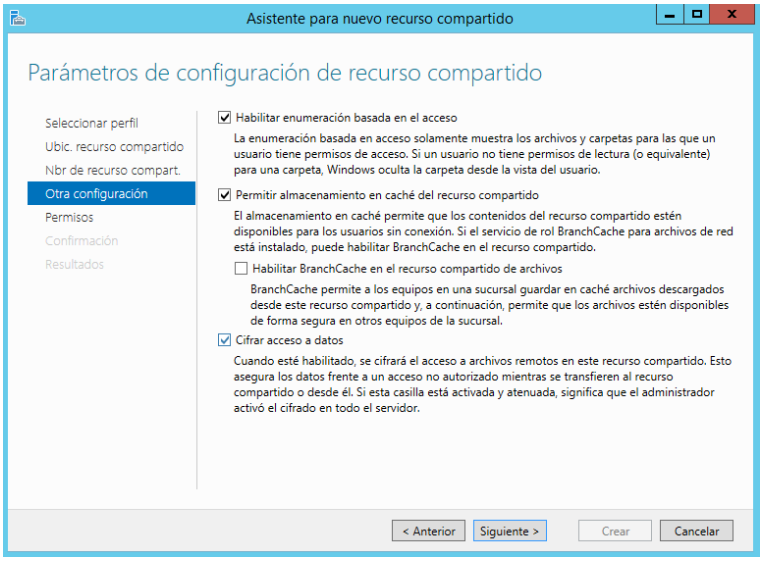
Captura 108 Selección de la ruta del recurso compartido

En la tercera ventana el nombre se dejará por defecto, ya que en este caso tiene el mismo nombre que el departamento y se clicará en "Siguiente".



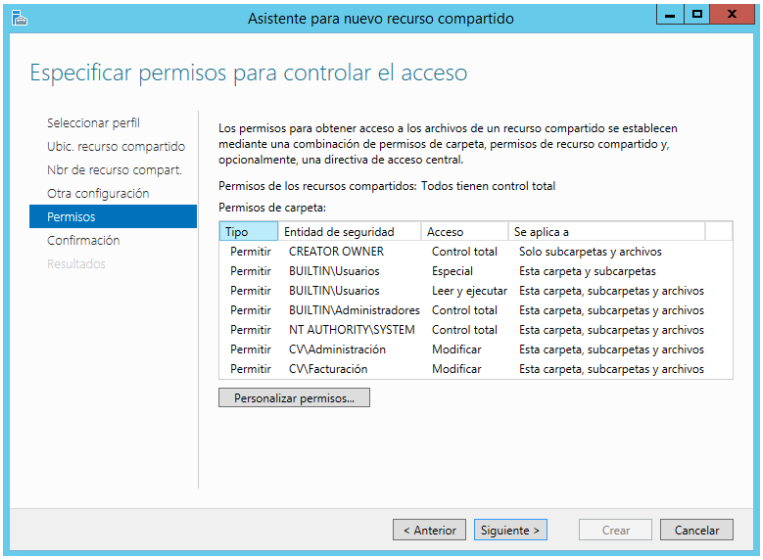
Captura 109 Especificar el nombre del recurso compartido

En la cuarta ventana se marcarán todas las opciones menos la de "Habilitar el BranchCache…", debido a que la empresa solo tiene un domino, y se clicará en "Siguiente".



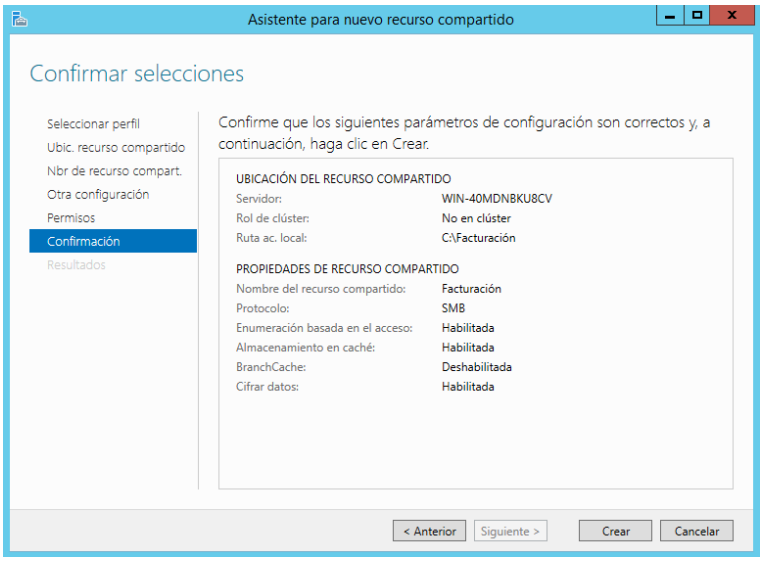
Captura 110 Configuración del recurso compartido

En la quinta ventana en la que se especifican los permisos, no haría falta hacer nada debido a que ya se han configurado anteriormente los permisos, con lo cual se clicará en “Siguiente”.



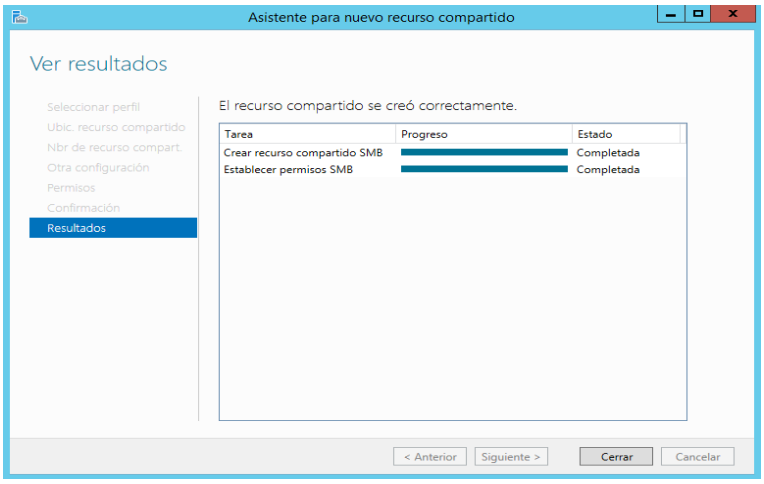
Captura 111 Especificar permisos del recurso compartido

En la sexta ventana aparece una descripción de la configuración del recurso en el cual se clicará en “Crear” para crear el recurso compartido.



Captura 112 Confirmación de la configuración del recurso compartido

Y en la última ventana nos mostrará el proceso de creación de recurso compartido el cual al terminar se clicará en “Cerrar”.

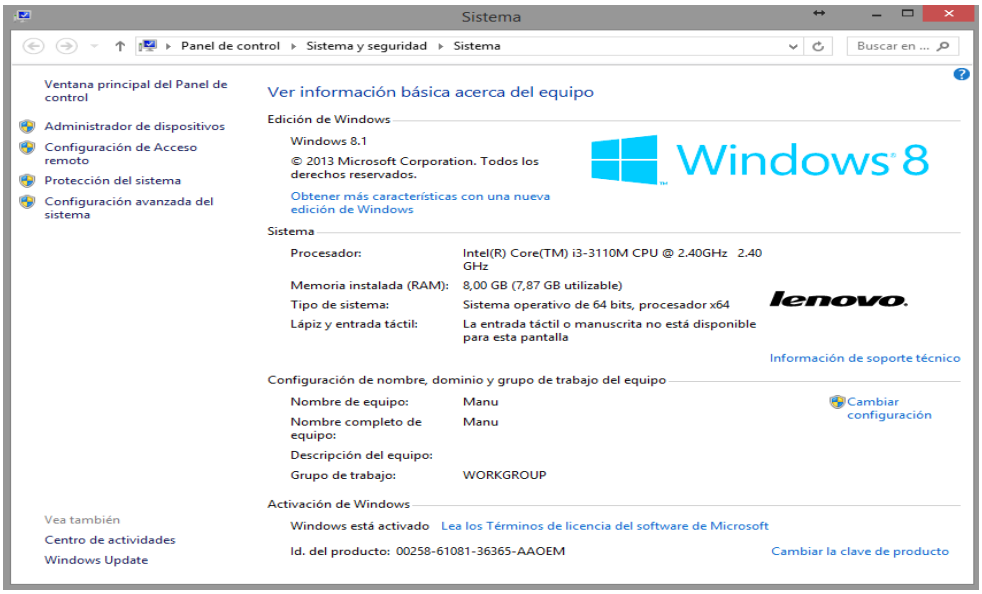


Captura 113 Proceso de compartición del recurso

3.5.2. Equipos

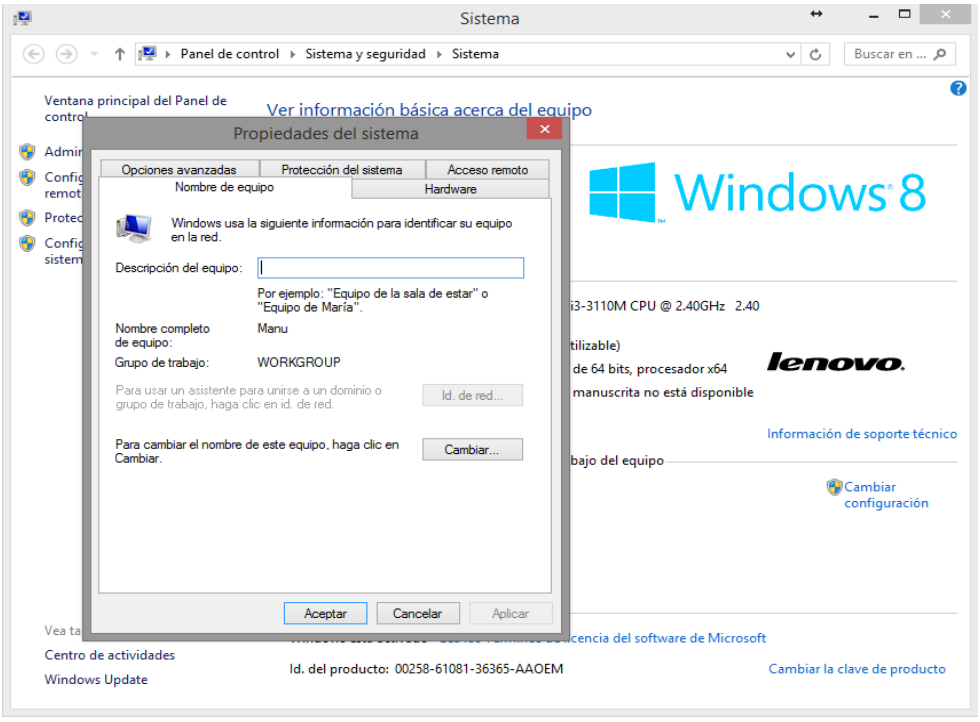
Se puede unir un equipo a un dominio de varias formas, en ese caso es necesario que se cree la cuenta del equipo en el dominio. Ésta creación se puede realizar de forma automática o desde la herramienta administrativa “Usuarios y equipos de *Active Directory*”, de igual forma a como anteriormente se han creado a los usuarios. En este caso se harán de forma automática, debido a que en la empresa del caso de estudio lo realiza de esta forma, el sistema será el encargado de crear la cuenta en la carpeta “*Computers*” del dominio “cv.local” de AD.

El equipo que se utilizará para las pruebas tiene instalado el sistema Windows 8.1, en susodicho equipo accedemos a la ventana “Sistema” que se encuentra en “Panel de control/Sistema y seguridad”. En esta esta ventana, en la sección “Configuración de nombre, dominio y grupo de trabajo del equipo” se clicará en “Cambiar configuración”.



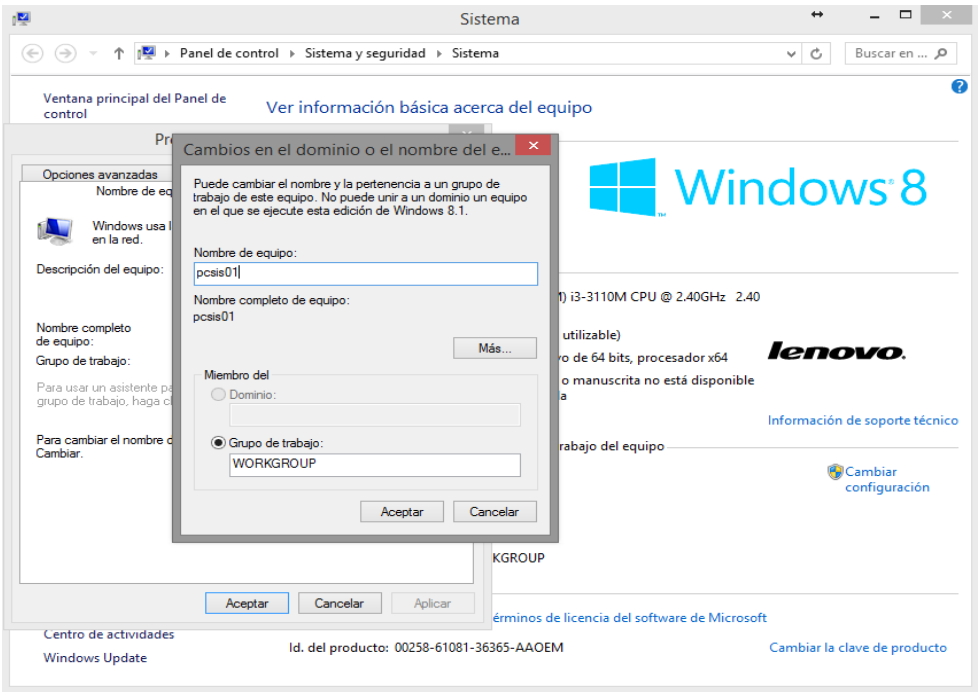
Captura 114 Información del sistema de Window 8.1

Se abrirá la ventana de propiedades del sistema donde en la pestaña “Nombre del equipo” se clicará en “Cambiar”.



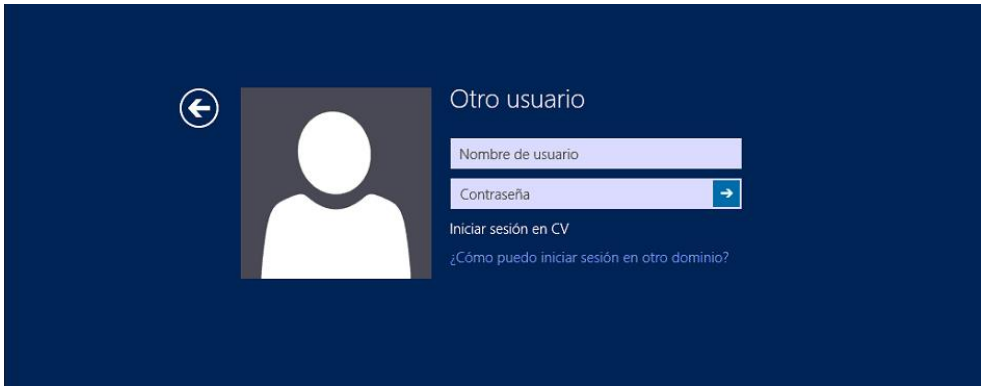
Captura 115 Propiedades del sistema

En la ventana de cambio de dominio se pondrá un nombre al equipo, en el caso de estudio se ha especificado en nombre que contendrá cada equipo pero en equipo de pruebas no llevara ninguno de estos nombres, y se seleccionará la opción “Dominio”, en la sección “Miembro de”, e se escribirá el dominio “cv.local”.



Captura 116 Cambios en el dominio o el nombre del equipo

Cuando se añade un equipo al domino nos solicita las credenciales de un usuario con privilegios de administrador para poder realizar dicha acción. Tras proporcionar las credenciales el sistema mostrará una ventana con el resultado de dicha operación y solicitará el reinicio del equipo. Una vez se reinicie el equipo estará preparado para que cualquier usuario del dominio pueda iniciar sesión en él.



Captura 117 Inicio de sesión en el equipo añadido al dominio

En conjunto con el equipo de Windows 8.1 se creará una máquina virtual con Windows 7 x64 el cual se agregará el AD de la misma forma como se ha hecho con el equipo mencionado anteriormente.

4. Configuración de la seguridad del sistema mediante directivas de grupo

4.1. Introducción a la seguridad mejorada en WS 2012

En las empresas y organizaciones es muy importante que los sistemas dispongan de mecanismos que proporcionen seguridad para proteger su activo más preciado, que son los datos y la información privada. WS 2012 ha seguido innovando y evolucionando para satisfacer este campo, tales innovaciones o mejoras abarcar desde seguridad a nivel de red hasta nuevas políticas o copias de seguridad, entre otras. Las mejoras en WS 2012 son las siguientes:

BitLocker:

Este mecanismo una manera sencilla y segura de cifrar los datos y desde su aparición se han ido añadiendo múltiples funcionalidades y mejoras, que son las siguientes:

- **Configuración de *BitLocker*:** es posible habilitarlo en el entorno de preinstalación de *Windows* (WinPE), lo que posibilita el despliegue de sistemas operativos desde los servicios de implementación de *Windows* con unidades ya cifradas anteriormente a la instalación del sistema.
- **Cambio de contraseña y PIN del usuario estándar:** en los sistemas posteriores a WS 2012 para implementar y modificar *BitLocker* se requerían tener privilegios de administrador, todavía se requieren de estos permisos pero los usuarios pueden cambiar las contraseñas y PIN de manera que les sea más fácil de recordarlos. No obstante al usuarios se les concienciará con unas características mínimas que debe tener la contraseña o el PIN para hacerlos más robustos por temas de seguridad.
- **Desbloqueo de red:** esta característica incluida en WS 2012 permite desbloquear unidades cifradas con BitLocker desde una red cableada de confianza en el entorno del dominio.
- **Cifrado solo del espacio en disco utilizado:** anteriormente cuando se habilitaba el *BitLocker* en algún volumen los cifraba completamente, ahora ofrece dos métodos de cifrado:
    - Cifrado solo del espacio utilizado: este método es obviamente es más rápido al cifrar solo los datos almacenados en el volumen.
    - Cifrado del volumen completo: este método cifra el volumen completo tal y como se hacía en anteriormente.

Es posible seleccionar el tipo de cifrado con la utilización de directivas de grupo, dentro de este conjunto de directivas aparecen 3 grupos: unidades de datos extraíbles, unidades de datos fijas y unidades de sistema operativo. En cada uno de los grupos existe una directiva (“Aplicar tipo de cifrado de unidad”) seguida del grupo en el que esté situada.

Secure Boot:

Este mecanismo de protección evita que se cargue un MBR (*Master Boot Record*) de un sistema desconocido, para que cargue un MBR el arranque del sistema operativo vendrá firmado digitalmente. Esta firma se comprobará antes de lanzar el arranque del sistema o al liberar las de cifrado desde el chip TPM (*Trusted Plataform Module*) para que se descifren los discos con el mecanismo *BitLocker*.

Secure Boot viene incorporado de serie en los firmwares UEFI (evolución de la BIOS) y es totalmente compatible con el estándar UEFI 2.3.1 que no se requiere un chip TPM.

Copias de seguridad online:

En el apartado de copias de seguridad de WS se incluye una nueva característica denominada *Online Backup*. Esta característica se ofrece como alternativa la cual podrá realizar copias de seguridad de los datos en una ubicación en la nube, de esta manera utilizando el servicio *Microsoft Online Backup Service* se podrá diseñar una política de recuperación antidesastres o daño de la información con las copias almacenadas fuera de la empresa.

La característica *Online Backup* ofrece sencillas opciones de configuración y administración, con el desarrollo de esta característica se cumplen una serie de objetivos, que son los siguientes:

- **Copias de seguridad incrementales:** con estas copias únicamente se transferirán aquellos bloques en los que se detecten cambios.
- **Compresión y cifrado de datos:** asegura la confidencialidad de los datos, estos serán cifrados en el servidor local antes de ser transferidos a la ubicación en la nube.
- **Verificación de la integridad de los datos:** cuando al realizar la copia de seguridad algunos de los datos hubieran sido daños en la transmisión, sería detectado rápidamente y se corregiría de forma automática en la siguiente tarea de *backup*.
- **Políticas de retención:** se podrá crear una política para que cuando una copia de seguridad exceda la fecha de retención se elimine automáticamente, para mantener optimizado el espacio de almacenamiento de la nube.

DNSSEC:

DNSSEC (*Domain Name System Security Extensions*) es un conjunto de extensiones para aumentar la seguridad del protocolo DNS. Los servidores con el rol de DNS no autoritativos son capaces de validar las respuestas que reciben cuando estos consultan a otros servidores DNS.

Este método utiliza varias maneras de validar la autenticidad de las respuestas DNS, principalmente mediante firmas digitales y claves criptográficas, que son las siguientes:

- **Denegación de existencia autentificada:** asegura que una respuesta como "No existente" sea válida, creado registros NSEC los cuales definen el conjunto de los tipos de RR para el nombre de dominio entero dentro de una zona de DNS.
- **Firmas digitales:** estas firmas generadas con DNSSEC están situadas en la zona DNS de los nuevos registros de recursos, estos se denominan registros RRSIG (firma de registro de recursos) los cuales se añaden a la respuesta de la solicitud.

- **Firma de zona:** cuando se firma una zona DNS con DNSSEC, la firma se aplica individualmente a todos los registros contenidos en ella. Esto agiliza la gestión de los registros sin tener que volver a firmar toda la zona.
- **Anclaje de veracidad:** es una clave pública previamente configurada y asociada a una zona específica del DNS para la realizar validaciones de las solicitudes.
- **NRPT (Tabla de directivas de resolución de nombre):** son una serie de reglas que se pueden configurar para especificar ciertos parámetros de DNS o incluso comportamientos especiales para ciertas entradas DNS.

La función y objetivo de la administración de las claves DNSSEC consiste en planear la generación, el almacenamiento, la expiración y el reemplazo de las mismas.

Auditoría de seguridad:

WS 2012 dispone de mecanismos para auditar si las normas establecidas son efectivas. Las auditorias de seguridad ayudan a detectar comportamientos anómalos, identificar y mitigar brechas en la seguridad del sistema e impedir el comportamiento irresponsable del usuario, creando un registro de la actividad del mismo el cual se podrá utilizar para un análisis forense.

Para realizar una tarea de auditoría eficiente es necesario tener en cuenta ciertos aspectos, que son los siguientes:

- **Controlar el volumen de auditoría:** se debe controlar la intensidad de la auditoría para evitar recolectar eventos inútiles con el fin de no generar una carga de trabajo adicional innecesaria.
- **A la hora de analizar los eventos de una auditoría:** es necesario saber identificar los eventos relevantes de aquellos que se pueden descartar.
- **Necesidades para generar directivas de auditoría:**
    - Las directivas de varios GPO no se combinan.
    - La auditoría de acceso a objetos global genera un gran volumen de auditoría.

Cambios introducidos en la auditoría de seguridad en WS 2012:

CARACTERÍSTICA	VERSIONES ANTERIORES	*WINDOWS SERVER 2012*
Auditoría de acceso a archivos.	X	X
Auditoría de dispositivos de almacenamiento extraíbles.		X
Auditoría de inicio de sesión de usuario mejorado.	X	X
Auditoría de nuevos tipos de objetos protegibles.		X
Directivas de auditoría basadas en expresiones.		X

Tabla 4 Introducción de cambios en la auditoría de seguridad[3]

[3] Tabla sacada de la página 254 del libro *Windows Server 2012 para IT Pros*. Edición Informática64, 2012.

Se han mejorado las auditorías de acceso a archivos e inicio de sesión con las directivas de auditoría basadas en expresiones, esta nueva característica permite crear directivas de auditoría concretas mediante la utilización de expresiones basadas en notificaciones de usuario, de equipo y de recurso. WS 2012 también permite configurar directivas para auditar dispositivos extraíbles generando un evento cada vez que el usuario obtiene acceso a un dispositivo de almacenamiento extraíble.

Políticas de seguridad:

Las políticas de seguridad son un mecanismo para poder especificar denegaciones o configuraciones de acceso específicas para los usuarios y equipos. Las novedades y actualizaciones en las funcionalidades de WS 2012 en referencia a las políticas de seguridad son las siguientes:

FUNCIONALIDADES	NUEVA O ACTUALIZADA
Actualización remota de las políticas de grupo.	Nueva
Configuración de directiva de grupo en *Internet Explore 10*.	Nueva
Estado de la infraestructura de las políticas de grupo.	Nueva
Estado del servicio de políticas de clientes inactivos.	Actualizada
Mejoras en el archivo *Registry.pol*.	Actualizada
Nueva directiva de grupo (GPO) de inicio	Nueva
Nuevos *cmdlets* para gestionar políticas de grupo.	Actualizada
Preferencias de directivas de grupo en *Internet Explore 10*.	Nueva
Puesta en marcha rápida (Inicio rápido)	Nueva
Se mejora los reportes del estado de las políticas.	Actualizada
Singin optimizado.	Actualizada
Soporte a las políticas de grupo local para *Microsoft Windows 8 NT*.	Nueva

Tabla 5 Funcionalidades nuevas o actualizadas en las políticas de seguridad[4]

AppLocker:

AppLocker permite gestionar de manera sencilla que aplicaciones pueden ser instaladas en los equipos mediante directivas. Este mecanismo utiliza reglas, junto con las propiedades de los archivos, para gestionar el control de acceso a las aplicaciones y decidir a grupos o usuarios se les aplican dichas reglas.

El mecanismo ha sido mejorado y modificado para adaptarse a los nuevos tipos de aplicaciones introducidas con la nueva interfaz. A los formatos de archivo que era capaz de controlar *AppLocker* se han añadido los siguientes: .mst y .appx. Las nuevas funcionalidades

[4] Tabla sacada de la página 256 del libro *Windows Server 2012 para IT Pros*. Edición Informática64, 2012.

hacen que WS 2012 se pueda generar reglas para archivos ejecutables, *Windows installer*, *scripts* y aplicaciones empaquetadas.

SmartScreen:

SmartScreen es una característica implementada en *Internet Explore* que ayuda a detectar sitios web que utilizan técnicas de *phishing* (suplantación de identidad). También protege el sistema contra la descarga y la instalación de programas de tipo *malware* (*software* malintencionado).

Esta característica protege la navegación y la descarga de archivos de las siguientes maneras:

- A medida que se navega por la web la característica analiza el código de los sitios web que se visita en tiempo real y determina si tiene algún código sospechoso, en caso afirmativo se avisara al usuario para que actué con precaución mientras navega por la web.
- Utilización una lista dinámica de sitios *phishing* y de *software* malintencionado, notificados por los usuarios o entidades.
- Comparar los archivos descargados con una lista de *malware* que se sabe que no son de confianza al ser notificados por usuarios y entidades.

Schannel SSP:

Schannel es un proveedor de compatibilidad para seguridad (SSP) que implementa los protocolos de autentificación de Internet: SSL, TLS (*Transport Layer Security*) y DTLS (*Datagram* TLS). La interfaz del SSP (SSPI) es una API que usan los sistemas para realizar funciones basadas en seguridad (entre ellas la autentificación) que funciona como una interfaz común a varios SSP.

Novedades añadidas:

- Permite hospedar varios sitios web con autenticación SSL en un puerto y dirección IP única.
- Reducción del uso de memoria cuando se hospedan varios sitios web con autenticación SSL en un único servidor.
- Permite una mayor cantidad de conexiones de usuarios a los sitios web SSL simultáneamente.
- Permite dar consejos a los usuarios finales a través de la interfaz del equipo para seleccionar el certificado correcto durante el proceso de autenticación.

Características mejoradas:

- Soporte TLS para las extensiones SNI (Indicación de nombre de servidor) para que la comunicación entre el cliente y el servidor se asegure de forma adecuada, el cliente es el encargado de solicitar el certificado al servidor.
- Protocolo DTLS proporciona privacidad en las comunicaciones UDP, también permite que las aplicaciones cliente/servidor se comuniquen de acuerdo a como fueron diseñadas para evitar interceptaciones, alteraciones o falsificación de los mensajes.

Tabla resumen de las novedades y mejoras introducidas el mecanismo *Schannel SSP* en WS 2012:

CARACTERÍSTICA	*WINDOWS SERVER 2008*	*WINDOWS SERVER 2012*
Inclusión de DTLS		X
Inclusión de TLS 1.2	X	X
Mejoras de capacidad de administración para la configurar una lista de certificados que se usarán en un sitio web como anclajes de veracidad.		X
Mejoras de capacidad de administración para la configurar una lista de sugerencias de certificados para su selección por parte del usuario.		X
Soporte TLS para extensiones SNI.		X

Tabla 6 Agregación de nuevas características a Schannel SSP en WS 2012[5]

User Account Control:

User Account Control (en adelante UAC) es el encargado de mostrar una serie de notificaciones cuando las aplicaciones intenten realizar algún cambio en el equipo. El control de cuentas de usuario es quien envía las notificaciones siempre y cuando estos cambios requieran del permiso del administrador. Se puede configurar atendiendo a 4 niveles que son los siguientes:

- **Notificarme siempre.** Es la configuración más segura y sus características son las siguientes:
  - Avisar antes de que las aplicaciones realicen cambios en el sistema utilizando privilegios de administrador.
  - La notificación aparecerá con la pantalla atenuada, debiendo aprobar o denegar los cambios que realicen las aplicaciones en el sistema.
- **Notificarme sólo cuando una aplicación intente realizar cambios en el equipo.** Este es el modo configurado por defecto en el control de cuentas y sus características son las siguientes:
  - Avisar antes de que las aplicaciones realicen cambios en el equipo utilizando privilegios de administrador.
  - Mostrará notificaciones si una aplicación intenta realizar cambios en una configuración de *Windows*.
  - No mostrará notificaciones en el caso de realizar cambios en una configuración de *Windows* que requieran privilegios de administrados.
- **Notificarme solo cuando una aplicación intente realizar cambios en el equipo.** Es exactamente igual a la anterior a excepción de que el escritorio no se atenúa.

[5] Tabla sacada de la página 262 del libro *Windows Server 2012 para IT Pros*. Edición Informática64, 2012.

- **No notificarme nunca.** Es la configuración menos segura, las aplicaciones tendrán el mismo acceso al equipo que el usuario y podrán realizar cambios en áreas protegidas del sistema, datos personales, archivos guardados y cualquier elemento almacenado en el equipo. Las características son las siguientes:
    - Nunca notificará antes de que se realicen los cambios en el equipo.
    - Si un usuario inicia sesión como administrador las aplicaciones tendrán los privilegios de administrador.
    - Si un usuario inicia sesión con cuenta de usuario estándar a las aplicaciones se le denegaran todos los cambios que requieran privilegios de administrador.

Si UAC y *AppLocker* se utilizan conjuntamente se tendrá control sobre las aplicaciones que se ejecuten en los equipos y de los cambios que estas puedan realizar en él.

4.2. Directivas de grupo: conceptos generales

Las directivas de grupo es una infraestructura que le permite implementar configuraciones y preferencias específicas para los usuarios y equipos. Las configuraciones de dichas directivas se encuentran en los objetos de directiva de grupo (en adelante GPO), que se vinculan con los siguientes contenedores de servicio de directorio de AD: sitios, dominios u OU. Posteriormente los destinos afectados evalúan las configuraciones dentro de las GPO mediante la naturaleza jerárquica de AD.

Se puede administrar la configuración y las preferencias de las directivas de grupo en un entorno de AD DS a través de la Consola de administración de directivas de grupo (en adelante GPMC). En el paquete de Herramientas de administración remota del servidor se incluyen herramientas de administración de directicas de grupo para administrar la configuración desde el escritorio.

Al instalar la GPMC también se instala el módulo *Windows PowerShell* con toda la funcionalidad y al instalar el paquete de Herramientas de administración remota del servidor, también se instalan los cmdlets más recientes de *Windows PowerShell*, los cuales pueden configurar las características de las directivas de grupo.

Las aplicaciones prácticas de Las directivas de grupo permiten reducir considerablemente el costo total de propiedad en una organización. Varios factores, como el gran número de opciones de configuración de directiva disponibles, la interacción entre varias directivas y las opciones de herencia pueden hacer que el diseño de una directiva de grupo resulte complejo. Mediante la planificación, el diseño, la comprobación y la implementación de una solución basada en los requisitos de negocios de su organización puede proporcionar la funcionalidad, seguridad y control de administración normalizados que la organización necesita.

Funcionalidades nuevas o actualizadas de las directivas de grupo:

FUNCIONALIDAD	NUEVA O ACTUALIZADA	DESCRIPCIÓN
Actualización remota de la directiva de grupo	Nueva	Programa una actualización de directiva de grupo remota para uno o más equipos.
Mejoras del informe de resultados de la directiva de grupo	Actualizada	Ahora los resultados de la directiva de grupo incluyen más información.
Estado de la infraestructura de la directiva de grupo	Nueva	Muestra el estado de replicación de *Active Directory* y SYSVOL en relación con la directiva de grupo.

Tabla 7 Funcionalidades de las GPO[6]

4.3. Directivas por defecto

Cuando se creó el domino de AD al mismo tiempo se crearon las dos directivas por defecto siguientes:

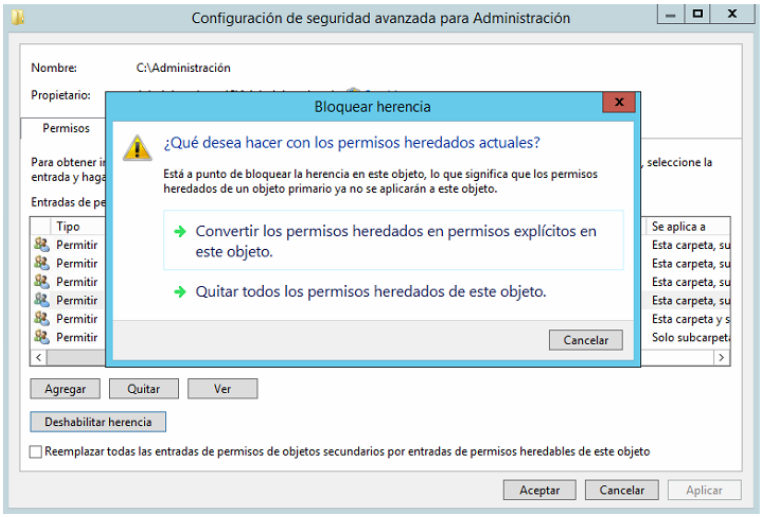
- ***Default Domain Policy***. Esta directiva se sitúa en la raíz del dominio y afecta al conjunto de unidades organizativas. Los parámetros que contiene son de contraseña y de bloqueo, al igual se pueden configurar los parámetros comunes a todos los objetos del dominio o parámetros de auditoría.
- ***Default Domain Controller Policy***. Esta directiva se sitúa y afecta a la unidad organizativa *Domain Controllers*. Los parámetros de la directiva se reservan a los controladores de domino y se pueden configurar los siguientes tipos de parámetros:
    - Directivas de asignaciones de derechos: permiten atribuir permisos suplementarios a un usuario.
    - Directiva de opciones de seguridad: permite la configuración de los parámetros de auditoría así como otros parámetros.

4.4. Preparativo previos a las configuraciones de seguridad

Con el fin de realizar las pruebas necesarias en la configuración de la seguridad en los siguientes puntos se hará una preparación previa, debido a que en el caso de estudio de este TFG no se contemplan ciertas características de seguridad que se configurarán.

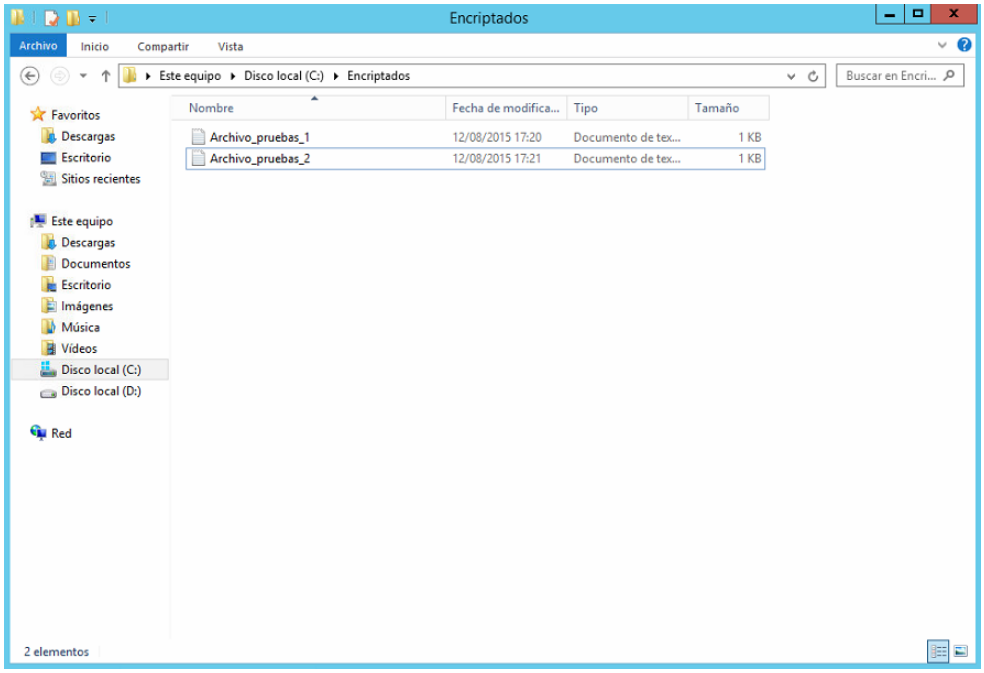
[6] Tabla sacada de la web de Microsoft: *Introducción a la directiva de grupo*, 2013 (https://technet.microsoft.com/library/hh831791)

Se creará un usuario de pruebas, de la misma forma que se ha realizado el apartado 3.5.1, con los permisos mínimos de acceso a los directorios el cual no pertenecerá a ningún OU o grupo creado en el TFG. Al directorio "Administración" se deshabilitará la herencia de permiso accediendo a la configuración avanzada de seguridad, se clicará en "Deshabilitar herencia" y en la ventana que aparecerá se clicara en "Quitar todos los permisos heredados de este objeto". Una vez realizado esta acción se aplicará y se aceptará.



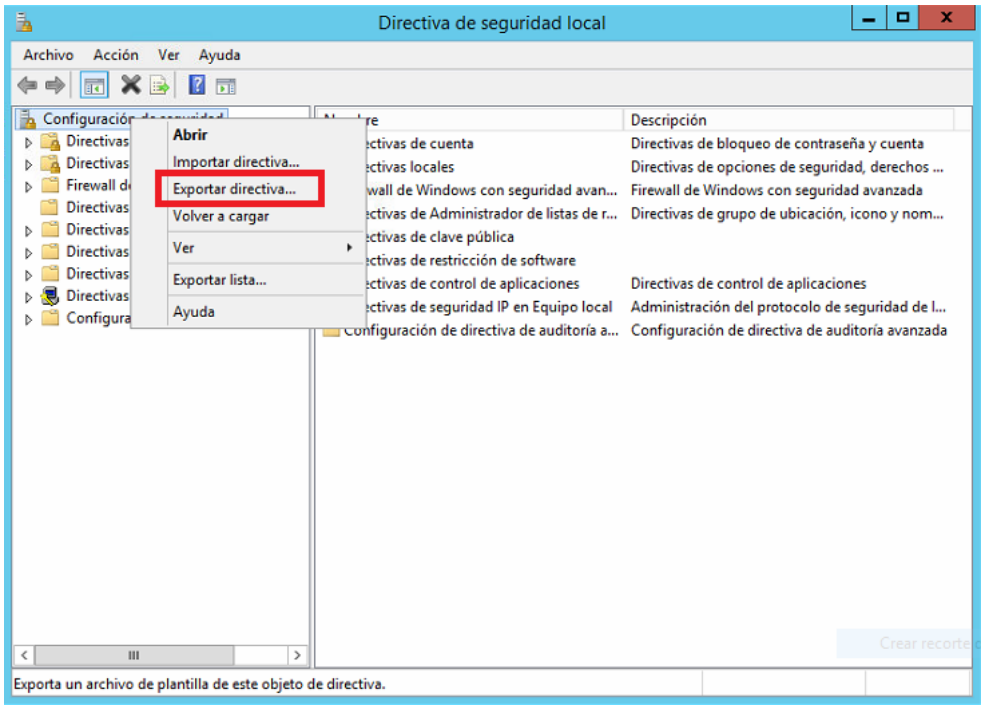
Captura 118 Quitar permisos heredados

También se creará un directorio en "C/:" con el siguiente nombre "Encriptados" en el cual se crearán dos archivo .txt tal y como se aprecia en la captura.



Captura 119 Carpeta y archivos para pruebas

Una buena práctica es importar la configuración de seguridad del sistema antes de realizar todos los cambios previstos, para ello se accederá a "Herramientas administrativas/Directivas de seguridad local" donde allí se clicará con el botón derecho sobre la directiva y se exportará con el nombre, por ejemplo, "Seguridad base".



Captura 120 Exportar directivas de seguridad local

Con estos preparativos previos realizados se empezará con la configuración y prueba de la seguridad de WS 2012.

4.5. Directivas de auditoria

La auditoría permite almacenar una entrada en un registro de eventos cuando un usuario realiza alguna acción en el sistema, registrando al usuario y que acción ha realizado. Es posible registrar dos tipos de acciones: acciones que hayan fracasado o acciones que hayan tenido éxito.

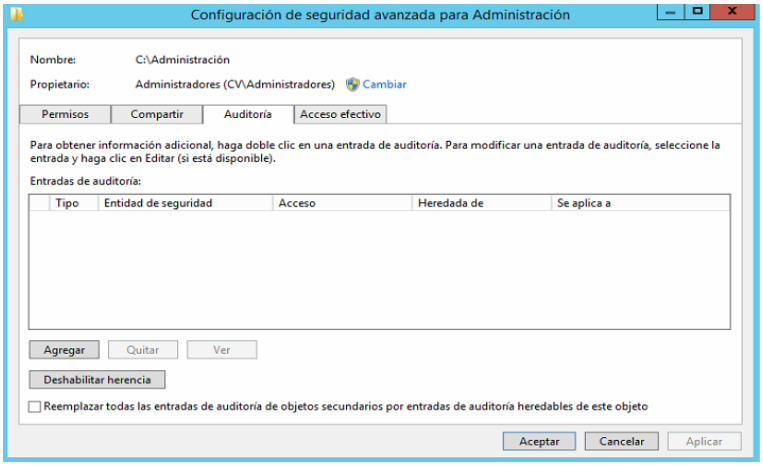
Es posible auditar varios tipos de eventos, mencionados a continuación:

- **Eventos de inicio de sesión de cuenta:** permite auditar cada conexión y desconexión de un usuario o equipo diferente al que registra el evento y también valida la cuenta.
- **Auditar la administración de cuentas:** cuando se administran las cuentas en un equipo se genera un evento, al registrar este evento resulta muy sencillo saber quién ha creado, modificado o eliminado una cuenta.
- **Auditar el acceso del servicio de directorio:** permite auditar el acceso de un usuario a un objeto de AD. Este objeto tiene una lista de control de acceso de sistema (SACL) la cual permite determinar que usuarios y grupos cuyas acciones deben ser auditadas.
- **Auditar sucesos de inicio de sesión:** se produce una auditoría tras cada conexión o desconexión de un usuario.
- **Auditar el acceso a objetos:** permite auditar el acceso a un objeto que contiene una lista de SACL.

En este TFG se practicará auditando el acceso a recursos y carpetas compartidas y las modificaciones sobre objetos de AD

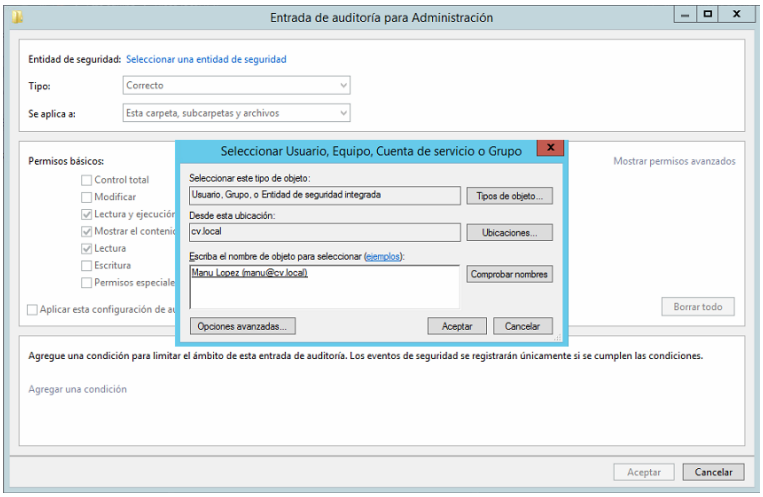
4.5.1. Auditar el acceso a recursos y carpetas compartidas

Para auditar el acceso a recursos y carpetas compartidas se deberá añadir al usuario de pruebas en la auditoria del directorio compartido "Administración", debido a que los usuarios de las OU tienen acceso a los directorios no habrá errores en la auditoria. Se procederá accediendo a la configuración avanzada del directorio en la pestaña "Auditoria".



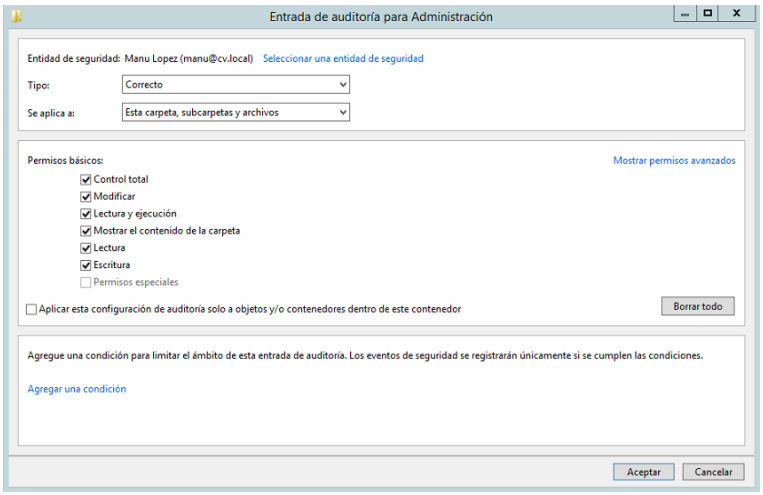
Captura 121 Pestaña de auditoria de la carpeta Administración

En la pestaña "Auditoria" se clicará en "Agregar" con lo cual aparecerá la ventana "Entrada de auditoria para Administración", se clicará en "Seleccionar una entidad de seguridad" para seleccionar al usuario, en este caso utilizaremos el usuario de pruebas, y una vez seleccionado se clicará en "Aceptar".



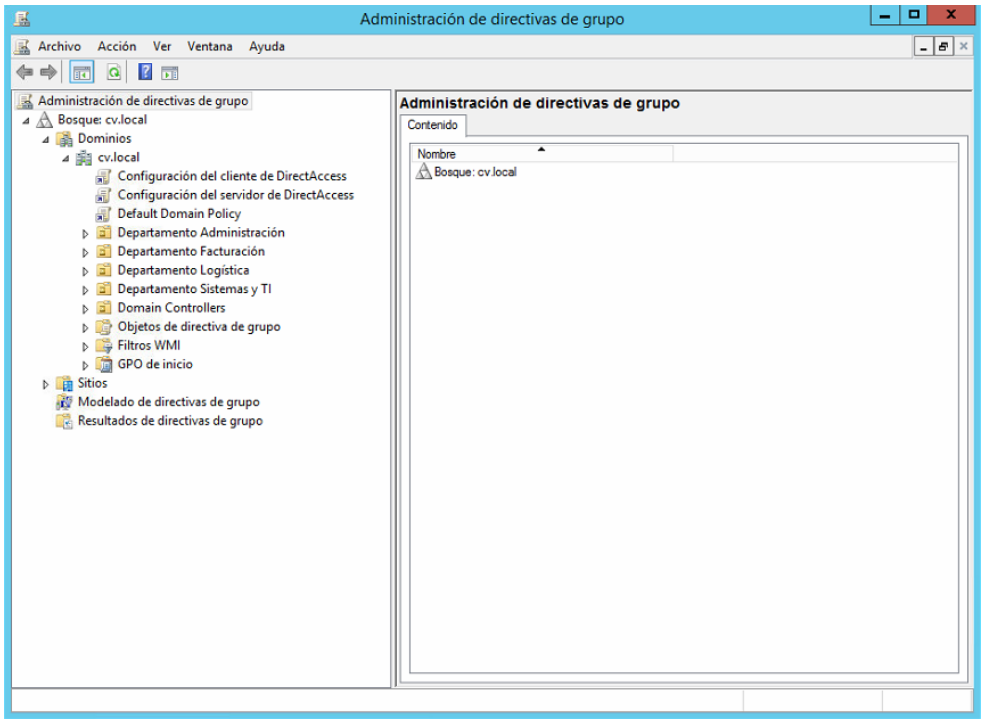
Captura 122 Añadir usuario de pruebas a la auditoria de la carpeta

A ese usuario se le dará control total sobre el directorio. Una vez realizado esta acción se saldrá de la configuración avanzada aceptando los cambios.



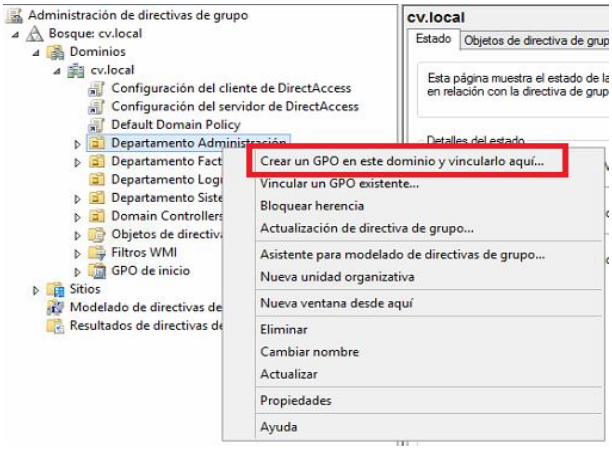
Captura 123 Control total al usuario de pruebas en la carpeta

Después, se procederá con la creación de las directivas de grupo que auditará el acceso. Para ello se accederá a "Herramientas administrativas/Administración de directivas de grupo".



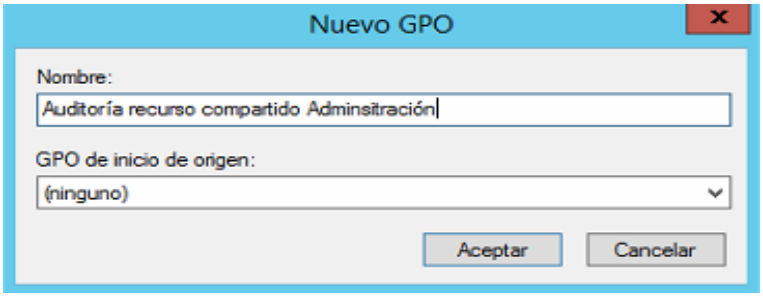
Captura 124 Ventana Administración de directivas de grupo

En la ventana de administración se clicará con el botón derecho sobre la OU y en las opciones que aparecerán se clicará en “Crear un GPO en este dominio y vincularlo aquí…”.



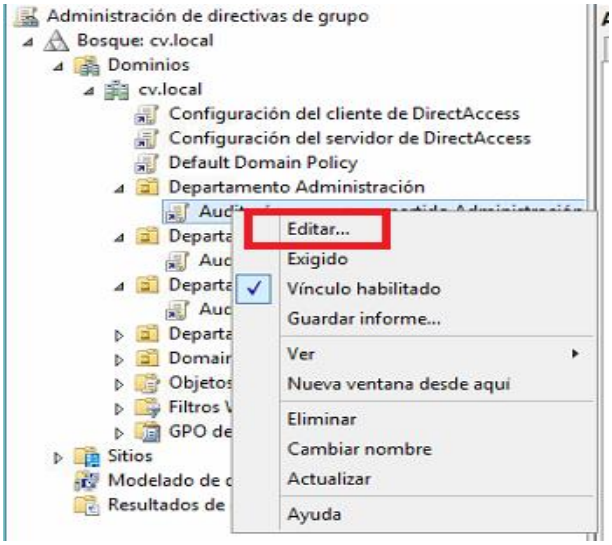
Captura 125 Crear nuevo GPO

Se abrirá la ventana “Nuevo GPO”, en la cual se le asignará un nombre y se clicará en “Aceptar”.



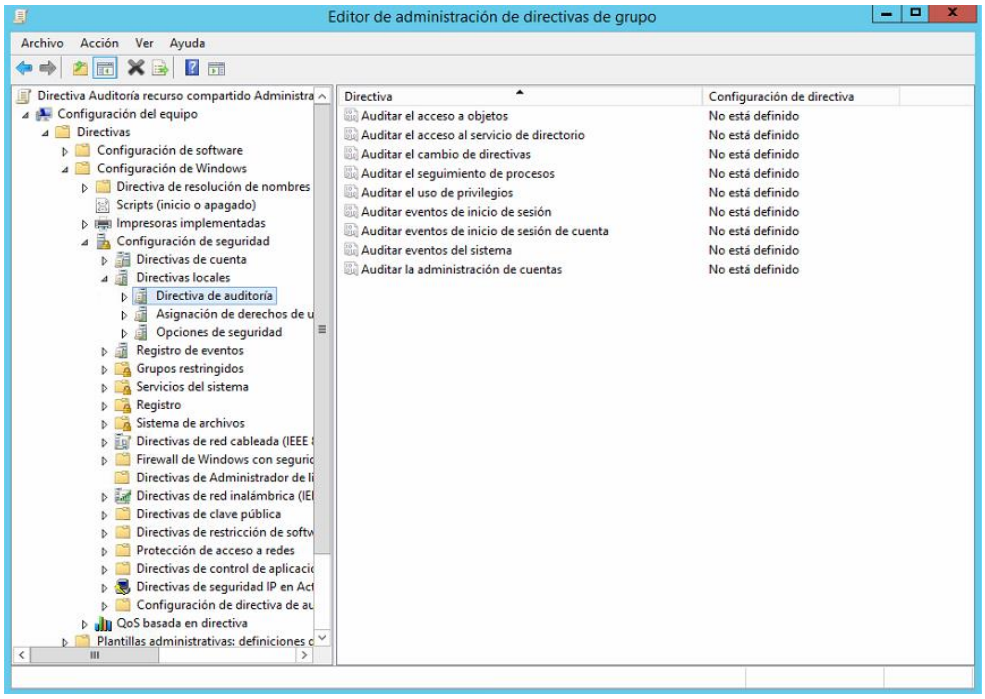
Captura 126 Nombre del nuevo GPO

Una vez creado el GPO en la OU se observará como se ha asignado dicha directiva, se clicará con el botón derecho sobre ella y en “Editar” para empezar con la configuración de la misma.



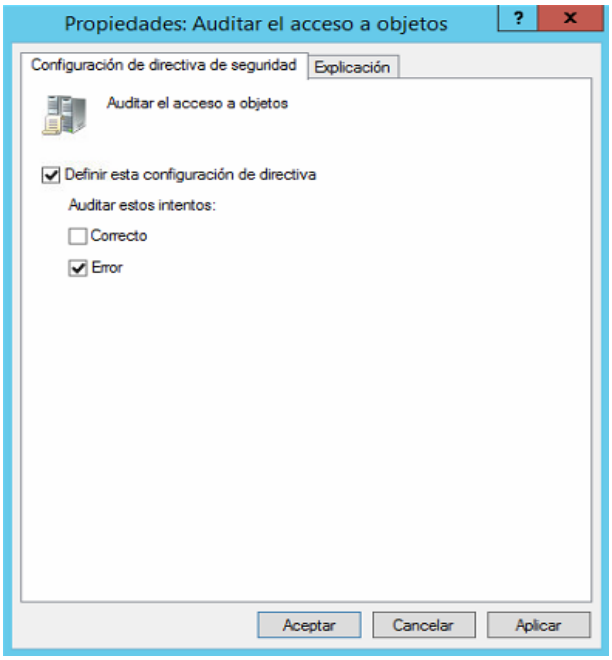
Captura 127 Editar nuevo GPO

En el editor de la directiva se accederá a "Configuración del equipo/Directivas/Configuración de Windows/Configuración de seguridad/Directivas locales/Directiva de auditoria" en la cual aparecerán las auditorias locales que se pueden programar.



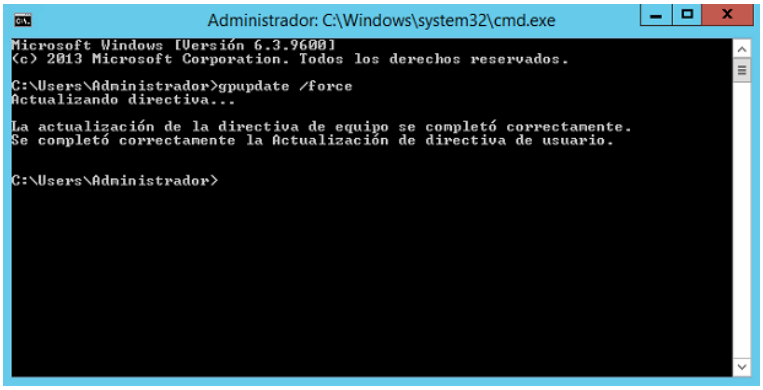
Captura 128 Editor del nuevo GPO

Para auditar el acceso la directiva que se activará será "Auditar el acceso a objetos", haciendo doble clic sobre ella se abrirá la ventana de propiedades de la auditoria en la cual se activará casilla "Definir esta configuración de directivas" y posteriormente se seleccionará la opción "Error". Se aplicará y aceptará para guardar la configuración.



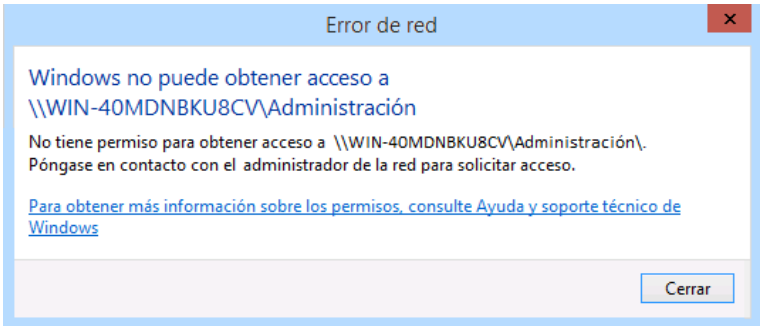
Captura 129 Auditoria del acceso a objeto

Se abrirá un ventana "Símbolo del sistema" para reiniciar las directivas de grupo sin tener que reiniciar el servidor, para que estas funcionen, con el comando "gpupdate /force".



Captura 130 Reiniciar directivas del sistema

Se procederá con las pruebas de acceso a los recursos, para ello se iniciará sesión en la máquina virtual con el usuario de pruebas y se intentará acceder al recurso. Al intentar acceder le aparecerá el error de la captura 132 al usuario.

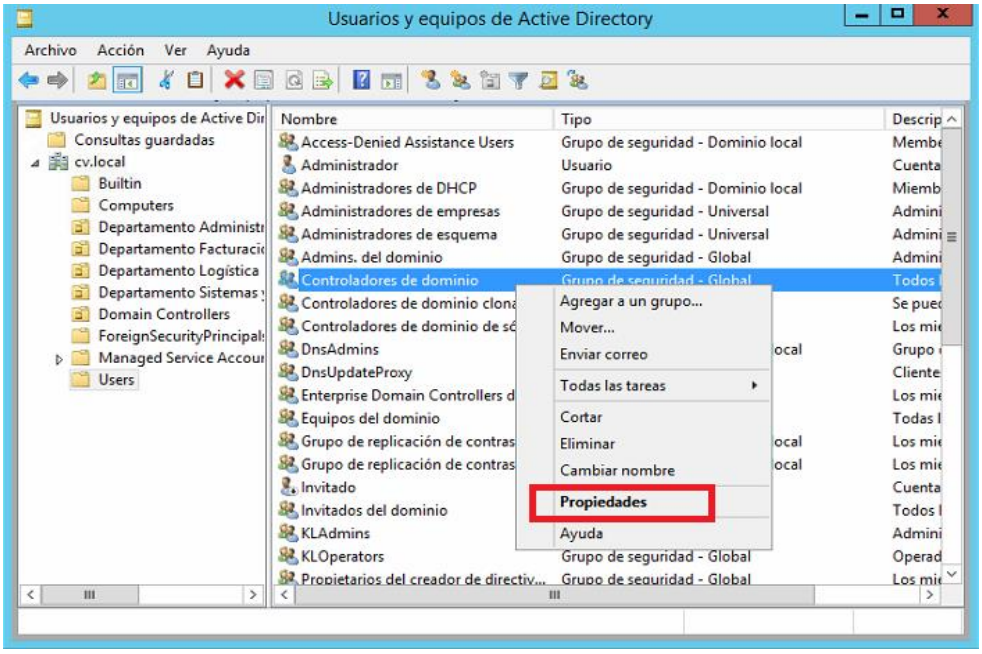


Captura 131 Error de acceso al recurso compartido

Una vez abierta la ventana "Administración de equipos" que está en "Herramientas administrativas" y en la sección "Visor de eventos/Registros de Windows/Seguridad" aparecerá un registro de error.

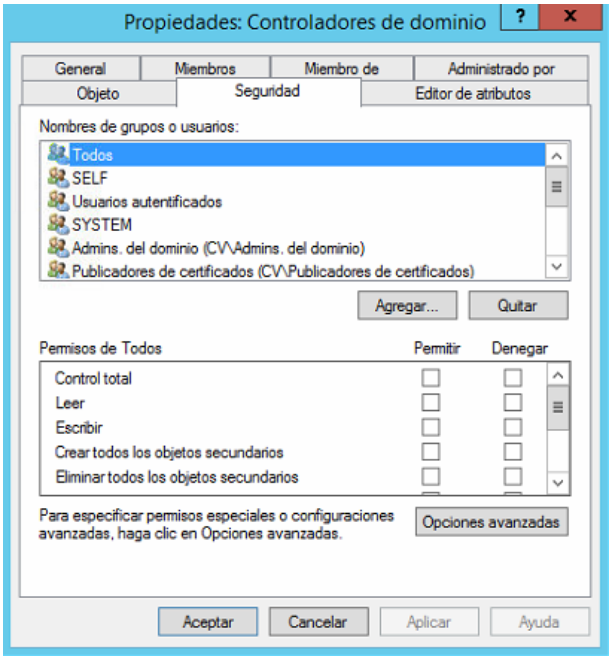
4.5.2. Auditar las modificaciones sobre los objetos de AD

Para auditar las modificaciones sobre objetos de AD se accederá a "Herramientas administrativas/Usuarios y equipos de *Active Directory*" a la OU "*Users*", en dicha unidad se clicará con el botón derecho en el grupo "Controladores de dominio" y se accederá a las "Propiedades".



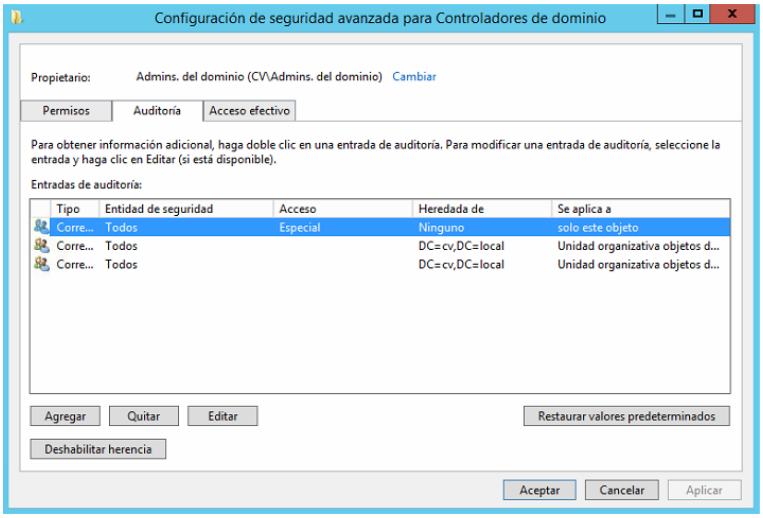
Captura 132 Ventana Usuarios y equipos de AD en la OU Users

En la pestaña "Seguridad" de las propiedades se clicará en "Opciones avanzadas".



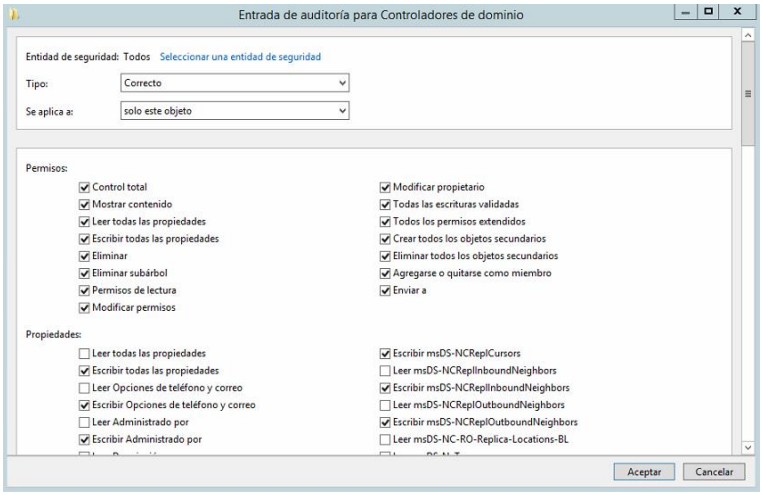
Captura 133 Propiedades del grupo Controladores de dominio

En la ventana de configuración avanzada de seguridad en la pestaña auditoria se seleccionará de la lista la entrada que tienen acceso especial y se clicará en “Editar”.



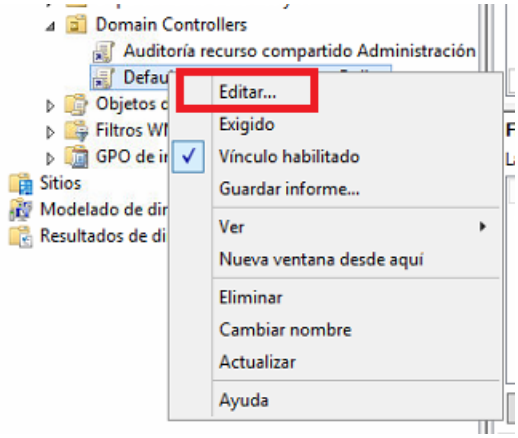
Captura 134 Ventana de auditoria del grupo Controladores de domino

En la ventana de la entrada de la auditoria se seleccionará “Control total” y se aceptará.



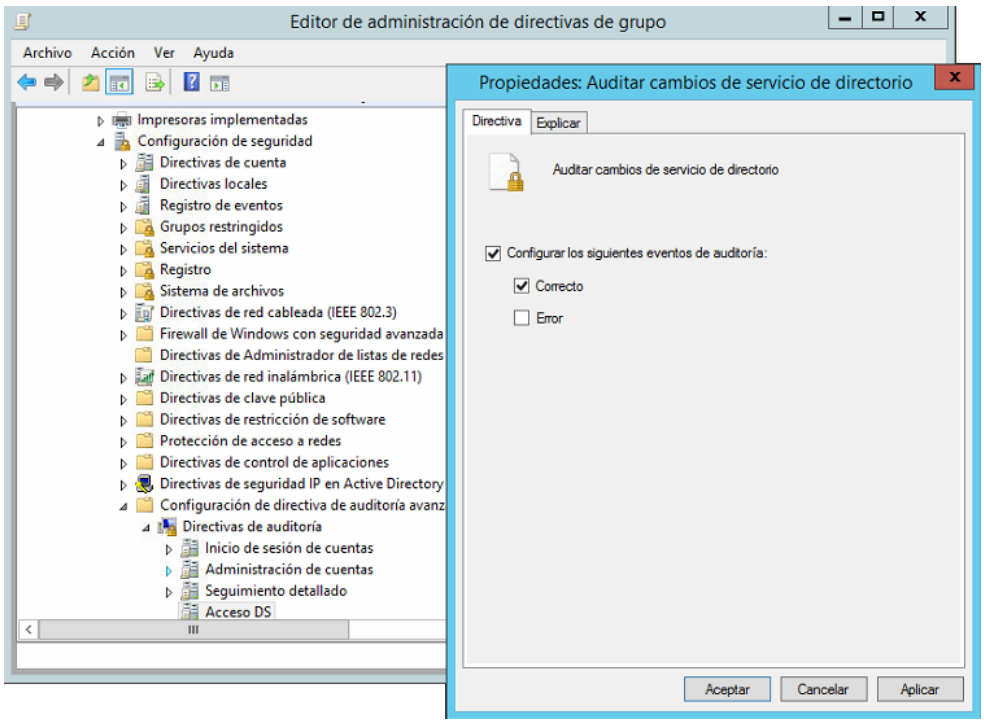
Captura 135 Ventana de la entrada de auditoria con control total

A continuación, se procederá con la modificación de las directivas "*Default Domain Controllers Policy*". Para ello se accederá a "Herramientas administrativas/Administración de directivas de grupo", en dicha ventana se desplegará la OU "*Domain Controllers*", se clicará con el botón derecho sobre el grupo "*Default Domain Controllers Policy*" y se clicará en "Editar".



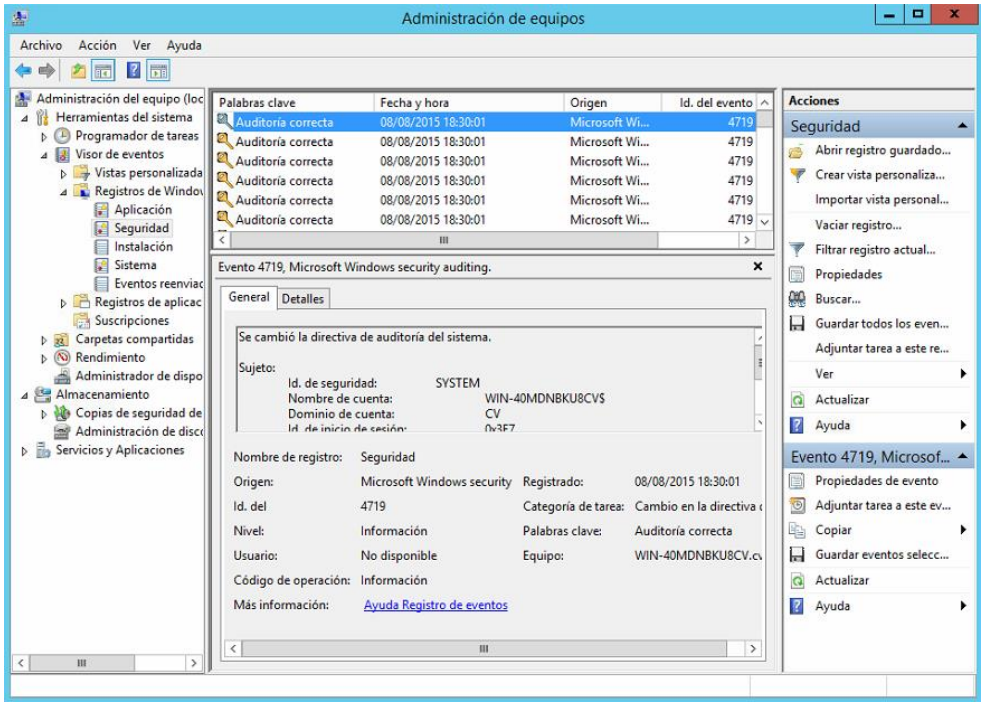
Captura 136 Editar grupo Default Domain Controllers Policy

En el editor de la directiva se accederá a "Configuración del equipo/Directivas/Configuración de Windows/Configuración de seguridad/Configuración de directiva de auditoría avanzada/Acceso DS" en la que aparecerá una lista de auditorías, la que se activará será "Auditar cambios de servicio de directorio". Haciendo doble clic sobre ella se abrirá la ventana de la auditoria en la cual se activará casilla "Configurar los siguientes eventos de auditoria" y posteriormente se seleccionará la opción "Correcto". Se aplicará y aceptará para guardar la configuración.



Captura 137 Habilitar la auditoria de Acceso DS

Al abrir la ventana “Administración de equipos” que está en “Herramientas administrativas” y en la sección “Visor de eventos/Registros de Windows/Seguridad” aparecerán registros sobre acciones que realizan los usuarios, permitiendo conocer la cuenta que ha realizado la acción, el objeto que se ha modificado, etc.



Captura 138 Visor de eventos del sistema

4.6. Gestión de la seguridad

Una directiva de seguridad engloba los parámetros relativos a la política de contraseña y de bloqueo de cuentas. Estos parámetros se configuran como se ha comentado anteriormente en la directiva por defecto *Default Domain Policy*.

4.6.1. Directivas de contraseña muy específica

La directiva de contraseña muy específica permite definir varias directivas de contraseña o de bloqueo, éstas solo se aplican a un usuario o grupo global. Sólo los usuarios que estén en el grupo *Domain Controllers* pueden definir este tipo de directiva.

En WS 2008 aparecen dos nuevas clases que también las encontramos en WS 2012, dichas clases son las siguientes:

- **El objeto configuración de contraseña (en adelante PSO, *Password Settings Object*):** tiene atributos de todos los parámetros de una directiva de dominio por defecto, salvo la configuración Kerberos.
- **El contenedor de configuraciones de contraseña (en adelante PSC, *Password Settings Container*):** se crea en el interior del contenedor del sistema de dominio, el cual permite almacenar PSO.

Los parámetros de la directiva de contraseña son los siguientes:

- **Complejidad de la contraseña:** si se habilitada este parámetro la contraseña no puede contener parte del nombre de la cuenta, como mínimo si longitud será de seis caracteres y al menos deberá estar forma con tres de las cuatro siguientes categorías: letras minúsculas, letras mayúsculas, cifras y caracteres especiales.
- **Vigencia de la contraseña:** se configura una duración mínima en la que no se podrá cambiar a contraseña y máxima que tras pasado este tiempo será necesario cambiarla.
- **Longitud de la contraseña:** permite establecer el número mínimo de caracteres que contendrá contraseña.
- **Exigir historial de contraseñas:** para evitar que un usuario introduce la misma contraseña, al configurar el historial se prohíbe el uso de las últimas contraseñas del usuario, estableciendo el número de estas almacenadas en el historial.
- **Cifrado reversible:** permite almacenar la contraseña utilizando un cifrado reversible lo que equivale a almacenarlas en texto plano sin cifrar.

Los parámetros de la directiva de bloqueo son los siguientes:

- **Duración del bloqueo de cuenta:** permite definir el tiempo en minutos de bloqueo de una cuenta.
- **Restablecer recuentos de bloqueo de cuenta tras:** define el tiempo en minutos tras el cual el contador de bloqueos se pone a 0.
- **Umbral de bloqueo de cuenta:** define el número de intentos erróneos (en el inicio de sesión) tras los cuales se bloquea la cuenta.

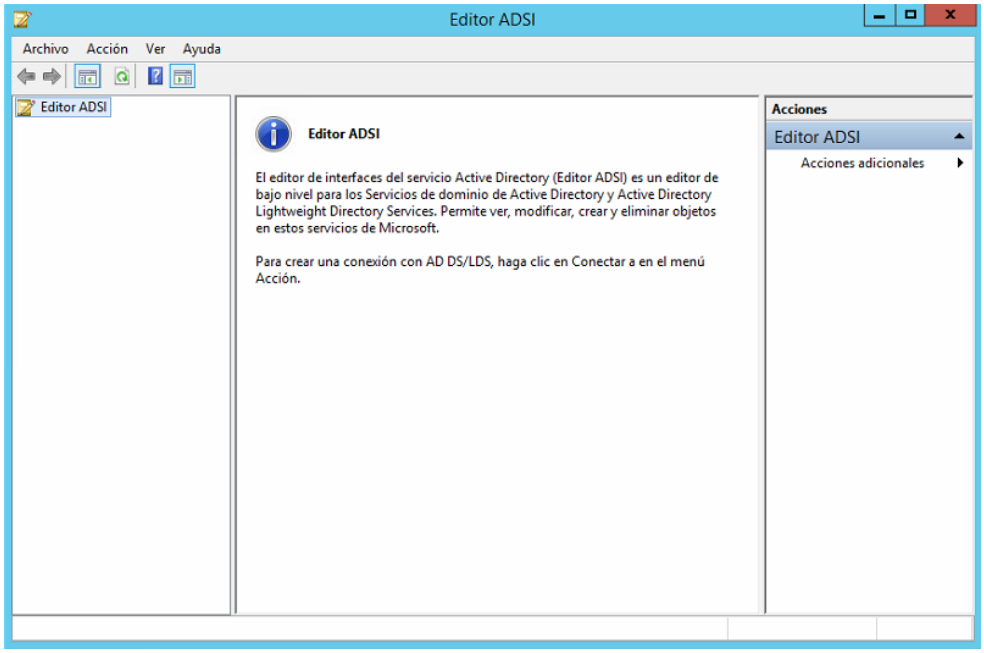
Además de estos parámetros, se han incluido dos nuevos atributos:

- **Vínculo PSO:** permite vincular un objeto PSO a un usuario o a un grupo.
- **Prioridad:** número entero que define la prioridad del objeto en caso de aplicar varios PSO a un mismo objeto.

La directiva de contraseña muy específica se puede configurar de varias maneras utilizando el editor de interfaces del servicio AD (en adelante Editor ADSI) o mediante interfaz gráfica utilizando la ventana del “Centro de administración de AD” como se observará en los dos siguientes apartados. Para la primera forma a los usuarios que se verán afectados serán la de las OU “Administración”, “Facturación” y “Logística” y al usuario de pruebas. La segunda forma afectara a los administradores del sistema en este coso la OU “Sistemas y TI”.

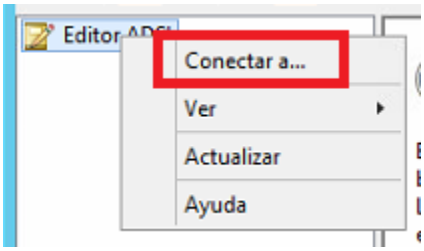
4.6.1.1. Utilizando la modificación ADSI

El Editor ADSI es un editor de LDAP que se puede usar para administrar objetos y atributos de AD DS. También ofrece una vista de cada objeto y atributo de un bosque de AD. Se puede usar este editor para administrar directivas de bloqueo de cuentas y contraseñas específicas. Con el editor ADSI se configurará la directiva de contraseña muy específica de los grupos Administración, Facturación y Logística y al usuario de pruebas. Se abrirá un editor accediendo a "Herramientas administrativas/Editor ADSI".



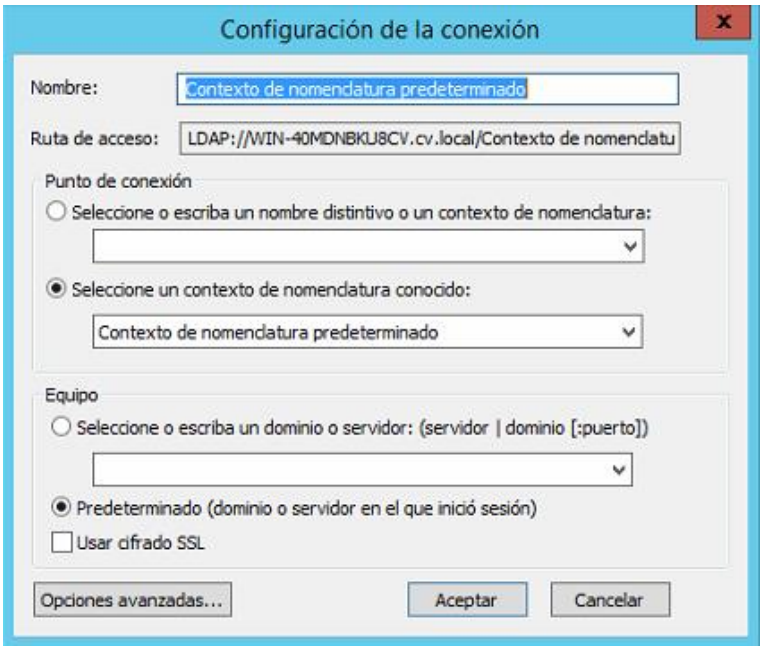
Captura 139 Editor ADSI

En la ventana del editor se clicará con el botón derecho sobre "Editor ADSI" y en sus opciones se clicará en "Conectar a…".



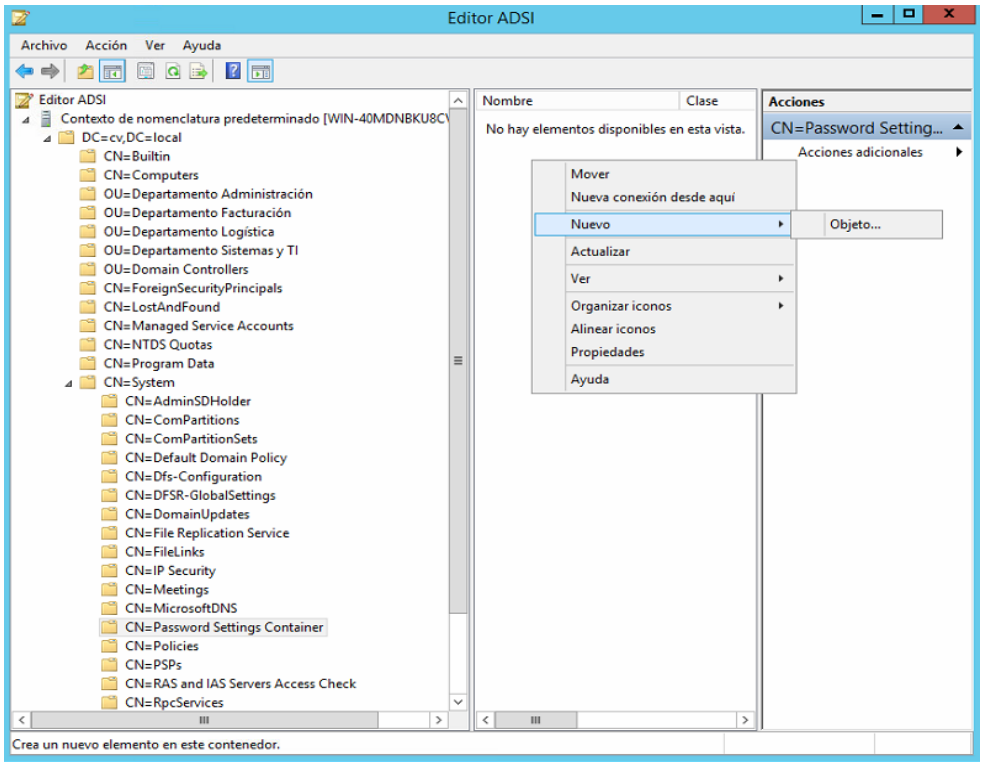
Captura 140 Conectar a sistema

En la ventana de "Configuración de la conexión" se le asignará un nombre a la conexión y se aceptará.



Captura 141 Configuración de la conexión

En la nueva conexión se accederá a "Conexión de nomenclatura predeterminado/DC=cv,DC=*local*/CN=*System*/CN=*Password Settings Container*", allí en la lista de la derecha se clicará en "Acciones adiciones/Nuevo/Objeto" (u otro opción es haciendo clic con el botón derecho sobre "CN=*Password Settings Container*").

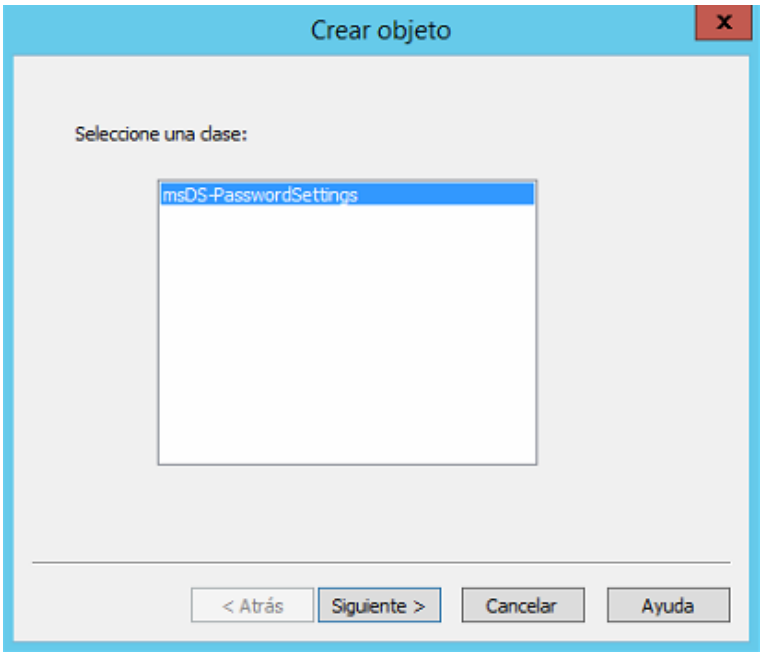


Captura 142 Nuevo objeto en CN=Password Setting Container

Con ello se ejecutará el asistente para un nuevo objeto PSO, dicho objeto se configurará con las siguientes características:

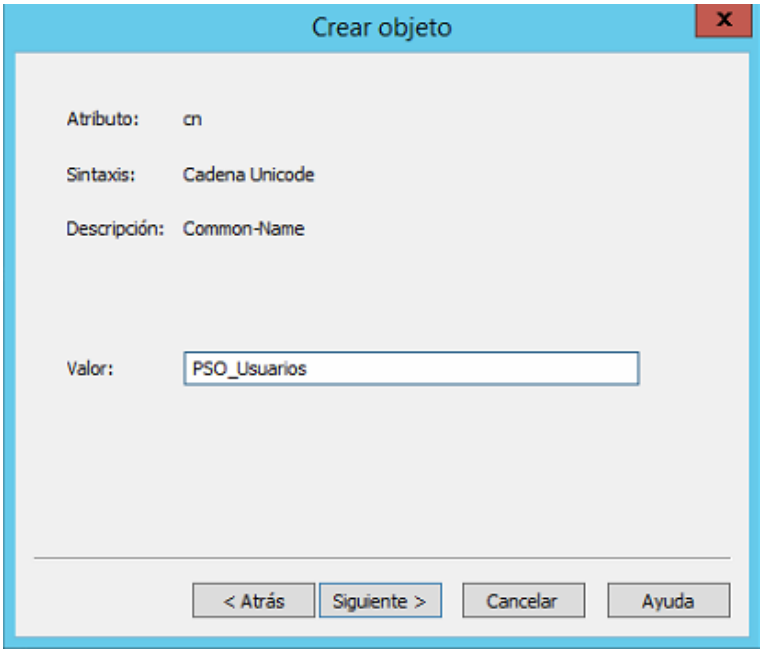
- **Preferencia sobre otros PSO:** 1.
- **Almacenar contraseñas usando cifrado reversible:** Deshabilitada.
- **Exigir historial de contraseñas:** 4 contraseñas.
- **La contraseña debe cumplir los requisitos de complejidad:** Habilitada.
- **Longitud mínima de la contraseña:** 6 caracteres.
- **Vigencia mínima de la contraseña:** 1 día.
- **Vigencia máxima de la contraseña:** 30 días.
- **Umbral de bloqueo de cuenta:** 3 intentos.
- **Restablecer recuentos de bloqueo de cuenta tras:** 30 minutos.
- **Duración del bloqueo de cuenta:** 30 minutos.

Posteriormente, se procederá con el asistente en el que en su primera ventana solo aparecerá una clase para el objeto por consiguiente se clicará en "Siguiente".



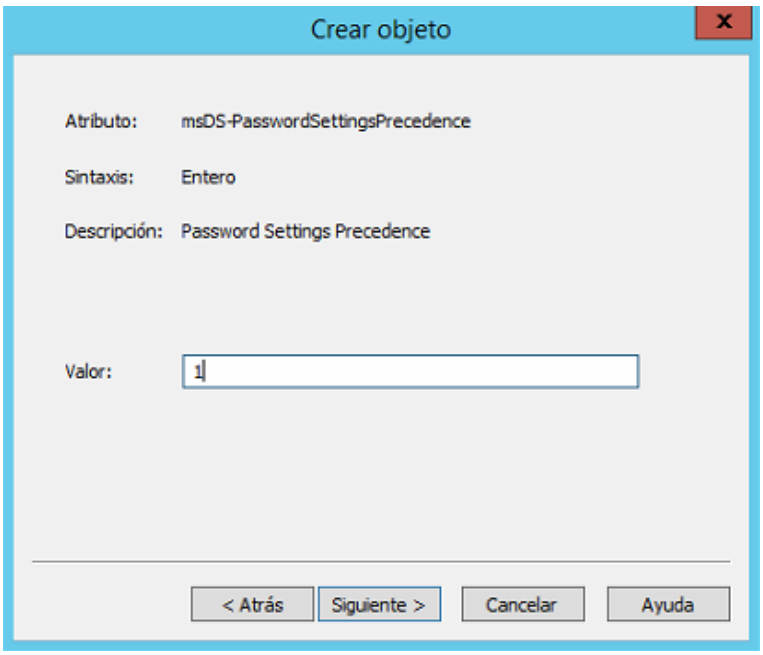
Captura 143 Clase del objeto

En la segunda ventana se le asignará un nombre al PSO y se clicará en “Siguiente”.



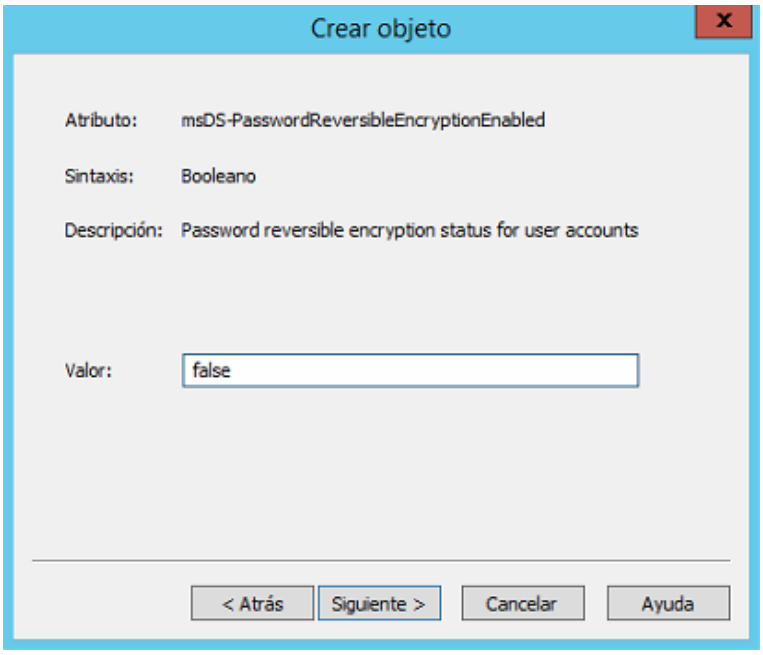
Captura 144 Nombre del objeto

En la tercera ventana se le asignará que prioridad deberá tener sobre otras PSO, como es una configuración de seguridad y debe tener mayor prioridad el valor que se le asignará será 1, cuanto mayor sea el valor menor prioridad tendrá el PSO.



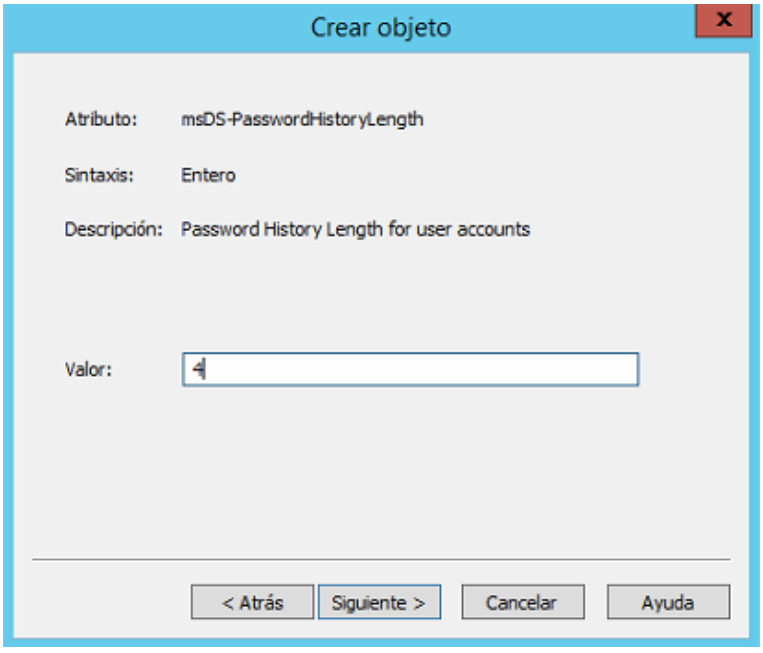
Captura 145 Preferencia del objeto

En la cuarta ventana se escribirá "*false*" para deshabilitar la encriptación reversible debido a que si se activa es como si se almacenarán las contraseñas en texto plano, con lo cual se crearía una deficiencia en la seguridad del sistema. Una vez escrito se clicará en "Siguiente".



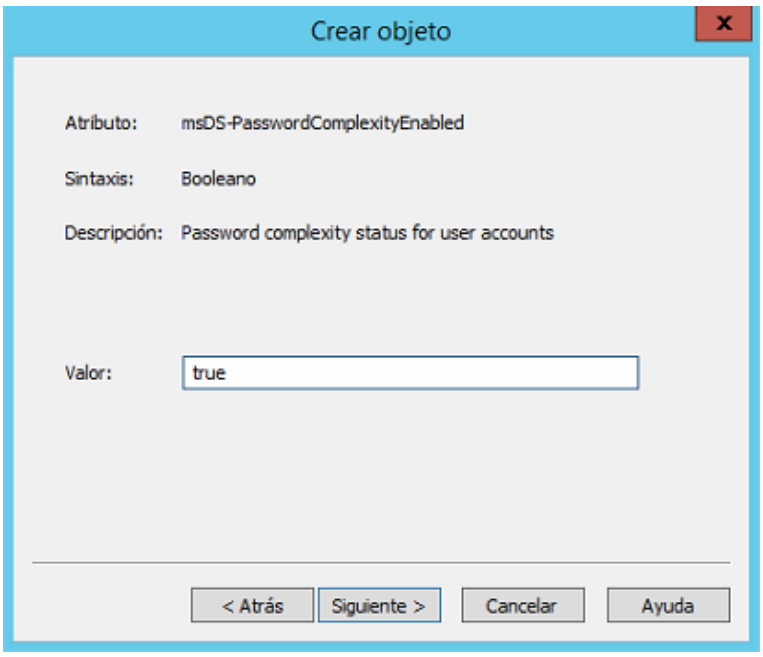
Captura 146 Encriptación reversible de contraseña del objeto

En la quinta ventana se tiene que especificar cuantas contraseñas se guardarán en el historial del sistema. Se le asignará el valor 4 y se clicará en "Siguiente".



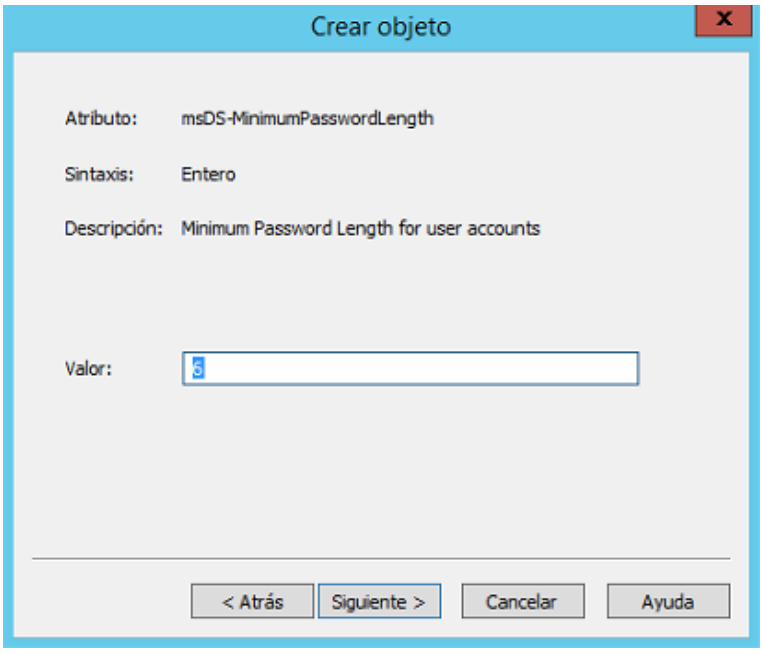
Captura 147 Historial de almacenamiento de contraseñas del objeto

En la sexta ventana se escribirá "*true*" para habilitar la complejidad de las contraseñas de los usuarios, estas contraseñas estarán formadas por mayúsculas, minúsculas, números y caracteres no alfanuméricos, y se clicará en "Siguiente".



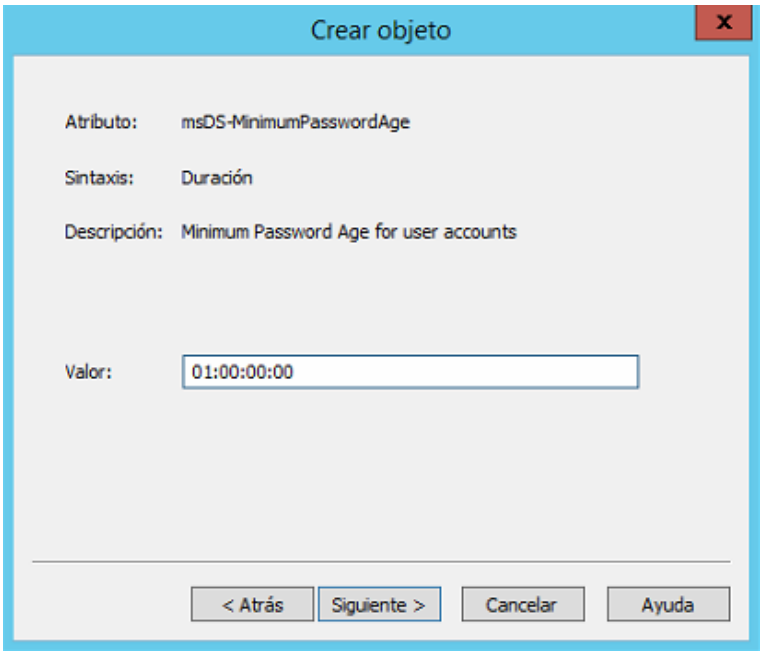
Captura 148 Complejidad de contraseña del objeto

En la séptima ventana se asignará el tamaño mínimo de las contraseñas, se le asignará el valor 6 y se clicará en "Siguiente".



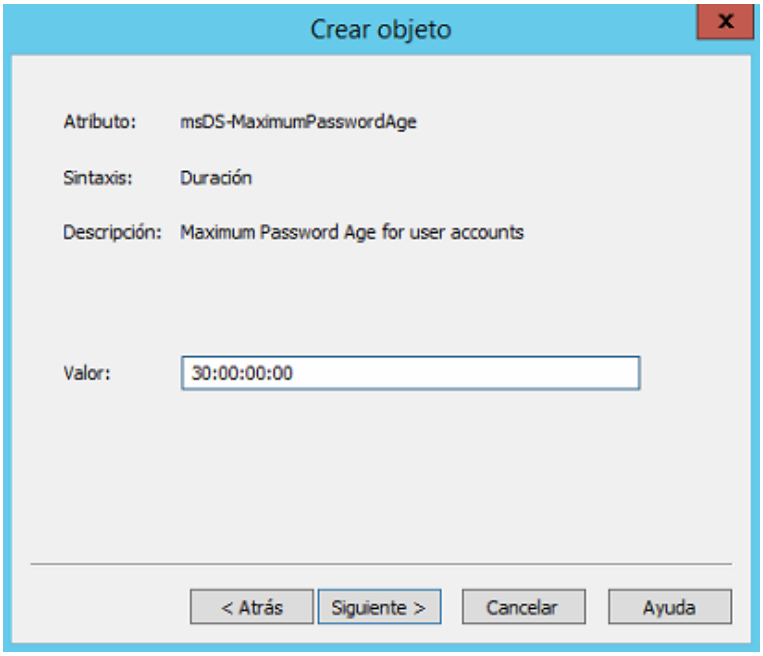
Captura 149 Longitud mínima de contraseña del objeto

En la octava ventana se le asignará el tiempo de vida mínimo que tendrán las contraseñas, esta duración será de un día escrito de la siguiente manera 01:00:00:00 (Formato DIAS:HORAS:MINUTOS:SEGUNDOS) y se clicará en "Siguiente".



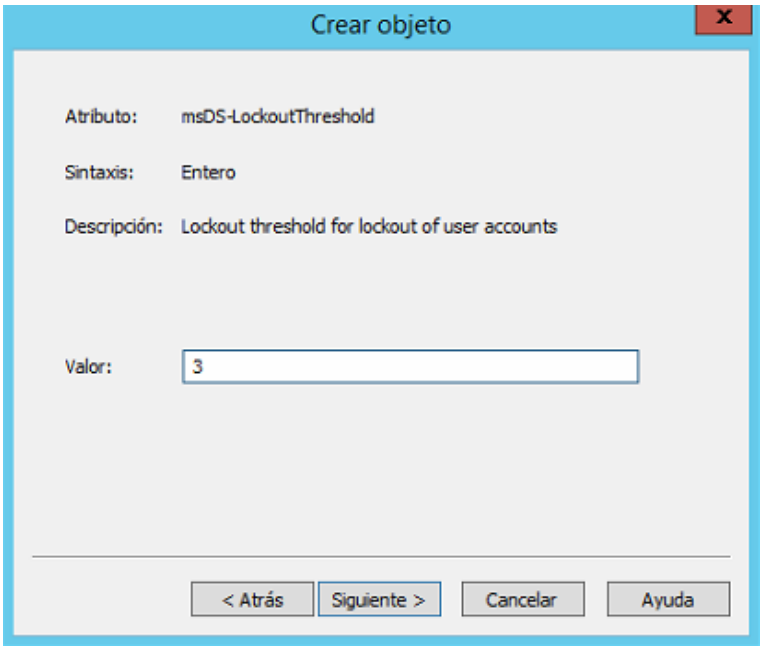
Captura 150 Tiempo de vida mínima de contraseña de objeto

En la novena ventana se le asignará el tiempo de vida máximo que tendrán las contraseñas, esta duración será de 30 días (30:00:00:00) y se clicará en "Siguiente".



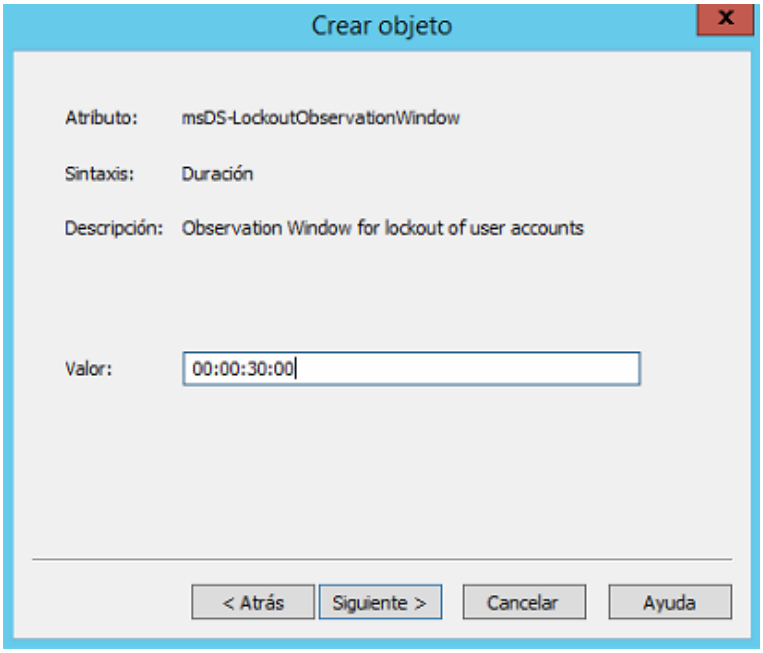
Captura 151 Tiempo de vida máxima de contraseña de objeto

En la décima ventana se asignará los intentos de inicio de sesión antes de que se bloquee la cuenta, se podrá el valor 3 y se clicará en “Siguiente”.



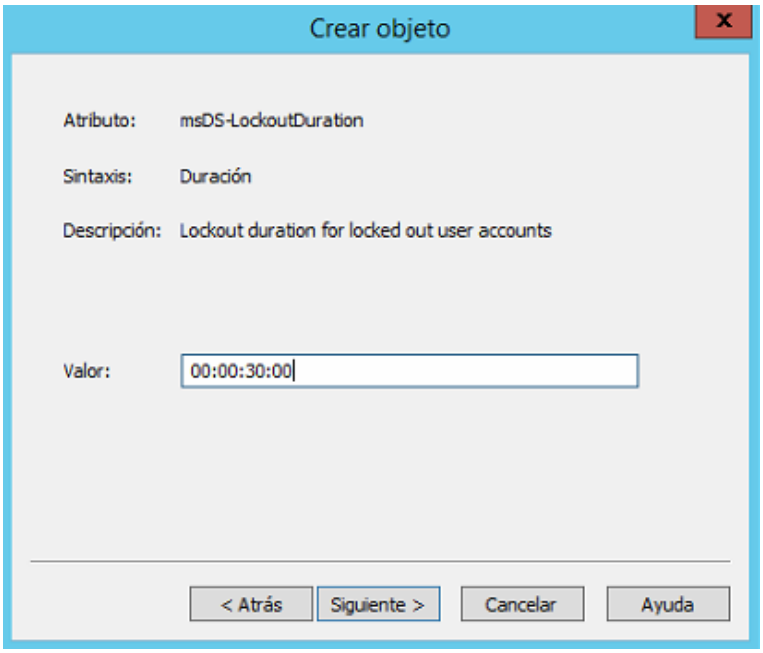
Captura 152 Nº de intentos de sesión del objeto

En la undécima ventana se especificará cada cuanto tiempo se reiniciará el contador de intentos, se pondrá que se reinicie cada 30 minutos (00:00:30:00) y se clicará en “Siguiente”.



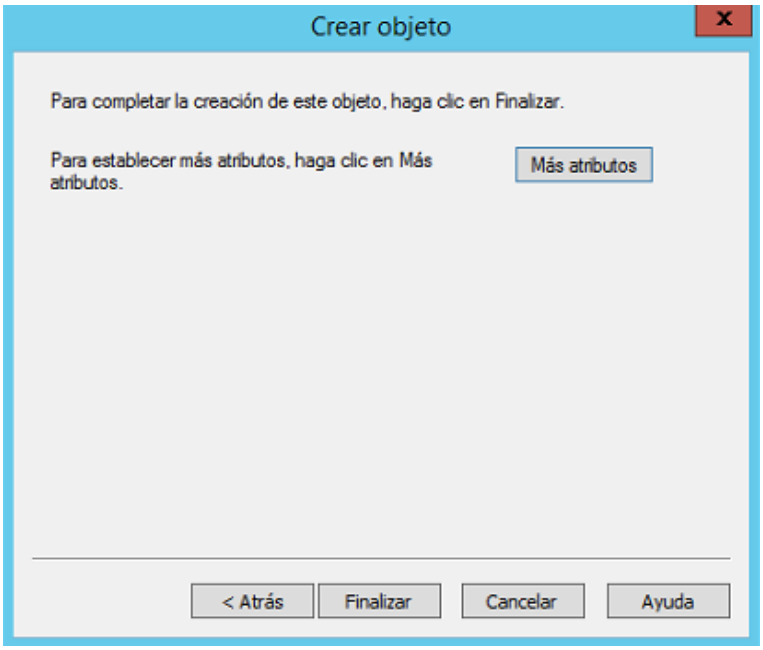
Captura 153 Tiempo de reinicio de contador de inicios de sesión del objeto

En la duodécima ventana se especificará cada cuanto tiempo estará bloqueada la cuenta. Se pondrá que este bloqueada 30 minutos (00:00:30:00), después de ese tiempo se desbloqueará, y se clicará en "Siguiente".



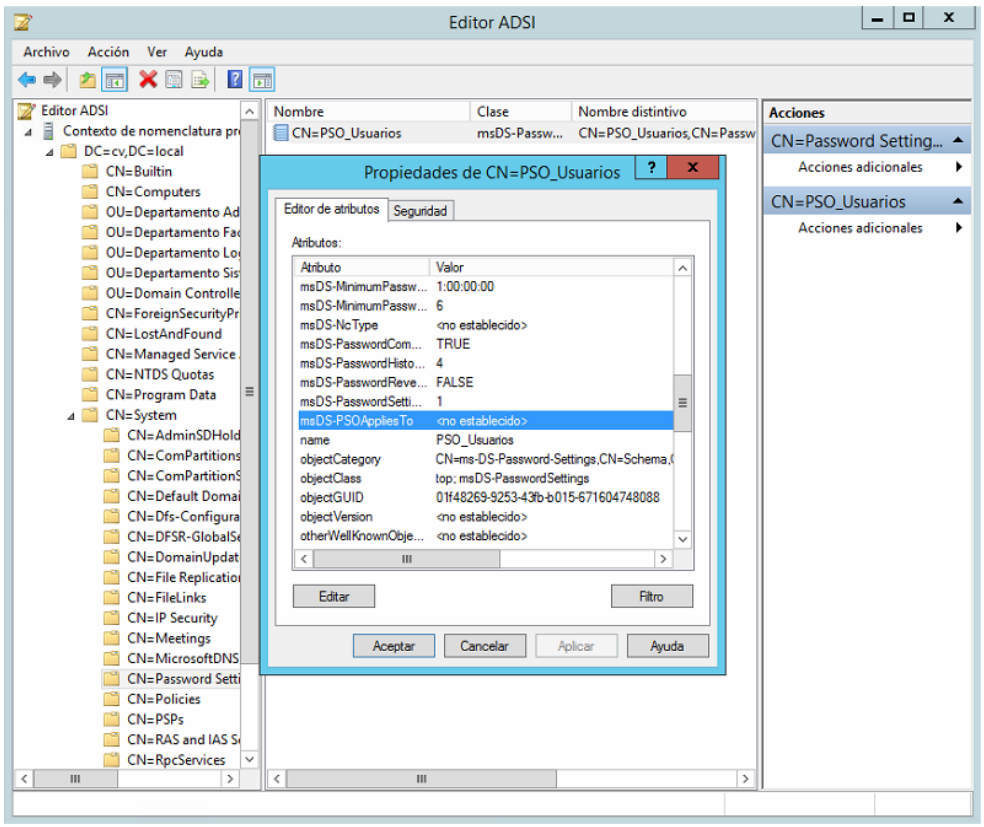
Captura 154 Tiempo de bloqueo de cuenta del objeto

En la última ventana del asistente se clicarán en "Finalizar", debido a que no se configurarán más atributos, para crear el PSO.



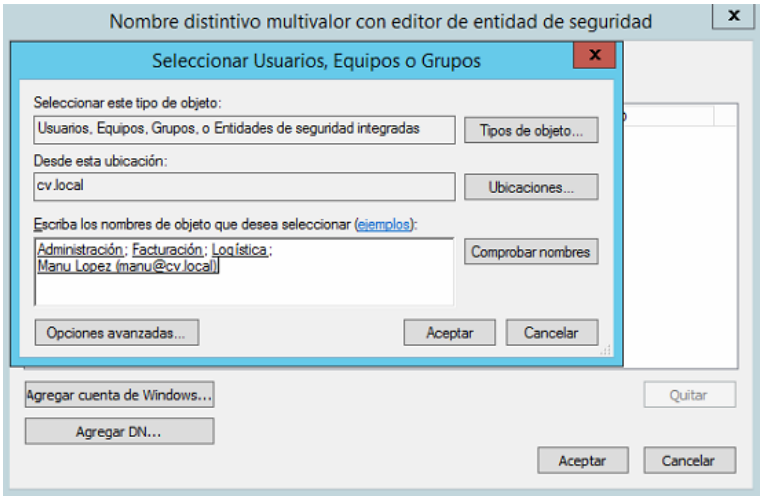
Captura 155 Finalizar la creación del objeto

Después, se procederá con la agregación de usuarios y grupos a los que afectará, para ello se hará doble clic sobre el PSO, en la ventana de propiedades que se nos abre se seleccionará de la lista "msDS-PSO *Applies to*" y se clicará en "Editar".



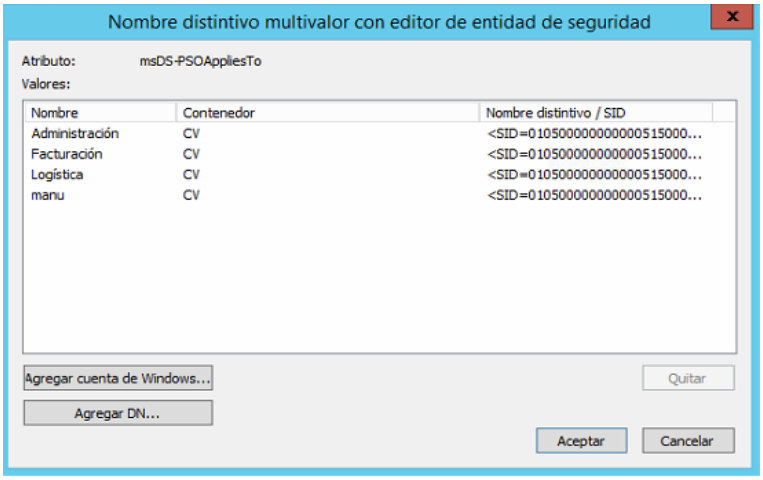
Captura 156 Propiedades del objeto PSO creado

En la ventana del servicio se clicará en "Agregar cuenta de Windows…", posteriormente se escribirán los grupos y el usuario de pruebas, se comprobarán los nombre y se clicará en "Aceptar".



Captura 157 Añadir usuarios y grupos al objeto

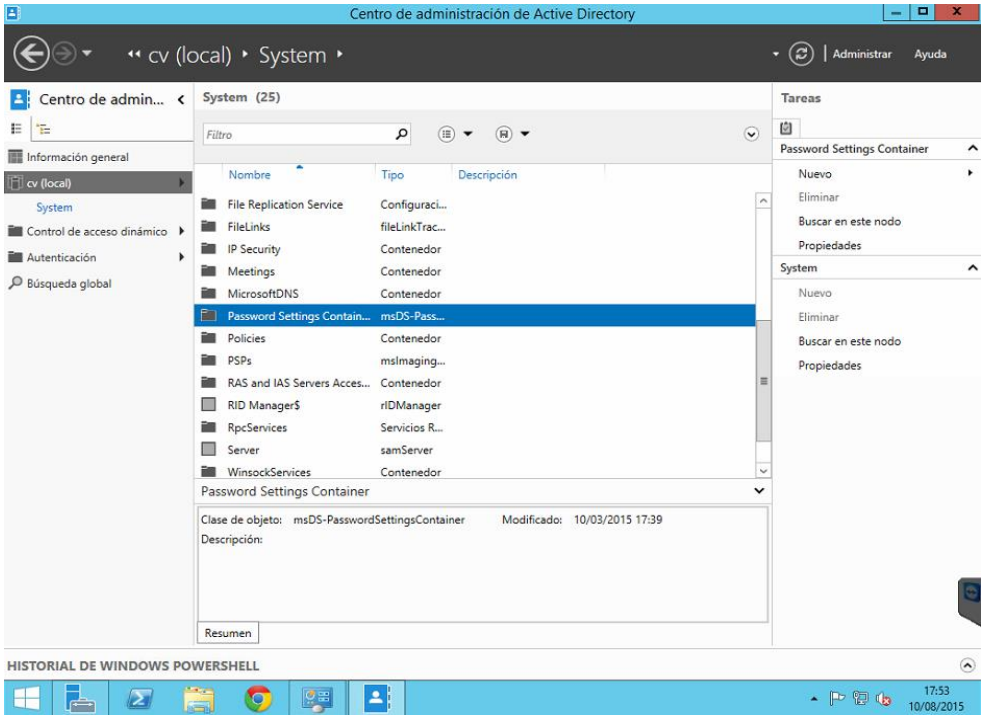
Se observará en la lista de la ventana aparecen los grupos y el usuario de pruebas. Se clicará en "Aceptar" para que comience a afectar a dichos usuarios la PSO creada.



Captura 158 Lista de usuarios y grupos añadidos al objeto

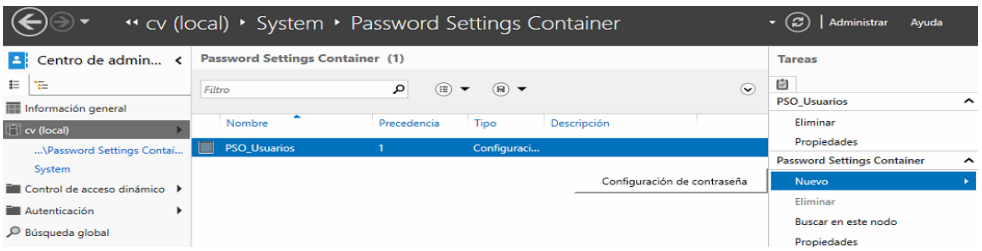
4.6.1.2. Utilizando la interfaz gráfica

En WS 2012 se ha mejorado la administración y la creación de directivas de contraseña muy específica, incorporado una interfaz de usuario que ayuda a ver las distintas directivas de manera sencilla. Con interfaz gráfica se configurará la directiva de contraseña muy específica de los usuarios Fede y Manuel que pertenecen a la OU "Sistemas y TI" que son los administradores del sistema. Para abrir la interfaz se accederá a "Herramientas administrativas/Centro de administración de *Active Directory"*, en la ventana del centro de administración se accederá al contenedor "cv (local)/*System*/*Password Settings Container*".



Captura 159 Password Settings Container desde el centro de administación de AD

Se observará que aparece en ese contenedor el PSO creado anteriormente con el editor ADSI. Para crear otro contener gráficamente en la lista de la derecha se clicará en "Nuevo/Configuración de contraseña".

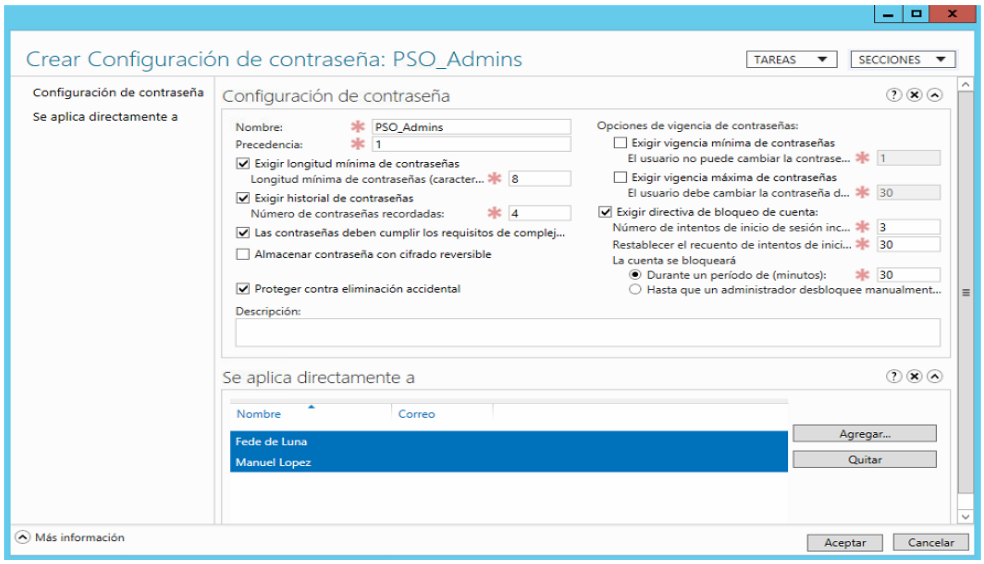


Captura 160 Nuevo objeto PSO desde el centro

En la ventana de creación del PSO, como se observa todo se configura en la misma ventana. Al objeto se le pondrá otro nombre, los parámetros serán los mismos que en el apartado anterior a excepción que la longitud mínima de contraseña será de 8 y no tendrá vigencia mínima ni máxima. A este PSO se le añadirán los dos usuarios mencionados en el inicio del apartado. Dicha configuración del objeto será la siguiente:

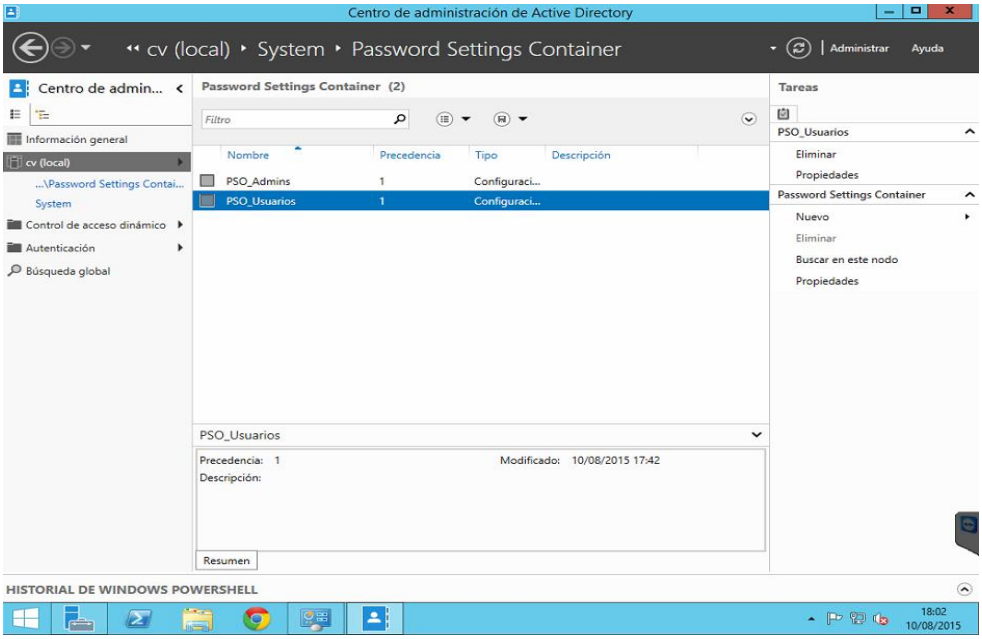
- **Preferencia sobre otros PSO:** 1.
- **Almacenar contraseñas usando cifrado reversible:** Deshabilitada.
- **Exigir historial de contraseñas:** 4 contraseñas.
- **La contraseña debe cumplir los requisitos de complejidad:** Habilitada.
- **Longitud mínima de la contraseña:** 8 caracteres.
- **Vigencia mínima de la contraseña:** Deshabilitada.
- **Vigencia máxima de la contraseña:** Deshabilitada.
- **Umbral de bloqueo de cuenta:** 3 intentos.
- **Restablecer recuentos de bloqueo de cuenta tras:** 30 minutos.
- **Duración del bloqueo de cuenta:** 30 minutos.

Una vez configurado el objeto como muestra en la captura 162 se clicará "Aceptar" para crear el PSO.



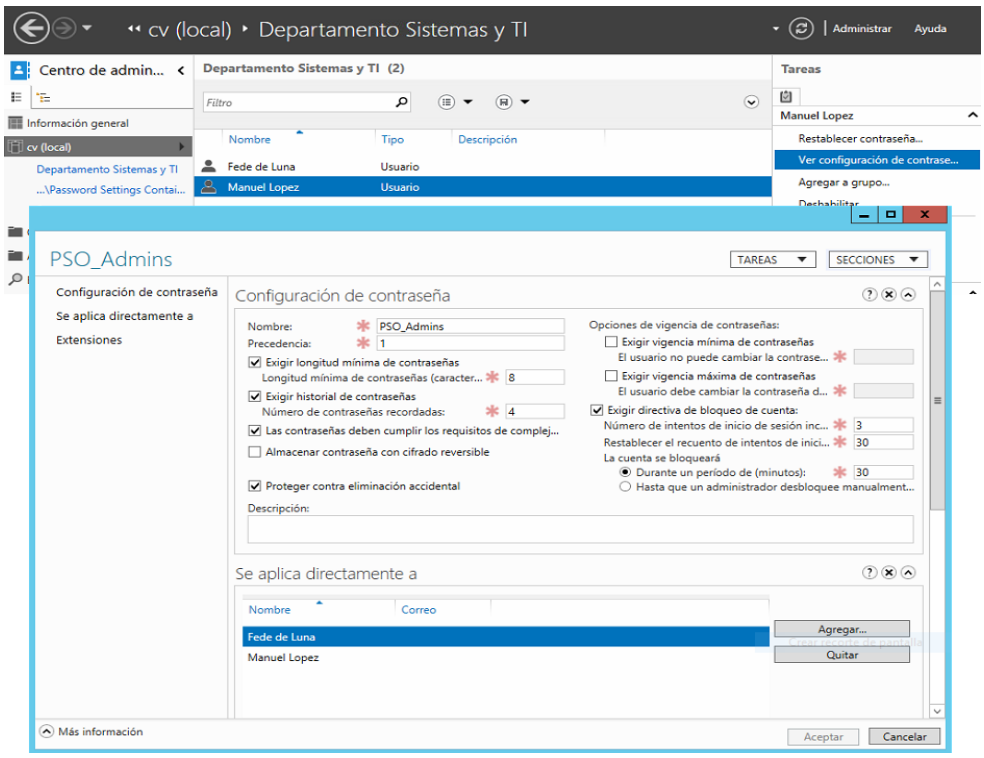
Captura 161 Configuración del objeto PSO

A continuación, en el contendor "*Password Settings Container*" aparecerán los dos PSO creados con los dos sistemas.



Captura 162 Objetos PSO creados

Se puede comprobar cómo afecta a los usuarios, como por ejemplo se podría para ver cómo afecta al usuario Manuel. Para ello se accederá a "cv (local)/Departamento Sistemas y TI", se seleccionará al usuario y en la lista de la derecha se clicará en "Ver configuración de contraseña". La ventana que se abrirá corresponderá al PSO del cual es afectado.



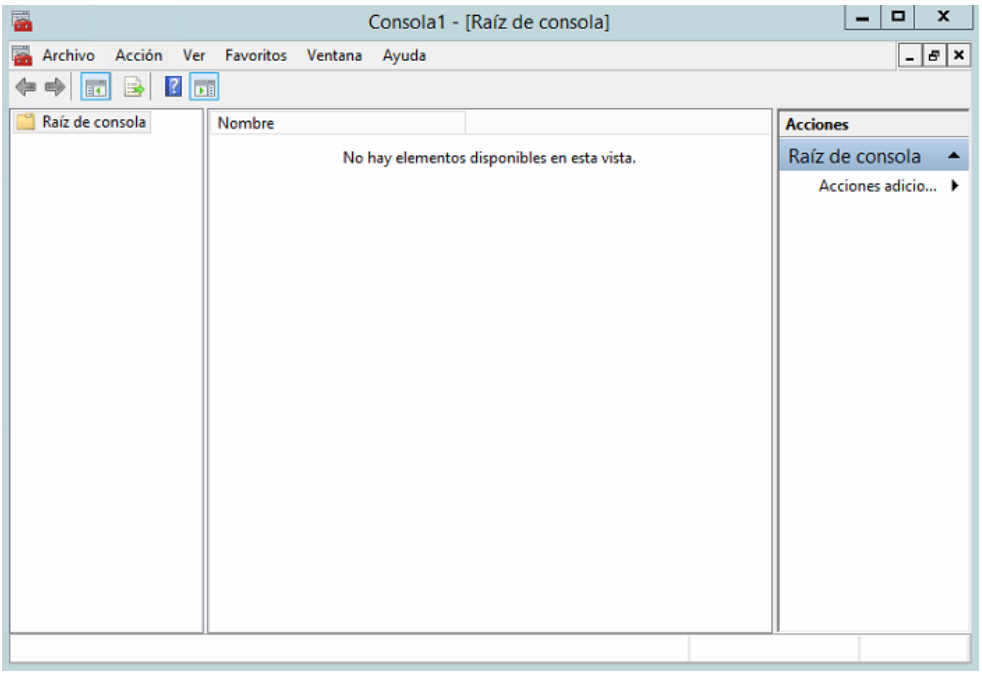
Captura 163 PSO del usuario Manuel López

4.6.2. Implementación de directivas de seguridad

En este apartado se procederá con la configuración y análisis de la seguridad de WS 2012 utilizando el caso de estudio propuesto para este TFG, en este proceso también se mostrará cómo restaurar la configuración de seguridad inicial del sistema.

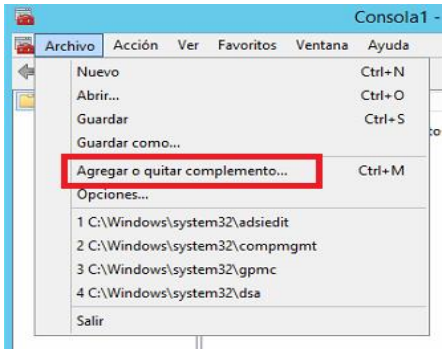
4.6.2.1. Trabajo con plantilla de seguridad

Primero se procederá con la creación de una plantilla de seguridad. Una plantilla de seguridad es un archivo con formato .inf que puede importarse en una directiva de grupo. Esta permite homogeneizar la política de seguridad en toda la organización imponiendo el modelo propuesto. En dicha plantilla se configurarán aspectos como los realizados en el apartado 4.6.1, se cogerá la configuración del subapartado 4.6.1.1, entre otros como base de seguridad para el sistema. Para crear la plantilla se abrirá una consola MMC, para abrir la consola se escribirá "mmc" en buscador de sistema y en la lista que aparece se ejecutará la aplicación.



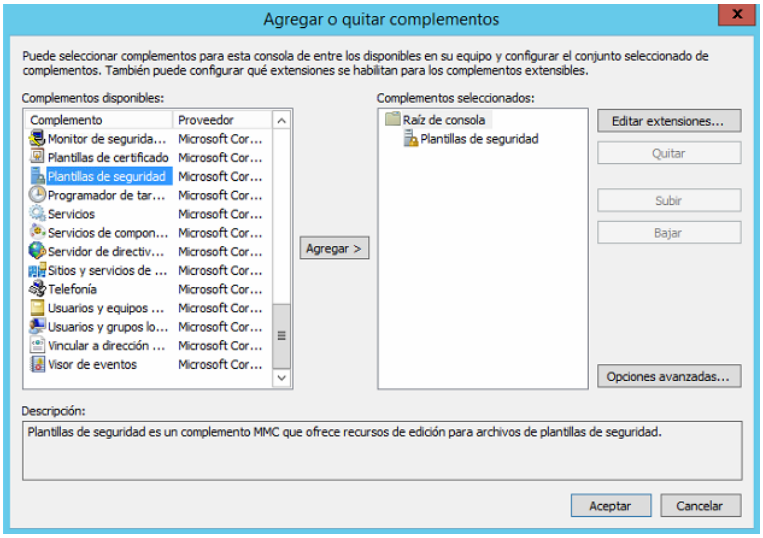
Captura 164 Consola MMC

Una vez abierta la consola para agregar la plantilla se irá a "Archivo/Agregar o quitar complementos…".



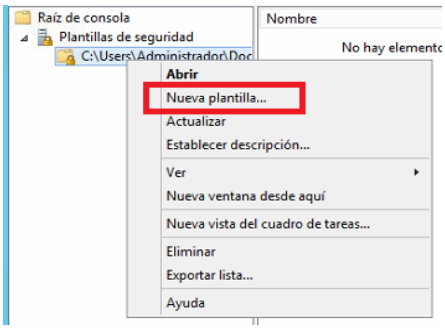
Captura 165 Agregar complemento a la consola

En la ventana "Agregar o quitar complementos" en la lista de "Complementos disponibles" se seleccionara "Plantillas de seguridad" y posteriormente se clicará en "Agregar". Una vez agregado el complemento se clicará en "Aceptar".



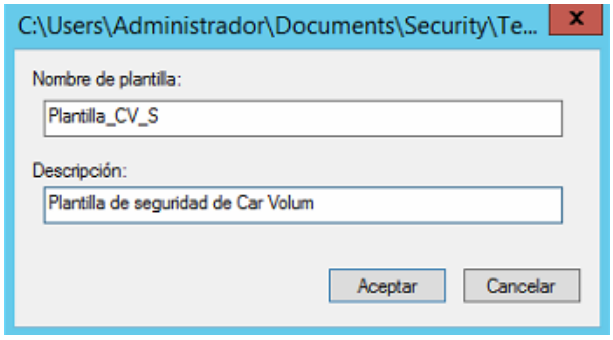
Captura 166 Complemento Plantillas de seguridad a agregar

Después, se desplegará de la lista de la izquierda las plantillas de seguridad y se clicará con el botón derecho sobre la carpeta "C/User/…". Entre las opciones se clicará en "Nueva plantilla…".



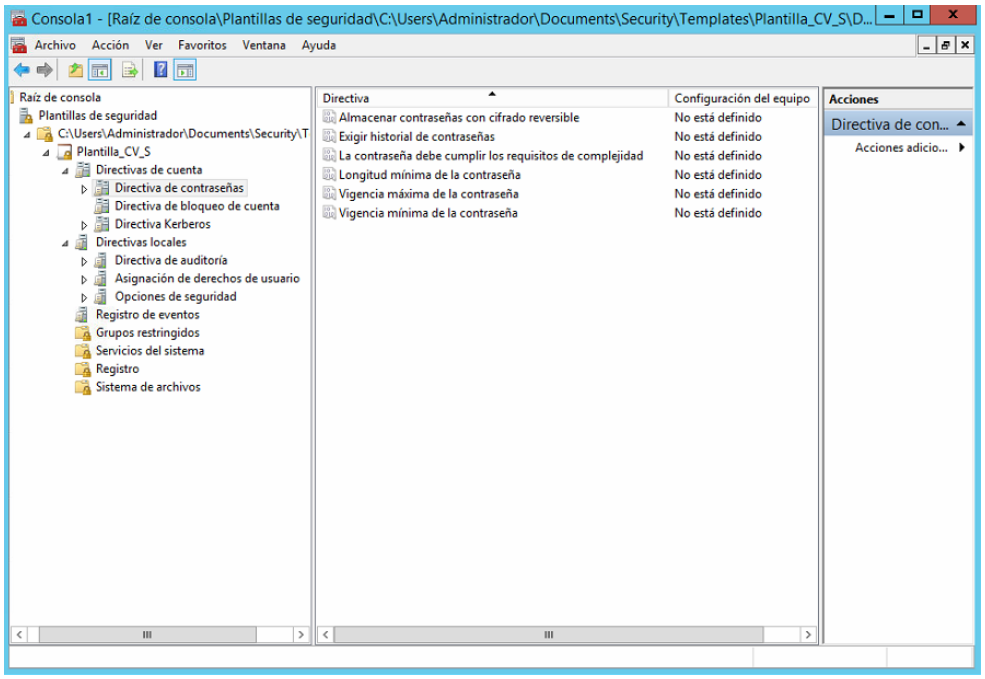
Captura 167 Nueva plantilla de seguridad

A la plantilla se le pondrá un nombre, una descripción y se aceptará para crearla.



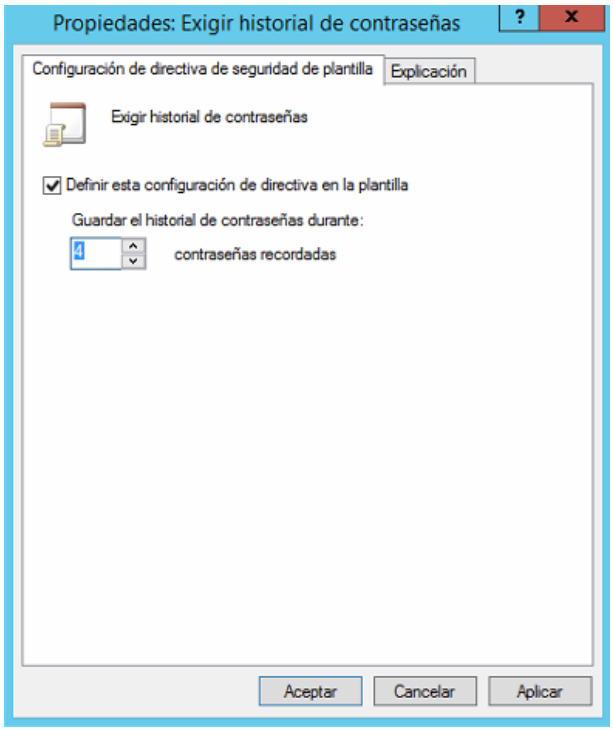
Captura 168 Nombre de la nueva plantilla

Una vez creada la plantilla, primero se configurarán las directivas de cuentas, se empezará configurando la directiva de contraseñas. Para configurar cada directiva bastará con hacer doble clic sobre ellas.



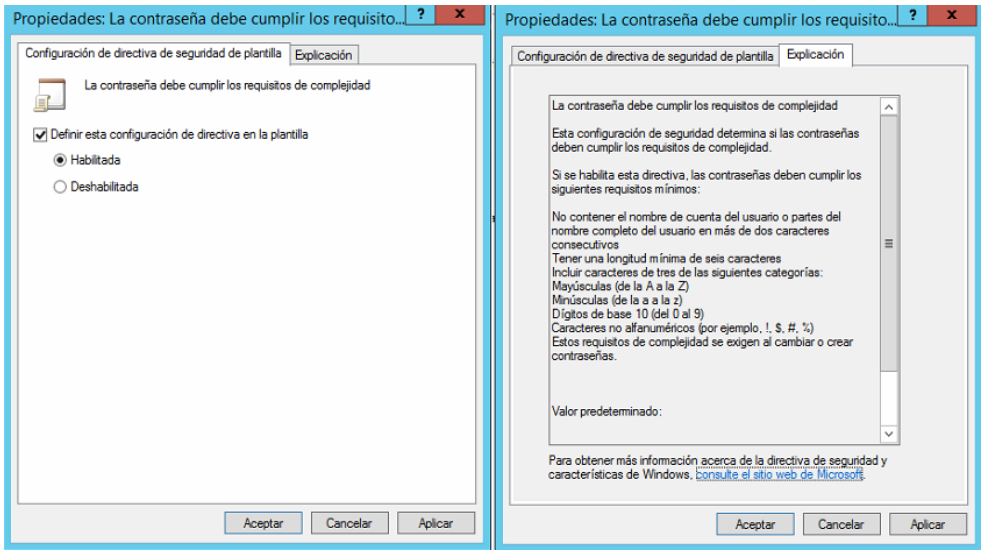
Captura 169 Configurar directivas de contraseña de la plantilla

La directiva “Almacenar contraseñas usando cifrado reversible” no se configurará, debido a que por defecto viene deshabilitada. La directiva “Exigir historial de contraseñas” se habilitará y se le asignará el valor 4, para que el sistema recuerde 4 contraseñas.



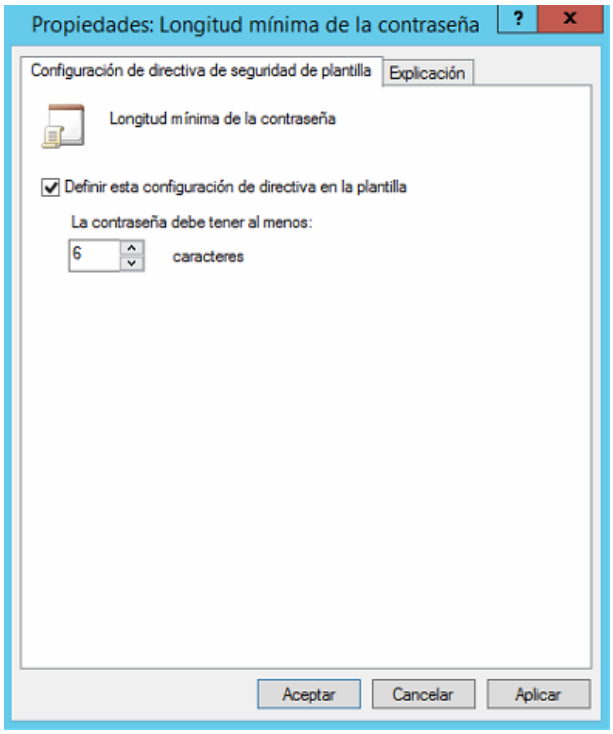
Captura 170 Directiva “Historial de contraseñas” de la plantilla

La directiva “La contraseña debe cumplir los requisitos de complejidad” se habilitará.



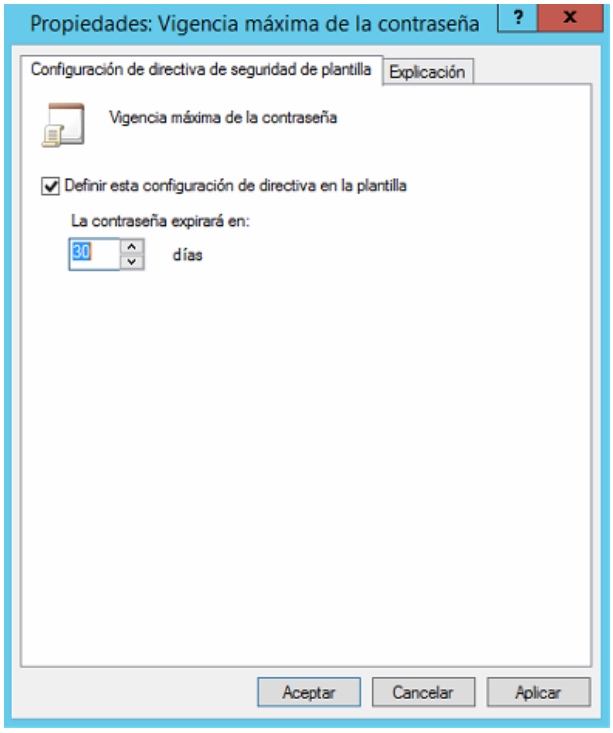
Captura 171 Directiva “Complejidad de contraseña” de la plantilla

La directiva "Longitud mínima de la contraseña" se habilitará y se le asignará 6 de longitud.



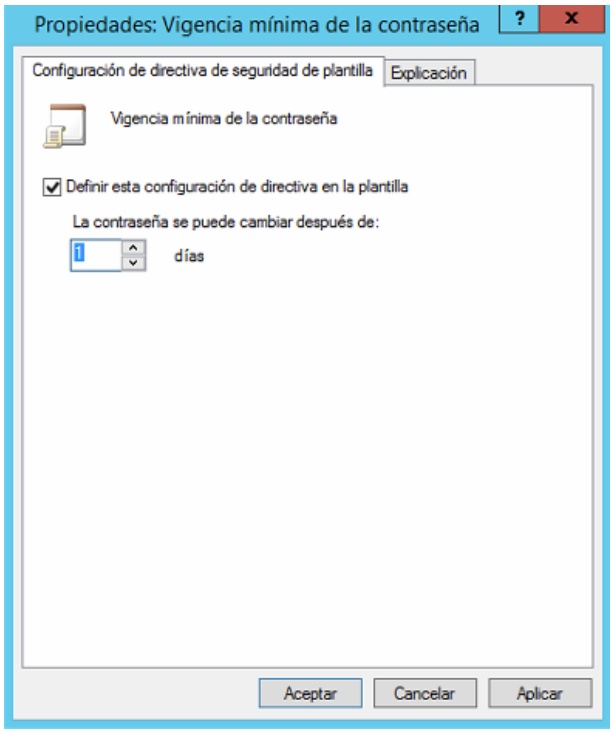
Captura 172 Directiva "Longitud mínima de contraseña" de la plantilla

La directiva "Vigencia máxima de la contraseñas" se habilitará y se le asignará 30 días.



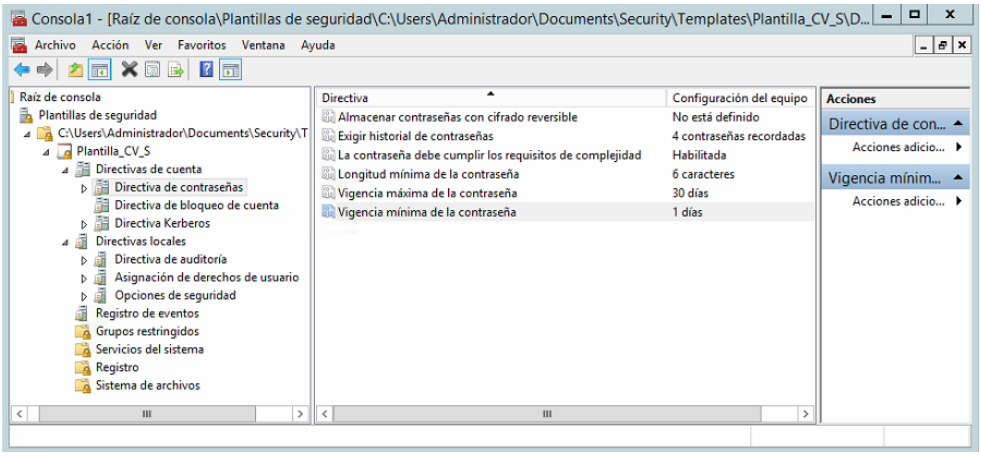
Captura 173 Directiva "Vigencia máxima de contraseña" de la plantilla

La directiva “Vigencia mínima de la contraseñas” se habilitará y se le asignará 1 día.



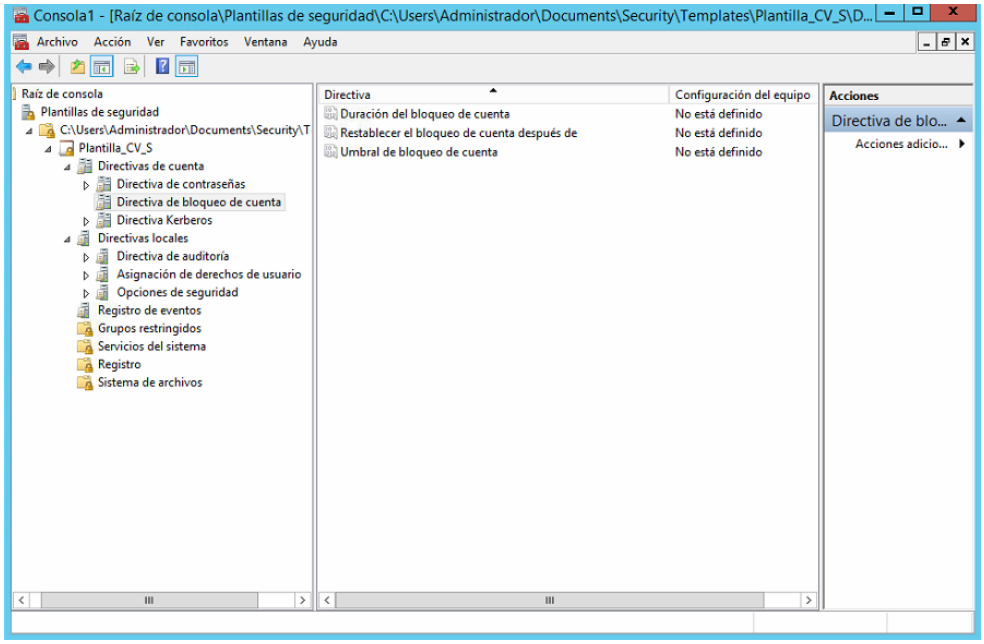
Captura 174 Directiva “Vigencia mínima de contraseña” de la plantilla

Se observará que las configuraciones realizadas en la directiva de contraseñas nos aparecen al lado de cada uno de sus directivas, eso ocurrirá en todas las directivas de la plantilla.



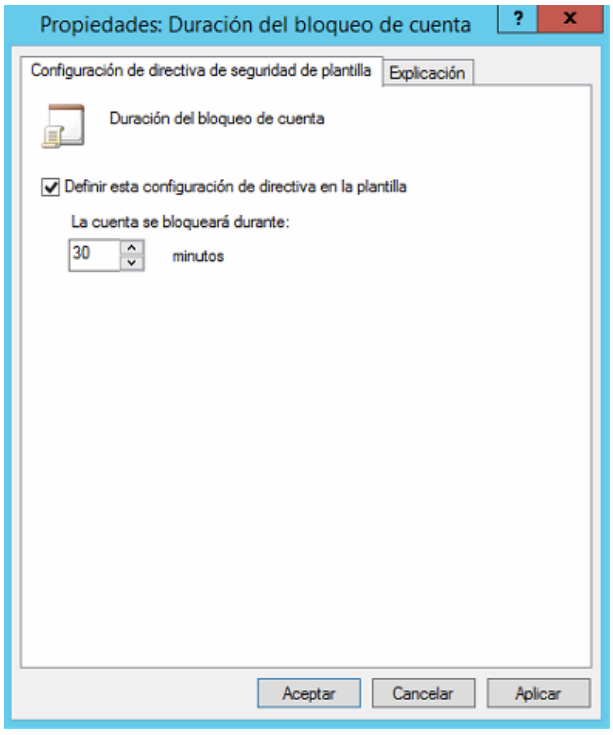
Captura 175 Directivas de contraseña configuradas de la plantilla

Se finalizará con las directivas de cuentas configurando la directiva de bloqueo de cuenta.



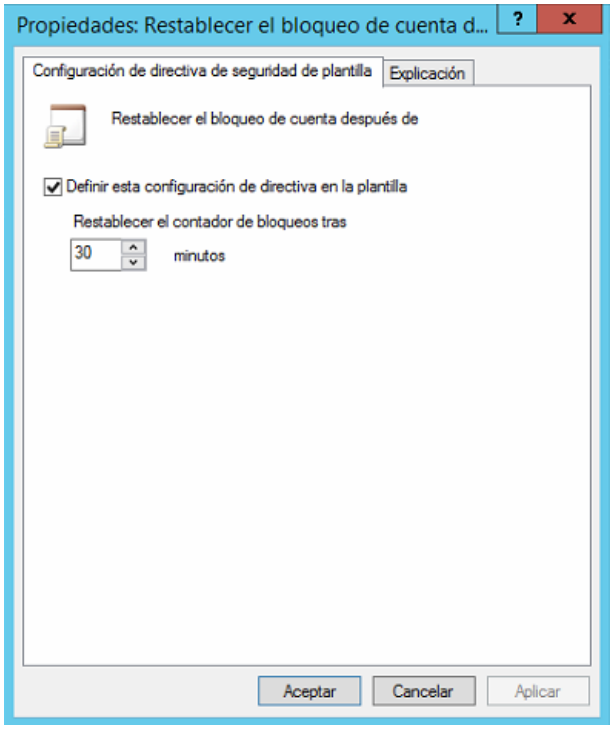
Captura 176 Configurar directivas de bloqueo de cuenta de la plantilla

La directiva "Duración de bloqueo de cuenta" se habilitará y se le asignará 30 minutos.



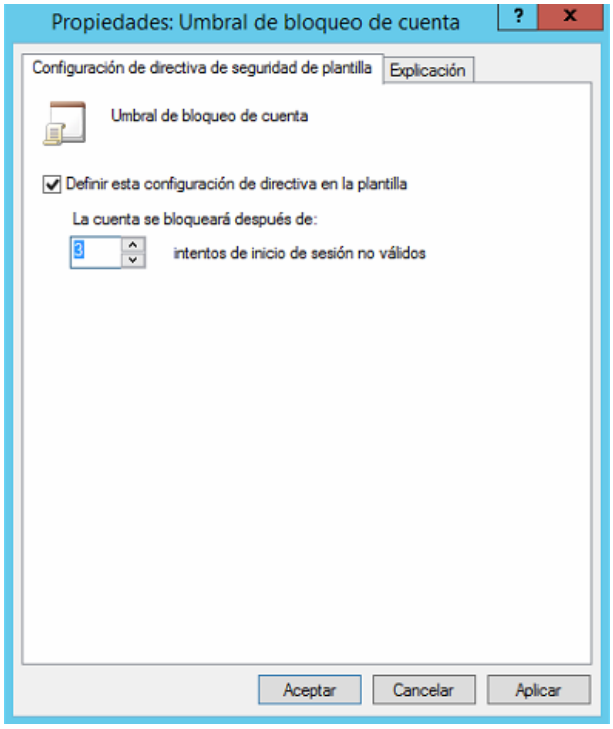
Captura 177 Directiva "Duración de bloqueo de cuenta" de la plantilla

La directiva “Restablecer el bloqueo de la cuenta después de” se habilitará y se le asignará 30 minutos.



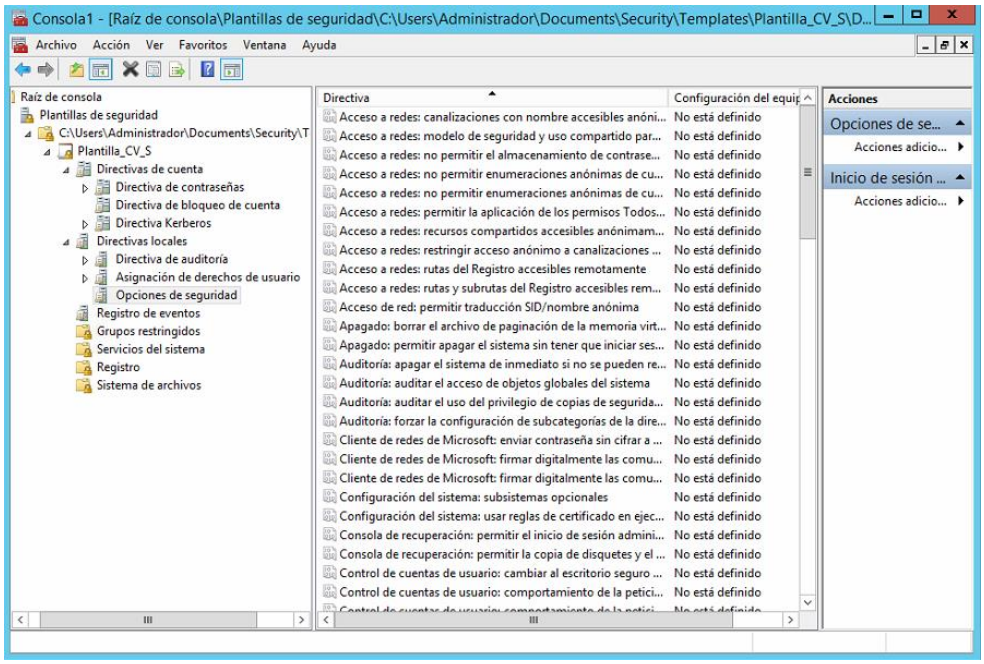
Captura 178 Directiva “Restablecer el bloqueo de cuenta” de la plantilla

La directiva “Umbral de bloqueo de cuenta” se habilitará y se le asignará 3 intentos.



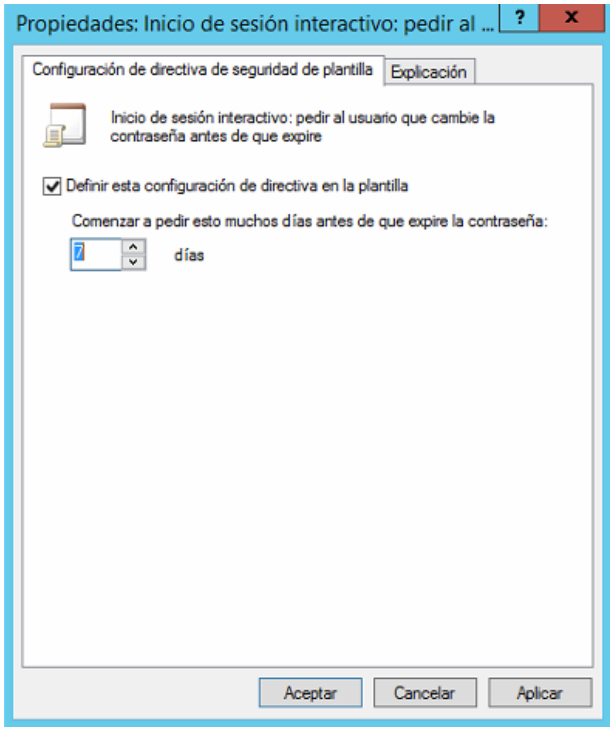
Captura 179 Directiva “Umbral de bloqueo de cuenta” de la plantilla

Segundo, se configurarán las directivas de las cuales se configurarán la opciones de seguridad, de esta directivas solo se habilitarán 3 las demás se dejarán por defecto.



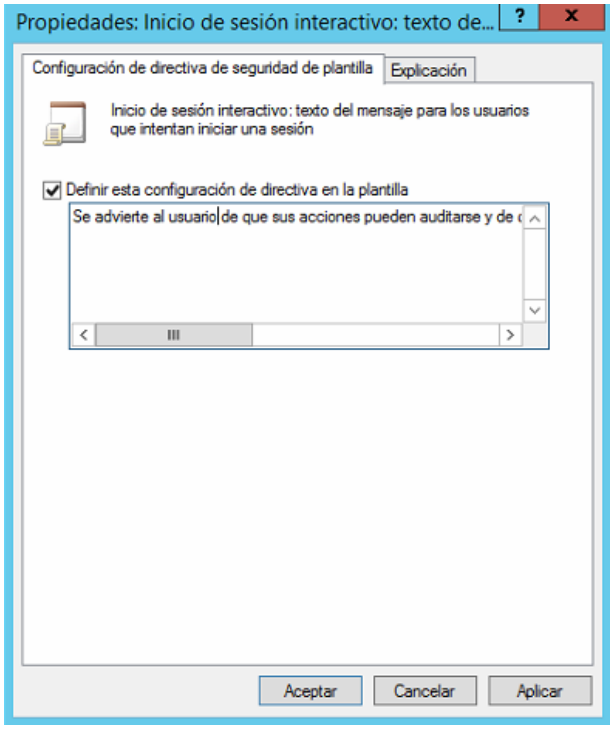
Captura 180 Configurar opciones de seguridad de la plantilla

La directiva “Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire” se habilitará y se le asignará 7 días.



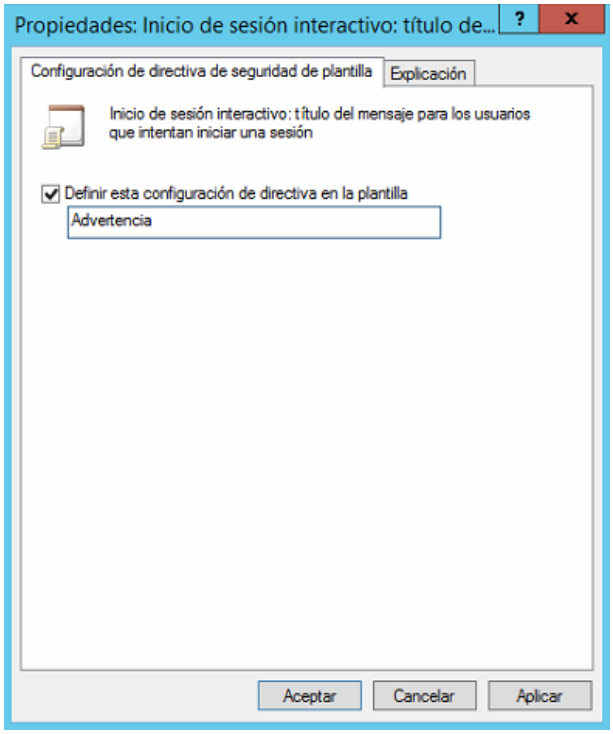
Captura 181 Directiva “Inicio de sesión advertencia para cambio de contraseña” de la plantilla

La directiva "Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión" se habilitará y se le asignará texto que mejor le convenga a la empresa.



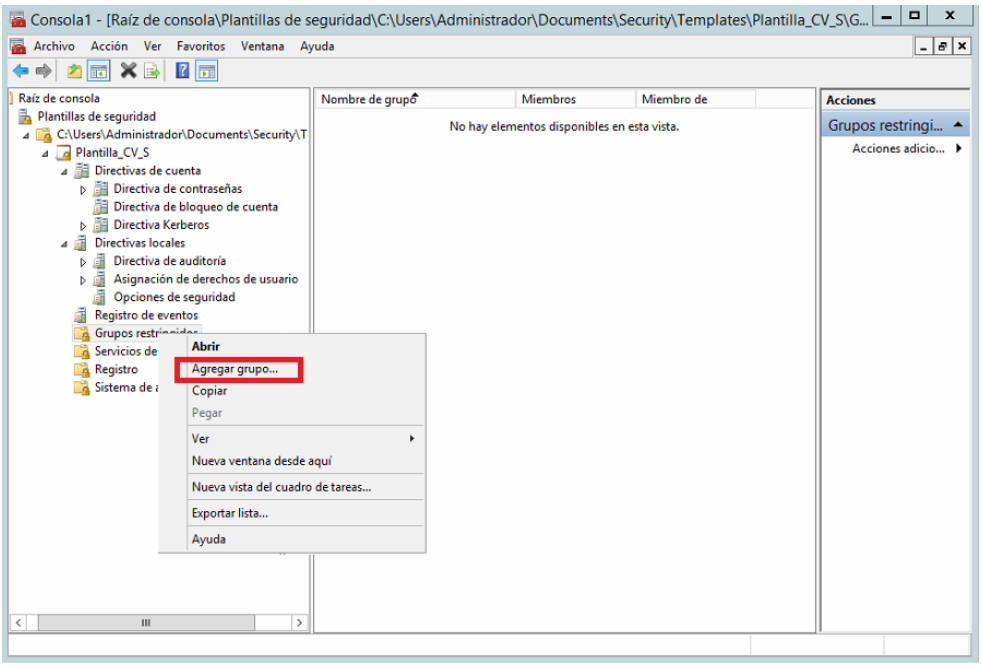
Captura 182 Directiva "Mensaje de inicio de sesión" de la plantilla

La directiva "Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión" se habilitará y se le asignará el correspondiente con el texto del mensaje.



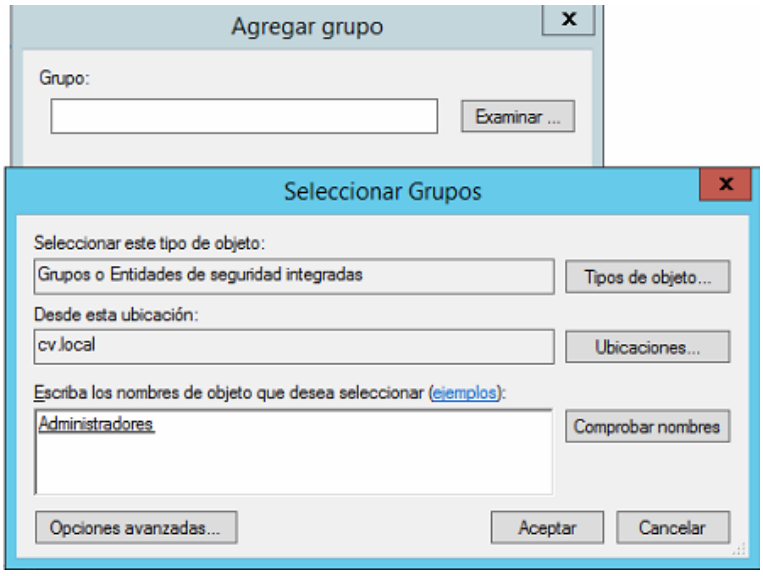
Captura 183 Directiva "Título del mensaje de inicio de sesión" de la plantilla

Una vez configuradas las directivas se configurarán los "Grupos restringidos" para añadir al grupo "Administradores" del sistema, a los usuarios Administrador, Fede y Manuel. Para agregar el grupo se clicará con el botón derecho sobre "Grupos restringidos" y se clicará en "Agregar grupo…".



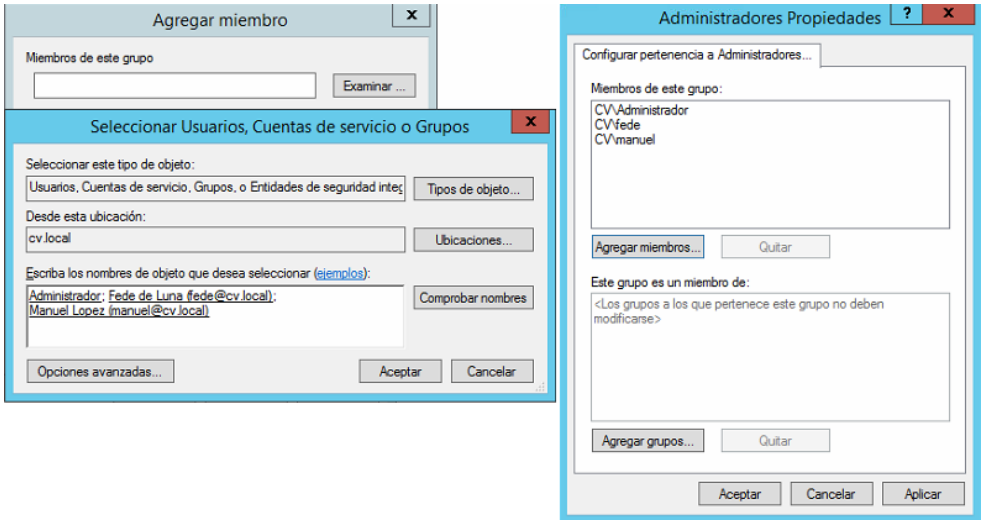
Captura 184 Agregar grupo restringido

En la ventana "Agregar grupo" se seleccionará al grupo "Administradores" y se aceptará.



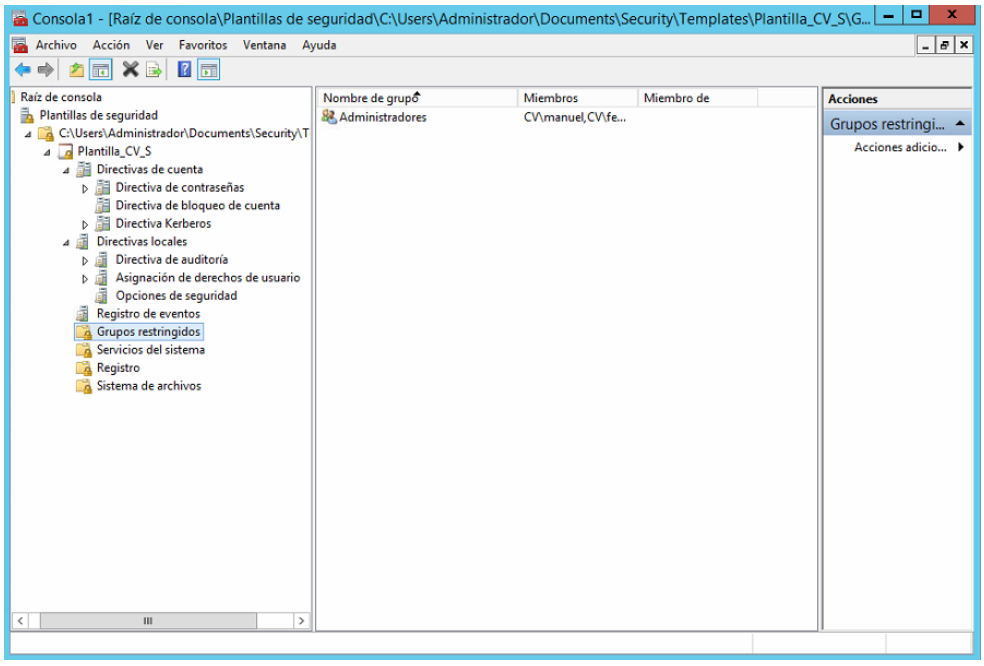
Captura 185 Agregar grupo

En las ventana de propiedades del grupo “Administradores” se añadirán los usuarios anteriormente mencionados para terminar de crear la plantilla, se aplicará y se aceptará.



Captura 186 Agregar usuarios al grupo

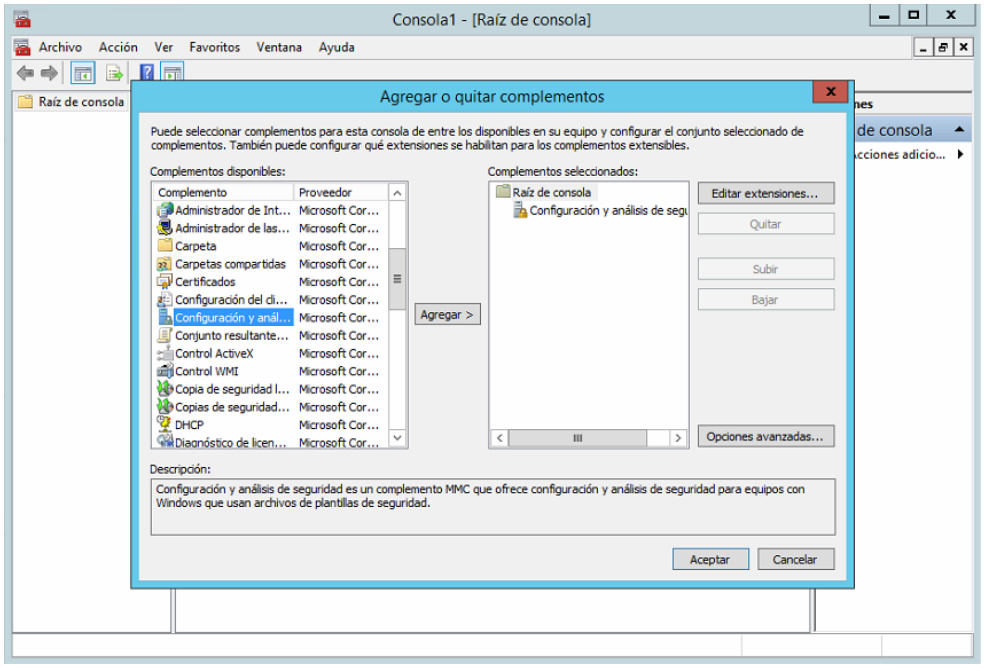
En la ventana se observará que se tiene el grupo “Administradores” añadido a la lista de los grupos restringidos.



Captura 187 Grupo añadido

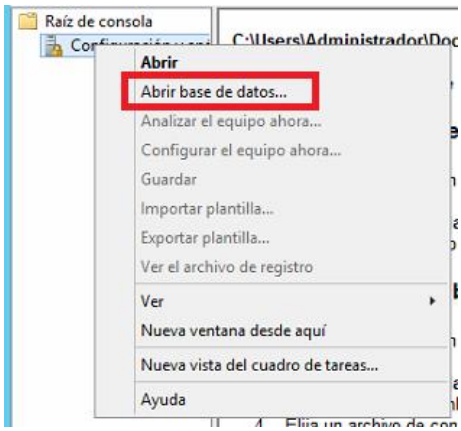
4.6.2.2. Análisis de seguridad

A continuación, se procederá con el análisis de la seguridad comparando la plantilla creada con la configuración actual del sistema. Para realizar el análisis se abrirá una consola MMC en la que se agregara el complemento “Configuración y análisis de seguridad”.



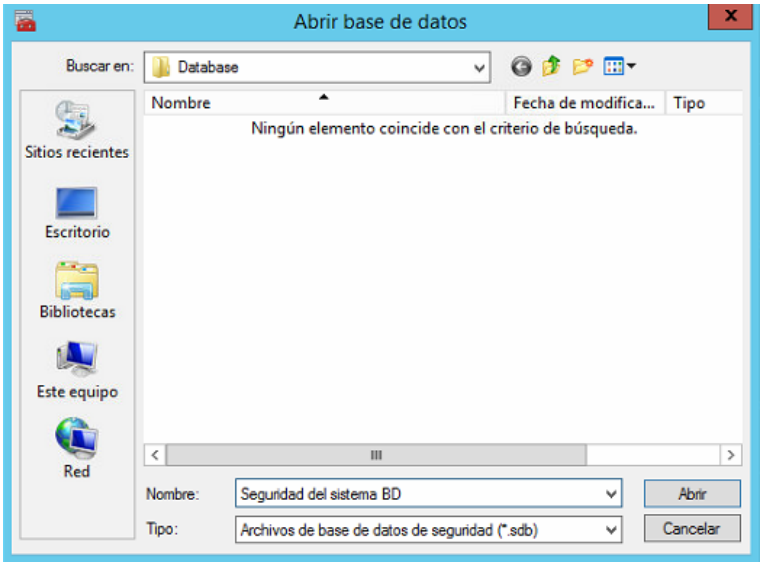
Captura 188 Agregar complemento "Configuración y análisis de seguridad"

Añadido el complemento se hará clic con el botón derecho sobre él y se clicará en “Abrir base de datos…”.



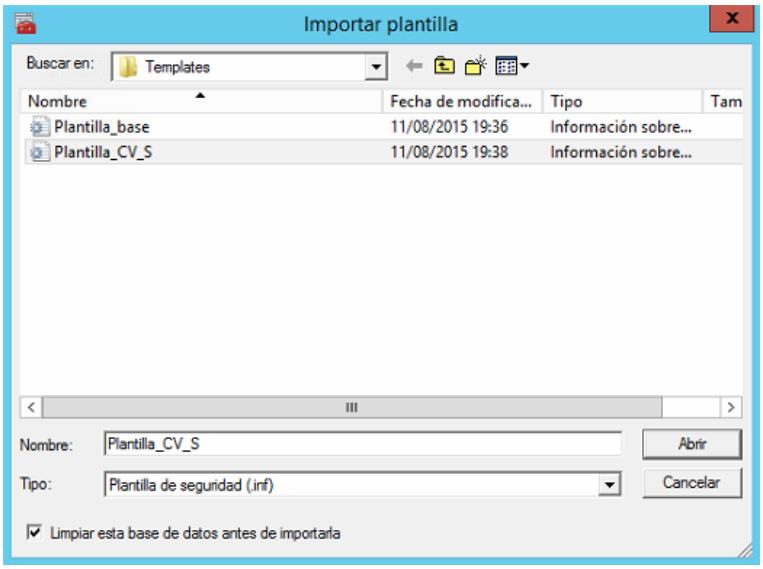
Captura 189 Abrir BD

En la ventana “Abrir base de datos” se escribirá el nombre la base de datos (en adelante BD), en este caso será “Seguridad del sistema BD”, y se clicará en “Abrir”.



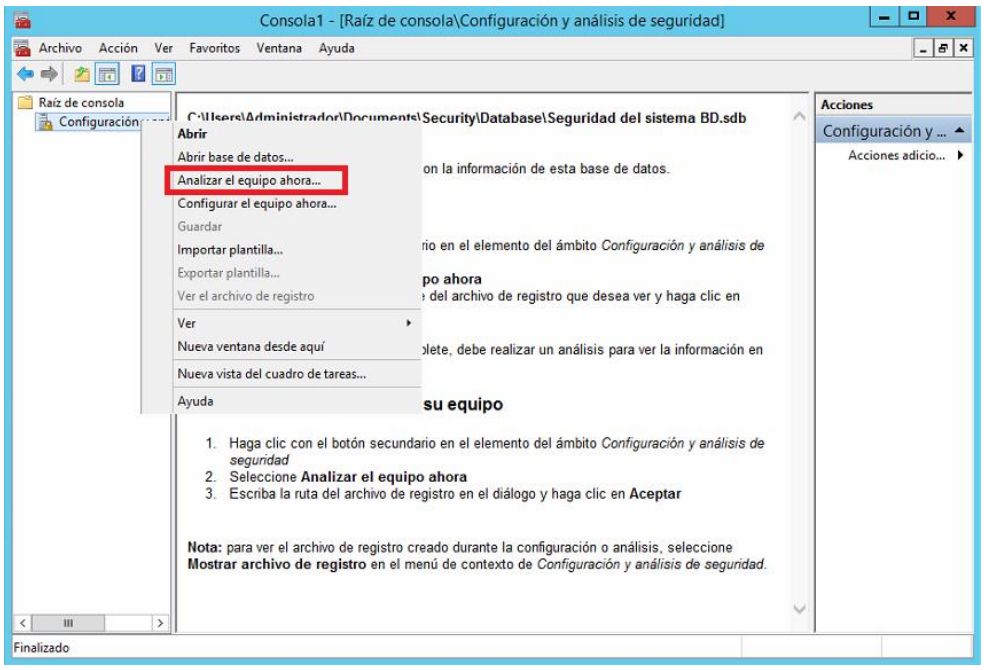
Captura 190 Nombre de la BD

En la ventana “Importar plantilla” se importará la plantilla creada. Se seleccionará y se clicará en “Abrir”.



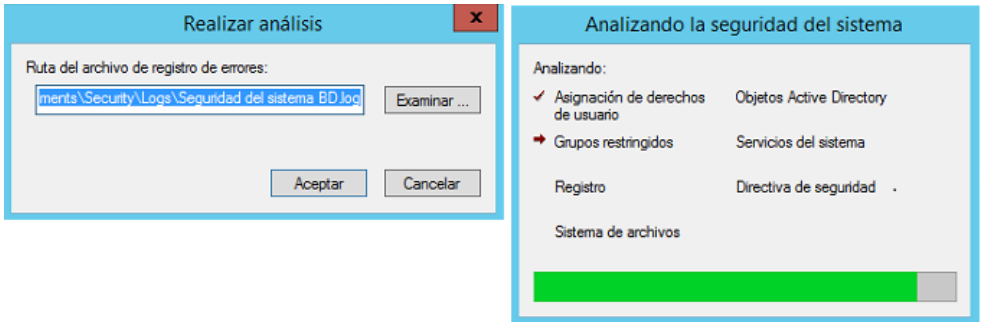
Captura 191 Selección de plantilla

Una vez creada la base de datos e importado la plantilla se procederá con el análisis, para ello se clicará con el botón derecho sobre el complemento y se clicará en la opción "Analizar el equipo ahora…".



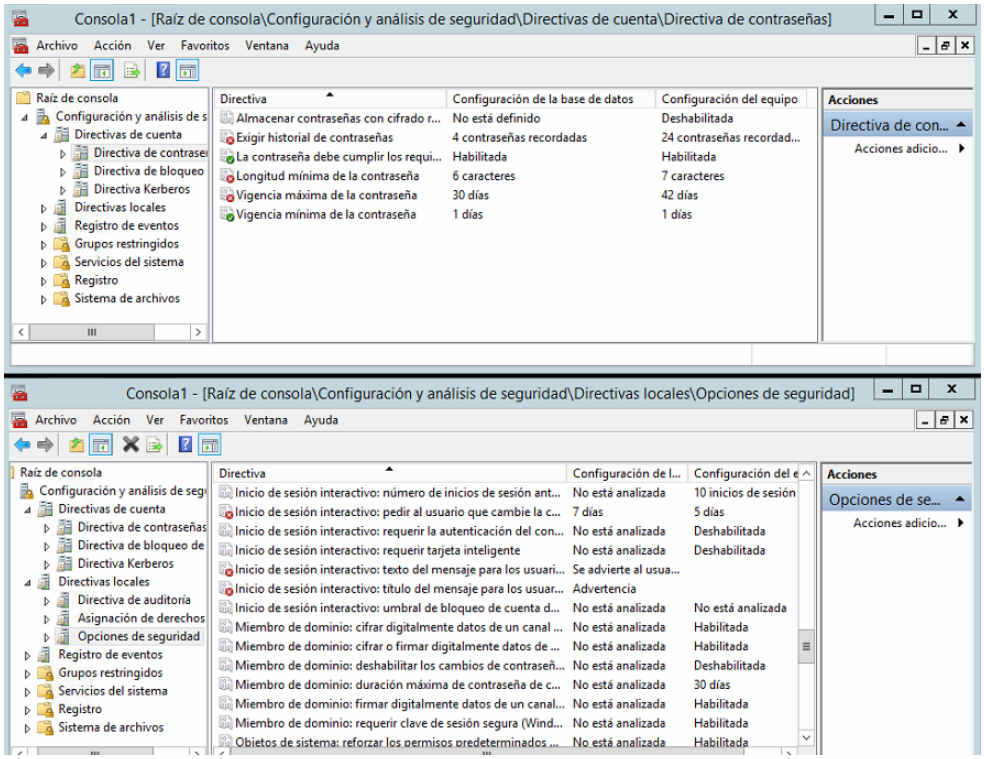
Captura 192 Análisis del equipo

Se dejará la ruta por defecto y se clicará en "Aceptar", con esto empezará el proceso de análisis.



Captura 193 Analizando la seguridad del sistema

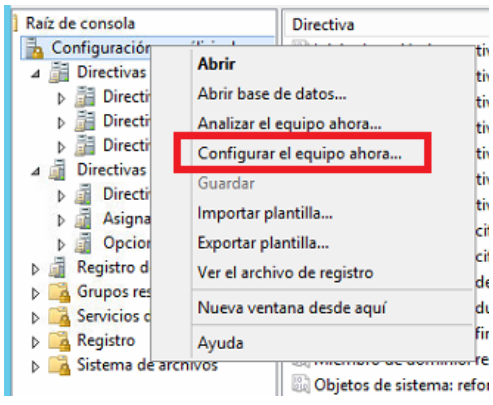
Una vez terminado el análisis se puedo comprobar las diferencias en la configuración de seguridad del sistema con la plantilla, todas las directivas con configuración diferentes aparecen en la consola MMC con un aspa roja al lado del nombre de la directiva como se comprueba en la captura 195.



Captura 194 Resultados del análisis

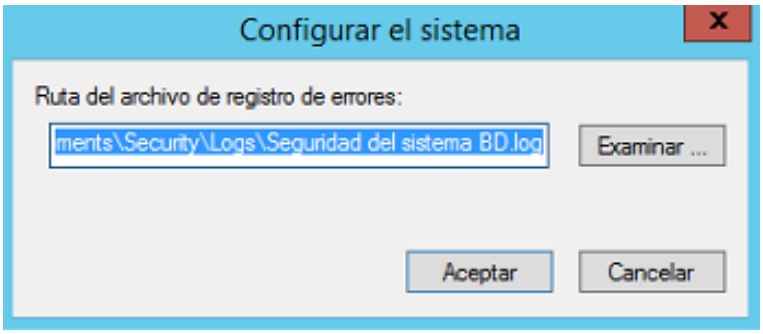
4.6.2.3. Configuración de la seguridad del sistema

Con el análisis del sistema realizado se procederá con importación de la configuración de seguridad de la plantilla creada, para ello desde la consola MMC de análisis de seguridad se clicará con el botón derecho sobre el complemento y se clicara en la opción “Configurar equipo ahora…”, al hacer esto se configurará en el sistema la plantilla utilizada en el análisis.



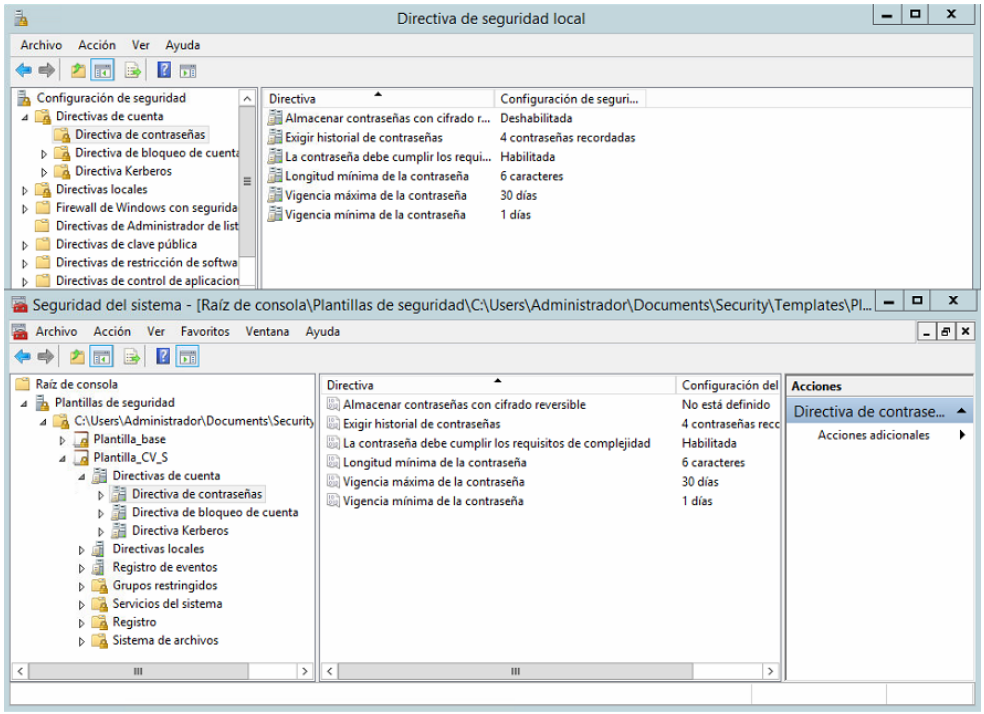
Captura 195 Configurar el equipo ahora

Se dejará la ruta por defecto y se clicará en “Aceptar” para que comience la configuración del sistema.



Captura 196 Ruta de la BD

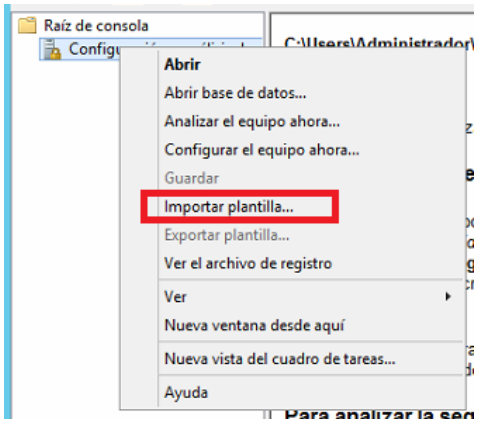
Pudiéndose comprobar que se ha configurado la seguridad comparando la consola MMC con la plantilla creada con la ventana de “Directivas de seguridad local”.



Captura 197 Comparación de la seguridad

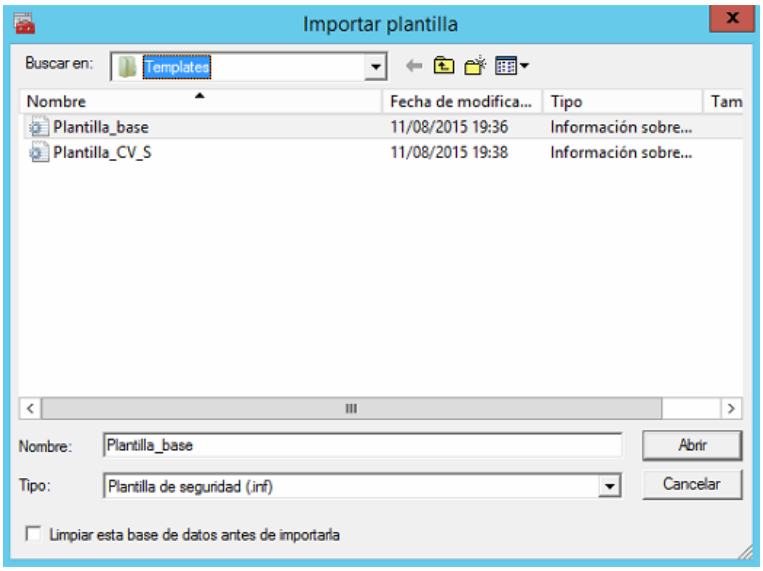
4.6.2.4. Restaurar la configuración de seguridad inicial

Para restaurar la configuración inicial de seguridad o importar cualquier plantilla, en este caso se restaurará la configuración, se procederá desde la consola MMC del análisis donde se clicará con el botón derecho sobre el complemento "Configuración y análisis de seguridad" y en la opción "Importar plantilla…".



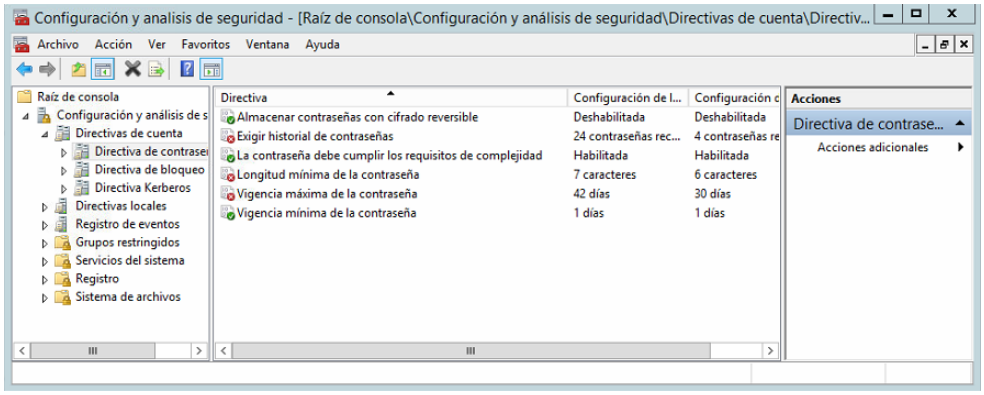
Captura 198 Importar plantilla

Se seleccionará la plantilla base anteriormente salvada en el apartado 4.4 y se clicará en "Abrir".



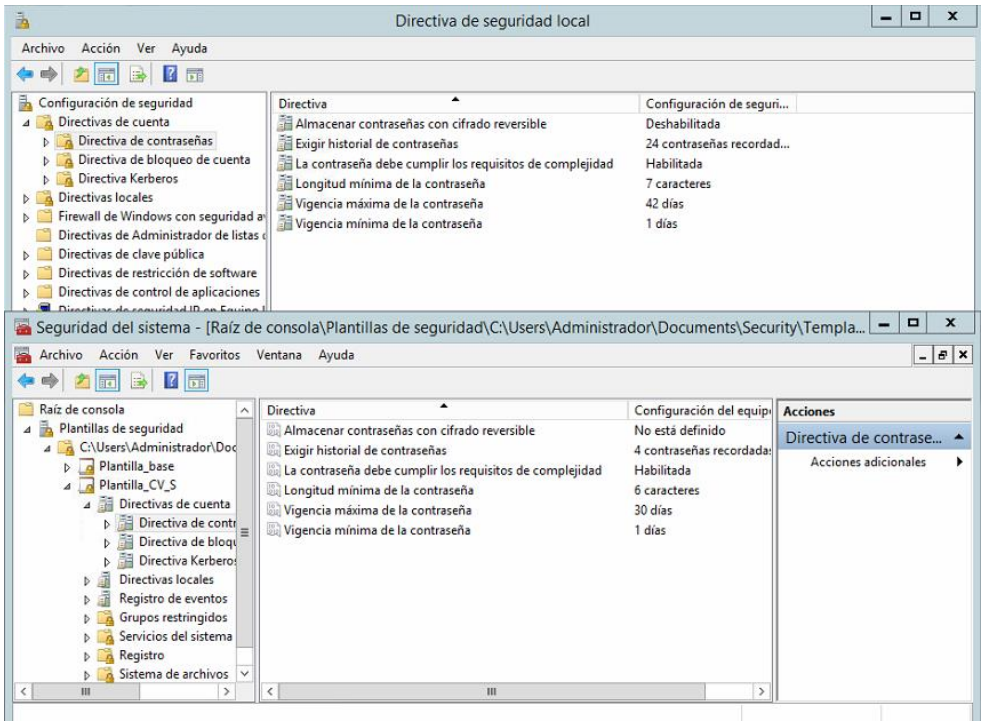
Captura 199 Selección de la plantilla a importar

Se volverá a realizar un análisis de seguridad.



Captura 200 Resultados del análisis de seguridad con la plantilla importada

Se configurará el equipo con la plantilla base, se comprueba que se ha configurado la seguridad comparando la consola MMC con la plantilla creada con la ventana de "Directivas de seguridad local".



Captura 201 Configuración de la seguridad con la plantilla importada

Una vez comprobado su funcionamiento se dejará configurada la seguridad de la plantilla creada.

4.6.3. Cifrado/Descifrado de archivos

La funcionalidad *Encryption File System* (EFS) permite cifrar los archivos para dotar de seguridad su acceso, pero es preciso su almacenamiento en una partición NTFS[7]. Para utilizar

[7] NTFS (New Technology File System): Es un sistema de archivos de Windows NT incluido en las versiones de Windows: 2000, XP, WS 2003, WS 2008, Vista, 7, 8, WS 2012 y 10.

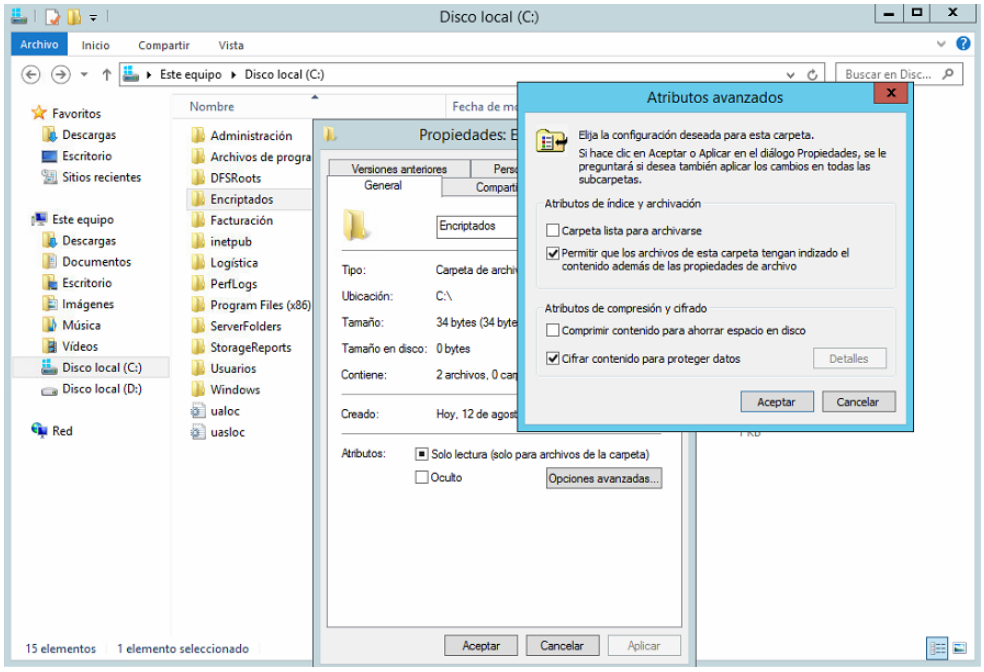
esta funcionalidad no se necesitan privilegios de administrador. Para realizar el cifrado, es preciso acceder a las propiedades de la carpeta o del archivo correspondiente. Se utiliza un certificado para el cifrado y el descifrado de los datos, y solo aquellas personas autorizadas pueden descifrar el archivo y acceder a su información.

Al cifrar un archivo se asigna un certificado digital por defecto autofirmado al usuario, generando un par de claves que permiten realizar el cifrado y el descifrado. También se posibilita en el cifrado la utilización de certificados emitiros por una entidad de certificación. EFS utiliza un sistema de cifrado simétrico utilizando una clave simétrica para cifrar el archivo y uno asimétrico que utiliza una clave pública para cifrar la clave simétrica que permite el descifrado del archivo. Con esto sólo los usuarios que posean un certificado tendrán la posibilidad de acceder al contenido del archivo.

Para la recuperación de un archivo encriptado en el cual se ha perdido la clave privada es necesario implementar procedimientos que permitan dar respuesta a este tipo de problemas. Existen varias soluciones a este problema:

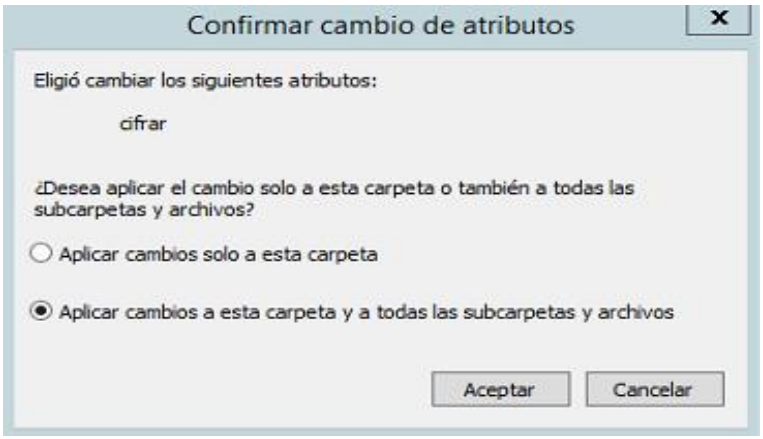
- **Salvaguardar el certificado digital.** En caso de que se pierda el certificado es posible restaurar dicho certificado.
- **Uso de un agente de recuperación.** Este agente es una cuenta con permiso para descifrar todos los archivos cifrados mediante EFS, la cuenta Administrador de dominio posee este rol.

Se procederá con un ejemplo práctico de encriptación de directorios y archivos, para ello se accederán a las propiedades de la carpeta “Encriptados” creada en el apartado 4.4, en la pestaña “General” se clicará en “Opciones avanzadas” donde se habilitará la opción “Cifrar contenido para proteger datos” y se aceptará.



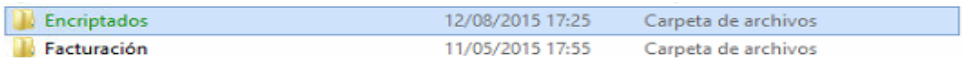
Captura 202 Cifrar carpeta

En la ventana para confirmar los cambios se seleccionará la segunda opción "Aplicar cambios a esta carpeta y a todas las subcarpetas y archivos" y se clicará en "Aceptar".



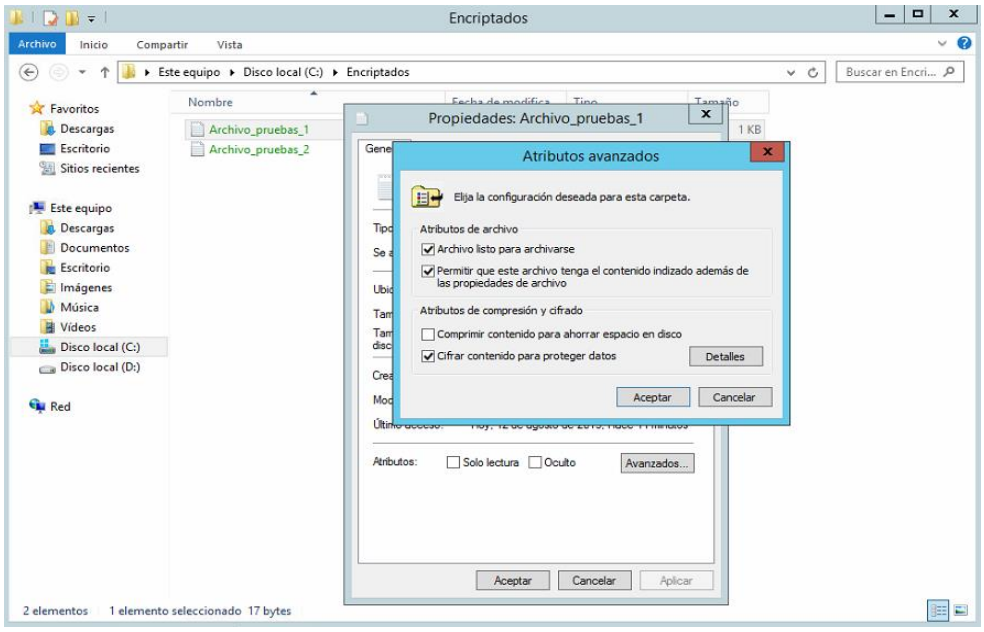
Captura 203 Confirmación del cifrado

Se observará que el color del texto de la carpeta ha cambiado a un color verde, todas las subcarpetas y archivos serán del mismo color verde.

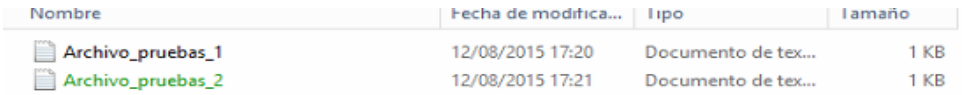


Captura 204 Carpeta cifrada en color verde

Para realizar las pruebas uno de los archivos de la carpeta no estará cifrado, el descifrado se hará de la misma forma que cuando se cifró la carpeta.

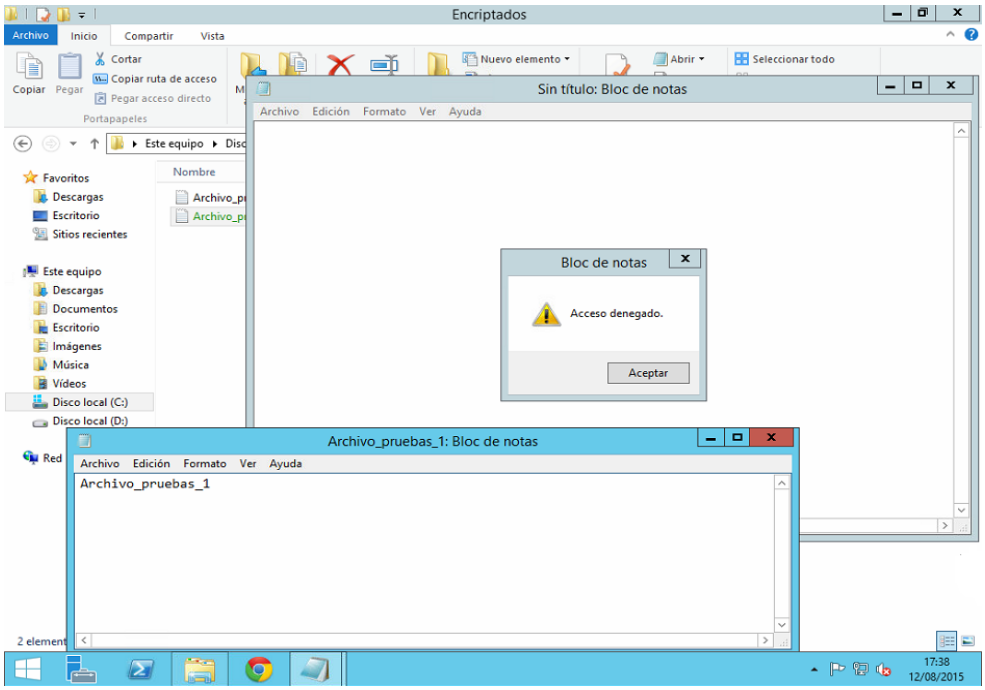


Captura 205 Descifrar archivo



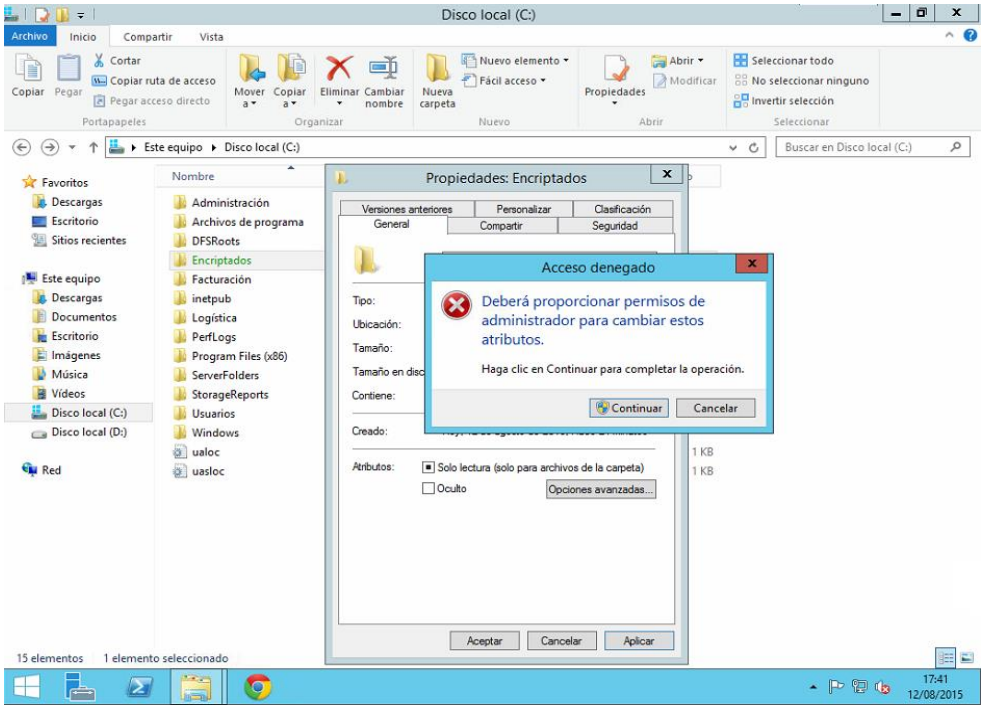
Captura 206 Diferencia entre archivos cifrados y descifrados

Después, se accederá con el usuario de pruebas a la carpeta encripta desde Windows 7, al intentar abrir los archivos el archivo que esta encriptado dará el error "Acceso denegado" mientras que en el otro se podrá abrir.



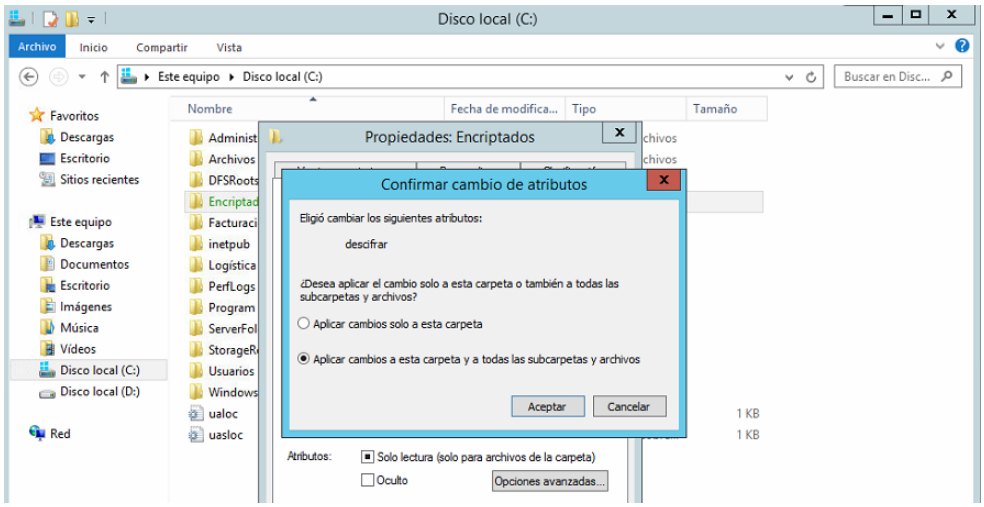
Captura 207 Pruebas de acceso a archivos cifrados

Si se intenta quitar la encriptación a la carpeta desde el usuario de pruebas le aparecerá el error "Deberá proporcionar permisos de administrador para cambiar estor atributos".



Captura 208 Prueba de intento de descifrado de carpeta

Solo las personas autorizadas pueden ver los archivos encriptados o modificar ese atributo. Para este caso de estudio todavía no se han barajado este tipo de restricciones por consiguiente se descifrará la carpeta y sus subcarpetas y archivos desmarcando la opción "Cifrar contenido para proteger datos" y posteriormente seleccionando la opción "Aplicar cambios a esta carpeta y a todas las subcarpetas y archivos", el color del texto de las carpetas y archivos volverá a estar negro.



Captura 209 Descifrar carpetas

5. Conclusiones

Como se ha observado en el TFG, haciendo hincapié en el apartado 4, mediante la utilización de directivas de grupo se puede configurar la seguridad del sistema WS 2012 R2. Este tipo de configuración ha cambiado en pocos aspectos con respecto a su antecesor WS 2008 R2. Los sistemas de WS a lo largo de sus ediciones Microsoft ha ido enfocado más gráficamente y organizada, como se observa en su última edición WS 2012, en la configuración de seguridad y otros aspectos del sistema.

En este TFG se ha desarrollado una guía base de la configuración de la seguridad, dicha configuración se implementará en la empresa del caso de estudio, donde se contempla su diseño, implementación y configuración con algunos ejemplos prácticos.

Uno de los mayores desafíos a los que se enfrenta un sistema de información es la seguridad de los datos que contenga la empresa, debido a que un sistema no puede asegurarse al 100%. Dicho esto, una parte de la seguridad va dirigida a planes de contingencias para amenazas futuras (catástrofes naturales, ataques al sistema, etc.) mediante antivirus, *firewalls*, SAIs, etc. La otra parte es la configuración de las directivas de seguridad del sistema y concienciando a los usuarios con aspectos básicos en seguridad, por ejemplo que el usuario tenga sus contraseñas apuntas en papel o en algún documento en texto plano en el ordenador de trabajo o casa, esto provocará una vulnerabilidad en el sistema de la empresa.

Con la realización del TFG hemos enriquecido las bases de conocimiento adquiridas en el Grado en Ingeniería Informática y además las hemos ampliado, con lo cual nos ayudará con la configuración del sistema WS 2012 R2 cuando se realice el proyecto en la empresa. Un posible futuro TFG sería profundizar en todas las opciones de seguridad de las cuales hemos dado una breve descripción en el apartado 4.1.

6. Referencias bibliográficas

- *Active Directory* [Wiki en Internet]. St. Petersburg (FL): Wikimedia Foundation, 2015. [Consulta: de mayo a julio 2015]. Disponible en: http://es.wikipedia.org/wiki/Active_Directory
- Benichou, Juli. *Las directivas de grupo (GPO) en Windows Server 2008 y 2008 R2: implementación, funcionalidades, depuración*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2012.
- Bonnet, Nicolás. *Windows Server 2012 R2 – Instalación y Configuración*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2014.
- Bonnet, Nicolás. *Windows Server 2012 R2 – Instalación y configuración: Examen nº. 70-410: 42 prácticas, 145 preguntas-respuestas*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2014.
- Bonnet, Nicolás. *Windows Server 2012 – Las bases imprescindibles para administrar y configurar su servidor*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2013.
- Bonnet, Nicolás. *Windows Server 2012 R2 – Las bases imprescindibles para administrar y configurar su servidor*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2014.
- Deman, Thierry; Elmaleh, Freddy; Neild, Sébastien; Van Jones, Maxence. *Windows Server 2008 R2 – Administración avanzada*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2012.
- Deman, Thierry; Elmaleh, Freddy; Neild, Sébastien; Van Jones, Maxence. *Windows Server 2012 R2: Administración avanzada*. Cornellà de Llobregat (Barcelona): Ediciones ENI, 2014.
- González Pérez, Pablo; Alonso Franco, Francisco Jesús; Remondo Álvarez, Alejandro; San Román Moreno, Sergio; Álvarez Martín, Carlos; Alonso, Chema. *Windows Server 2012 para IT Pros*. Móstoles (Madrid): Edición Informática64, 2012.
- In SlideShare. *Novedades en Windows Server 2012 R2* [En línea]. LinkedIn Corporation, 2014. [Consulta: de marzo a julio 2015]. Disponible en: https://technet.microsoft.com/es-es/library/Cc770842(v=WS.10).aspx
- José Ángel Fernández. *Novedades en Windows Server 2012 R2* [En línea]. TechNet Spain: IT Pro Evangelist, 2013. [Consulta: de marzo a julio 2015]. Disponible en: http://blogs.technet.com/b/estechnet/archive/2013/11/06/novedades-en-windows-server-2012-r2.aspx
- Jair Gómez Arias. *Windows Server 2012 – Configuración y administración de directivas de contraseñas* [En línea]. JGAITPro, 2012. [Consulta: de marzo a julio 2015]. Disponible en: http://blogs.itpro.es/jairgomez/2012/05/09/windows-server-2012-configuracin-y-administracin-de-directivas-de-contraseas/
- Microsoft. *Directiva de grupo* [En línea]. Redmond (Estados Unidos): Microsoft, 2012. [Consulta: de marzo a julio 2015]. Disponible en: https://technet.microsoft.com/es-es/windowsserver/bb310732.aspx
- Microsoft. *Guía paso a paso de la directiva de auditoría de seguridad avanzada* [En línea]. Redmond (Estados Unidos): Microsoft, 2011. [Consulta: de marzo a julio 2015]. Disponible en: https://technet.microsoft.com/es-es/library/Dd408940(v=WS.10).aspx

- Microsoft. *Guía paso a paso para la configuración de directivas de bloqueo de cuenta y contraseña específica* [En línea]. Redmond (Estados Unidos): Microsoft, 2009. [Consulta: de marzo a julio 2015]. Disponible en: https://technet.microsoft.com/es-es/library/Cc770842(v=WS.10).aspx
- Microsoft. *Información general de Servicios de dominio de Active Directory* [en línea]. Redmond (Estados Unidos): Microsoft, 2012. [Consulta: de mayo a julio 2015]. Disponible en: https://technet.microsoft.com/library/hh831484.aspx
- Microsoft. *Introducción a la directiva de grupo* [en línea]. Redmond (Estados Unidos): Microsoft, 2013. [Consulta: de mayo a julio 2015]. Disponible en: https://technet.microsoft.com/library/hh831791
- Microsoft. *Novedades de Servicios de Escritorio remoto* [en línea]. Redmond (Estados Unidos): Microsoft, 2014. [Consulta: de mayo a julio 2015]. Disponible en: https://technet.microsoft.com/library/hh831527
- Terrasa Barrena, Andrés; Espinosa Minguet, Agustín. Asignatura de la rama Tecnologías de la Información: *Administración de Sistemas*. Dpto. de Sistemas Informáticos y Computación (ETSINF, Universidad Politécnica de Valencia). Valencia.