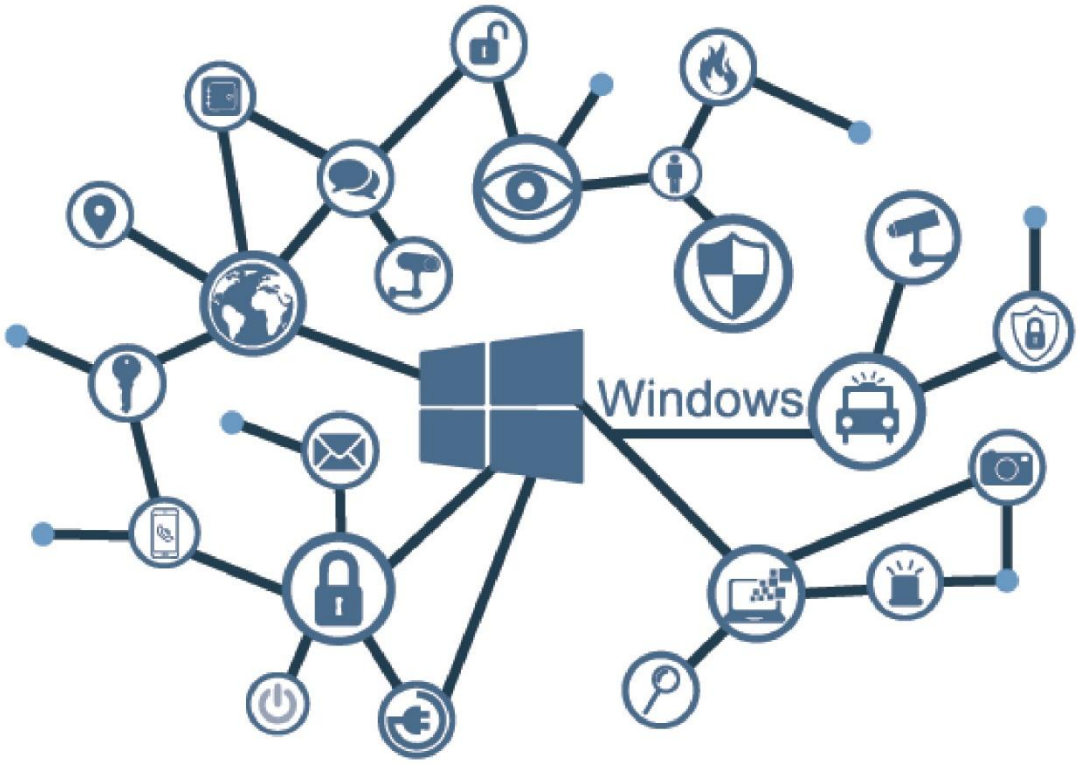
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 568

Windows Server Update Services (WSUS)



Julio 2017

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.03.12 13:22:37 +01'00'

NIPO: 785-17-069-9

Fecha de Edición: julio de 2017
Sidertia Solutions S.L. ha participado en la realización del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC-500) siendo de aplicación para la Administración y de obligado cumplimiento para los Sistemas que manejen información clasificada Nacional.
2. La serie CCN-STIC-500 se ha diseñado de manera incremental. Así que, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. Por ejemplo, para un servidor Windows Server 2012 R2 y Windows Server Update Services las guías que deberán aplicarse son:
   - CCN-STIC-560A Configuración segura de Windows Server 2012 R2 (Servidor miembro).
   - CCN-STIC-563 Implementación de IIS 8.5 sobre Windows Server 2012 R2 en servidor miembro de dominio.
   - La presente guía.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá ningún tipo de conexión con redes consideradas no seguras como puede ser Internet.

2. OBJETO

3. El propósito de este documento consiste en proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servicio Windows Server Update Services (WSUS) en un servidor miembro de una infraestructura de dominio y en un servidor fuera de dominio con comunicación directa a Internet.
4. La instalación, así como los procesos de administración, se han diseñado para que la implementación sea lo más restrictiva posible. Es posible que determinadas funcionalidades de Windows Server Update Services (WSUS) requieran modificar algunas de las configuraciones que se plantean con la presente guía.
5. Esta guía asume que el servidor de actualizaciones se va a implementar sobre un equipo con Windows Server 2012 R2 Standard de 64 Bits en donde se ha seguido el proceso de implantación definido en la guía CCN-STIC-560A.
6. Además, debido a que Windows Server Update Services (WSUS) requiere de Internet Information Services, será también necesario aplicar la guía de seguridad CCN-STIC-563 Implementación de IIS 8.5 en ese mismo servidor.
7. Cumpliendo con estos requisitos previos, puede iniciar la instalación de Windows Server Update Services (WSUS) basado en Microsoft Windows Server 2012 R2 Standard.

Nota: La información y procedimientos establecidos en este documento están enfocados y basados en el sistema operativo Microsoft Windows Server 2012 R2 Standard por ser el sistema operativo de tipo servidor de referencia en el mercado actual. No obstante, la configuración y el procedimiento indicados son válidos para la instalación del servicio Windows Server Update Services (WSUS) en un sistema operativo Microsoft Windows Server 2008 R2.
Si realiza la instalación del servicio WSUS sobre Windows Server 2008 R2 deberá haber seguido, de forma previa a la aplicación de este documento, las guías de seguridad CCN-STIC-521A (securización de Windows Server 2008 R2 miembro de dominio) y CCN-STIC-524 (securización de Internet Information Services 7.5 sobre Windows Server 2008 R2) para aplicar la configuración correcta de seguridad sobre el sistema.
Sin embargo, es necesario tener en consideración que es posible que las ventanas u opciones indicadas en este documento presenten variaciones con respecto al servicio de WSUS instalado en un sistema operativo Windows Server 2008 R2. Por lo tanto, deberá adaptar los pasos a la configuración de su entorno.

3. ALCANCE

8. La guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de Windows Server Update Services (WSUS) en una configuración restrictiva de seguridad.
9. El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:
   - Un único bosque de Directorio Activo.
   - Un único dominio dentro del bosque de Directorio Activo.
   - Nivel funcional del bosque y del dominio en Windows Server 2012 R2.
   - Un controlador de dominio basado en Windows Server 2012 R2 Standard.
   - Un servidor miembro del dominio basado en Windows Server 2012 R2 Standard con Windows Server Update Services (WSUS).
   - La instalación del servicio de Windows Server Update Services (WSUS) se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.
   - Un servidor Windows Server 2012 R2 con el rol de Windows Server Update Services (WSUS) habilitado y con conexión directa a Internet.
   - Un cliente Windows 7 64x Enterprise unido al dominio.
   - Un cliente Windows 10 64x Enterprise unido al dominio.
   - Un servidor Windows Server 2012 R2 Standard (Cliente WSUS).
10. Este documento incluye:

- **Mecanismos para la aplicación de configuraciones**. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.
- **Mecanismos para la creación de cuentas necesarias para la funcionalidad de la solución.** Tanto los procesos de implementación como de instalación requieren de cuentas específicas; se ha automatizado el proceso de creación de dichas cuentas.
- **Descripción de la seguridad en Windows Server Update Services (WSUS).** Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en el servicio de Windows Server Update Services (WSUS) de Windows Server 2012 R2, así como las medidas para reforzar dicha seguridad.
- **Instalación de un servidor Windows Server Update Services fuera de Dominio.** Descripción de la instalación de un servidor WSUS que se encuentra fuera de la red de dominio para la descarga de actualizaciones.
- **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad de un servidor de actualizaciones de Windows Server 2012 R2.
- **Guía de administración.** Va a permitir realizar tareas de administración en el entorno de seguridad establecido.
- **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

11. Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará, a grandes rasgos, de los siguientes pasos:
    - Antes de comenzar a aplicar la guía, además de los requisitos para la instalación del servicio de Windows Server Update Services (WSUS), será necesario cumplir los requisitos definidos para Windows Server 2012 R2.
    - Así mismo, antes de instalar la característica de Windows Server Update Services (WSUS), será necesario aplicar las guías de seguridad codificadas como CCN-STIC-560A y CCN-STIC-563 Implementación de IIS 8.5
    - A continuación, se deberá instalar y configurar el rol de Windows Server Update Services de Windows Server 2012 R2 tal y como se describe en la presente guía.

4.1. AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

12. Los contenidos de esta guía son de aplicación para servidores con Sistemas Operativos Microsoft Windows Server 2012 R2 Standard.
13. La guía ha sido probada y verificada con la versión de Windows Server 2012 R2 Standard de 64 bits, con los parámetros por defecto de instalación y aplicando las guías CCN-STIC-560A y CCN-STIC-563 para su configuración. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2012 R2 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor podría llegar a implementarse la siguiente guía sobre la versión Datacenter. La presente guía no será funcional con las versiones Windows Server 2012 R2 Essentials, ni Windows Server 2012 R2 Foundation.
14. Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de rol de servidor de actualizaciones en un entorno de dominio de Directorio Activo.
15. La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2012 R2 con las siguientes características técnicas:
    - Servidor Dell PowerEdgeTM T320:
        - Intel Pentium Xeon CPU ES 2430 2.20 GHz.
        - HDD 1 TB.
        - 64 GB de RAM.
        - Interfaz de Red 1 Gb/s.
16. Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2012 R2 Standard de 64 bits. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2 GB de memoria RAM.
17. Así mismo, hay que tener en cuenta que el rol de servidor de actualizaciones requiere, para un entorno de producción, un mínimo de 4 GB de memoria RAM para funcionar adecuadamente, aunque se recomiendan 6 GB.
18. Se espera, por tanto, que el rendimiento de Windows Server 2012 R2 pueda exceder dichos límites. Es por ello que se recomienda al menos disponer de 4 GB de memoria RAM en entornos en producción.
19. La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas en Microsoft Windows Server 2012 R2.

20. Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento.
21. Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que en ocasiones se realizan para las distintas actualizaciones de seguridad.
22. Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado donde se han aplicado los test y cambios en la configuración, que se ajustan a los criterios específicos de cada organización.
23. El espíritu de estas guías no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones sino a servir como la línea base de seguridad, que deberá ser adaptada a las necesidades propias de cada organización.

5. DESCRIPCIÓN DE WINDOWS SERVER UPDATE SERVICES

24. Windows Server Update Services (WSUS) permite a los administradores de tecnologías de la información implementar las actualizaciones de productos de Microsoft más recientes.
25. Con WSUS, los administradores pueden administrar por completo la distribución de actualizaciones que se publiquen en Microsoft Update para los equipos de su red.

5.1. ROL DE SERVIDOR DE WINDOWS SERVER UPDATE SERVICES

26. El servidor WSUS proporciona las características que los administradores necesitan para administrar y distribuir actualizaciones mediante una consola de administración.
27. Un servidor WSUS puede ser el origen de actualización para otros servidores WSUS de la organización. El servidor WSUS que actúa como origen de actualización es el *"servidor que precede en la cadena"*.
28. En una implementación de WSUS, al menos un servidor WSUS de la red debe conectarse a Microsoft Update para obtener información sobre actualizaciones disponibles. El administrador puede determinar, en función de la configuración y seguridad de red, la cantidad de servidores que desea que se conecten directamente a Microsoft Update.

Nota: Para la presente guía, este servidor se implantará fuera de la red de dominio y así evitar cualquier comunicación con internet, evitando lo máximo posible cualquier intrusión en su red de dominio.

5.2. ADMINISTRACIÓN DE ACTUALIZACIONES

29. La administración de actualizaciones es el proceso por el cual se controla la implementación y el mantenimiento de versiones provisionales de software en entornos de producción.
30. Permite preservar la eficiencia operativa, superar vulnerabilidades de seguridad y mantener la estabilidad del entorno de producción.
31. Si su organización no puede determinar y mantener un nivel conocido de confianza en sus sistemas operativos y software de aplicación, podría tener una serie de vulnerabilidades de seguridad que, si se explotan, afectarían los ingresos y la propiedad intelectual. Minimizar esta amenaza requiere que tenga sistemas correctamente configurados, que use el software más reciente y que instale las actualizaciones de software recomendadas.
32. Los escenarios principales en los que WSUS favorece a su infraestructura son los siguientes:
    - Administración centralizada de actualizaciones.
    - Automatización de administración de actualizaciones.

6. ESCENARIOS DE IMPLEMENTACIÓN DE WINDOWS SERVER UPDATE SERVICES

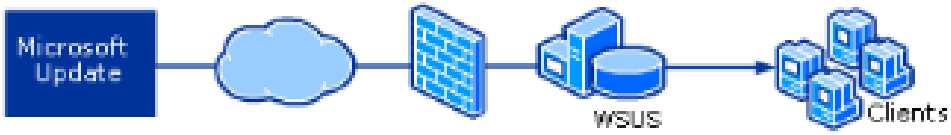
6.1. IMPLEMENTACIÓN SIMPLE DE WSUS

33. La implementación de WSUS más básica consiste en un servidor dentro de un firewall corporativo que sirve a equipos cliente en una intranet privada.
34. El servidor WSUS se conecta con Microsoft Update para descargar las actualizaciones. Esto se conoce como sincronización, en cada una de ellas, WSUS determina si, desde la última realizada, se ha puesto a disposición alguna actualización nueva. Si es la primera vez que se sincroniza WSUS, todas las actualizaciones están disponibles para su descarga.

Nota: La sincronización inicial puede tardar más de una hora. Todas las actualizaciones siguientes deberán ser mucho más rápidas.

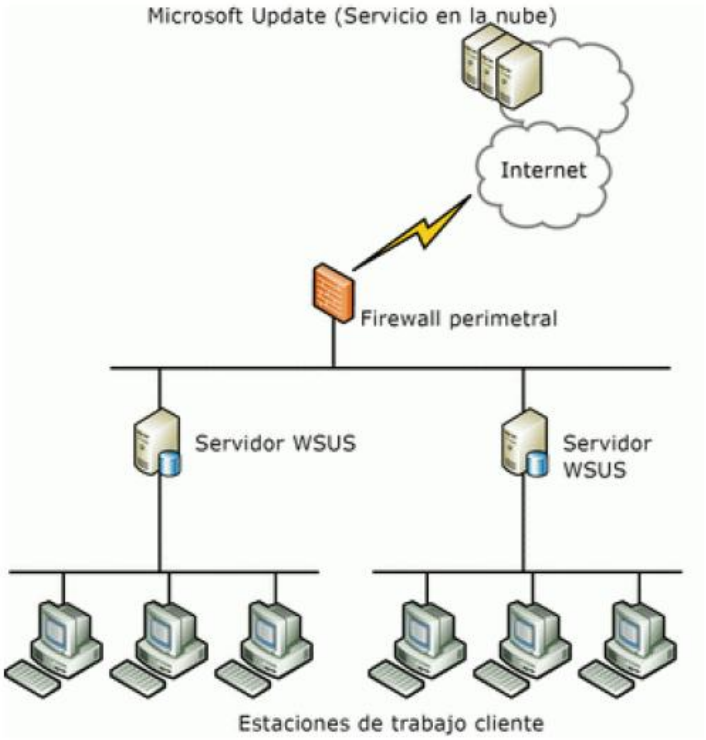
35. El servidor WSUS usa el puerto 80 para el protocolo HTTP y el puerto 443 para el protocolo HTTPS, a fin de obtener actualizaciones de Microsoft.
36. Si hay un firewall corporativo entre su red e Internet, deberá abrir estos puertos en el servidor que se comunica directamente con Microsoft Update.
37. El servidor WSUS usa el puerto 8530 para el protocolo HTTP y el puerto 8531 para el protocolo HTTPS, a fin de proporcionar actualizaciones a estaciones de trabajo cliente.
38. La siguiente figura muestra un escenario simple de servidor WSUS, un administrador puede establecer un servidor que ejecuta WSUS dentro del

firewall corporativo, para que sincronice contenido directamente con Microsoft Update y distribuya actualizaciones a los equipos cliente.



6.2. VARIOS SERVIDORES WSUS

39. Los administradores pueden implementar varios servidores que ejecutan WSUS para que sincronicen todo el contenido dentro de la intranet de la organización.
40. Se expone solamente un servidor a Internet, este es el único servidor que descarga actualizaciones de Microsoft Update.
41. El servidor se configura como el servidor que precede en la cadena, es el origen con el que se sincronizan los servidores que siguen la cadena.
42. Los servidores pueden estar geográficamente dispersos en una red para proporcionar una mejor conectividad a todos los equipos clientes.

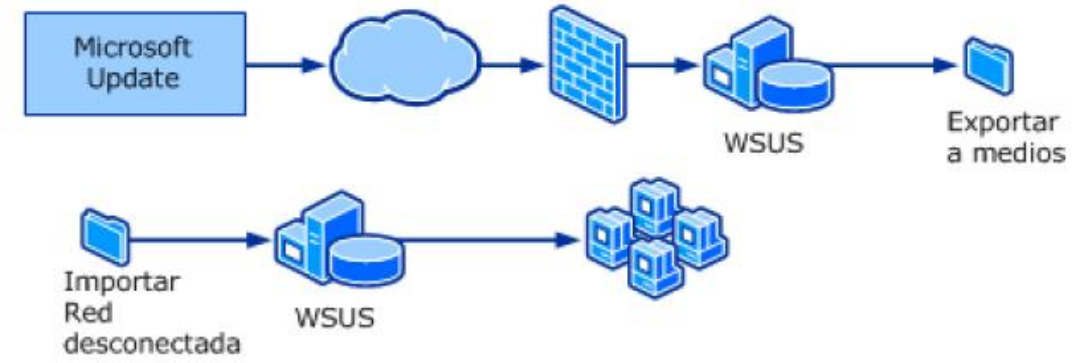


6.3. SERVIDOR WSUS DESCONECTADO

43. Para la presente guía, este será el escenario de despliegue que se tendrá presente para la implementación de un servidor de Windows Server Update Services (WSUS).

44. Si una directiva u otras condiciones limitan el acceso de los equipos cliente a Internet, los administradores pueden configurar un servidor interno para que se ejecute WSUS.

45. Después de descargar, probar y aprobar las actualizaciones en el servidor fuera de su red de dominio, un administrador exportaría los metadatos y el contenido de las actualizaciones a un almacenamiento de datos, para después importarlos a servidores que ejecuten WSUS en la intranet.



Nota: Esta guía establece el procedimiento adecuado para utilizar un equipo cliente Windows 7/10 miembro del dominio como cliente del servicio WSUS. Si desea conectar un equipo cliente Windows 7/10 independiente (standalone) con el servicio WSUS, deberá aplicar los cambios en el registro que se indican en la URL https://technet.microsoft.com/en-us/library/cc720464(v=ws.10).aspx y realizar las modificaciones correspondientes en la configuración de comunicación entre ambos sistemas para permitir la conexión con el servicio.

6.4. JERARQUÍAS DE SERVIDORES WSUS

46. Es posible crear jerarquías complejas de servidores WSUS. Dado que los servidores WSUS se pueden sincronizar entre sí en lugar de hacerlo con Microsoft Update, solo es necesario un servidor WSUS único que se conecte a Microsoft Update.

47. Cuando se vinculan varios servidores WSUS, hay uno que precede en la cadena y otro que continua con la cadena. Una implementación de jerarquía de servidores WSUS ofrece los siguientes beneficios:

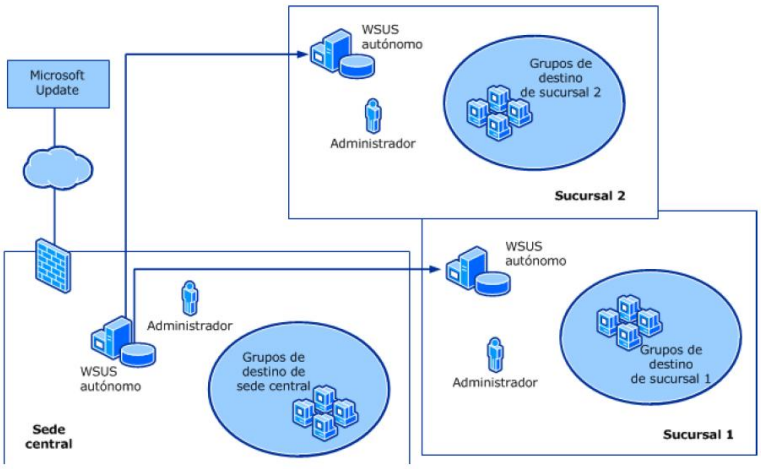
    - Se puede descargar actualizaciones desde Internet una sola vez y después distribuirlas a los equipos cliente mediante servidores que siguen una cadena. Este método ahorra ancho de banda en la conexión corporativa a Internet.
    - Se puede descargar actualizaciones en un servidor WSUS que esté físicamente cerca de los equipos cliente, por ejemplo, en sucursales.
    - Se pueden configurar servidores WSUS independientes para equipos cliente que usan productos de Microsoft en distintos idiomas.

– Puede escalar WSUS para una organización grande, cuyos equipos clientes superan la cantidad que un servidor WSUS puede administrar con eficacia.

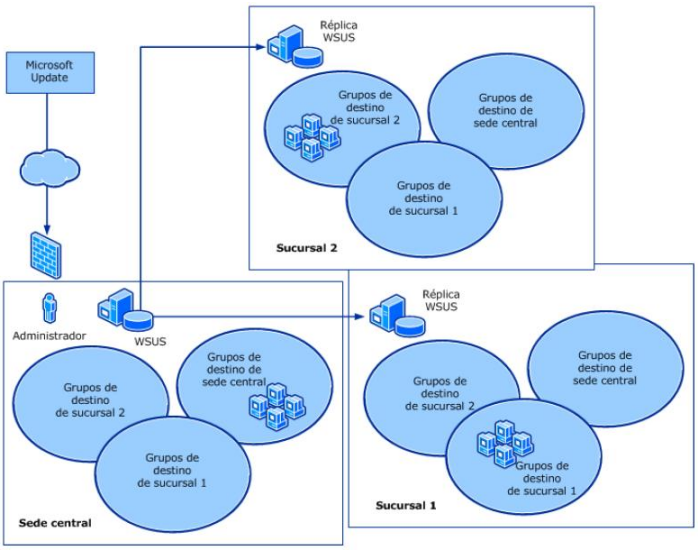
Nota: Se recomienda no crear una jerarquía de servidores WSUS con una profundidad mayor que tres niveles. Cada nivel requiere tiempo para propagar actualizaciones a todos los servidores conectados. Si bien no hay un límite teórico de jerarquía, Microsoft Corporation solo ha probado implementaciones con una jerarquía de cinco niveles de profundidad.

48. Puede conectar servidores WSUS en modo autónomo (para una administración distribuida) o en modo de réplica (para una administración centralizada):

– Modo autónomo: es la opción de instalación predeterminada para WSUS. Un servidor WSUS que precede en la cadena comparte actualizaciones con los servidores que siguen la cadena, durante la sincronización. Los servidores WSUS que siguen la cadena se administran de forma independiente y no reciben el estado de aprobación de una actualización, ni información del grupo de equipos del servidor que precede en la cadena. Al usar el modelo de administración distribuida, el administrador de cada servidor WSUS selecciona idiomas de actualizaciones, crea grupos de equipos, asigna equipos a grupos, prueba y aprueba actualizaciones y se asegura de que las actualizaciones correctas se instalen en los grupos de equipos adecuados.



– Modo de réplica: Este modo funciona con un servidor WSUS que precede en la cadena y que comparte actualizaciones, estados de aprobación y grupos de equipos con los servidores que siguen en la cadena. Los servidores de réplica heredan las aprobaciones de actualizaciones y no puede administrarse al margen del servidor WSUS que los precede.



Nota: Si configura varios servidores de réplica para que se conecten con un servidor WSUS único, el cual los precede, no programe la sincronización para que se ejecute al mismo tiempo en todos los servidores de réplica. Este procedimiento evitará un repentino aumento del uso del ancho de banda.

7. ESTRATEGIA DE ALMACENAMIENTO DE WINDOWS SERVER UPDATE SERVICES

49. Windows Server Update Services (WSUS) usa dos tipos de sistemas de almacenamiento: una base de datos para almacenar la configuración de WSUS y los metadatos de actualizaciones, y un sistema de archivos local opcional para almacenar archivos de actualización.
50. Las actualizaciones se componen de dos partes: los metadatos que describen la actualización y los archivos necesarios para instalarla.
51. Los metadatos de una actualización normalmente son mucho más pequeños que la actualización en sí y se almacenan en la base de datos de WSUS.
52. Los archivos de una actualización se almacenan en un servidor WSUS local o en un servidor web de Microsoft Update.

7.1. BASE DE DATOS WSUS

53. WSUS requiere una base de datos para cada servidor WSUS. Windows Server Update Services admite el uso de una base de datos que resida en otro equipo distinto, con algunas restricciones.
54. La base de datos de WSUS almacena la siguiente información:
    - Información de configuración de servidores WSUS.
    - Metadatos que describen cada actualización.
    - Información sobre equipos cliente, actualizaciones e interacciones.

55. Si existen varios servidores WSUS, debe tener una base de datos independiente para cada uno de ellos, sean autónomos o de réplica. No puede almacenar varias bases de datos de WSUS en una instancia única de SQL Server.
56. SQL Server, SQL Server Express y Windows Internal Database proporcionan las mismas características de rendimiento para una configuración de servidor único, donde la base de datos y el servicio de WSUS se ubican en el mismo equipo.

Nota: No intente administrar WSUS accediendo directamente a la base de datos. La manipulación directa de la base de datos puede dañarla. Los daños podrían no detectarse de inmediato, y en este caso pueden impedir actualizaciones a las siguientes versiones del producto. Para administrar WSUS, puede usar la consola de WSUS o las interfaces de programación de aplicaciones (API) de WSUS.

7.2. WSUS CON WINDOWS INTERNAL DATABASE (WID)

57. El asistente para la instalación de manera predeterminada crea y usa Windows Internal Database con el nombre SUSDB.mdf. Esta base de datos se ubica en la carpeta %windir%\wid\data\, donde %windir% es la unidad local en la que se instala el software del servidor WSUS.

Nota: Windows Internal Database (WID) se incluye con Windows Server 2012 y las versiones posteriores del sistema operativo Windows Server.

58. WSUS admite la autenticación de Windows solo para la base de datos. No se puede usar la autenticación de SQL Server con WSUS.
59. Si usa Windows Internal Database para la base de datos de WSUS, el programa de instalación de WSUS crea una instancia de SQL Server con el nombre server\Microsoft##WID, donde server es el nombre del equipo.
60. Con cualquiera de las opciones de base de datos, el programa de instalación de WSUS crea una base de datos con el nombre SUSB (Este no es configurable).
61. Se recomienda que use Windows Internal Database en los siguientes casos:
    - La organización aún no ha adquirido y no necesita un producto de SQL Server para ninguna otra aplicación.
    - La organización no necesita una solución NLB WSUS.
    - Se intenta implementar varios servidores WSUS. En este caso, debe considerar usar Windows Internal Database en servidores secundarios, aún si va a usar SQL Server para el servidor WSUS raíz. Dado que cada servidor WSUS requiere una instancia independiente de SQL Server, pronto experimentará problemas de rendimiento de la base de datos si una sola instancia de SQL Server administra varios servidores WSUS.

Nota: Windows Internal Database no proporciona una interfaz de usuario ni herramientas de administración de bases de datos. Si selecciona esta base de datos para WSUS, debe de usar herramientas externas para administrarla.

7.3. WINDOWS SERVER UPDATE SERVICES CON SQL SERVER

62. Se recomienda que use SQL Server con Windows Server Update Services en los siguientes casos:
    - Necesita una solución NLB WSUS.
    - Ya tiene por lo menos una instancia de SQL Server instalada.
    - No puede ejecutar el servicio de SQL Server con una cuenta local, que no sea del sistema, ni usando la autenticación de SQL Server. WSUS admite la autenticación de Windows únicamente.

7.4. ELEGIR IDIOMAS DE ACTUALIZACIÓN DE WSUS

63. Cuando se implementa una jerarquía de servidores WSUS, debe determinar los idiomas de actualización que se usan en toda la organización. Debe configurar el servidor WSUS raíz para que descargue actualizaciones en todos los idiomas utilizados en la organización.

Nota: La configuración establecida para los idiomas en el servidor WSUS fuera de su red de domino, que será el que descargue las actualizaciones, tiene que ser la misma que en el servidor WSUS dentro de su red de dominio, dónde importará las actualizaciones. Ya que, si esto no es así, podrá tener problemas futuros en la implementación de las actualizaciones.

64. El asistente de "Elegir idiomas" en la configuración de WSUS, permite obtener actualizaciones en todos los idiomas o en un subconjunto de idiomas. Si se selecciona un conjunto de idiomas, ahorra espacio en disco, no obstante, es importante elegir todos los idiomas que se necesitan para todos los servidores que siguen la cadena y los equipos cliente de un servidor WSUS.
65. Antes de realizar la configuración de los idiomas en el asistente de configuración de WSUS debe considerar lo siguiente:
    - Siempre incluya inglés además de cualquier otro idioma necesario en la organización. Todas las actualizaciones se basan en paquetes de idioma en inglés.
    - Los servidores que siguen en la cadena y los equipos cliente no recibirán todas las actualizaciones adecuadas, si no se han seleccionado todos los idiomas necesarios para el servidor que precede en la cadena. Asegúrese seleccionando todos los idiomas que necesitan todos los equipos cliente asociados con los servidores, que siguen la cadena.
    - Por lo general, se puede descargar actualizaciones en todos los idiomas en el servidor WSUS raíz que se sincroniza con Microsoft Update. Esta selección garantiza que todos los servidores que siguen la cadena y los equipos cliente recibirán las actualizaciones en los idiomas adecuados.

66. Si almacena actualizaciones de forma local y ha configurado un servidor WSUS para que descargue una cantidad limitada de idiomas, podrá percibir actualizaciones en idiomas distintos a los que especificó. Muchos archivos de actualización son grupos de varios idiomas, que incluyen al menos uno de los idiomas especificados en el servidor.

7.5. PLANEAR GRUPOS DE EQUIPOS WSUS

67. WSUS le permite dirigir actualizaciones a grupos de equipos para asegurarse de que determinados equipos reciban siempre las actualizaciones correspondientes en los momentos más oportunos.

Nota: Si un servidor WSUS se ejecuta en modo réplica, no se puede crear grupos en ese servidor. Todos los grupos de equipos necesarios para equipos cliente del servidor de réplicas, deben crearse en el servidor WSUS que se encuentra en la raíz de la jerarquía de servidores WSUS.

68. Los equipos siempre se asignan al grupo “Todos los equipos” y permanecen en el grupo “Equipos sin asignar” hasta que los asigne a otro grupo. Los equipos pueden pertenecer a más de un grupo.
69. Los grupos de equipos pueden configurarse en jerarquías. Las actualizaciones aprobadas para un grupo superior se implementarán automáticamente en los grupos inferiores.
70. Dado que los equipos pueden asignarse a varios grupos, es posible que una actualización se apruebe más de una vez para el mismo equipo. No obstante, la actualización se implementará una sola vez y cualquier conflicto se resolverá en el servidor WSUS.
71. Puede asignar equipos a grupos de equipos por medio de dos métodos: asignación del lado del servidor o asignación del lado del cliente.
    - Asignación del lado servidor: se asigna de forma manual uno o más equipos cliente a varios grupos simultáneamente.
    - Asignación del lado cliente: se usa la directiva de grupo o se modifica la configuración del registro en los equipos cliente para habilitar esos equipos de manera que se agreguen automáticamente a los grupos de equipos creados anteriormente.
72. El servidor aplica las siguientes reglas para resolver conflictos y determinar la acción correspondiente en los clientes:
    - Prioridad: Las acciones asociadas al grupo de mayor prioridad reemplazan las acciones de otros grupos. Cuanto mayor sea la profundidad de un grupo dentro de la jerarquía de grupos, mayor será su prioridad. La prioridad solamente se asigna en función de la profundidad.

- Prioridad de instalación y desinstalación: Instalar acciones reemplaza a desinstalar acciones. Las instalaciones obligatorias reemplazan a las instalaciones opcionales.
- Prioridad de las fechas de entrega: Las acciones que tienen una fecha límite reemplazan a las que no la tienen. Las acciones con fechas límite anteriores reemplazan a las que tienen fechas límite posteriores.

Nota: Es conveniente crear varios grupos de control en su implementación WSUS para tener un control de la eficacia de las actualizaciones y así evitar implementar actualizaciones erróneas o que puedan causar cualquier trastorno en los equipos cliente de su organización.

8. ALMACENAMIENTO DE ACTUALIZACIONES WSUS

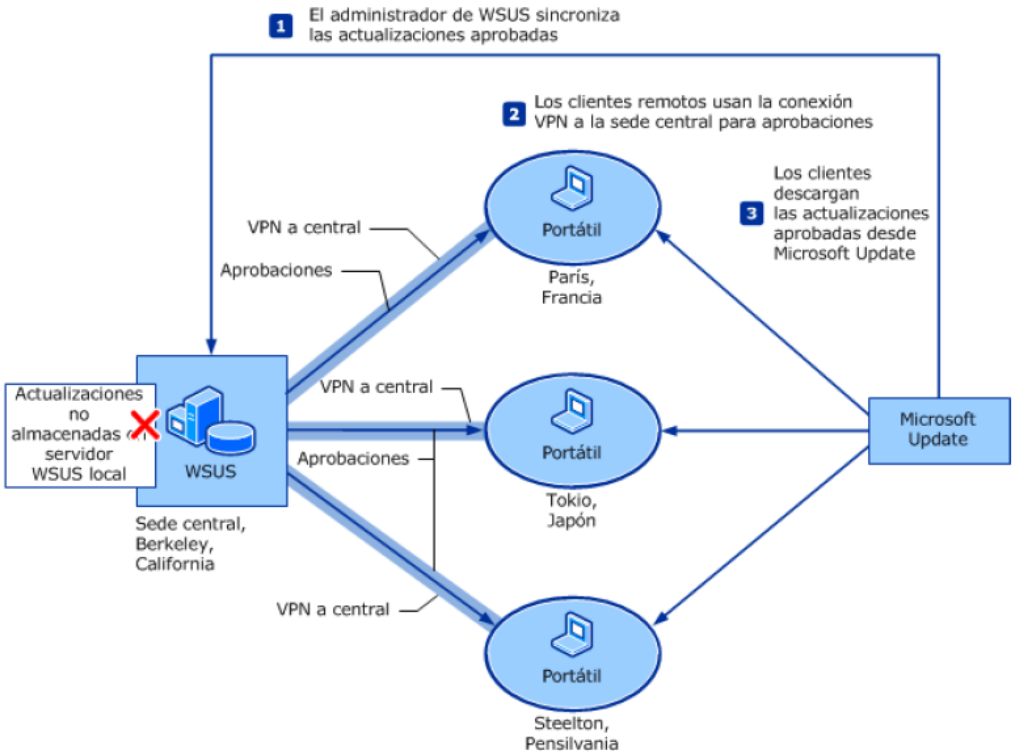
73. Cuando se sincronizan las actualizaciones con su servidor WSUS, los archivos de actualización y los metadatos se almacenan en dos ubicaciones independientes:
    - Los metadatos se almacenan en la base de datos de WSUS.
    - Los archivos de actualización se pueden almacenar en el servidor WSUS o en los servidores de Microsoft Update.
74. Si decide almacenar los archivos de actualización en el servidor WSUS, los equipos cliente descargarán actualizaciones aprobadas desde el servidor WSUS local. En caso contrario, los equipos clientes descargarán actualizaciones aprobadas directamente desde Microsoft Update.
75. La opción que más se adapte a su organización dependerá: del ancho de banda de red para conectarse a Internet, del ancho de banda de red de la intranet y de la disponibilidad de almacenamiento local.

8.1. ALMACENAMIENTO EN SERVIDOR WSUS LOCAL

76. El almacenamiento local de archivos de actualización es la opción predeterminada cuando instala y configura WSUS. Esta opción puede ahorrar ancho de banda en la conexión corporativa a Internet, porque los clientes descargan las actualizaciones directamente desde servidor WSUS local.
77. Esta opción requiere que el servidor tenga suficiente espacio en disco para almacenar todas las actualizaciones necesarias. Como mínimo, WSUS requiere de 20 GB para almacenar actualizaciones de forma local; sin embargo, se recomienda tener 30 GB en función de variables probadas.

8.2. ALMACENAMIENTO REMOTO EN SERVIDORES DE MICROSOFT UPDATE

78. Puede almacenar actualizaciones de forma remota en servidores de Microsoft Update. Esta opción es útil si la mayoría de los equipos cliente que se conectan al servidor WSUS cuentan con una conexión WAN lenta, pero se conectan a Internet con una conexión de ancho de banda alto.
79. El servidor WSUS raíz se sincroniza con Microsoft Update y recibe los metadatos de las actualizaciones. Una vez que se aprueban las actualizaciones, los equipos cliente las descargarán desde servidores de Microsoft Update.
80. Las sucursales recuperan actualizaciones aprobadas directamente desde servidores de Microsoft Update. Esto ahorra en disco y ancho de banda de red en la organización.
81. Esta opción de almacenamiento puede ofrecer descargas más rápidas para equipos cliente geográficamente distribuidos.



9. CONSIDERACIONES SOBRE EL RENDIMIENTO DE WSUS

9.1. CONFIGURACIONES DE RED

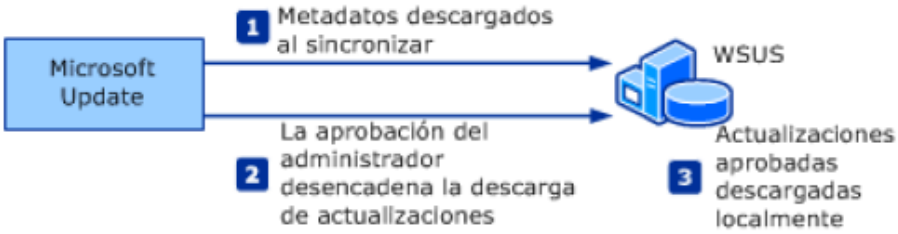
82. Para obtener un buen rendimiento en redes de WSUS, considere estas sugerencias:
    - Configure redes de WSUS en una topología de concentrada, en lugar de una topología jerárquica.

– Use el orden de máscara de red DNS para equipos cliente móviles y configure estos equipos para que obtengan actualizaciones del servidor WSUS local.

9.2. DESCARGA DIFERIDA

83. Se pueden aprobar actualizaciones y descargar los metadatos antes de descargar los archivos de actualización. Este método se denomina descarga diferida.

84. Al diferir descargas, una actualización se descarga solo después de haber sido aprobada. Se recomienda diferir descargas porque de esta manera se optimiza el ancho de banda de red y el espacio en disco.



85. En una jerarquía de servidores WSUS, se establece automáticamente la configuración de descarga diferida del servidor WSUS raíz en todos los servidores que siguen en la cadena.

86. Se puede configurar un servidor que precede en la cadena para que realice sincronizaciones completas e inmediatas, y después configurar un servidor que sigue en la cadena para que difiera las descargas.

87. Si implementa una jerarquía de servidores WSUS conectados, se recomienda que no anide servidores con profundidad.

88. Si habilita las descargas diferidas y un servidor que sigue en la cadena, solicita una actualización no aprobada en el servidor que precede, esta solicitud fuerza una descarga en el servidor que precede.

89. En una jerarquía profunda de servidores WSUS, se pueden producir demoras porque las actualizaciones se solicitan, se descargan y después se pasan a través de la jerarquía. De manera predeterminada, las descargas diferidas se habilitan cuando las actualizaciones se guardan de forma local.

9.3. FILTROS

90. WSUS permite filtrar sincronizadas las actualizaciones por idioma, producto y clasificación

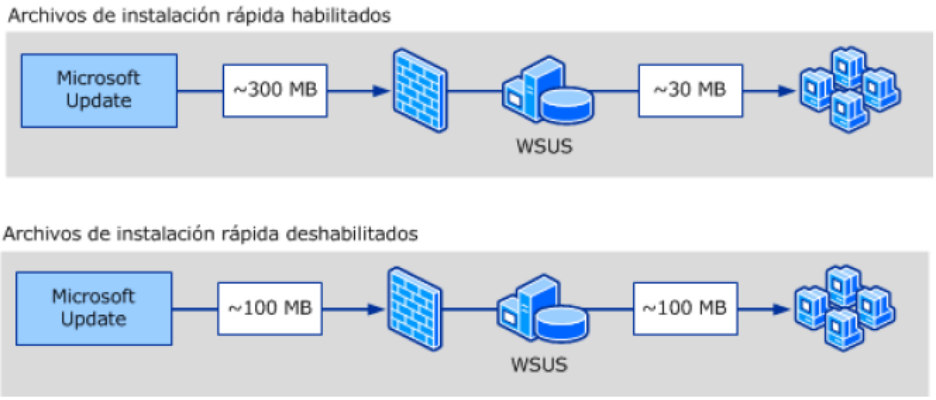
91. En una jerarquía de servidores WSUS, éste establece automáticamente las opciones de filtrado seleccionadas en el servidor WSUS raíz en todos los servidores que siguen en la cadena.

92. De manera predeterminada, los productos que se van actualizar son Windows y Office, y las clasificaciones predeterminadas son actualizaciones críticas, de seguridad y de definiciones.
93. Para conservar el ancho de banda y el espacio en disco, se recomienda limitar los idiomas a aquellos que realmente usa.

9.4. INSTALACIÓN

94. Las actualizaciones normalmente consisten en nuevas versiones de archivos que ya existen en un equipo que se está actualizando.
95. En un nivel binario, estos archivos existentes podrían no diferir demasiado de las versiones actualizadas.
96. Cuando se trabaja con archivos de instalación rápida, se identifica el número exacto de bytes entre versiones, se crea y se distribuye actualizaciones solo para esas diferencias y después combina el archivo existente con los bytes actualizados.
97. Esta característica se denomina *entrega de diferencia* porque descarga únicamente la diferencia (delta) entre dos versiones de un archivo.
98. Los archivos de instalación rápida son más grandes que las actualizaciones que se distribuyen a equipos cliente, porque un archivo de instalación rápida contiene todas las versiones posibles de cada archivo que se va a actualizar.
99. Puede usar archivos de instalación rápida para limitar el ancho de banda que se consume en la red local, ya que WSUS transmite solo el delta aplicable a una versión determinada de un componente actualizado.

Nota: Cuando se utilizan archivos de instalación rápida se requiere de un ancho de banda adicional entre el servidor WSUS, los servidores WSUS que preceden en la cadena y Microsoft Update, además de un espacio adicional en el disco local. De manera predeterminada, WSUS no usa archivos de instalación rápida.



Nota: Los tamaños de archivo en esta imagen solo se dan a modo ilustrativo. Cada actualización y tamaño de archivo de instalación rápida varían. El tamaño de cada actualización que se distribuye a equipos cliente depende del estado del equipo que se está actualizando.

100. No todas las actualizaciones son óptimas para su distribución con archivos de instalación rápida. Si selecciona esta opción, obtendrá archivos de instalación rápida para todas las actualizaciones. Si no almacena las actualizaciones de forma local, el agente de Windows Update decidirá que instalación es la más adecuada.

9.5. IMPLEMENTACIONES DE ACTUALIZACIONES GRANDES

101. Cuando implementa actualizaciones grandes (como Service Pack), puede evitar que se sature la red de la siguiente manera:

- Use el límite del Servicio de transferencia inteligente en segundo plano (BITS). Las limitaciones de ancho de banda de BITS se pueden controlar por hora del día, pero se aplican a todas las aplicaciones que usan BITS.
- Use el límite de Internet Information Services (IIS) para limitar uno o más servicios web.
- Use grupos de equipos para controlar el lanzamiento. Un equipo cliente se identifica a sí mismo como miembro de un determinado grupo de equipos, cuando envía información al servidor WSUS. El servidor WSUS usa esta información para determinar las actualizaciones que deben implementarse en ese equipo. Puede configurar varios grupos de equipos y aprobar secuencialmente grandes descargas de Service Packs para un subconjunto de estos grupos

9.6. SERVICIO DE TRANSFERENCIA INTELIGENTE EN SEGUNDO PLANO

102. WSUS usa el protocolo Servicio de transferencia inteligente en segundo plano (BITS) para todas sus tareas de transferencia de archivos. Esto incluye descargas a equipos cliente y sincronizaciones de servidores.

103. BITS habilita programas para que descarguen archivos usando ancho de banda de reserva. Este mantiene las transferencias de archivos cuando se producen desconexiones de red y se reinicia el equipo.

10. PLANEAR LA CONFIGURACIÓN DE ACTUALIZACIONES AUTOMÁTICAS

104. Puede planificar una fecha límite para aprobar actualizaciones en el servidor WSUS. La fecha límite hace que los equipos cliente instalen la actualización en un momento específico.

105. De manera predeterminada, el servicio actualizaciones automáticas sondea el servidor WSUS para detectar actualizaciones aprobadas, cada 22 horas. Si hay actualizaciones nuevas que necesitan actualizarse, estas se descargan. El

tiempo transcurrido entre cada ciclo de detección se puede manipular entre 1 y 22 horas.

106. Puede manipular las opciones de notificación de la siguiente manera:
    - Si actualizaciones automáticas se configura para que notifique al usuario cuando haya actualizaciones listas para instalarse, la notificación se envía al registro del sistema y al área de notificación del equipo cliente.
    - Cuando un usuario con credenciales apropiadas hace clic en el área de notificación, actualizaciones automáticas muestran las actualizaciones disponibles para instalar. El usuario debe hacer clic en Instalar para que la instalación comience.

Nota: Si se solicita el reinicio, el servicio actualizaciones automáticas no podrá detectar otras actualizaciones hasta que el equipo no reinicie.

107. Si este servicio se configura para instalar actualizaciones con una programación establecida, las actualizaciones aplicables se descargarán y se marcarán como listas para instalar.
108. En el día y hora programados, actualizaciones automáticas instala la actualización y reinicia el equipo (si es necesario), aun cuando ningún administrador local haya iniciado sesión.
109. Si un administrador inicia sesión en el equipo, éste debe reiniciarse, actualizaciones automáticas muestra una advertencia y una cuenta regresiva para el reinicio.
110. Si el equipo debe reiniciarse y cualquier usuario inició sesión, se muestra un cuadro de diálogo de cuenta regresiva similar, que advierte al usuario sobre el reinicio inminente. Puede manipular el reinicio del equipo con la directiva de grupo.
111. Una vez descargadas las actualizaciones nuevas, actualizaciones automáticas sondea la lista de paquetes aprobados en el servidor WSUS para confirmar que los paquetes que descargó, aún son válidos y están aprobados.

11. WSUS CON EL PROTOCOLO DE CAPA DE SOCKETS SEGUROS

112. Se puede usar el protocolo de Capa de sockets seguros (SSL) para ayudar a proteger la implementación de WSUS.
113. WSUS utiliza SSL para autenticar en el servidor WSUS los equipos cliente y los servidores WSUS que siguen en la cadena. WSUS también usa SSL para cifrar los metadatos de actualización.

Nota: Los clientes y los servidores que sigan la cadena y estén configurados para usar Seguridad de la capa de transporte (TLS) o HTTPS también deben configurarse para utilizar un nombre de dominio completo (FQDN) para su servidor WSUS que precede en la cadena.

114. WSUS usa SSL solo para los metadatos, no para los archivos de actualización. Se trata de la misma manera en que Microsoft Update distribuye actualizaciones.

115. Microsoft reduce el riesgo de enviar archivos de actualización a través de un canal no cifrado, mediante la firma de cada actualización.

116. Se calcula un hash y se envía junto con los metadatos de cada actualización. Cuando se descarga una actualización, WSUS comprueba la firma digital y el hash. Si la actualización ha cambiado, no se instala.

11.1. LIMITACIONES EN LAS IMPLEMENTACIONES SSL DE WSUS

117. Existen una serie de limitaciones que hay que tener en cuenta cuando use SSL para proteger una implementación de WSUS:

- El uso de SSL aumenta la carga de trabajo del servidor. Debe considerar una pérdida de rendimiento del 10 por ciento, debido al costo de cifrar todos los metadatos que se envían a través de la red.
- Si usa WSUS con una base de datos de SQL Server remota, la conexión entre el servidor WSUS y el servidor de la base de datos no está protegida con SSL. Si la conexión de la base de datos debe estar protegida, tenga en cuenta las siguientes recomendaciones:
  - Mueva la base de datos WSUS al servidor WSUS.
  - Mueva el servidor de la base de datos remota y el servidor WSUS a una red privada.
  - Implemente el protocolo de seguridad de Internet (IPsec) para ayudar el tráfico de la red.

11.2. CONFIGURACIÓN SSL EN EL SERVIDOR WSUS

118. WSUS requiere dos puertos para SSL, un puerto que use HTTPS para enviar metadatos cifrados y otro que utilice HTTP para enviar las actualizaciones.

119. Al configurar un servidor WSUS con SSL, hay que tener en cuenta algunas consideraciones:

- No se puede configurar el sitio web de WSUS que requiera SSL completamente, porque entonces debería cifrarse todo el tráfico al sitio de WSUS. WSUS sólo cifra los metadatos de actualización, por lo tanto, si un equipo intenta recuperar los archivos de actualización en el puerto HTTPS, se producirá un error en la transferencia.
- Debe requerir SSL solo para los siguientes objetos:
  - SimpleAuthWebService.

- DSSAuthWebService.
- ServerSyncWebService.
- APIRemoting30.
- ClienteWebService.

– Y no debe requerir SSL para los siguientes objetos:

- Content.
- Inventory.
- ReportingWebService.
- SelfUpdate.

– El certificado de la entidad de certificación (CA) debe importarse en la ubicación de la CA raíz de confianza del equipo local o el de Windows Server Update Services en los servidores WSUS que sigan la cadena.

– Si el certificado solo se importa en la ubicación de la entidad de certificación raíz de confianza del usuario local, el servidor WSUS que sigue en la cadena no se autenticará en el servidor que precede en la cadena.

– Debe importar el certificado en todos los equipos que se comuniquen con el servidor WSUS. El certificado debe importarse en la ubicación de la CA raíz de confianza del equipo local o el de Windows Server Update Service.

– Puede usar cualquier puerto para SSL. Sin embargo, el puerto que configure para SSL también determina el puerto que WSUS usa para enviar el tráfico HTTP sin cifrar.

– Debe volver a inicializar ClientServicingProxy si se cambia el nombre del servidor, la configuración SSL o el número del puerto.

11.3. CONFIGURACIÓN SSL EN LOS EQUIPOS CLIENTE

120. Debe incluir la dirección URL de un puerto seguro en el servidor WSUS. Dado que no se requiere SSL en el servidor, la única forma de asegurarse de que los equipos cliente pueden usar un canal de seguridad, es mediante una dirección URL que especifique HTTPS.

Nota: Si usa un puerto distinto del 443 para SSL, también debe incluir ese puerto en la dirección URL.

121. El certificado en un equipo cliente debe importarse en la ubicación de la CA raíz de confianza del equipo local o el del servidor WSUS. Si el certificado se importa solo en la ubicación de la CA raíz de confianza del usuario local, las actualizaciones automáticas no superarán la autenticación del servidor.

122. Los equipos cliente deben confiar en el certificado que se enlaza con el servidor WSUS. Según el tipo de certificado que se use, podría tener que configurar un servicio para permitir que los equipos confíen en el certificado que está enlazando al servidor WSUS.

Nota: La instalación del certificado en el equipo cliente, se hace mediante una GPO que se encuentra dentro de la unidad organizativa correspondiente, es decir, cada unidad organizativa, como por ejemplo "Equipos Windows 7 o "Equipos Windows 10", se le aplica una GPO donde se importará el certificado necesario para que la comunicación del equipo cliente con el servidor WSUS sea posible una vez configurado SSL en el servidor WSUS.

ANEXO A. PLANTILLAS DE SEGURIDAD DEL SERVIDOR DE WSUS DE WINDOWS SERVER 2012 R2

Para la aplicación de la presente guía se ha generado una plantilla de seguridad que deberá ser aplicada en la unidad organizativa donde se encuentren los servidores en donde se vaya a implementar el servicio WSUS de Windows Server 2012 R2.

Debe tener en cuenta el hecho de que, si implementa múltiples servicios sobre el servidor, se deberán aplicar todas aquellas políticas que le correspondiera de las guías CCN-STIC.

CCN-STIC-568 Incremental Servidor WSUS

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Asignación de derechos de usuario

Directiva	Configuración
Iniciar sesión como servicio	NT SERVICE\ALL SERVICES

Servicios del sistema

Servicio de transferencia inteligente en segundo plano (BITS) (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Servidor (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Administración remota de Windows (WS-Management) (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

WSusCertServer (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

WsusService (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Firewall de Windows con seguridad avanzada

Configuración global

Directiva	Configuración
Versión de directivas	2.22
Deshabilitar FTP con estado	No configurado
Deshabilitar PPTP con estado	No configurado
Exención de IPsec	No configurado
IPsec a través de NAT	No configurado
Codificación de clave previamente compartida	No configurado
Tiempo inactivo de SA	No configurado
Comprobación CRL fuerte	No configurado

Reglas de entrada

Nombre	Descripción
WSUS	

Esta regla puede incluir algunos elementos que la versión actual del módulo de informe GPMC no puede interpretar	
Habilitado	Verdadero
Programa	Cualquiera
Acción	Permitir
Seguridad	Requerir autenticación
Equipos autorizados	
Usuarios autorizados	
Protocolo	6
Puerto local	8530
Puerto remoto	Cualquiera
Configuración ICMP	Cualquiera
Ámbito local	Cualquiera
Ámbito remoto	Cualquiera
Perfil	Dominio
Tipo de interfaz de red	Todo

Servicio	Todos los programas y servicios
Permitir cruce seguro del perímetro	Falso
Grupo	

WSUS

Esta regla puede incluir algunos elementos que la versión actual del módulo de informe GPMC no puede interpretar	
Habilitado	Verdadero
Programa	Cualquiera
Acción	Permitir
Seguridad	Requerir autenticación
Equipos autorizados	
Usuarios autorizados	
Protocolo	6
Puerto local	8531
Puerto remoto	Cualquiera
Configuración ICMP	Cualquiera
Ámbito local	Cualquiera
Ámbito remoto	Cualquiera
Perfil	Dominio
Tipo de interfaz de red	Todo
Servicio	Todos los programas y servicios
Permitir cruce seguro del perímetro	Falso
Grupo	

ANEXO B. PLANTILLA DE SEGURIDAD DE CLIENTES WINDOWS 7 DEL SERVIDOR DE WSUS

Para que los clientes Windows puedan hacer uso de los servicios del servidor WSUS, es necesario aplicar la plantilla de seguridad para clientes Windows, que se incluye junto con esta guía. Esta plantilla habilita diferentes directivas de Windows Update, que son necesarias para obtener las actualizaciones del servidor WSUS. Además, esta guía habilita el servicio "WindowsUpdate", servicio que se deshabilita durante la aplicación de la guía CCN-STIC-522A.

CCN-STIC-568 Incremental Windows 10 - Clientes WSUS

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Windows Update (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de clave pública/Entidades de certificación raíz de confianza

Certificados

Emitido para	Emitido por	Fecha de expiración	Propósitos planteados
ejemplo.dominio.local	ejemplo.dominio.local	08/07/2017 2:00:00	Autenticación del servidor

Para obtener información adicional sobre la configuración individual, abra el Editor de objetos de directiva de grupo local.

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Componentes de Windows/Windows Update

Directiva	Configuración	Comentario
Configurar Actualizaciones	Habilitado	

automáticas

Configurar actualización automática:	3 - Descargar automáticamente y notificar instalación
Las siguientes opciones de configuración son necesarias y aplicables si se selecciona la opción 4.	
Instalar durante mantenimiento automático	Deshabilitado
Día de instalación programado:	0 - Todos los días
Hora de instalación programada:	16:00

Directiva	Configuración	Comentario
Especificar la ubicación del servicio Windows Update en la intranet	Habilitado	

Establecer el servicio de actualización de la intranet para detectar actualizaciones:	https://ejemplo.dominio.local:8531
Establecer el servidor de estadísticas de la intranet:	https://ejemplo.dominio.local:8531
(por ejemplo, http://IntranetUpd01)	

Directiva	Configuración	Comentario
Habilitar destinatarios del lado cliente	Habilitado	

Nombre de grupo de destino para este equipo	Clientes Windows 7

Directiva	Configuración	Comentario
No conectar con ninguna ubicación de Internet de Windows Update	Habilitado	

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO C. PLANTILLA DE SEGURIDAD DE CLIENTES WINDOWS 10 DEL SERVIDOR DE WSUS

Para que los clientes Windows puedan hacer uso de los servicios del servidor WSUS es necesario aplicar la plantilla de seguridad para clientes Windows que se incluye junto con esta guía. Esta plantilla habilita diferentes directivas de Windows Update que son necesarias para obtener las actualizaciones del servidor WSUS. Además, esta guía habilita el servicio "WindowsUpdate", servicio que se deshabilita durante la aplicación de la guía CCN-STIC-599A.

CCN-STIC-568 Incremental Windows 10 - Clientes WSUS

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Windows Update (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de clave pública/Entidades de certificación raíz de confianza

Certificados

Emitido para	Emitido por	Fecha de expiración	Propósitos planteados
ejemplo.dominio.local	ejemplo.dominio.local	08/07/2017 2:00:00	Autenticación del servidor

Para obtener información adicional sobre la configuración individual, abra el Editor de objetos de directiva de grupo local.

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Componentes de Windows/Windows Update

Directiva	Configuración	Comentario
Configurar Actualizaciones	Habilitado	

automáticas

Configurar actualización automática:	3 - Descargar automáticamente y notificar instalación
Las siguientes opciones de configuración son necesarias y aplicables si se selecciona la opción 4.	
Instalar durante mantenimiento automático	Deshabilitado
Día de instalación programado:	0 - Todos los días
Hora de instalación programada:	03:00

Directiva	Configuración	Comentario
Especificar la ubicación del servicio Windows Update en la intranet	Habilitado	

Establecer el servicio de actualización de la intranet para detectar actualizaciones:	https://ejemplo.dominio.local:8531
Establecer el servidor de estadísticas de la intranet:	https://ejemplo.dominio.local:8531
(por ejemplo, http://IntranetUpd01)	

Directiva	Configuración	Comentario
Habilitar destinatarios del lado cliente	Habilitado	

Nombre de grupo de destino para este equipo	Clientes Windows 10

Directiva	Configuración	Comentario
No conectar con ninguna ubicación de Internet de Windows Update	Habilitado	

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO D. PLANTILLA DE SEGURIDAD DE CLIENTES WINDOWS SERVER 2012 R2 DEL SERVIDOR DE WSUS

Para que los clientes Windows Server puedan hacer uso de los servicios del servidor WSUS es necesario aplicar la plantilla de seguridad para clientes Windows Server que se incluye junto con esta guía. Esta plantilla habilita diferentes directivas de Windows Update que son necesarias para obtener las actualizaciones del servidor WSUS. Además, esta guía habilita el servicio "WindowsUpdate", servicio que se deshabilita durante la aplicación de la guía CCN-STIC-560A.

CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Windows Update (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SYSTEM	Control total

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de clave pública/Entidades de certificación raíz de confianza

Certificados

Emitido para	Emitido por	Fecha de expiración	Propósitos planteados
ejemplo.dominio.local	ejemplo.dominio.local	08/07/2017 2:00:00	Autenticación del servidor

Para obtener información adicional sobre la configuración individual, abra el Editor de objetos de directiva de grupo local.

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Componentes de Windows/Windows Update

Directiva	Configuración	Comentario
Configurar Actualizaciones	Habilitado	

automáticas

Configurar actualización automática:	3 - Descargar automáticamente y notificar instalación
Las siguientes opciones de configuración son necesarias y aplicables si se selecciona la opción 4.	
Instalar durante mantenimiento automático	Deshabilitado
Día de instalación programado:	0 - Todos los días
Hora de instalación programada:	03:00

Directiva	Configuración	Comentario
Especificar la ubicación del servicio Windows Update en la intranet	Habilitado	

Establecer el servicio de actualización de la intranet para detectar actualizaciones:	https://ejemplo.dominio.local:8531
Establecer el servidor de estadísticas de la intranet:	https://ejemplo.dominio.local:8531
(por ejemplo, http://IntranetUpd01)	

Directiva	Configuración	Comentario
Habilitar destinatarios del lado cliente	Habilitado	

Nombre de grupo de destino para este equipo	Clientes Servidores 2012 r2

Directiva	Configuración	Comentario
No conectar con ninguna ubicación de Internet de Windows Update	Habilitado	

Configuración del usuario (habilitada)

Configuración no definida.

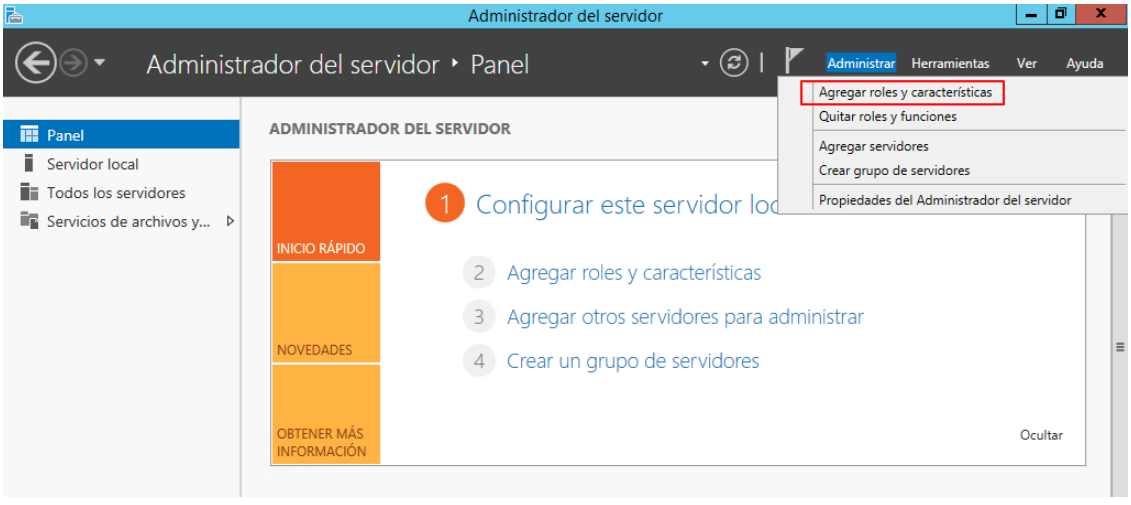
ANEXO E. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR DE DESCARGA DE ACTUALIZACIONES DE MICROSOFT UPDATE.

En el presente anexo, se va a detallar la instalación y la configuración de un servidor Windows Server 2012 R2 con el rol de Windows Server Update Services (WSUS) instalado. Este servidor se encargará de realizar la descarga de actualizaciones para luego exportarlas a los diferentes servidores WSUS que disponga en su infraestructura. Para ello, será muy importante que este servidor se encuentre fuera de la red clasificada, ya que este mismo tendrá acceso a Internet para poder descargar las actualizaciones.

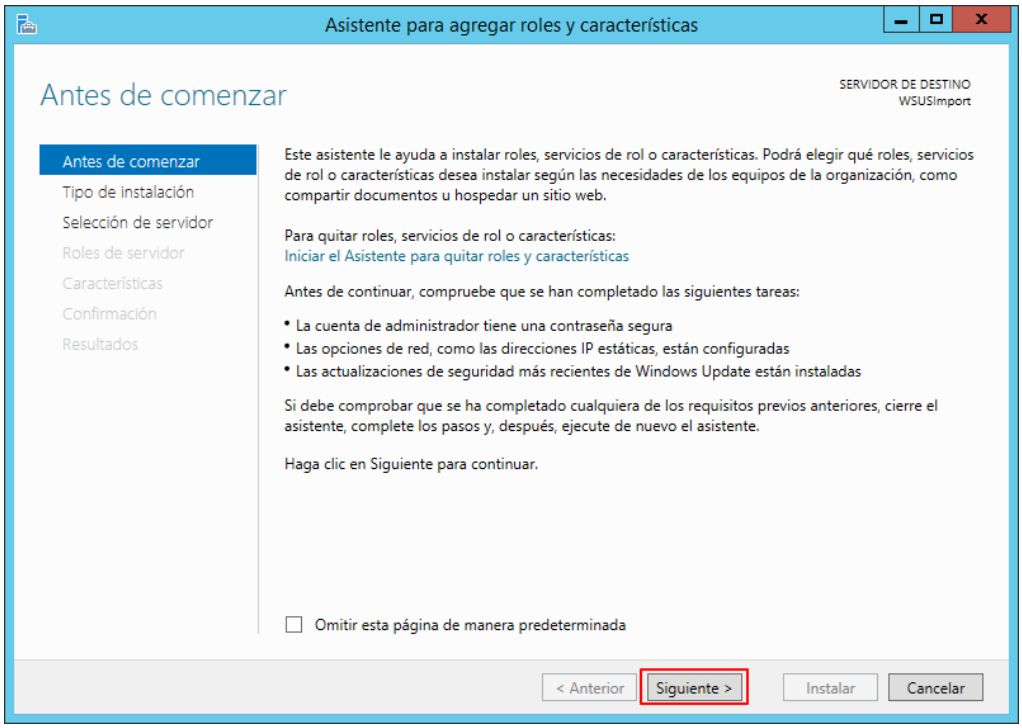
1. INSTALACIÓN DE WINDOWS SERVER UPDATE SERVICES (WSUS)

Los pasos que se describen a continuación se realizarán en un Windows Server 2012 R2 Standalone donde se desplegará el servidor de descarga de actualizaciones. Sólo es necesario realizar este procedimiento una vez.

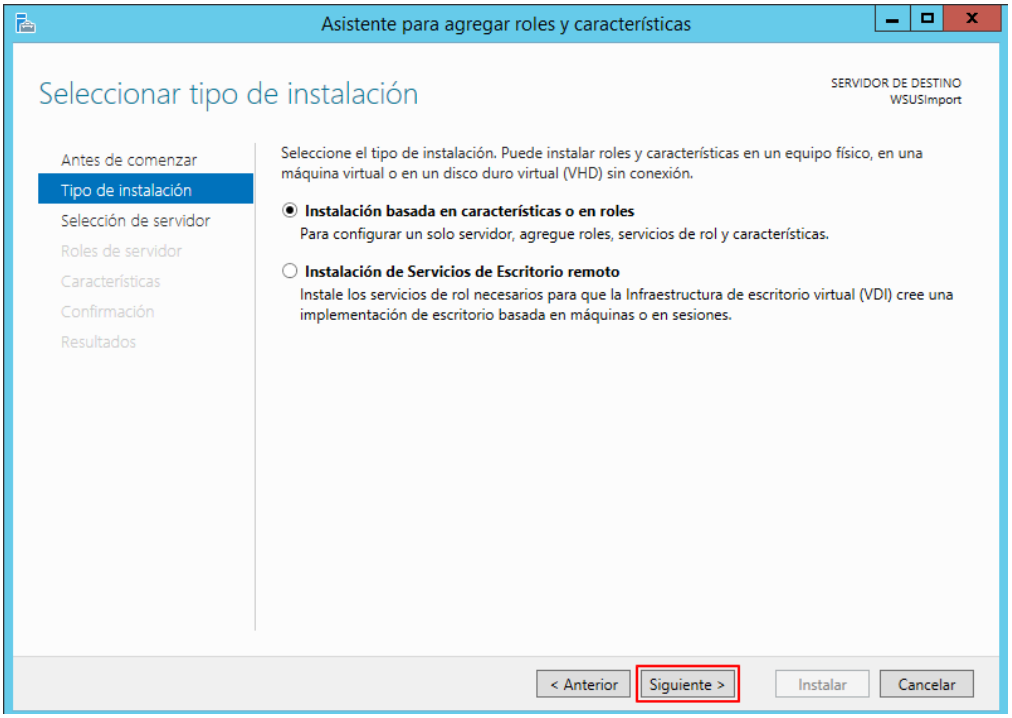
Nota: Es un requisito indispensable, que el equipo donde se vaya a instalar el rol de WSUS, contenga una partición o un disco duro nuevo con el objetivo de almacenar la base de datos que va a utilizar WSUS. Es muy importante que la letra de la unidad de la partición o del disco duro se le asigne la letra D:\. Para realizar esta operativa puede ser de gran ayuda la consola de "Administración de discos".

Paso	Descripción
1.	Inicie sesión en el servidor dónde vaya a instalar el rol de WSUS y, por lo tanto, vaya a cumplir con la descarga de actualizaciones.
2.	Debe iniciar sesión con una cuenta que sea Administrador local, ya que este servidor no estará unido a un dominio.
3.	A continuación, se va a instalar el rol de Windows Server Update Services (WSUS). Para ello diríjase a "**Inicio > Administrador del servidor > Administrar > Agregar roles y características**". 

Paso	Descripción
4.	Se iniciará el “Asistente para agregar roles y características”, en la página de “antes de comenzar” pulse “**Siguiente>**”.

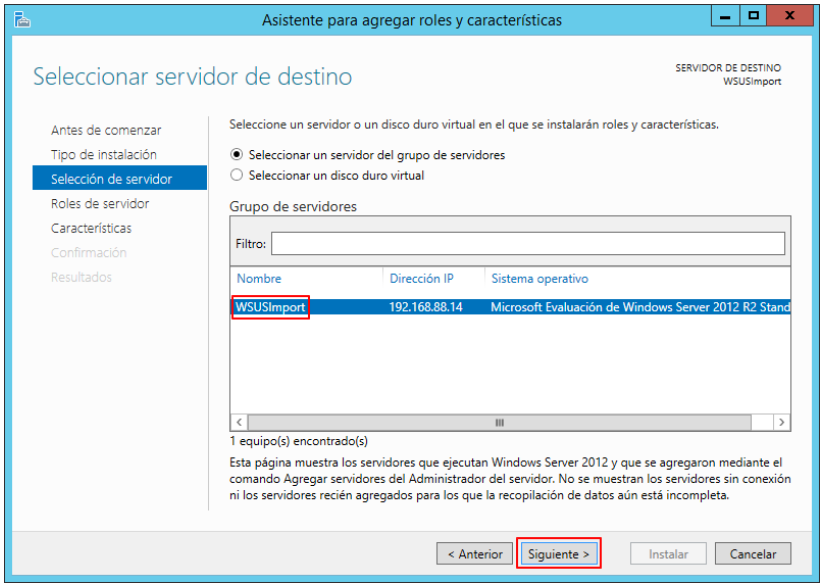


5.	En la página “Tipo de instalación” se dejará marcada la opción que viene por defecto “Instalación basada en características o en roles”, pulse “**Siguiente>**” para continuar.



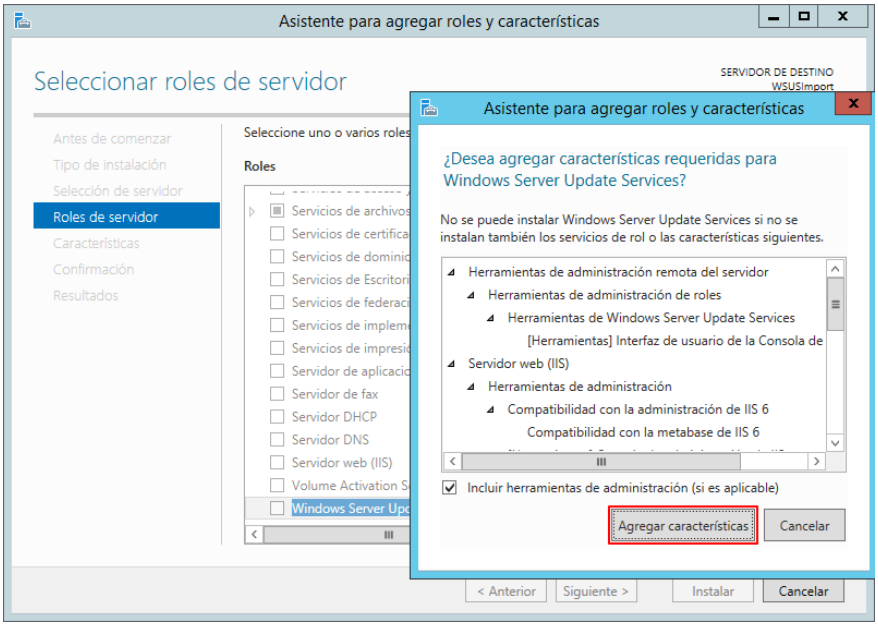
Paso	Descripción

6. A continuación, se selecciona el servidor de destino que en este caso es el propio servidor. Deje habilitado la opción por defecto "**Seleccionar un servidor del grupo de servidores**" y pulse "**Siguiente>**".



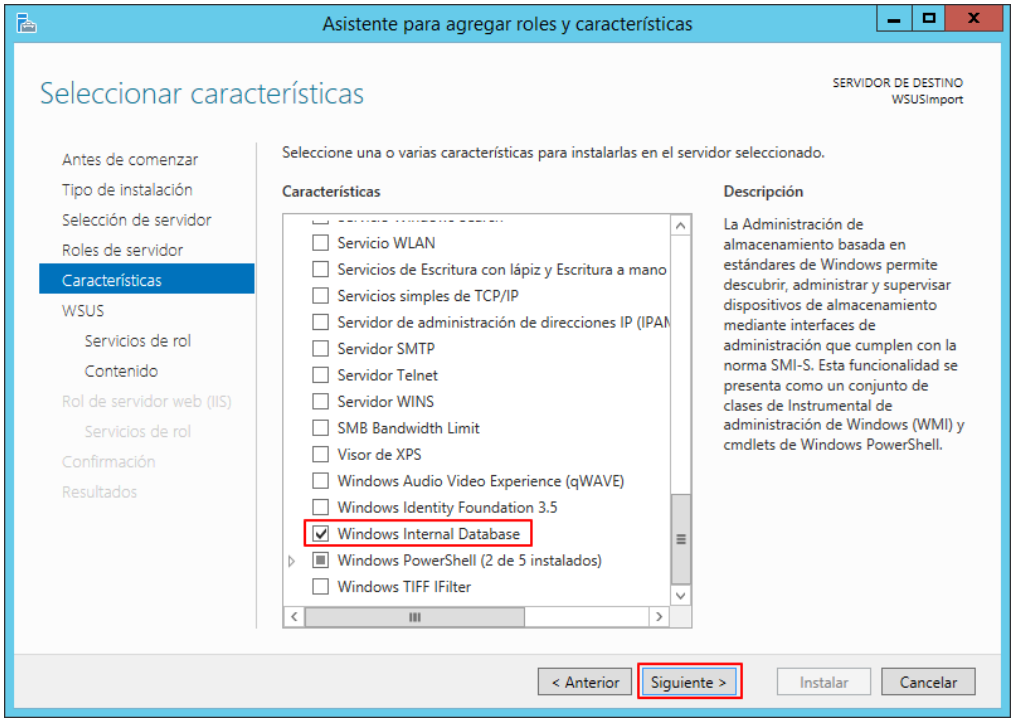
Nota: Deberá asegurarse que esté en la ventana de "grupo de servidores" marcando el servidor dónde se va a realizar la instalación de Windows Server Update Services (WSUS). En este ejemplo, se ha utilizado el servidor con el nombre WSUSImport.

7. En la página de "Seleccionar roles de servidor" se deberá habilitar el rol de "**Windows Server Update Services**", seguidamente se abrirá una venta para agregar las características necesarias, pulse en "**Agregar características**". En este momento, se habilitarán las características necesarias, a continuación, pulse en "**Siguiente>**".

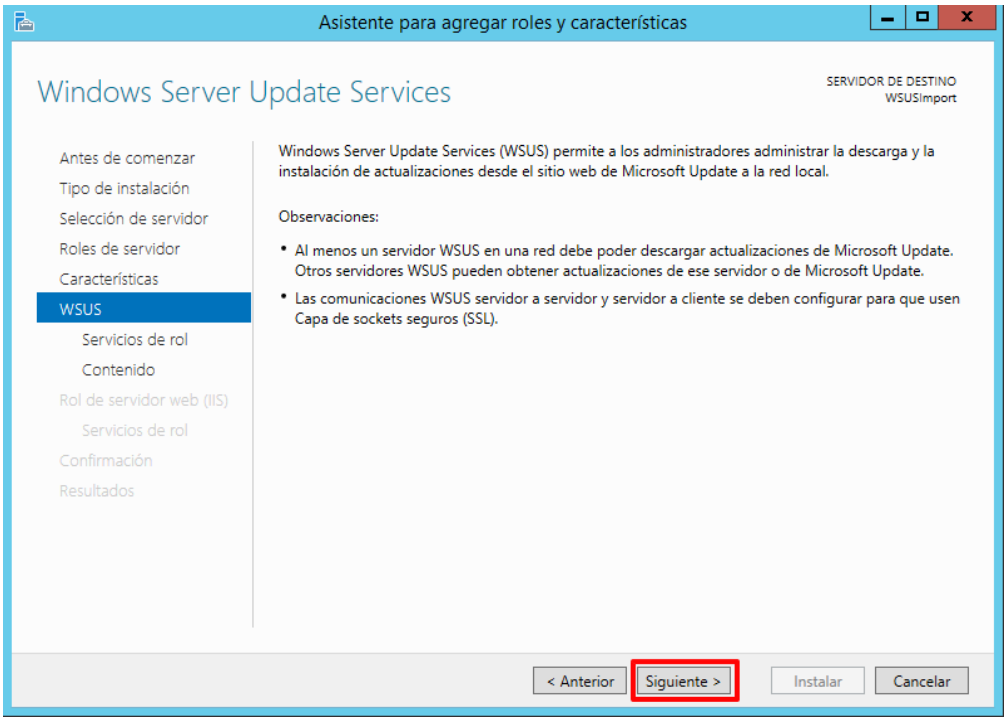


Paso	Descripción

8. En la página de “Seleccionar características” dejará seleccionado todo como se encuentra por defecto, automáticamente el asistente ha seleccionado las características requeridas por WSUS, pulse “Siguiente>” para continuar.

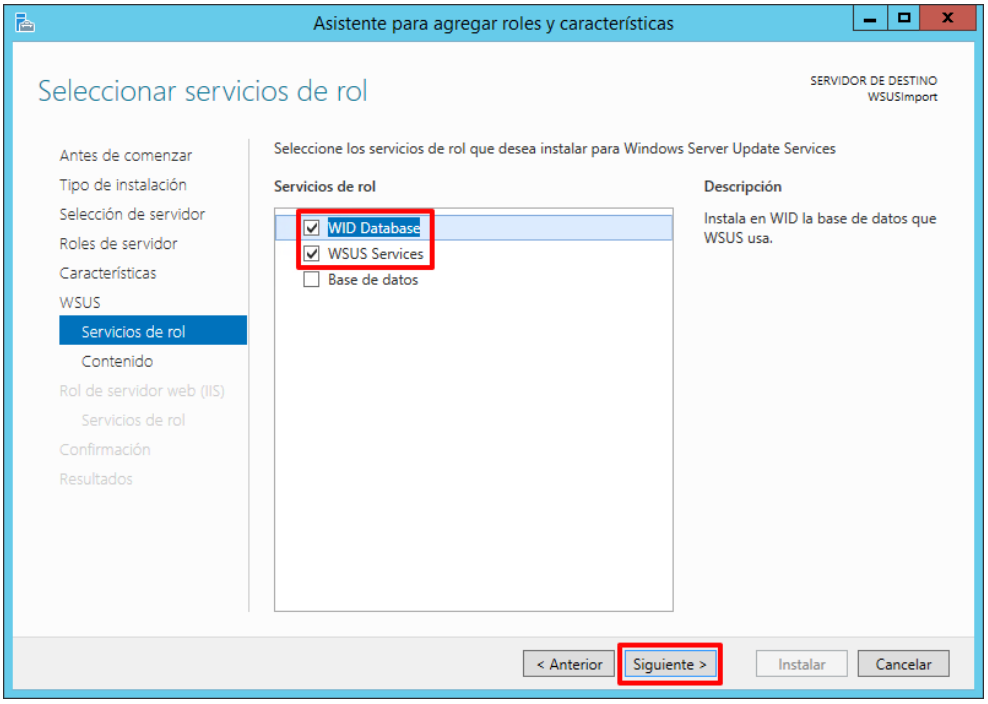


9. En la siguiente página (WSUS), deberá configurar algunos requisitos para poder instalar el rol en el servidor. Para ello pulse en “**Siguiente>**”.

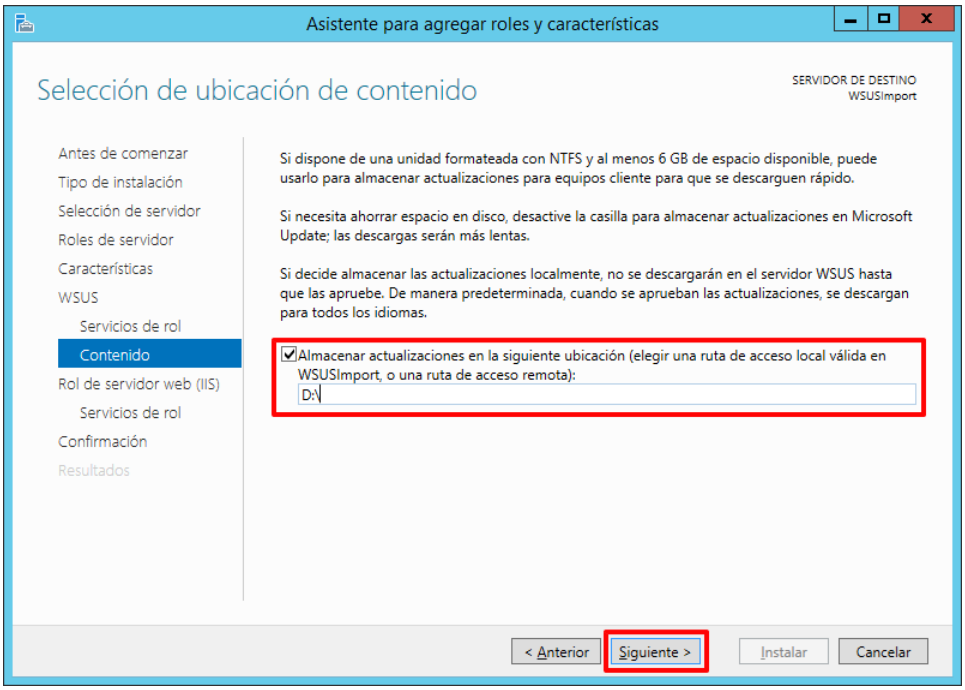


Paso	Descripción

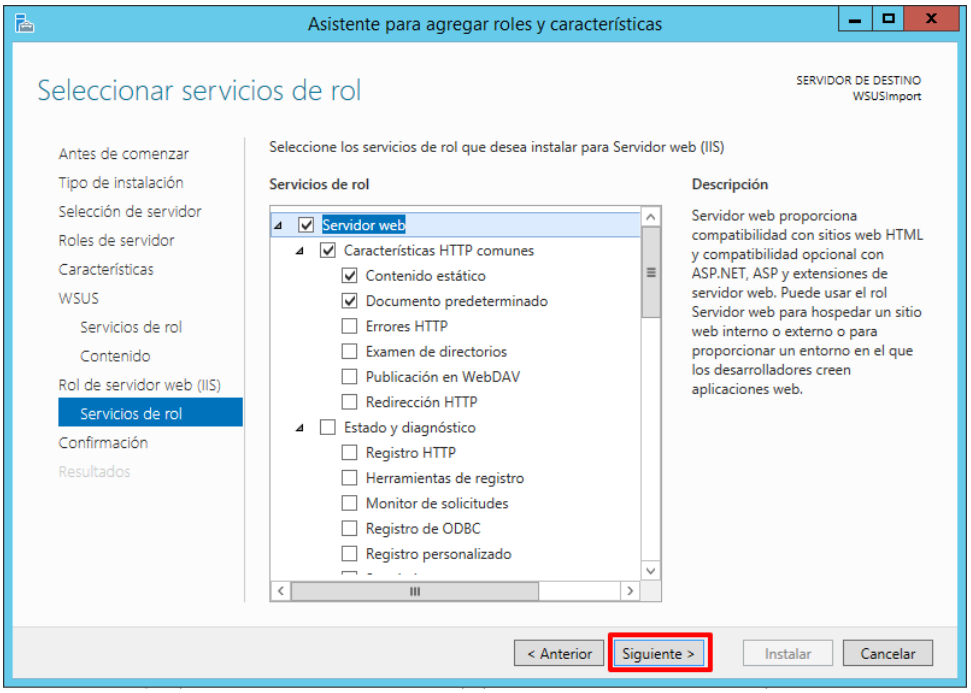
10. Seleccione los servicios del rol WSUS, para ello deje marcadas las dos opciones que se muestra a continuación, WID Database y WSUS Services. Después, pulse en "**Siguiente>**".



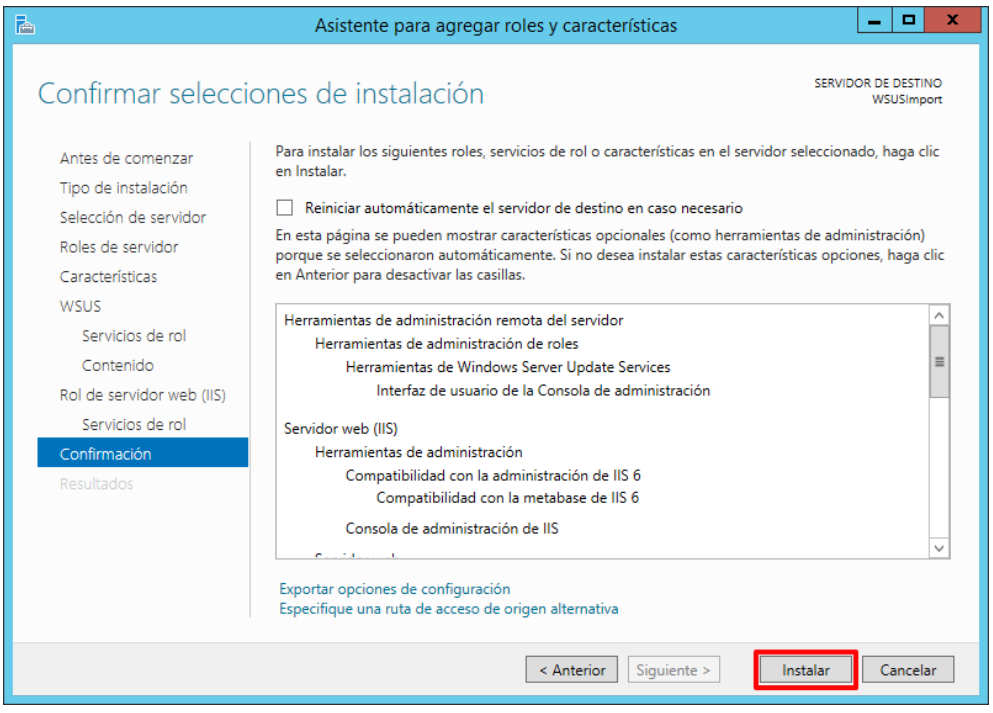
11. En la página "Selección de ubicación de contenido" debe indicar dónde se va almacenar las actualizaciones que el propio WSUS va a descargar. Para ello debe introducir la ubicación correcta. Como ya se ha comentado anteriormente debe de ubicarse en "**D:\".** Pulse "**Siguiente>**".



Paso	Descripción
12.	Sobre la página de “Rol de servidor web (IIS)”, pulse “**Siguiente>**”.
13.	En la siguiente página se deberá seleccionar los servicios del rol de IIS, deje marcados lo que viene por defecto, a continuación, pulse “**Siguiente>**”.

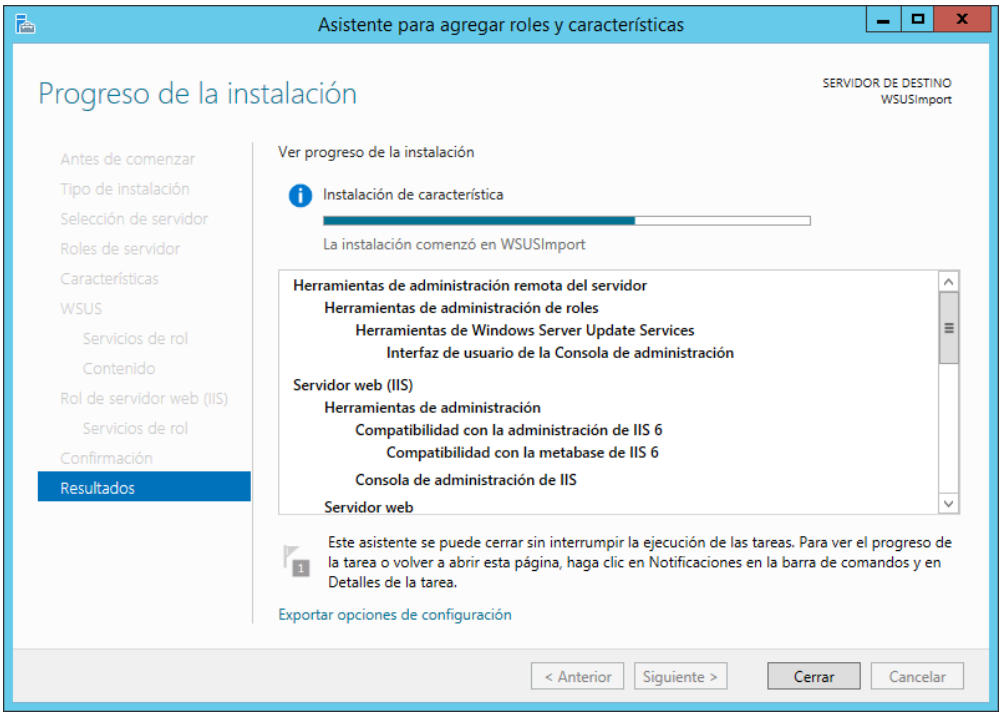


14.	Para terminar con el asistente y que comience la instalación se va a confirmar la configuración que se acaba de realizar, para ello pulse en “**Instalar>**”.

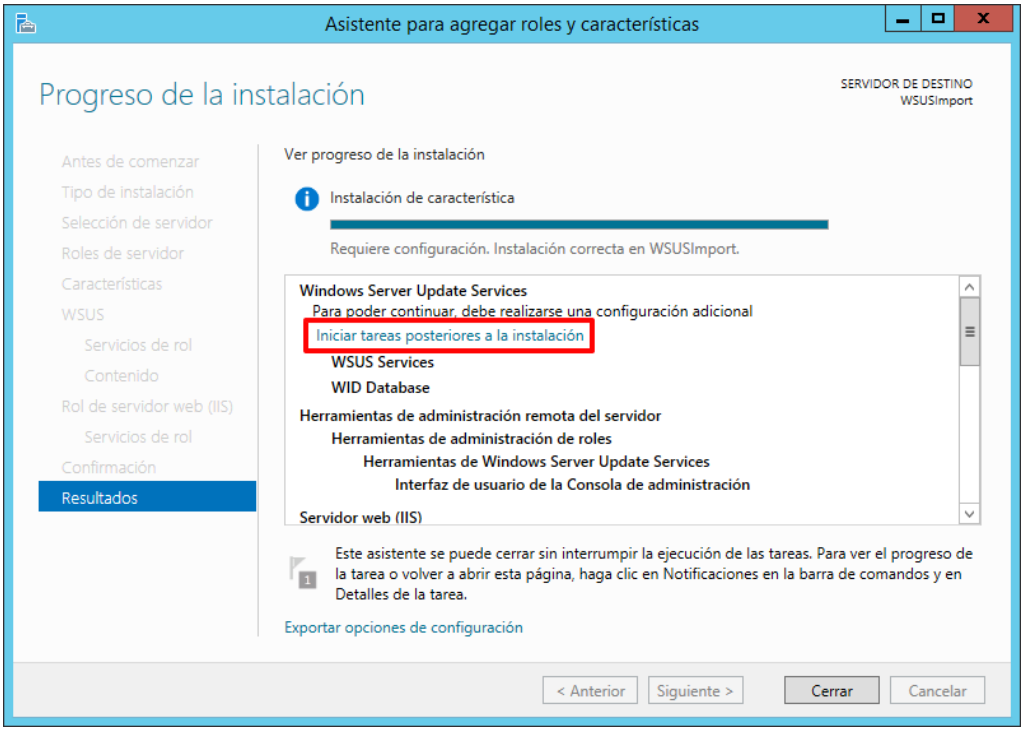


Paso	Descripción

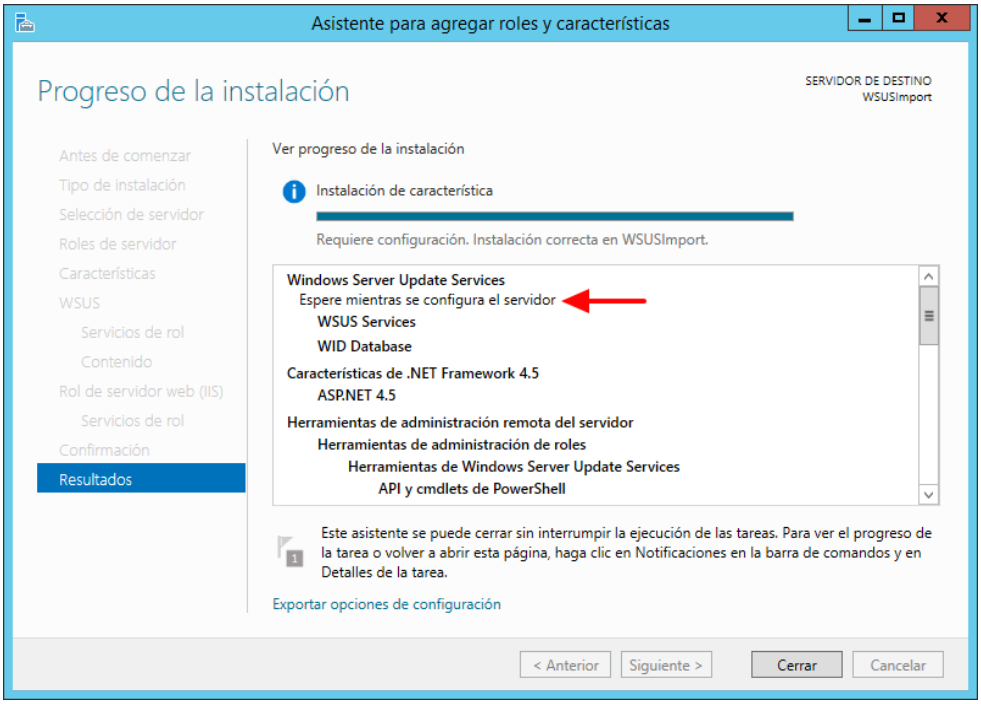
15. Automáticamente comenzará la instalación.



16. Una vez que el asistente termine con la instalación, deberá lanzar la instalación de tareas posteriores, para ello pulse en "**Iniciar tareas posteriores a la instalación**".



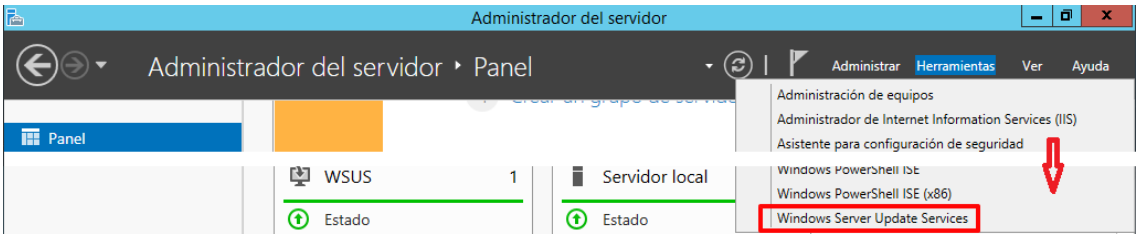
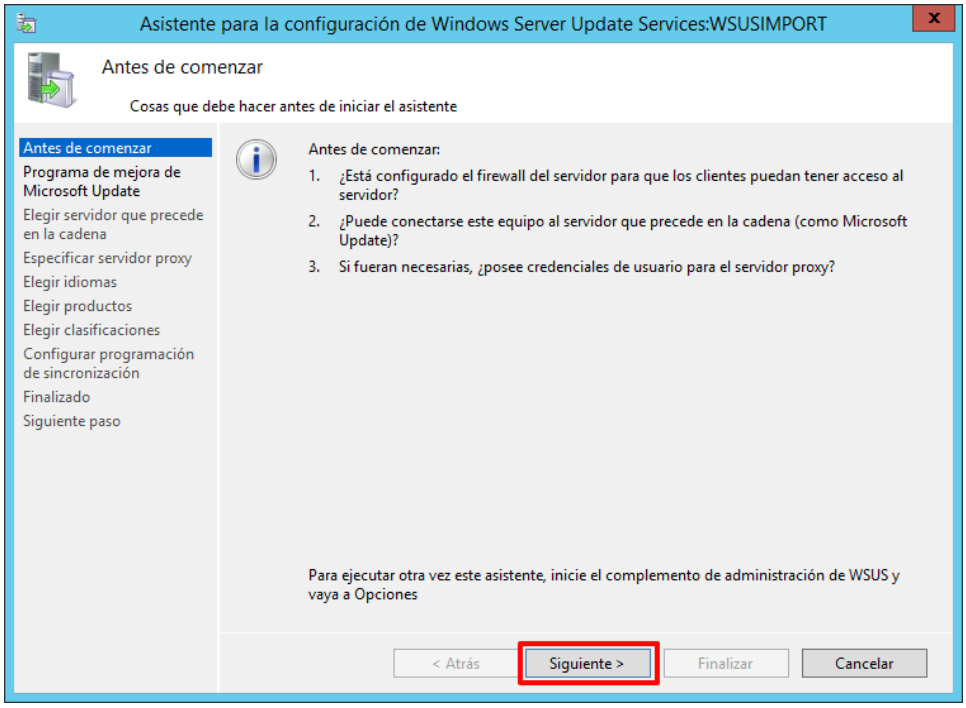
Paso	Descripción
17.	Espere hasta que termine la configuración de las tareas posteriores, el mensaje cambiará a "Configuración completada correctamente", cuando esto ocurra, puede cerrar la venta de instalación.

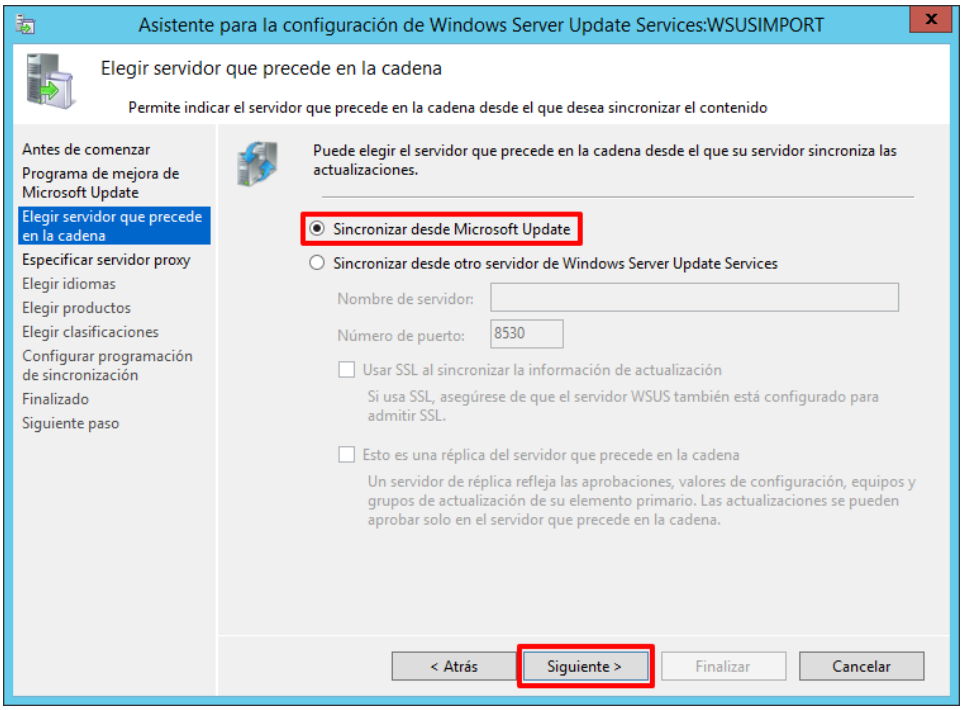
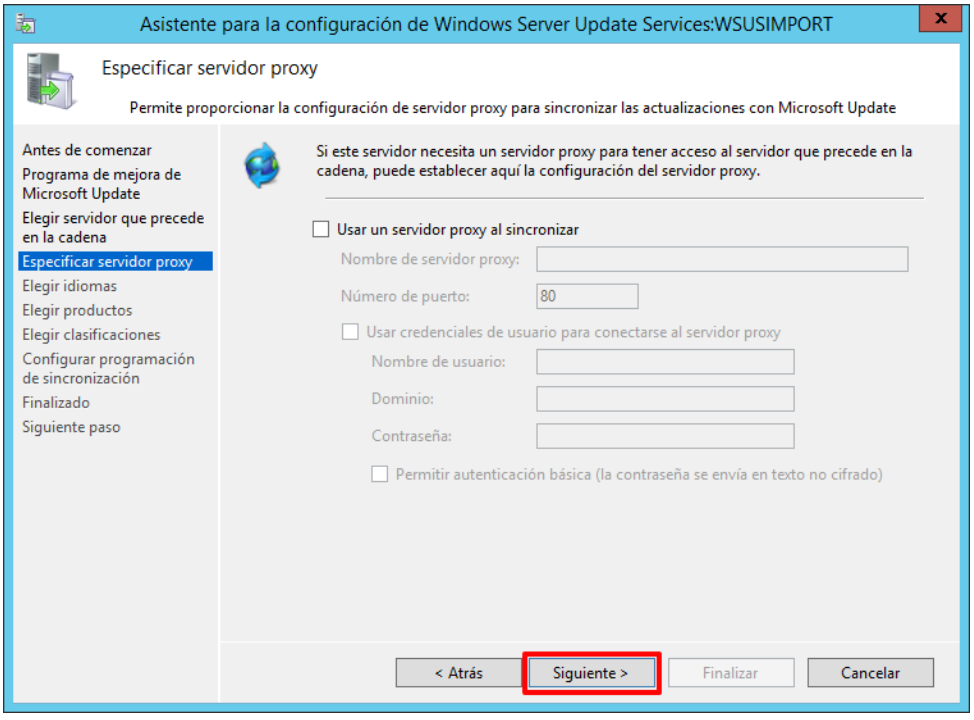


2. CONFIGURACIÓN DE WINDOWS SERVER UPDATE SERVICES (WSUS)

Una vez que tenga instalado correctamente el rol de Windows Server Update Services (WSUS) en el servidor apropiado, se va a realizar la configuración necesaria para que el rol cumpla con los objetivos correctamente y pueda realizar la descarga de actualizaciones para hacer la exportación adecuada a los diferentes servidores WSUS que estén dentro de la red clasificada.

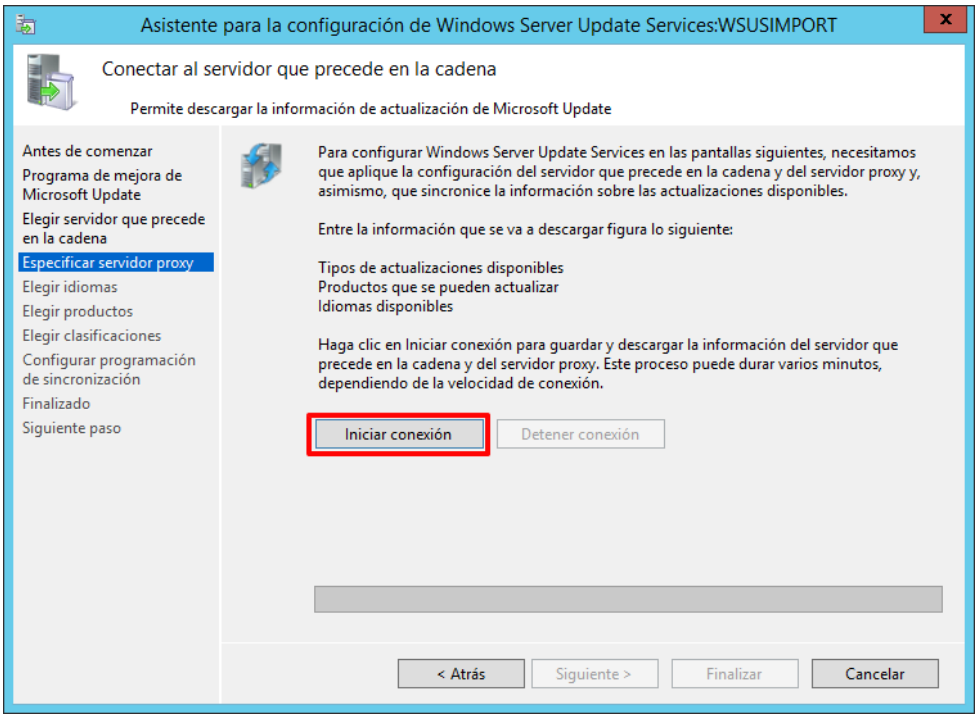
La configuración que se realiza en la presente guía es un ejemplo de una configuración sencilla de WSUS, se comentarán las diferentes posibilidades que existen en la configuración. En su caso deberá elegir la configuración que más se adecue a su infraestructura.

Paso	Descripción
18.	Para comenzar con la configuración de WSUS, deberá dirigirse a "**Inicio > Administrador del servidor > Herramientas > Windows Server Update Services**", pinche sobre él para que se abra el asistente de WSUS. 
19.	En la primera página del asistente pulse sobre "**Siguiente>**" para continuar con la configuración. Puede leer las preguntas que le propone el asistente para ver si tiene algún inconveniente. 
20.	En la página de "**Programa de mejora de Microsoft Update**" puede decidir si colaborar o no con el programa de Microsoft Update, esto es elección suya. Pulse "Siguiente>" para continuar.

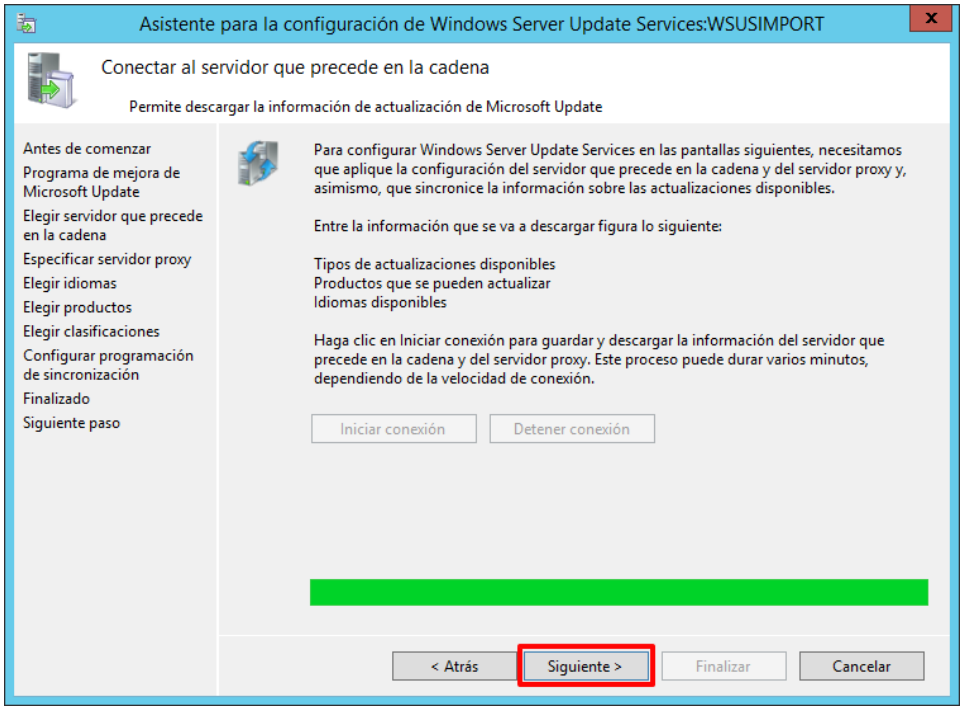
Paso	Descripción
21.	A continuación, debe indicar desde dónde va a sincronizar las actualizaciones el servidor WSUS, para ello marque la opción de "**Sincronizar desde Microsoft Update**", seguidamente pulse "**Siguiente>**". 
22.	En la siguiente página debe especificar si va a usar un servidor proxy para realizar la sincronización, en este caso, la guía no se implementa con un servidor proxy. Pulse "Siguiente>" sin marcar la casilla. 

Paso	Descripción
23.	Para terminar, deberá realizar una conexión con Microsoft Update, para ello pulse sobre el botón "**Iniciar conexión**" y espere a que termine.

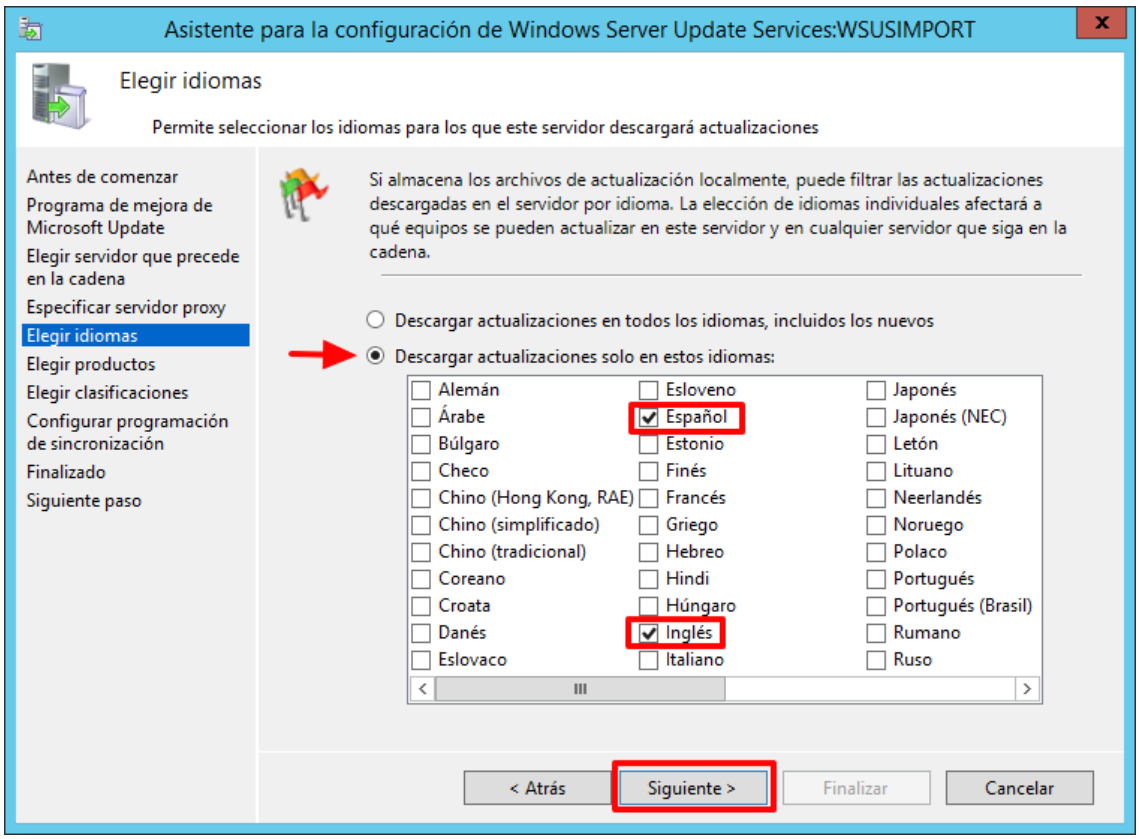
Nota: Esto puede tardar varios minutos, va a depender de la velocidad de conexión.



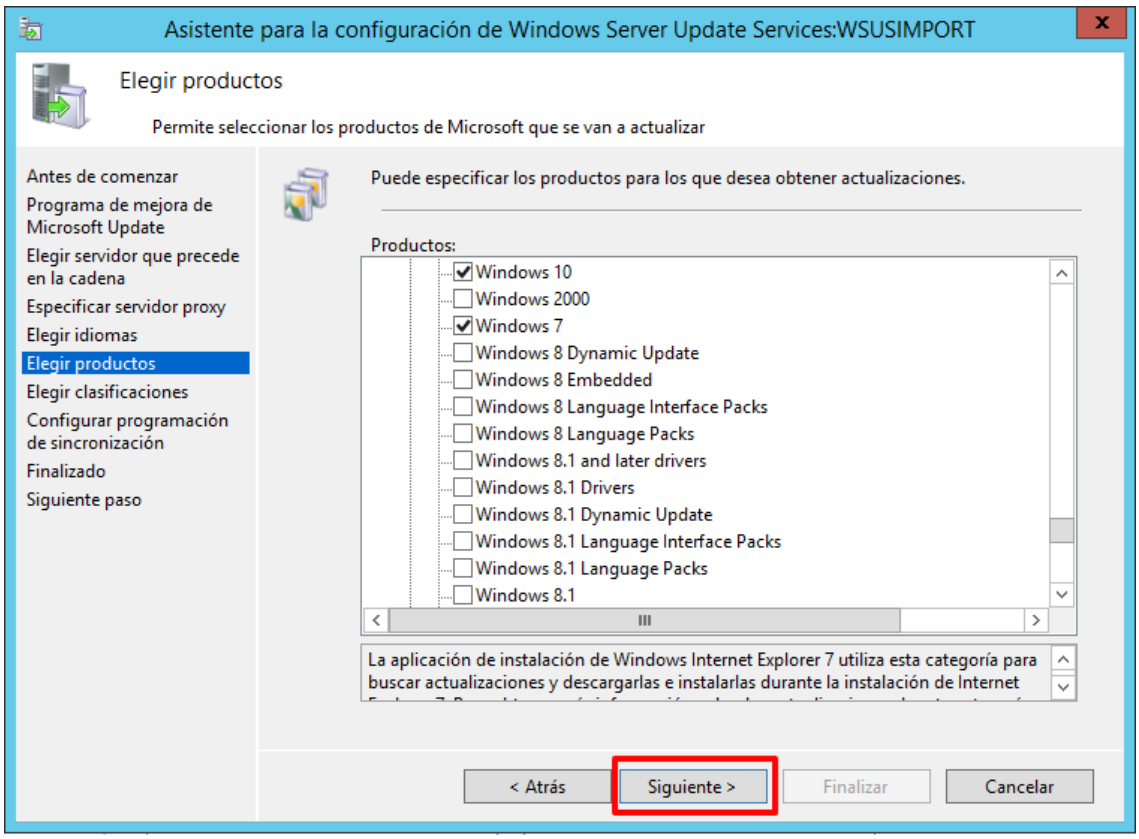
24.	Cuando termine de conectar con Microsoft Update, la barra cambiará a un color verde, esto confirmará que la conexión ha sido correcta, seguidamente pulse sobre **"Siguiente>".**



Paso	Descripción
25.	Seguidamente debe elegir el idioma de las actualizaciones que se van a descargar. Para esta guía se seleccionan los idiomas de inglés y español. Cuando haya seleccionado los idiomas pulse **"Siguiente>"**.

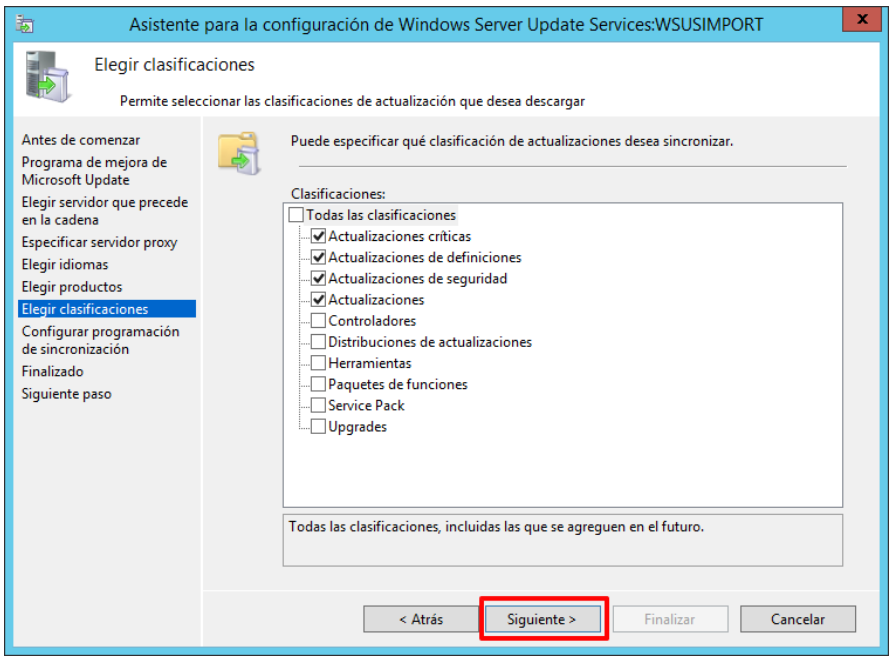


Paso	Descripción
26.	A continuación, debe seleccionar los productos de Microsoft que se van actualizar. Deberá seleccionar los que más se ajusten a sus necesidades. Una vez que haya seleccionado los productos, pulse **"Siguiente>".**



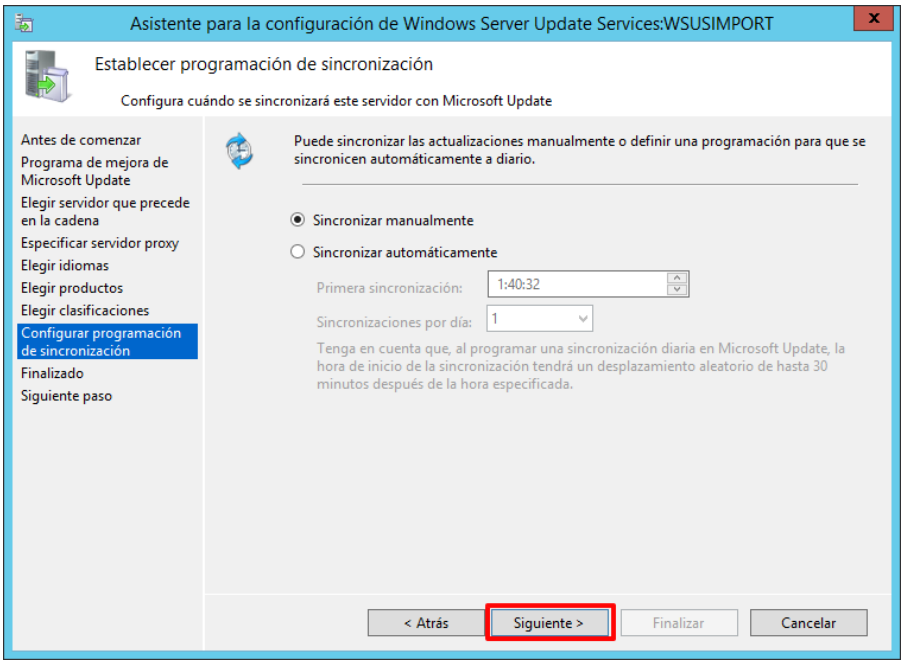
Nota: Usted deberá seleccionar todos los sistemas operativos y servicios que tenga integrados en su red clasificada y sigan la serie 500 de las guías CCN-STIC.
Como ejemplo en esta guía, se han seleccionado los productos de Windows 7, Windows 10 y Windows Server 2012 R2, ya que son los clientes que se van a utilizar para la implementación de la misma.

Paso	Descripción
27.	Seleccione la pestaña **“Actualizaciones”** y seguidamente pulse **“Siguiente>”**.



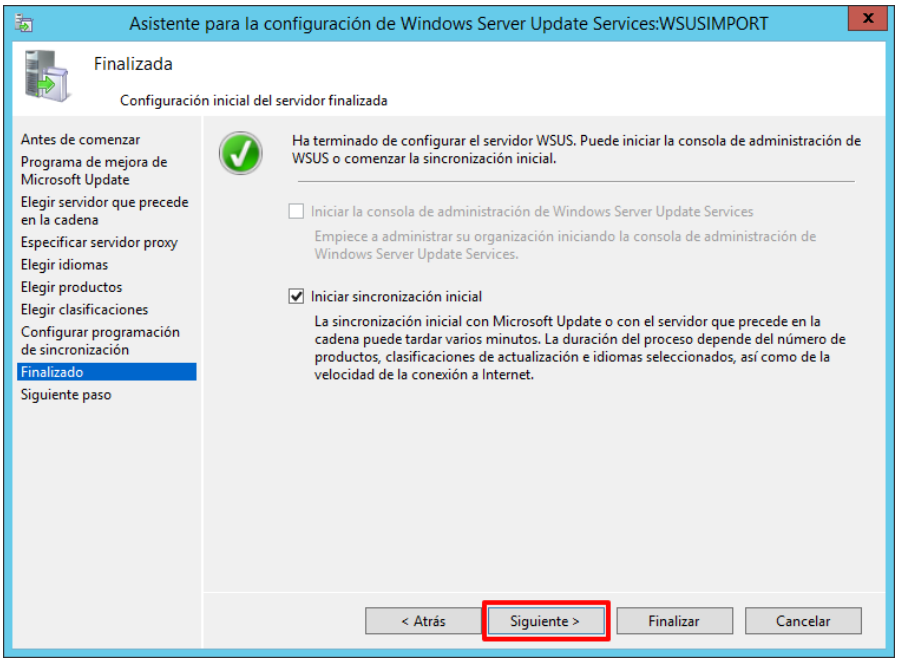
Nota: Usted deberá elegir las clasificaciones que más se ajusten a su red clasificada.
Como ejemplo de esta guía, se ha añadió la clasificación “Actualizaciones” a las que ya vienen por defecto marcadas en el asistente.

28.	En la página “Establecer programación de sincronización” deberá seleccionar si la descarga de actualizaciones debe ser “Manual” o “Automática”. Seleccione **“Sincronización Manual”** y pulse **“Siguiente>”**.



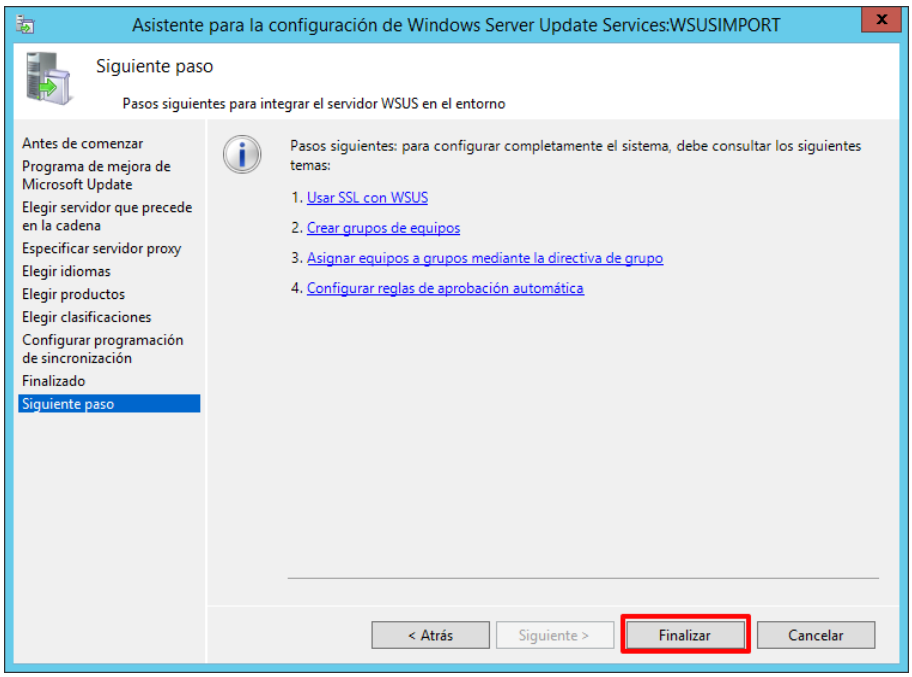
Paso	Descripción

29. Para finalizar, deberá realizar una sincronización inicial, para ello marque la casilla "**Iniciar sincronización inicial**" y pulse "**Siguiente>**".



Nota: Para que realice una sincronización inicial, es requisito indispensable que el equipo ya esté configurado con conexión a Internet. Si no lo está, podrá realizar este paso más adelante.

30. Pulse **"Finalizar"** para cerrar el asistente de configuración.



Nota: Una vez finalice el asistente, se abrirá automáticamente la consola de administración de WSUS.

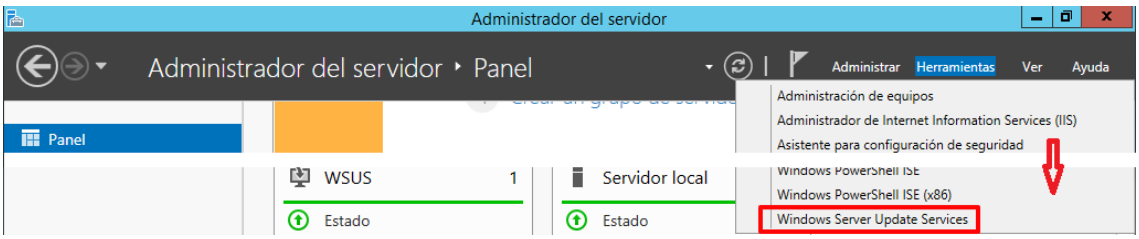
3. DESCARGA Y EXPORTACIÓN DE ACTUALIZACIONES DESDE WINDOWS SERVER UPDATE SERVICES

En este punto, se detalla cómo se realiza la descarga de las actualizaciones para los productos que se han seleccionado en el punto anterior. Estas actualizaciones se almacenan en la base de datos establecida en los pasos anteriores, en este caso D:\WsusContent.

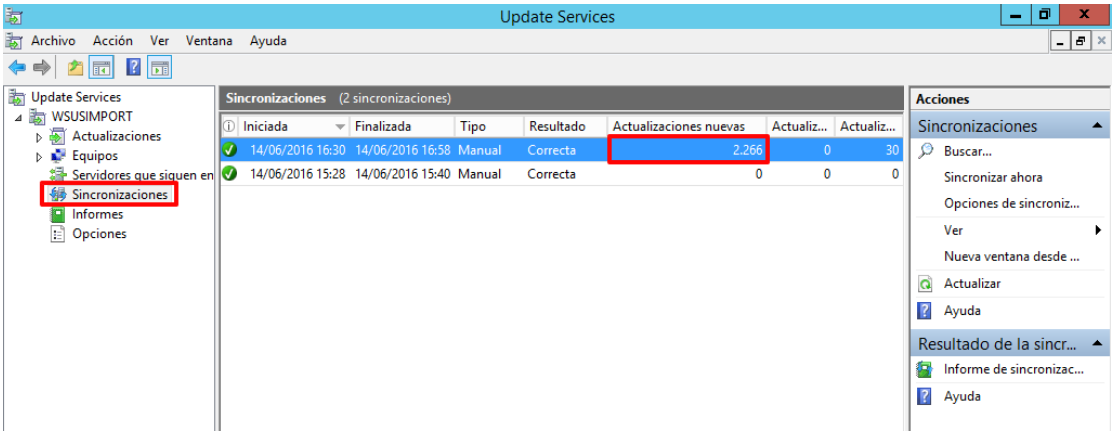
Nota: La carpeta WsusContent que se encuentra dentro de la unidad D:\. Ésta se crea en el proceso de configuración de las tareas posteriores a la instalación de Windows Server Update Services (WSUS).

También se detallará la manera de exportar todas estas actualizaciones mediante una herramienta propia de WSUS, para distribuirlas a los diferentes servidores de Windows Server Update Services que tenga en su red clasificada.

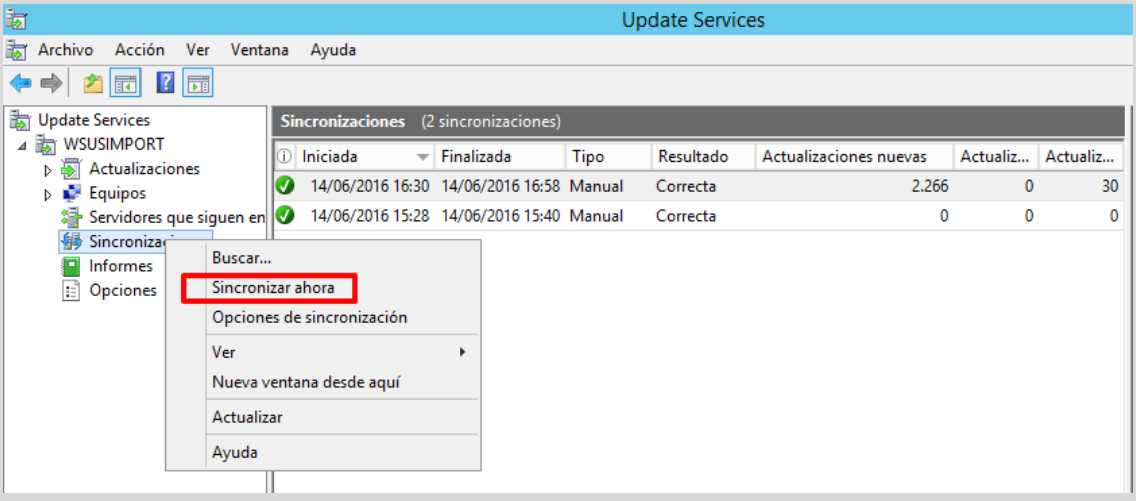
Nota: Recuerde que antes de introducir las actualizaciones descargadas de Internet en sistemas de red clasificada, el dispositivo de almacenamiento que utilice para introducir estas en la red, deberá pasar el análisis por el sistema de aduana con el que cuente su organización.

Paso	Descripción
31.	Si aún no lo ha hecho, inicie sesión en el servidor de Windows Server Update Services.
32.	Vaya a **Inicio>Administrador del servidor>Herramienta>Windows Server Update Services**, pulse sobre éste para iniciar la consola de administración de WSUS. 

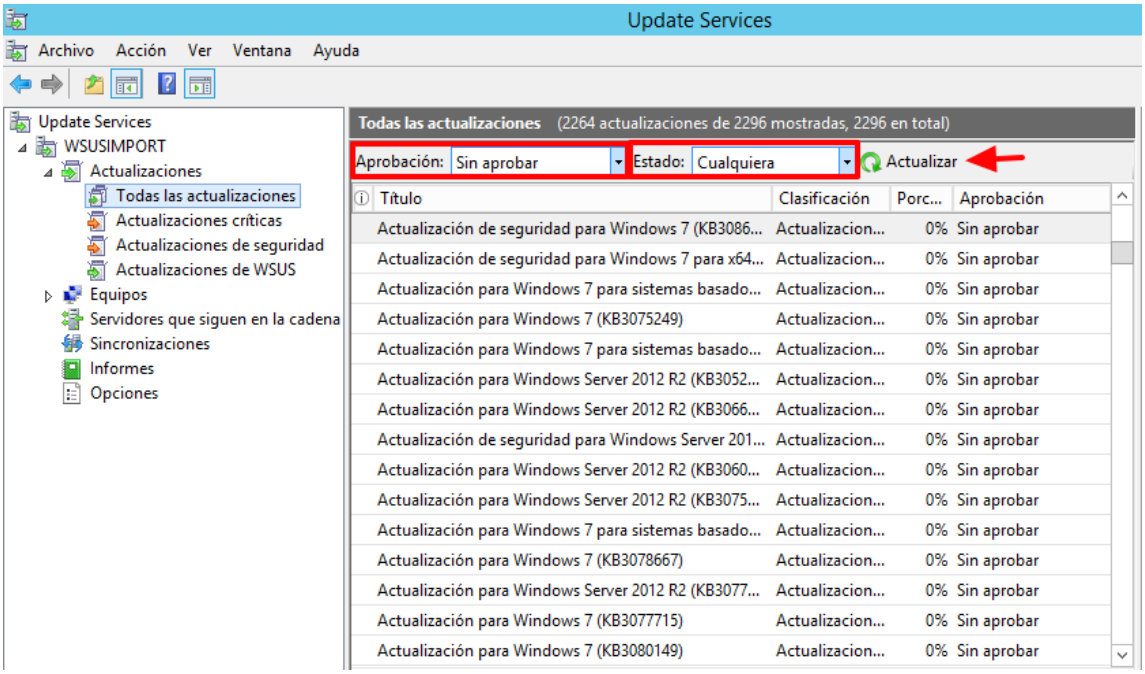
Paso	Descripción
33.	Una vez abierta la consola de WSUS, se va a comprobar que se ha realizado la "Sincronización Inicial". Para ello diríjase a **Update Services> [Su servidor WSUS]>Sincronizaciones.** En el panel central deberá existir una línea con la sincronización realizada correctamente y con un número de "actualizaciones nuevas" encontradas, tal y como se muestra en la siguiente imagen:



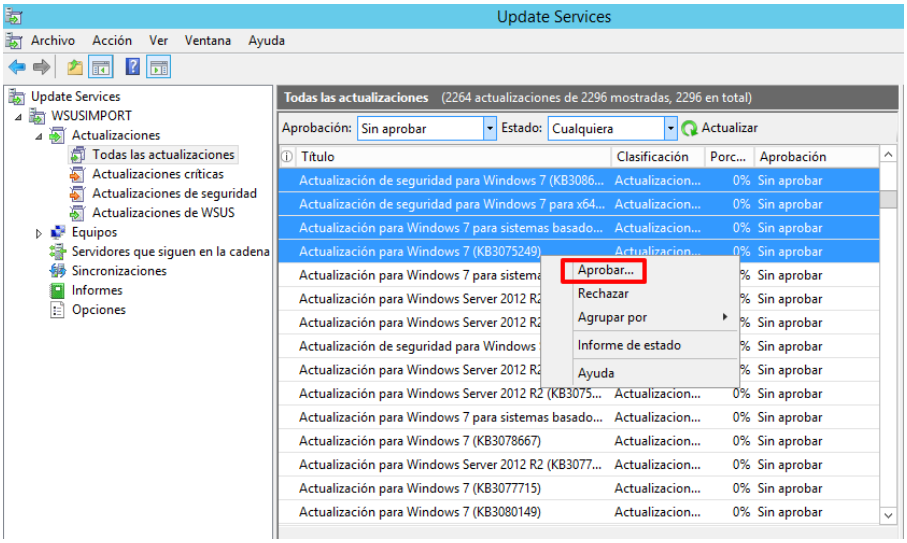
Nota: En el caso de no haber realizado una sincronización inicial en el proceso de configuración de WSUS, deberá dirigirse a la pestaña "Sincronizaciones" y con el botón derecho del ratón deberá seleccionar "Sincronizar ahora".



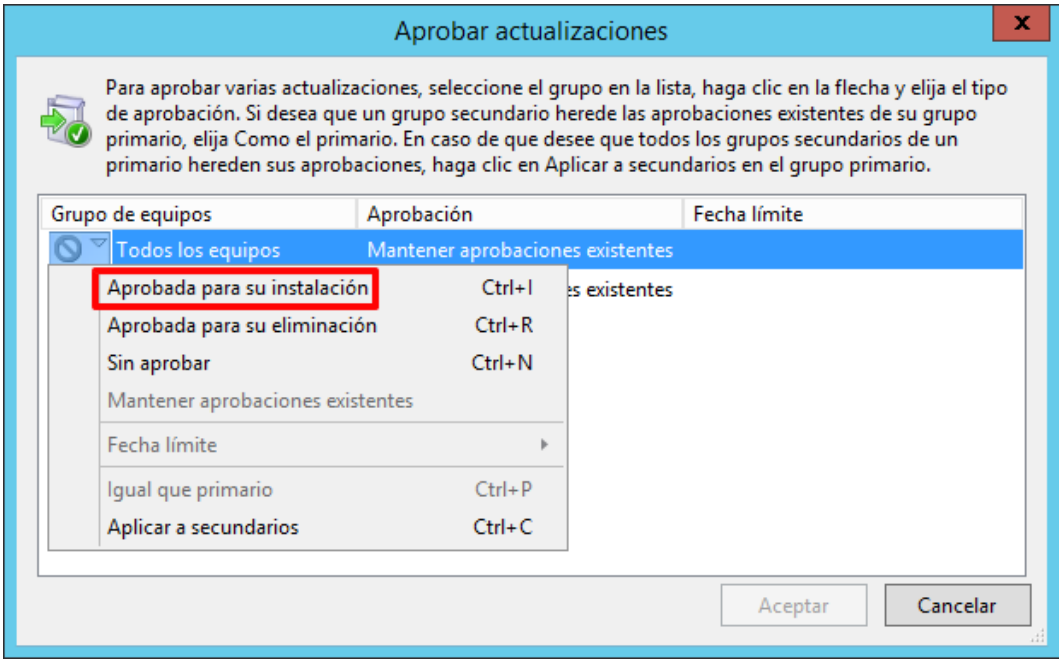
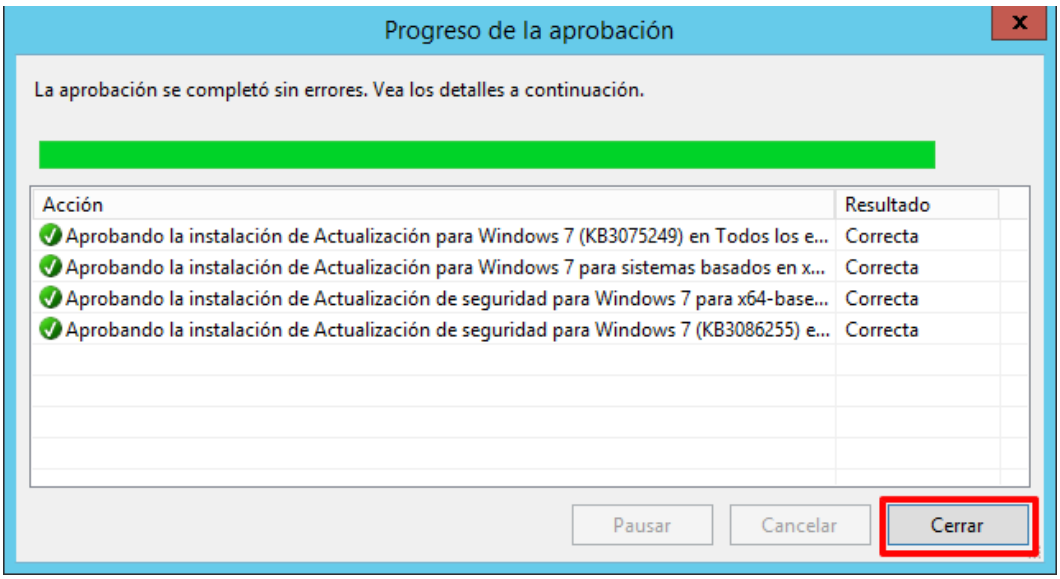
En este momento comenzará a sincronizar con Microsoft Update para descargar las actualizaciones seleccionadas anteriormente.

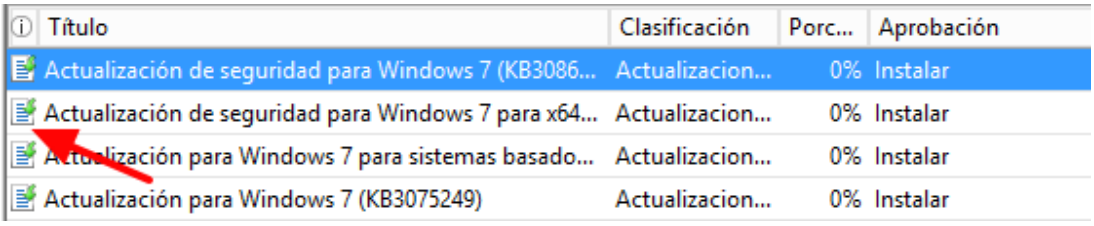
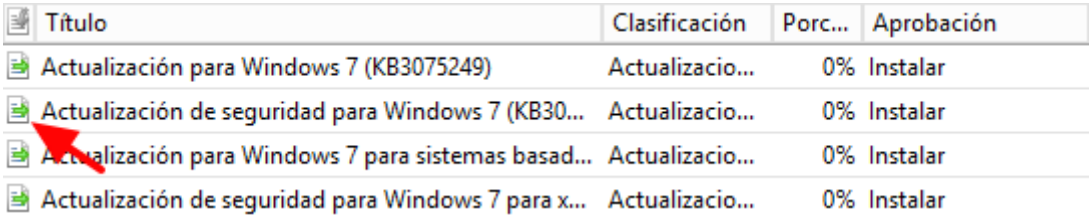
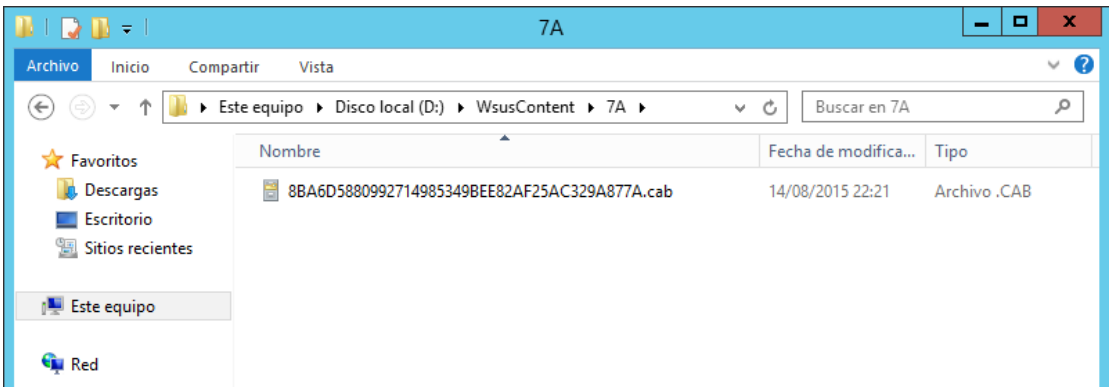
Paso	Descripción
34.	A continuación, sitúese en **Update Services>[Su servidor WSUS]>Todas las actualizaciones**, y en el panel central, configure las pestañas **"Aprobación"** y **"Estado"** de la siguiente manera: – Aprobación: Sin aprobar. – Estado: Cualquiera. Una vez hecho esto, pulse sobre **"Actualizar".** Seguidamente podrá observar todas las actualizaciones disponibles de Microsoft Update. 

Paso	Descripción
35.	Para que se realice la descarga de actualizaciones en la base de datos de WSUS, deberá aprobar las actualizaciones, para ello en la pestaña de "Todas las actualizaciones" seleccione la actualización que quiere aprobar de la siguiente manera, **botón derecho sobre la actualización y pulse sobre "Aprobar".**



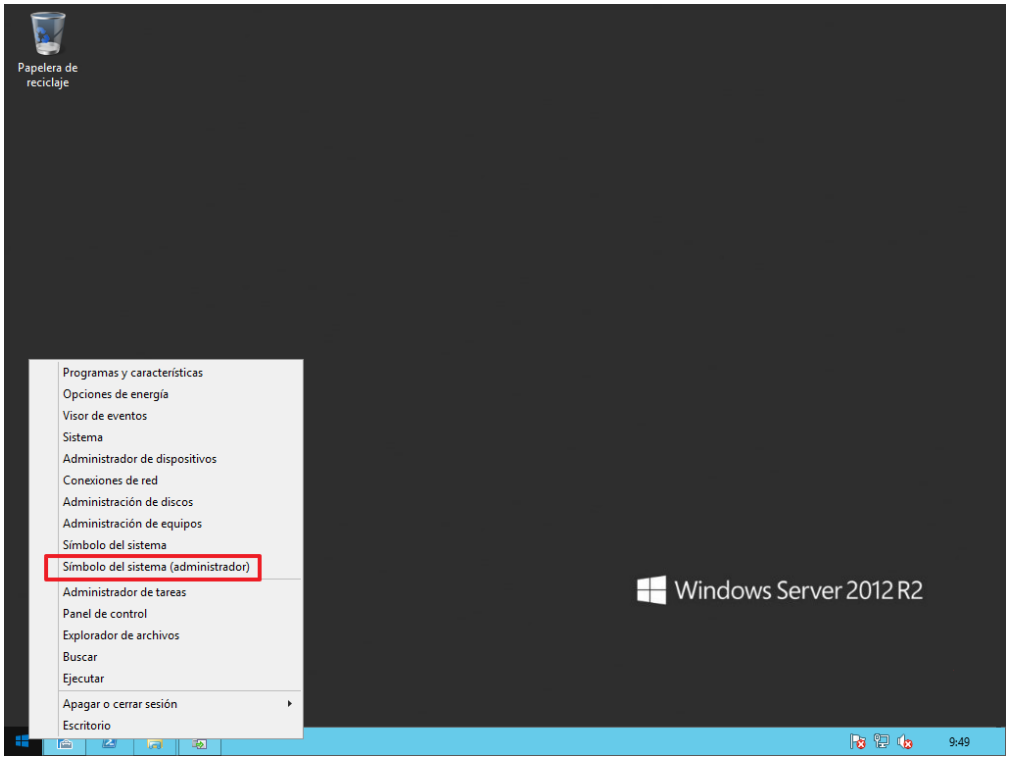
Nota: Como puede verse en la imagen, para la aplicación de esta guía solamente se han seleccionado cuatro actualizaciones del sistema operativo Windows 7. Dependiendo de las necesidades de su organización esta selección podrá variar.

Paso	Descripción
36.	Seguidamente, aparecerá un asistente donde indicará el grupo de equipos para los que quiere aprobar estas actualizaciones. Seleccione la pestaña "Todos los equipos" y a continuación pulse sobre **"Aprobada para su instalación"** y **"Aceptar"**. 
37.	Comenzará el proceso de aprobación, cuando haya terminado pulse sobre **"Cerrar"** para finalizar el asistente. 

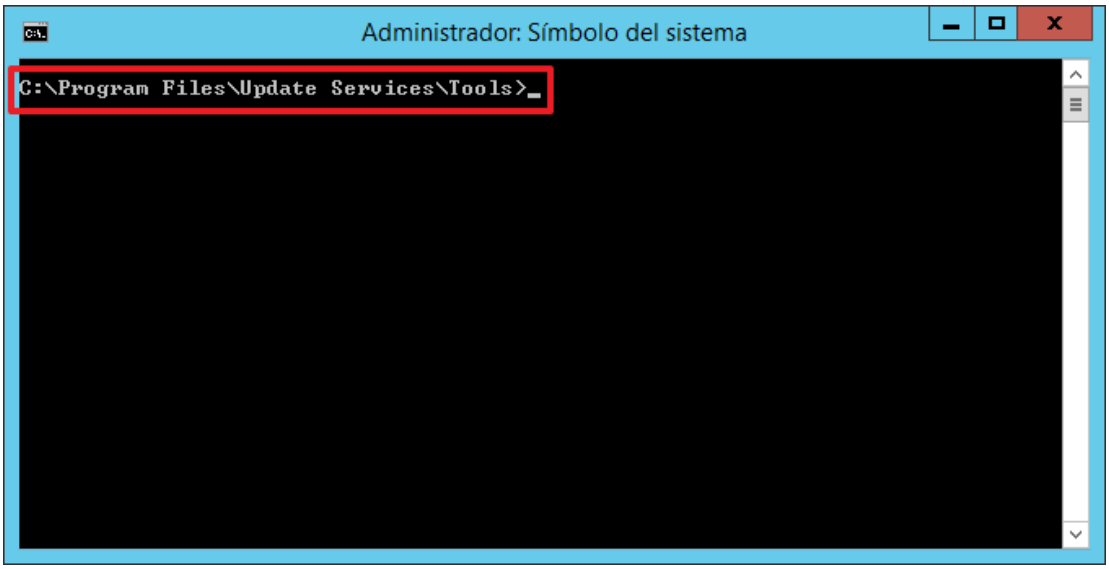
Paso	Descripción
38.	En este momento, empezará a descargar las actualizaciones que haya aprobado anteriormente, se habilitará un icono en la parte izquierda de la propia actualización, dónde se indicará el estado de la actualización.  **Nota**: Como puede verse en la imagen, en el proceso de descarga le notificará con la fecha verde hacia abajo y cuando haya terminado la descarga, esta flecha verde cambiará su orientación hacia el lado derecho, tal y como podrá observar en el punto siguiente. Si no es capaz de visualizar el estado del archivo de actualización, pinche con el botón derecho sobre el encabezado y seleccione la opción de "Estado del archivo". De esta manera podrá visualizar el estado de la descarga de la actualización.
39.	El proceso de descarga puede durar varios minutos, y tal y como puede observar en la siguiente imagen, el proceso de descarga ha finalizado y el estado de la actualización ha cambiado, tal y como se muestra en la siguiente imagen: 
40.	Por último, para dar por finalizado el proceso de descarga, deberá comprobar que las actualizaciones se han almacenado en la ubicación correcta, configurada en pasos anteriores. Para ello, diríjase a la unidad **D:\WsusContent** mediante un "Explorador de archivos".
41.	Como podrá observar, existirán todas las actualizaciones aprobadas y descargadas anteriormente en la base de datos de WSUS. Creará una carpeta independiente por cada actualización. Entrando en una de ellas, se puede visualizar el archivo **.cab** para la instalación. 

Una vez que tenga las actualizaciones que desea descargar, deberá exportarlas a los servidores WSUS configurados de forma Offline, para que éste las distribuya a los equipos clientes que se tenga asociados al servidor WSUS, y que se encuentra dentro de la red clasificada. A continuación, se va a detallar la manera adecuada para realizar una exportación correcta de las actualizaciones descargadas anteriormente.

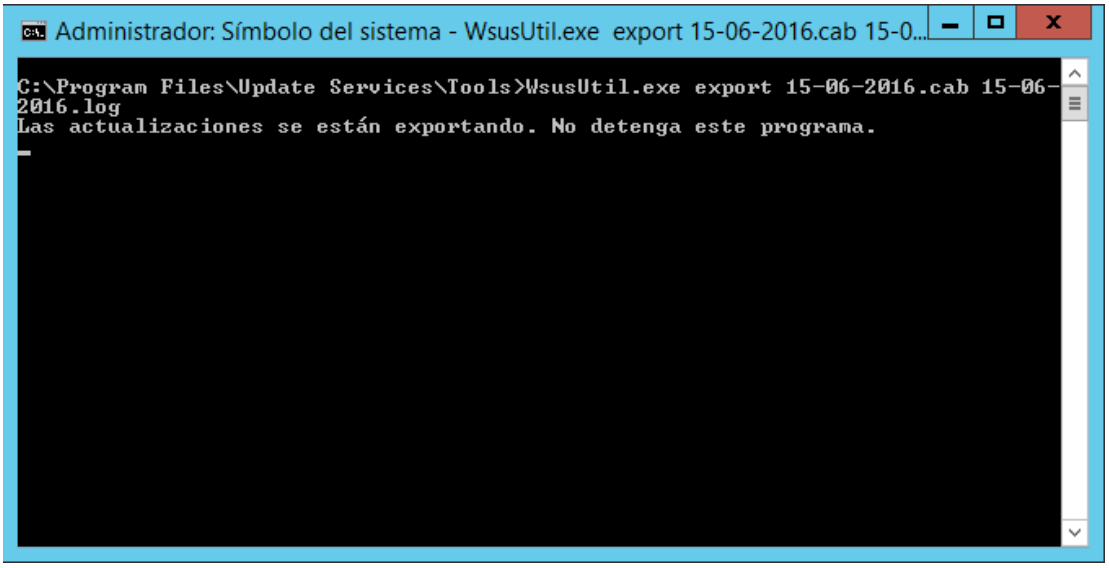
En el proceso de exportación hay que realizar dos operativas para que el resultado sea satisfactorio, uno es el copiado de los archivos descargados de las actualizaciones desde la base de datos de WSUS y otro es la exportación de los metadatos de las actualizaciones.

Paso	Descripción
42.	Ejecute un símbolo de sistema con derechos de administrador, para ello pinche con el botón derecho sobre el botón de inicio y pulse sobre **"Símbolo de sistema (administrador)"**, tal y como se muestra en la imagen: 

Paso	Descripción
43.	Se abrirá un símbolo de sistema con privilegios de administrador. Después sitúese en **"C:\ProgramFiles\UpdateServices\tools\".**

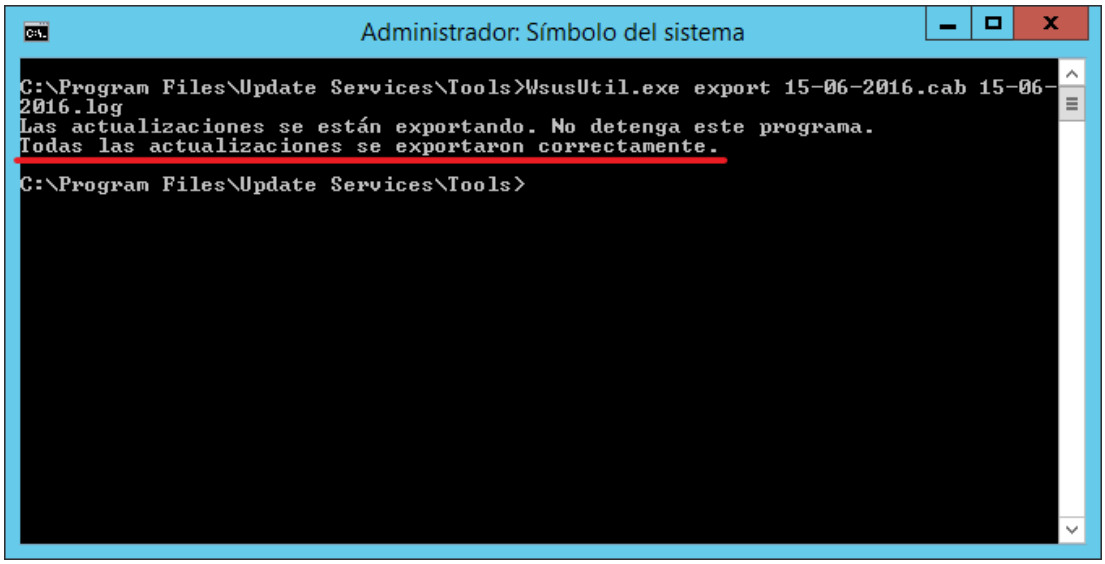


44.	Con la herramienta **"wsusutil.exe export"** generará los metadatos necesarios para asociar los paquetes de actualizaciones al servidor WSUS. Para ello, en el **"símbolo de sistema"** abierto anteriormente, ejecute **"wsusutil.exe export 15-06-2016.cab 15-06-2016.log"**, seguidamente se pulsará **"Intro",** para que se ejecute el comando introducido.



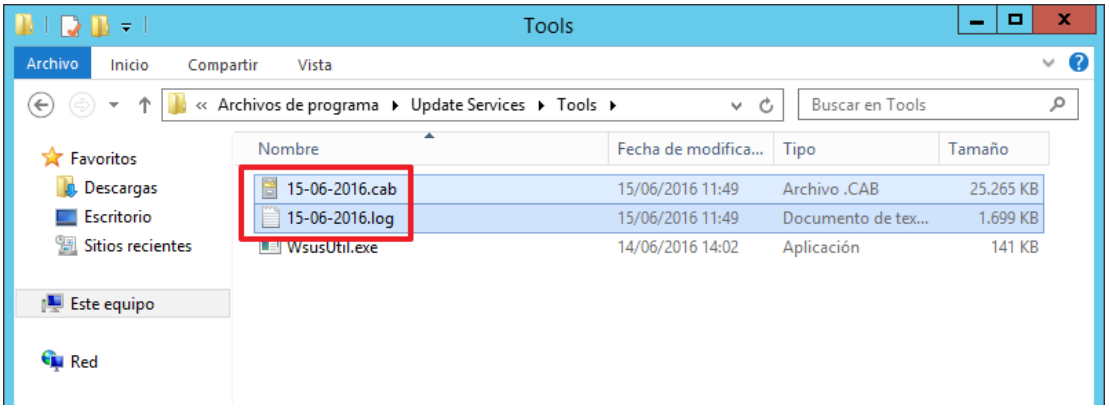
Nota: El nombre que se asigna al archivo .cab y .log en esta guía, es un ejemplo. Usted podrá asignar el nombre que mejor crea que identifique las actualizaciones. Sería conveniente que asigne un nombre que le ayude a tener controlado el período de exportación.

Paso	Descripción
45.	Espere a que termine, cuando el proceso acabe se emitirá un mensaje notificando que la exportación se ha realizado correctamente.

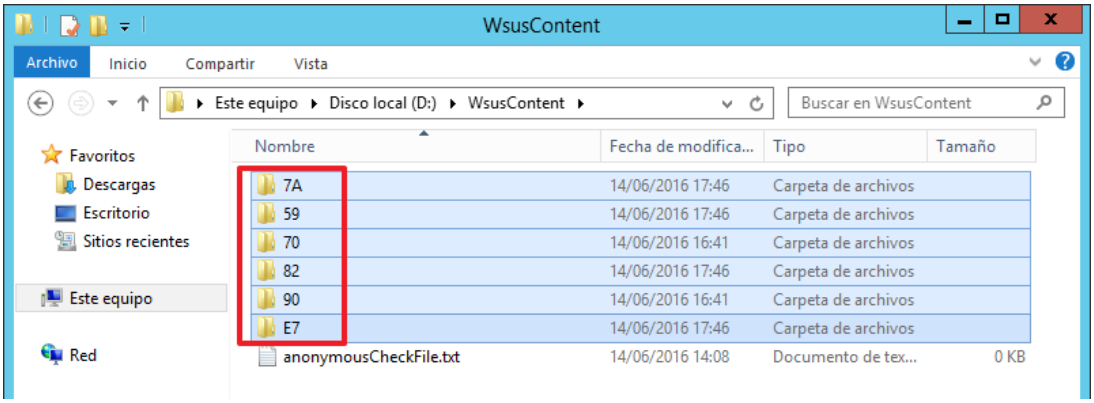


Nota: El tiempo que tarda el proceso de exportación dependerá de la cantidad de actualizaciones que quiera exportar y que se encuentren dentro de la base de datos de WSUS.

46. Compruebe que se han generado un archivo **.cab** y un archivo **.log** con el proceso de exportación. Ejecute un "Explorador de archivos" y vaya a **"Archivos de programa>Update Services>tools",** deberá contener los archivos generados anteriormente.



Nota: Deberá copiar estos dos archivos en una unidad de almacenamiento para trasladarlos al equipo correspondiente donde se vayan a importar, es muy importante que estos archivos vayan junto con los paquetes de actualizaciones descargados por WSUS. (Continúe con el siguiente punto para realizar el copiado de los paquetes de actualizaciones descargados por WSUS).

Paso	Descripción
47.	A continuación, deberá copiar en la misma unidad de almacenamiento que copió los metadatos, los paquetes de actualizaciones, para ello, diríjase a la base de datos de WSUS, que se encuentra en **"D:\WsusContent\".** Deberá copiar todos los directorios que se encuentran dentro de la carpeta WsusContent**.** 

ANEXO F. GUÍA PASO A PASO DE LA INSTALACIÓN DE UN SERVIDOR DE ACTUALIZACIONES OFFLINE EN WINDOWS SERVER 2012 R2

El presente anexo se ha diseñado para ayudar a los operadores a implementar el servicio de actualizaciones de Microsoft Windows Server 2012 R2 en un único servidor, miembro de un dominio de Directorio Activo.

Para la realización de los diferentes pasos de este anexo, se utiliza el siguiente usuario del dominio que pertenece a los grupos indicados a continuación.

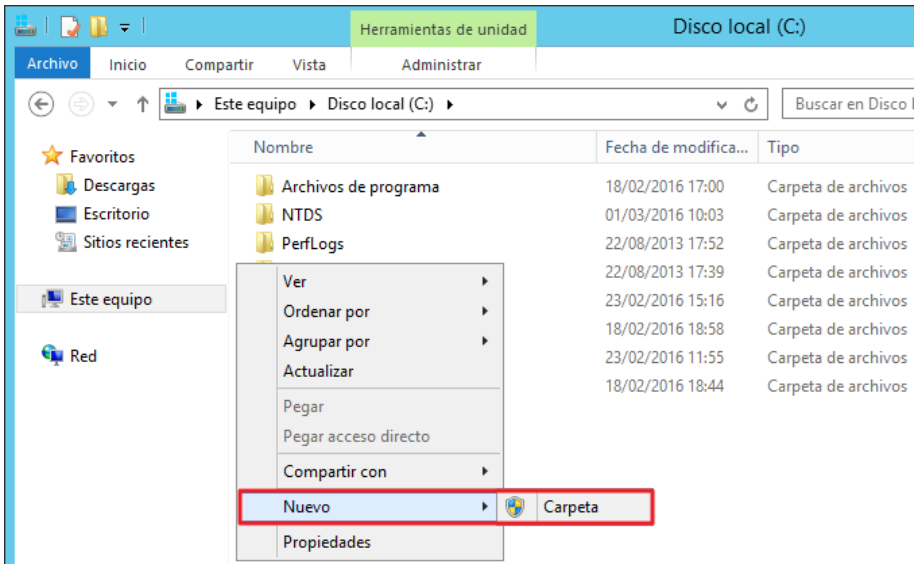
- DOMINIO\SDT:
  - Admins. del dominio.
  - Usuarios de shells.
  - Usuarios del dominio.

1. PREPARACIÓN DEL DIRECTORIO ACTIVO

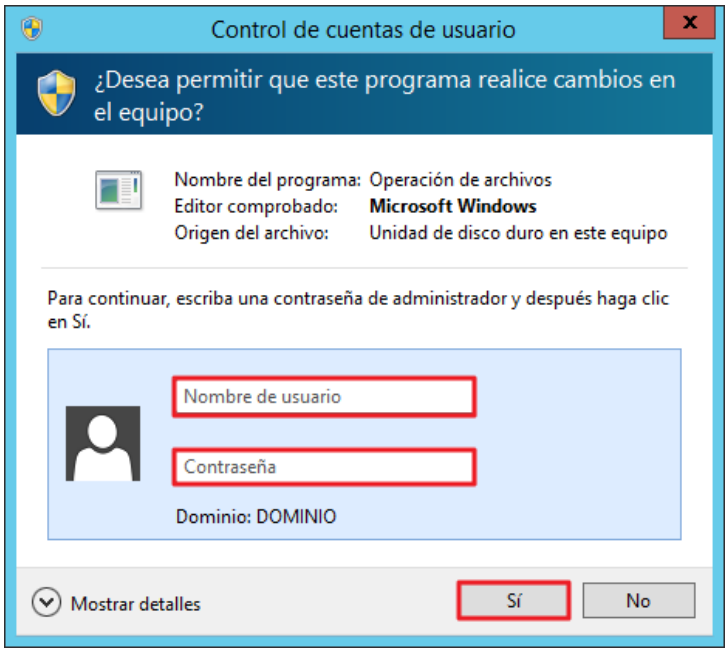
Los pasos que se describen a continuación se realizarán en un Controlador de Dominio del dominio donde se realizará la implementación del servidor de las actualizaciones. Sólo es necesario realizar este procedimiento una vez.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Para comenzar con la instalación de WSUS, es necesario haber aplicado con anterioridad la guía CCN-STIC-563 Implementación de IIS 8.5 sobre Windows Server 2012 R2. Exactamente se deberán aplicar los siguientes Anexos: – ANEXO E. PREPARATIVOS PARA LA INSTALACIÓN DE UN SERVIDOR INTERNET INFORMATION SERVICES 8.5 SOBRE UN SERVIDOR MIEMBRO WINDOWS SERVER 2012 R2 – ANEXO G. GUÍA PASO A PASO DE LA INSTALACIÓN DE UN SERVIDOR WEB DINÁMICO CON ASP.NET 4.5

Paso	Descripción
4.	Cree el directorio “Scripts” en la unidad C:\. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo > Carpeta”.**



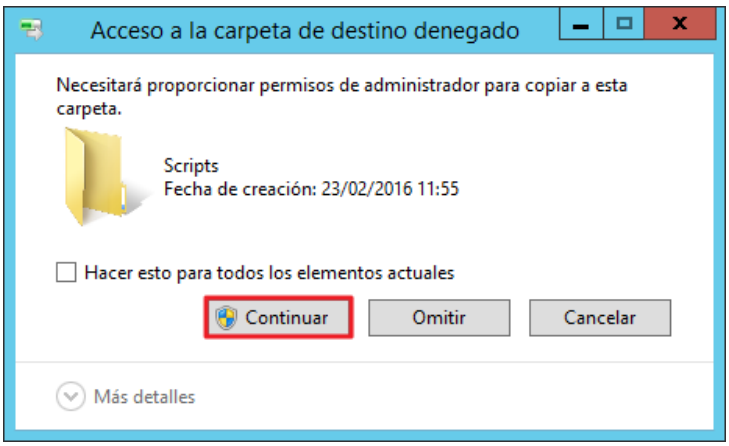
5.	El “control de cuentas de usuarios” le pedirá elevación de privilegios, para ello ingrese una cuenta “administrador del dominio”.



Nota: Para crear directorios en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Introduzca las credenciales de la cuenta con la que ha iniciado sesión, la cual debe ser al menos de administrador de dominio.
En este ejemplo, se utiliza la cuenta “DOMINIO\SDT”.

6.	Asigne el nombre **“Scripts”** al nuevo directorio.

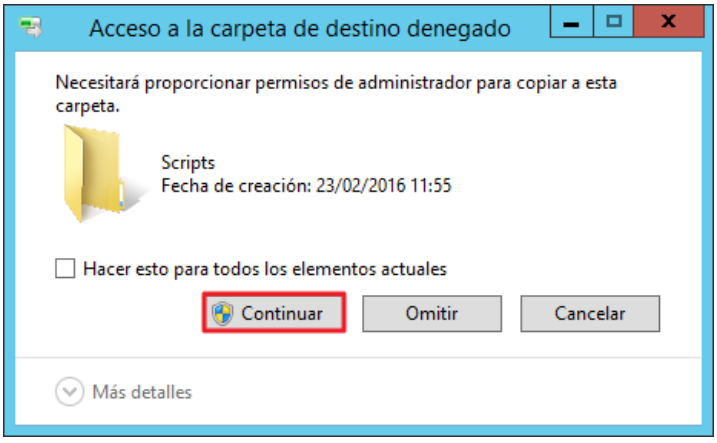
Paso	Descripción
7.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio **"C:\Scripts"**.



Nota: Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón "Continuar" e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio.
En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

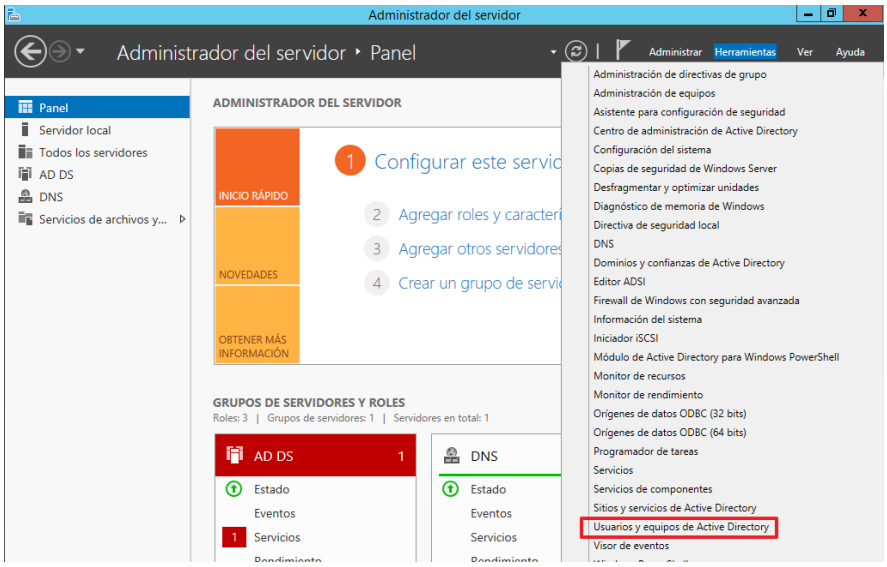
8. Copie los siguientes ficheros en el directorio **"C:\Windows\security\templates"** del Controlador de Dominio:

- "C:\Scripts\CCN-STIC-568 Plantilla Servidor WSUS.inf.
- "C:\Scripts\CCN-STIC-568 Plantilla Servidores 2012 R2 – Clientes WSUS.inf".
- "C:\Scripts\CCN-STIC-568 Plantilla Windows 7 – Clientes WSUS".
- "C:\Scripts\CCN-STIC-568 Plantilla Windows 10 – Clientes WSUS".



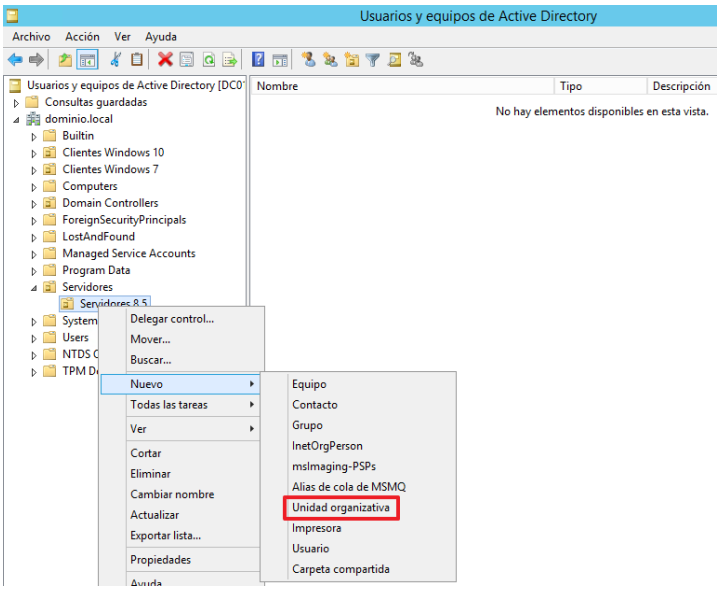
Nota: Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón "Continuar" e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio.
En el caso de que su sistema Windows esté instalado en otro directorio o unidad, deberá adaptar los pasos relacionados con la ruta "C:\Windows" para adecuarlos a su sistema en concreto.
En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
9.	Ejecute la consola administrativa Usuarios y equipos de Active Directory desde **"Inicio > Administrador del servidor > Herramientas > Usuarios y equipos de Active Directory"**.



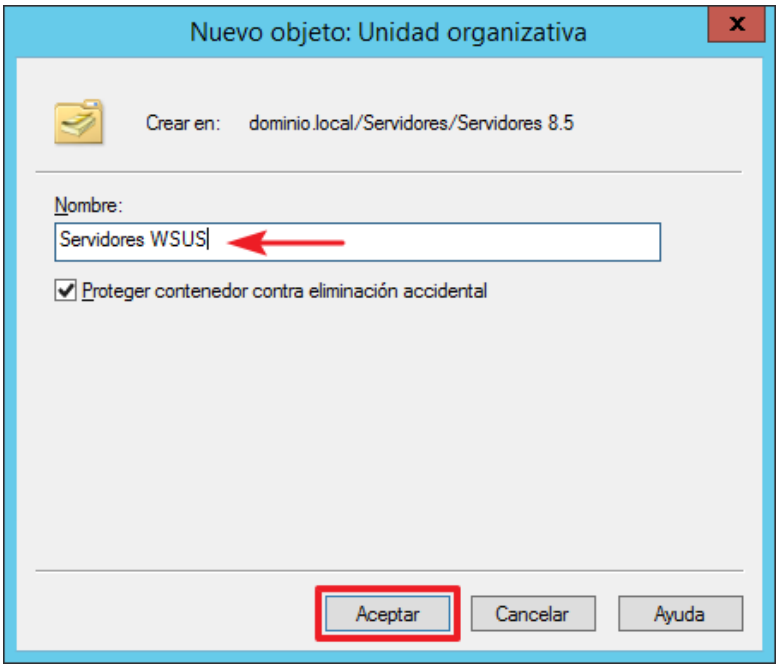
Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
10.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-560A. Para ello, seleccione el nodo **"<<dominio>> / <<unidad organizativa>/Servidores 8.5>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo > Unidad organizativa"**.

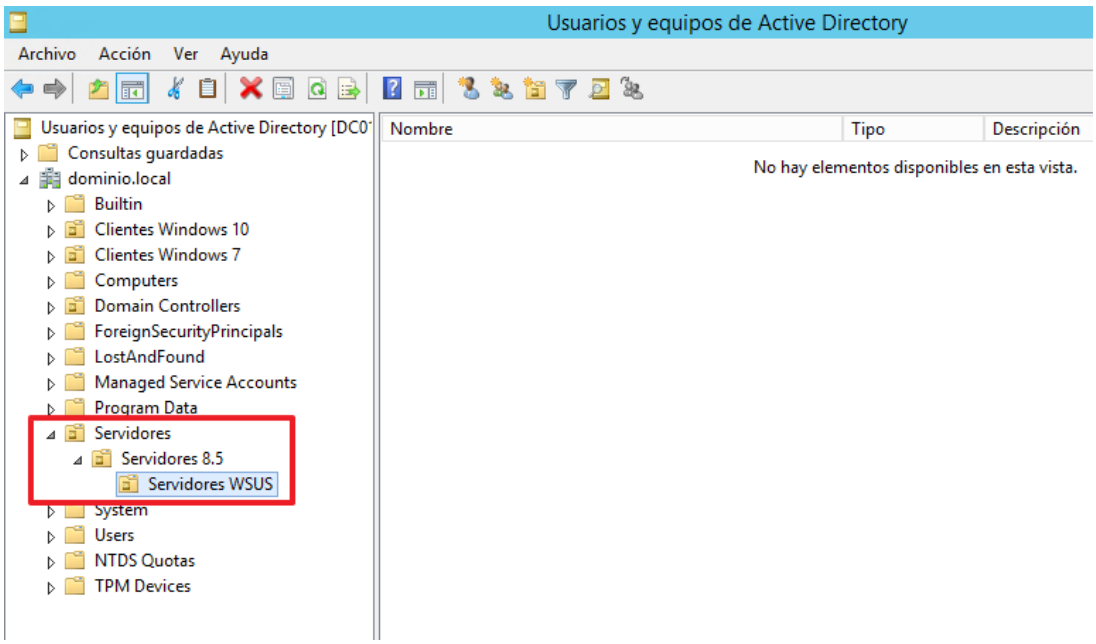


Nota: En este ejemplo, la unidad organizativa de servidores se encuentra en la siguiente ruta "dominio.local/servidores/servidores 8.5".

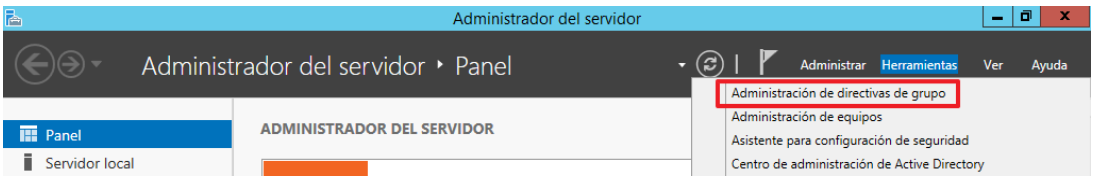
11.	Introduzca el nombre **"Servidores WSUS"** tal y como se muestra en la imagen y pulse sobre **"Aceptar".**



Paso	Descripción
12.	Se habrá creado una unidad organizativa tal y como se muestra en la siguiente imagen:

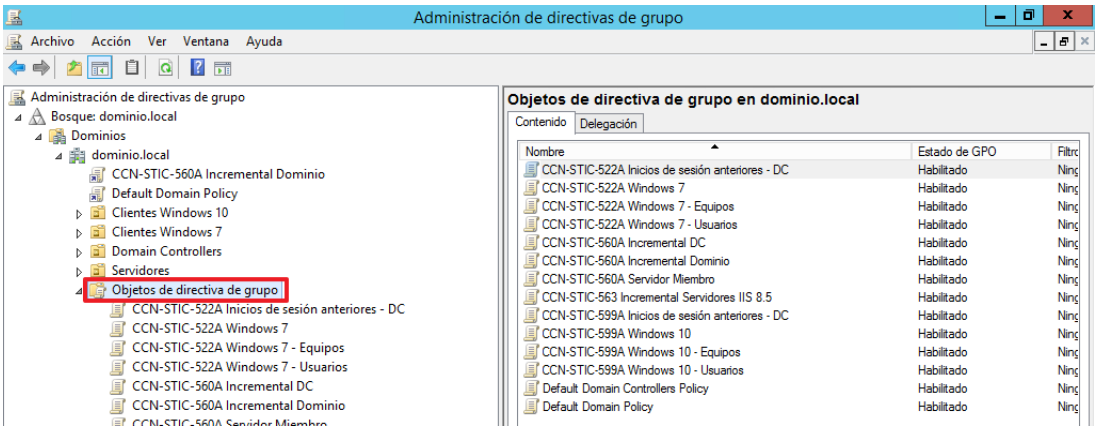


13.	Puede cerrar la consola de “Usuarios y equipos de Active Directory”.
14.	Ejecute la consola administrativa Administración de directivas de grupo desde **“Inicio > Administrador del servidor > Herramientas > Administración de directivas de grupo”**.

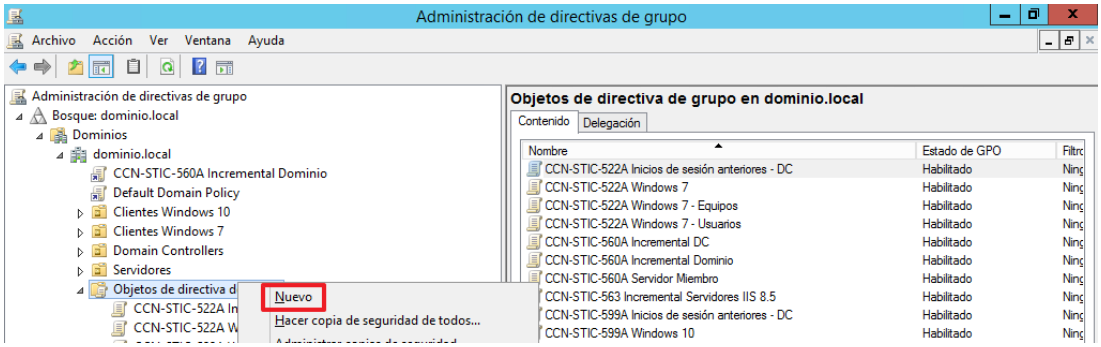


Nota: Si inicia por primera vez la consola de “Administrador del Servidor” le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio “DOMINIO\SDT”.

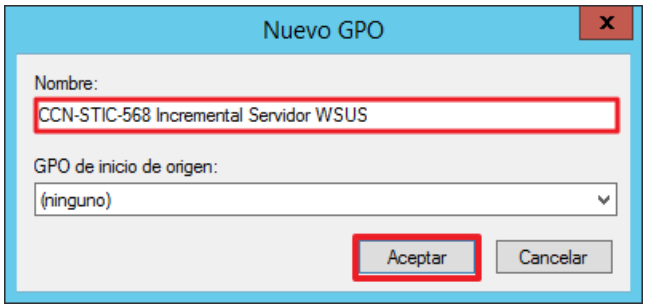
Paso	Descripción
15.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> / Dominios / <<nombre de dominio>> / Objetos de directiva de grupo"**.



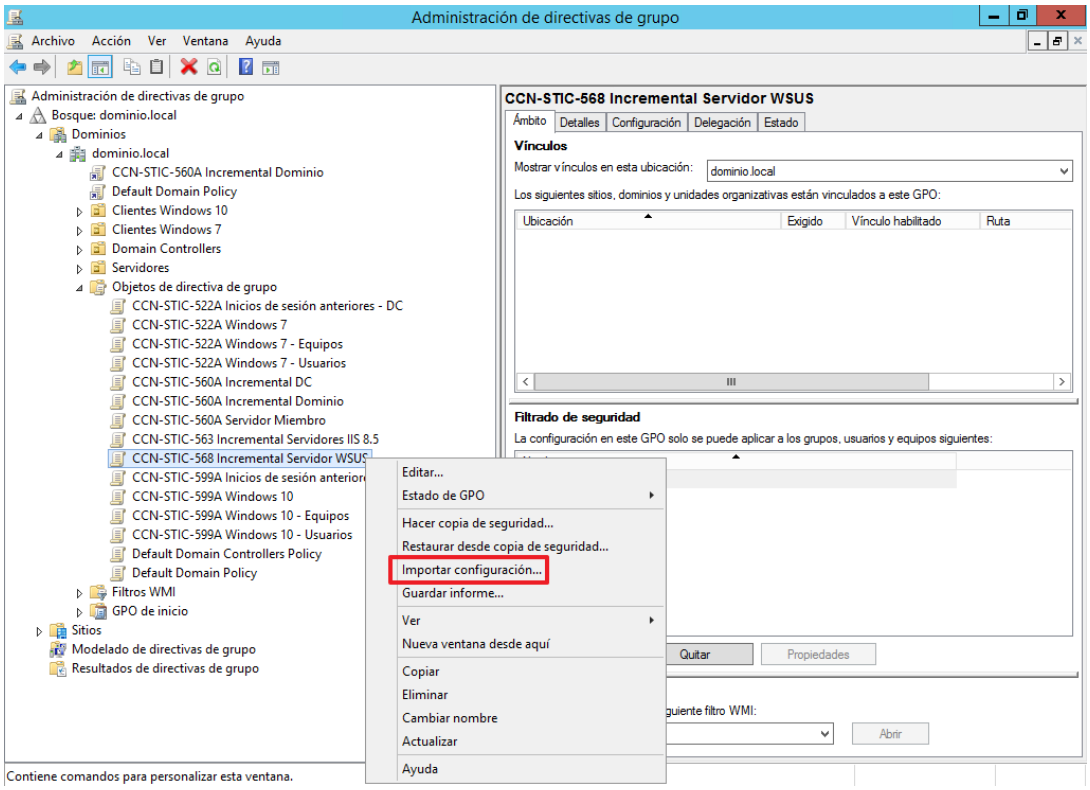
16.	Pulse con el botón derecho sobre **"Objeto de directiva de grupo"** y seleccione **"Nuevo".**



17.	Escriba el nombre de la GPO **"CCN-STIC-568 Incremental Servidor WSUS"** y haga clic en el botón **"Aceptar".**



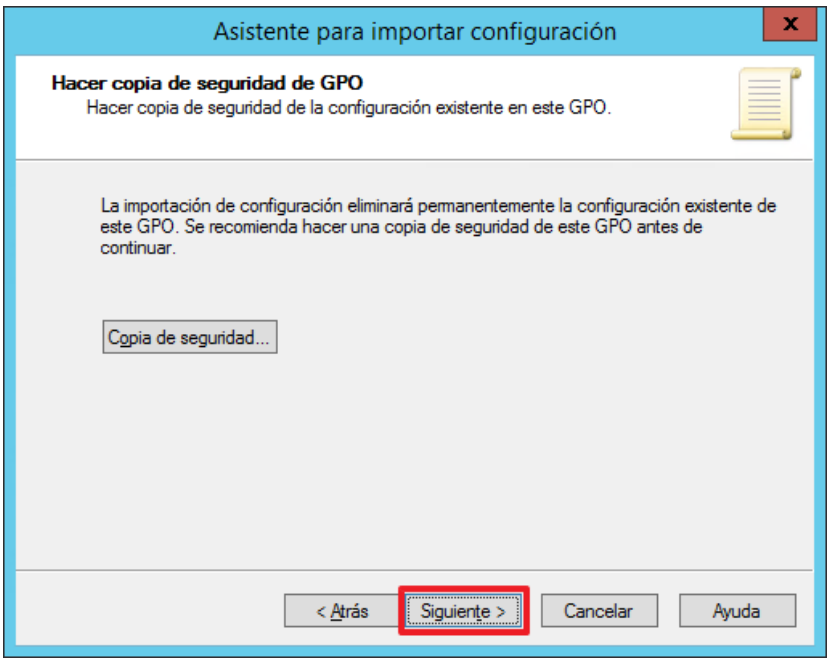
Paso	Descripción
18.	A continuación, pulse con el botón derecho sobre la GPO recientemente creada y pulse sobre **"Importar configuración…"**



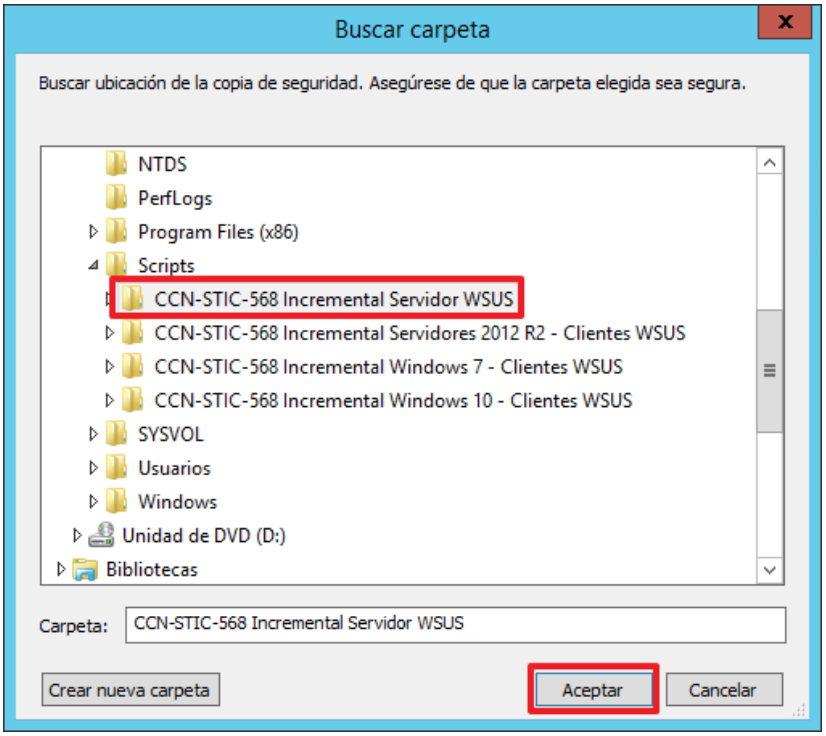
19.	En el asistente para importar configuración, pulse **"Siguiente >"** para continuar.

Paso	Descripción

20. No haga copia de seguridad y pulse **"Siguiente >".**

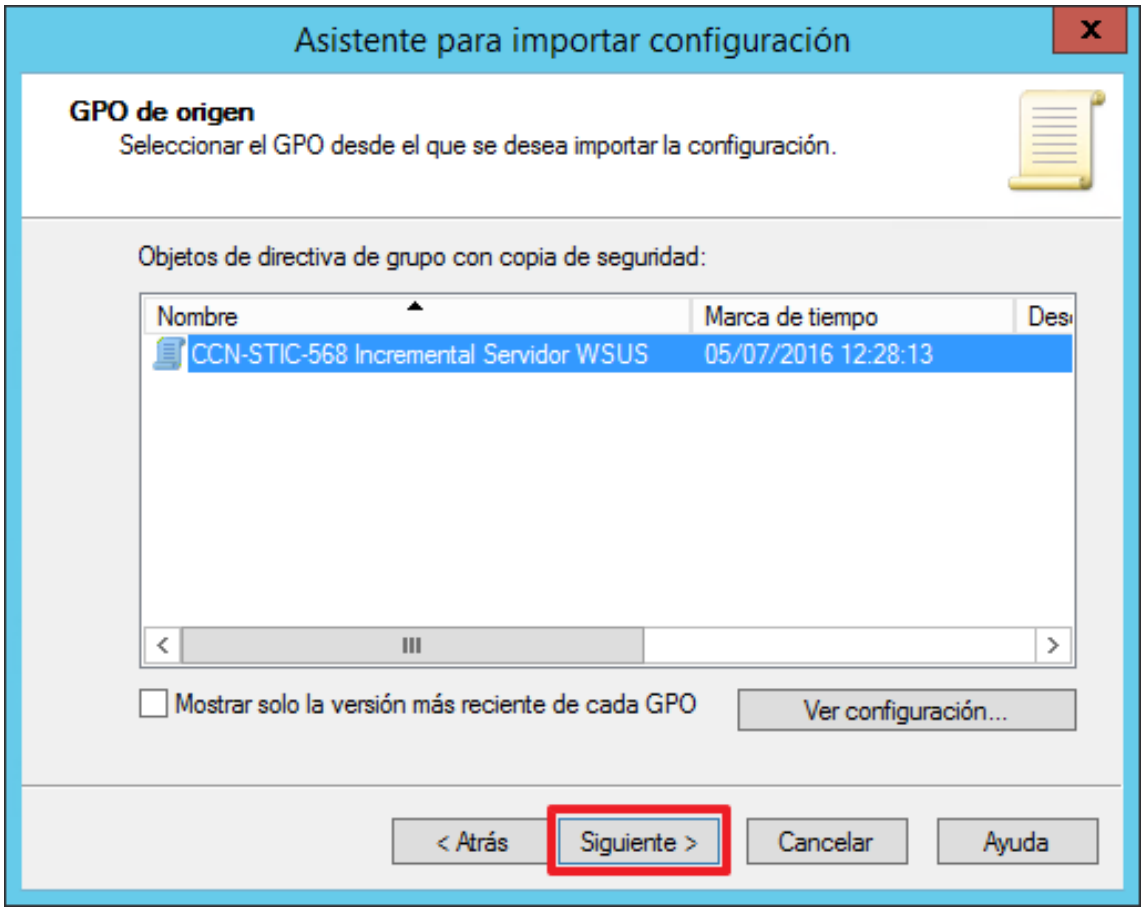


21. A continuación, pulse en **"Examinar"** y ubíquese en **"Este equipo > Disco local (C:) > Scripts"**, seleccione **"CCN-STIC-568 Incremental Servidor WSUS".**



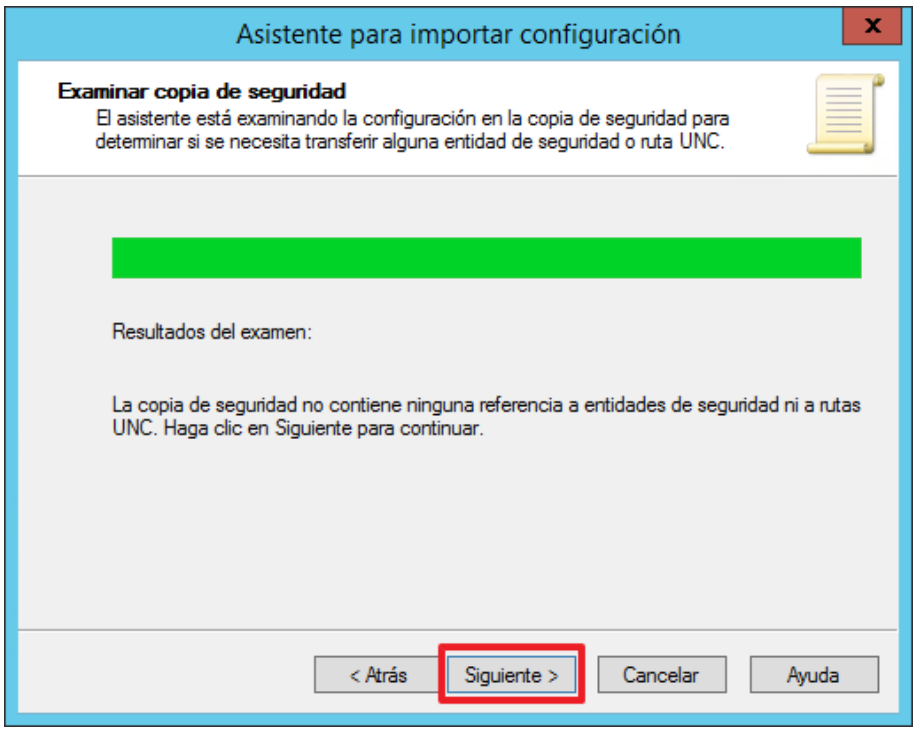
Pulse **"Aceptar".**

Paso	Descripción
22.	Una vez que ha indicado la ubicación donde se encuentra la configuración de la GPO, pulse **"Siguiente >".**
23.	En **"GPO de origen"**, pulse **"Siguiente >"** para continuar.

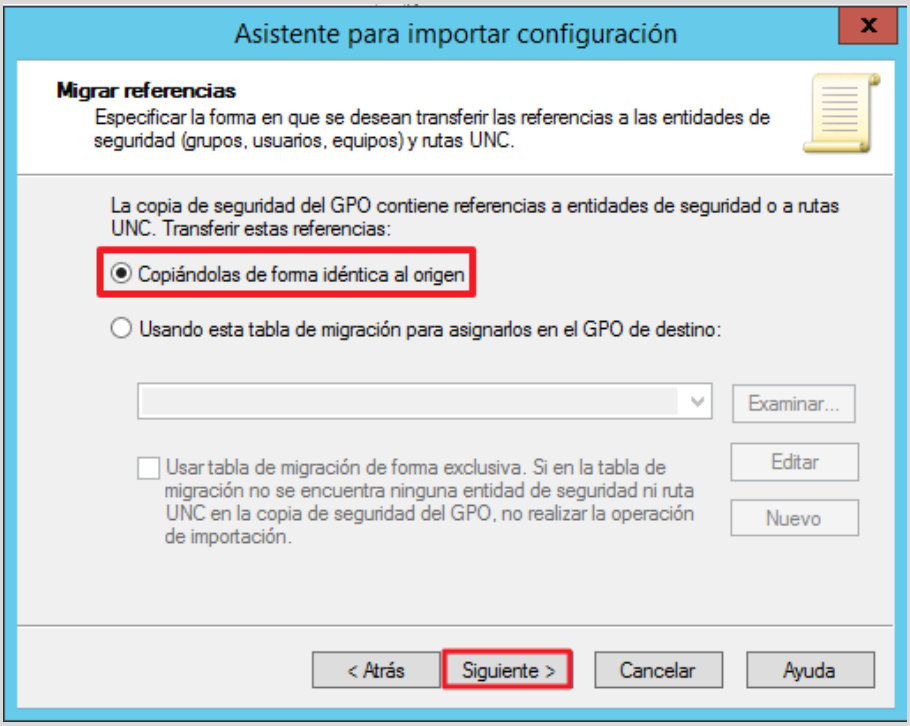


Paso	Descripción

24. Pulse **"Siguiente >"** una vez examinada la copia de seguridad.

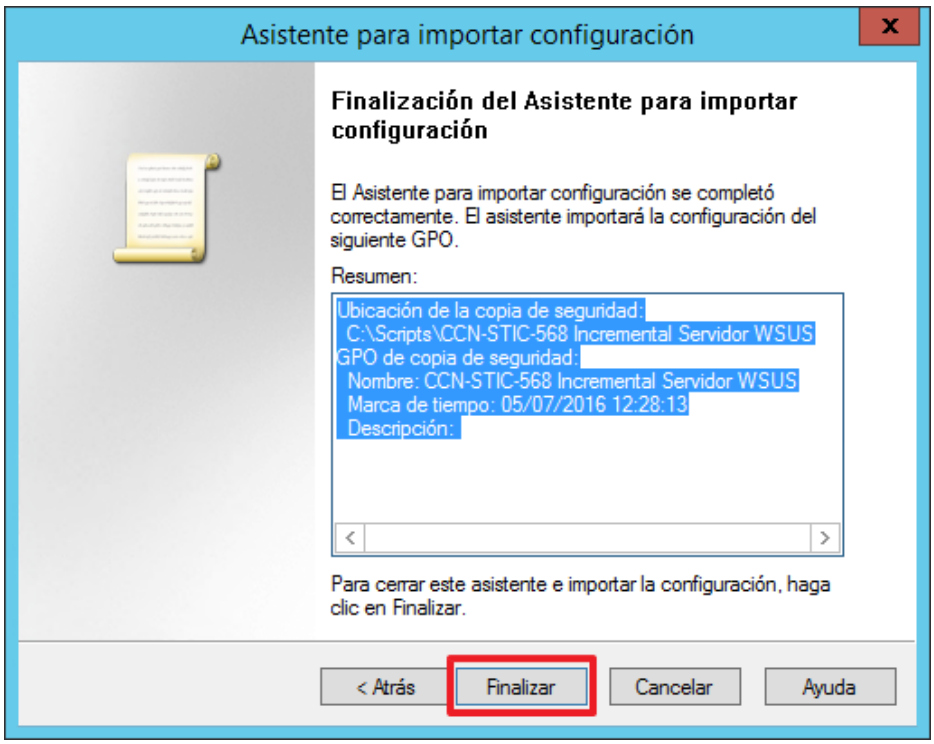


Nota: Hay que tener en cuenta que, si la copia de seguridad tiene referencias UNC, aparecerá un nuevo paso tal y como se muestra en la siguiente imagen, seleccione la opción "Copiándolas de forma idéntica al origen" y seguidamente pulse "Siguiente" para continuar.

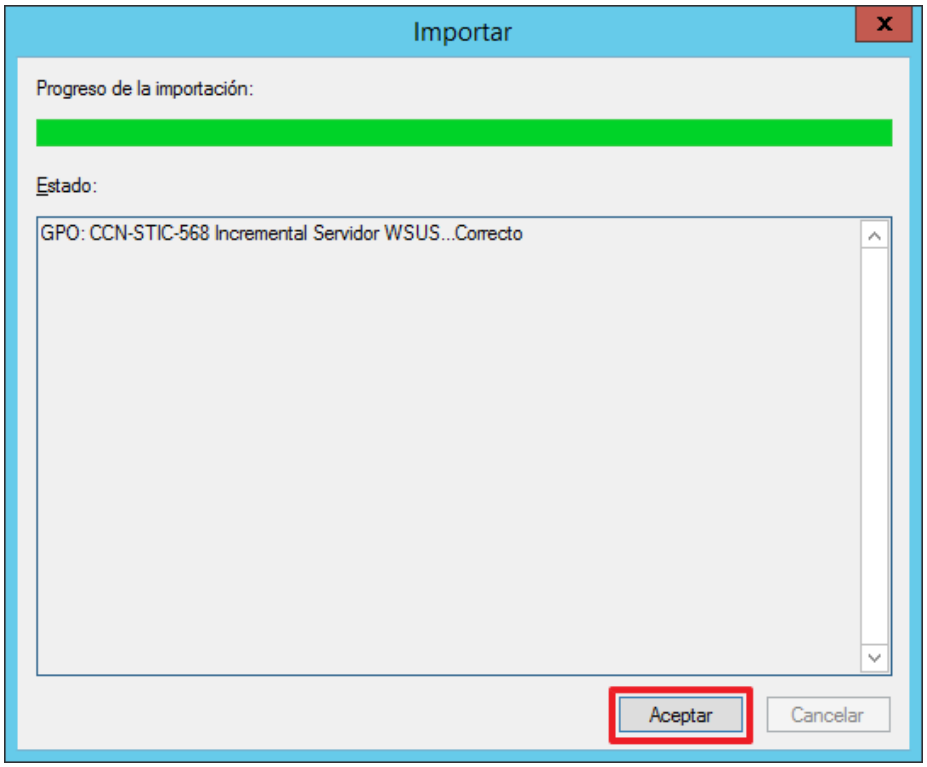


Paso	Descripción

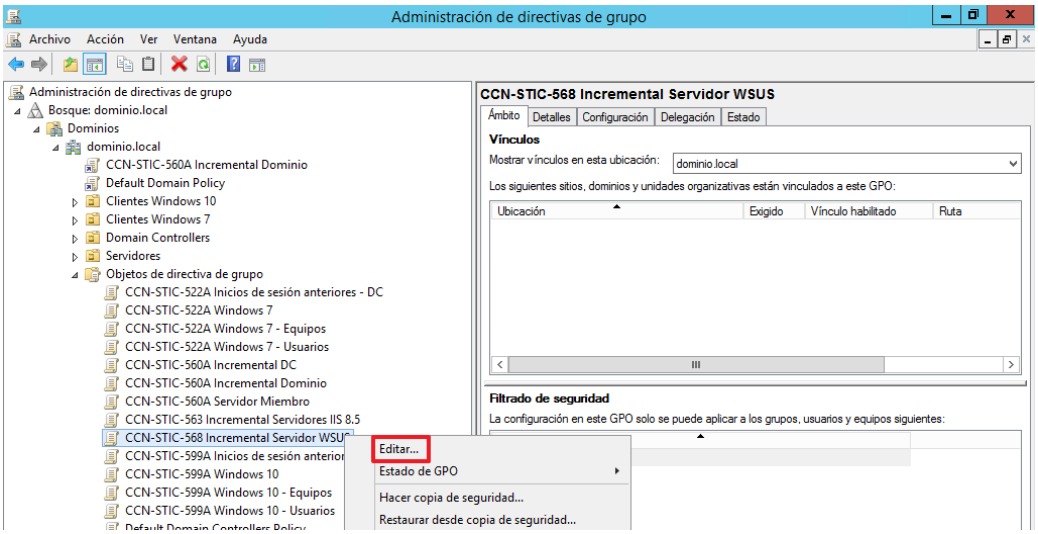
25. El asistente mostrará un resumen de la copia de seguridad, pulse en **"Finalizar"**.



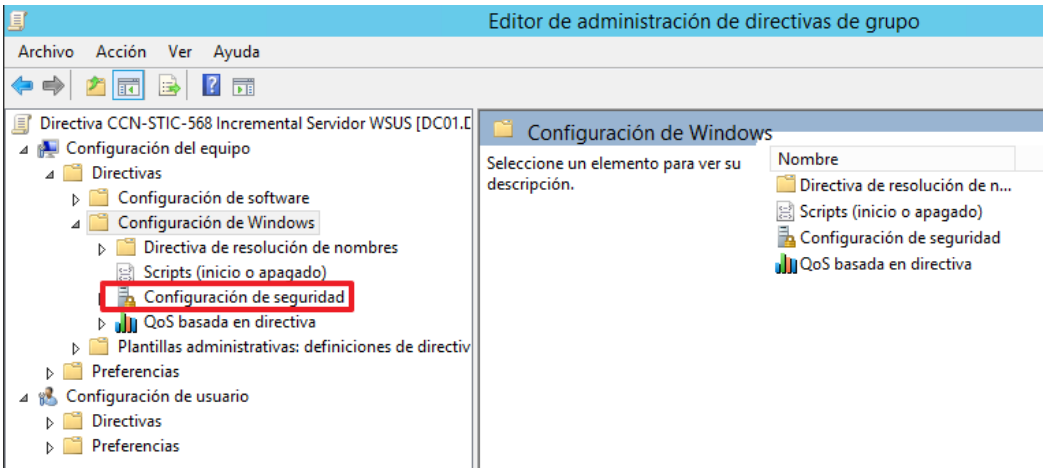
26. Si todo fue bien, el asistente mostrará que la importación se ha realizado correctamente, pulse en **"Aceptar"** para terminar con la importación.



Paso	Descripción
27.	A continuación, debe importar la configuración de seguridad, sobre la GPO **"CCN-STIC-568 Incremental Servidor WSUS"** pulse con el botón derecho y seleccione **"Editar"**.

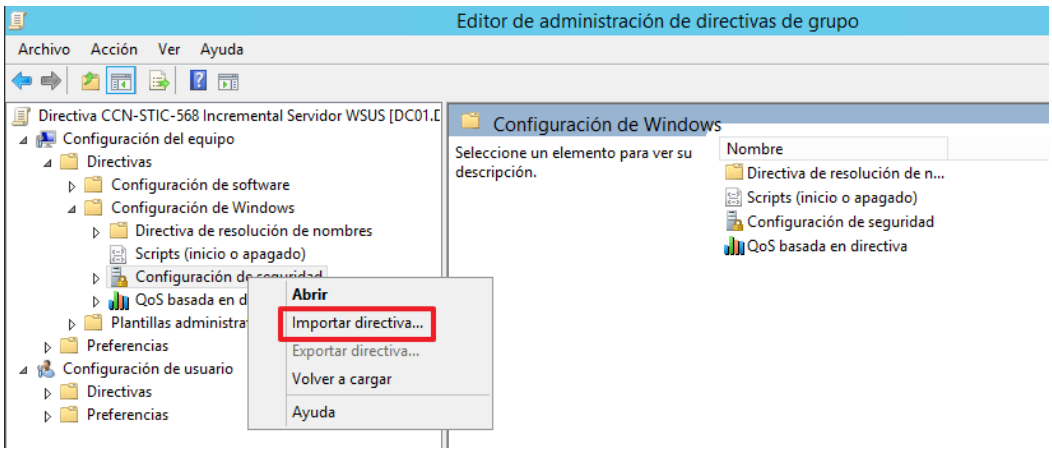


28.	En el "Editor de administración de directivas de grupo", ubíquese en **"Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad".**

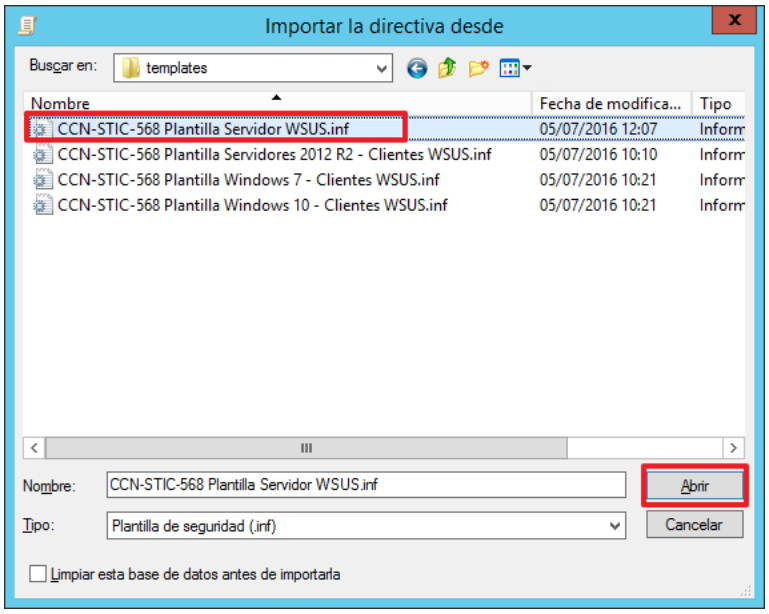


Paso	Descripción

29. Con el botón derecho seleccione el menú **"Importar directiva…".**



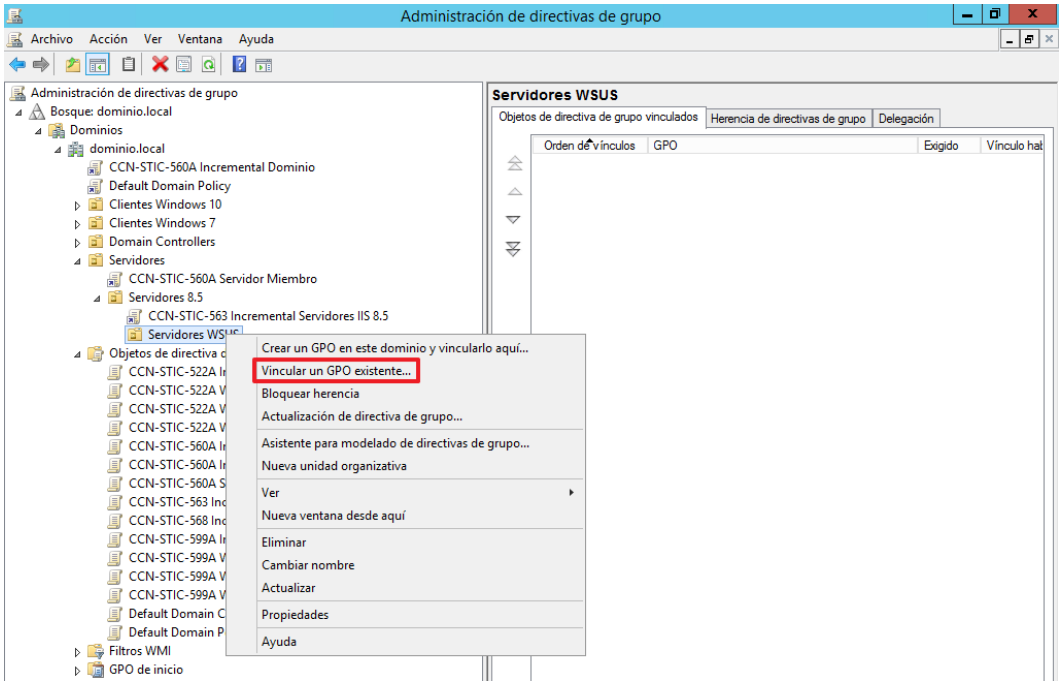
30. Seleccione la plantilla **"C:\Windows\security\templates\CCN-STIC-568 Plantilla Servidor WSUS"**.



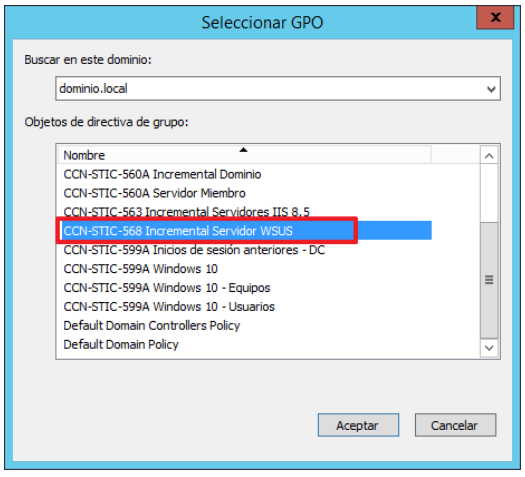
Haga clic en el botón **"Abrir".**

31. Cierre la ventana del Editor de administración de directivas de grupo.

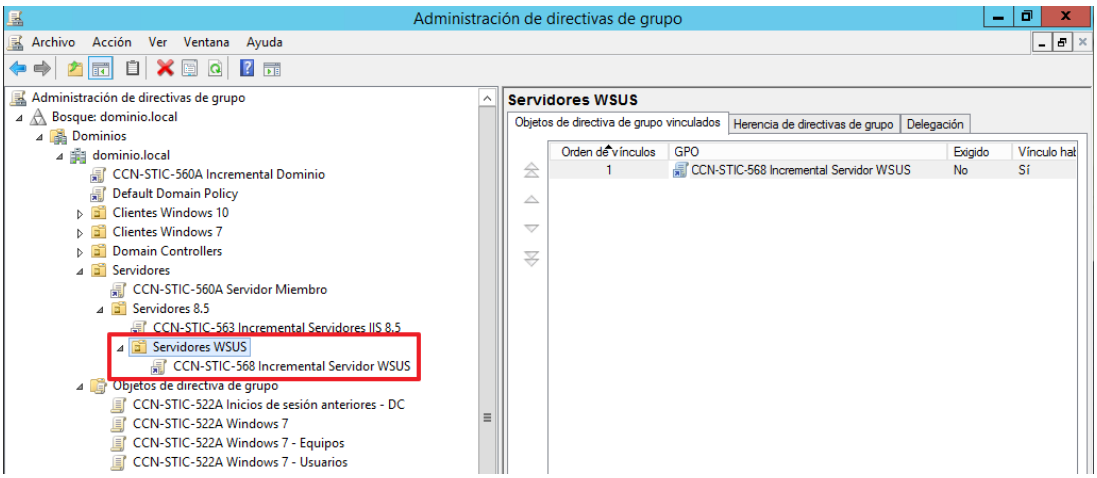
Paso	Descripción
32.	A continuación, debe vincular la GPO **"CCN-STIC-568 Incremental Servidor WSUS"** a la unidad organizativa que anteriormente ha creado, para ello, sobre la unidad organizativa **"<<dominio>> / <<unidad organizativa>/Servidores 8.5 / Servidores WSUS>"** pulse con el botón derecho y seleccione **"Vincular GPO existente…".**



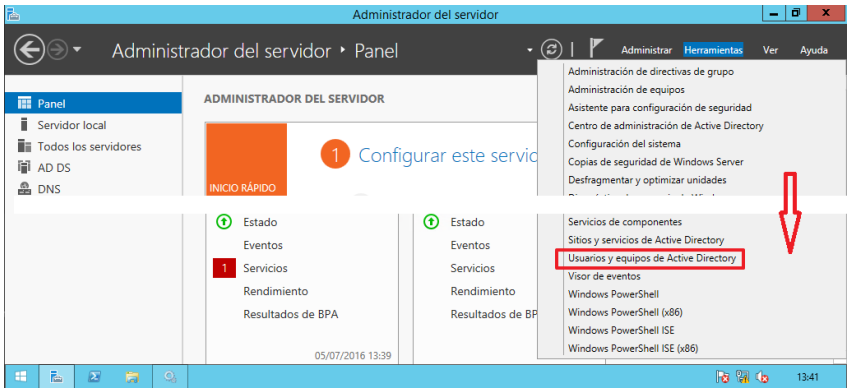
33.	Seleccione la GPO **"CCN-STIC-568 Incremental Servidor WSUS"** y pulse en **"Aceptar".**



Paso	Descripción
34.	Automáticamente, se habrá asociado a la unidad organizativa “Servidores WSUS”.



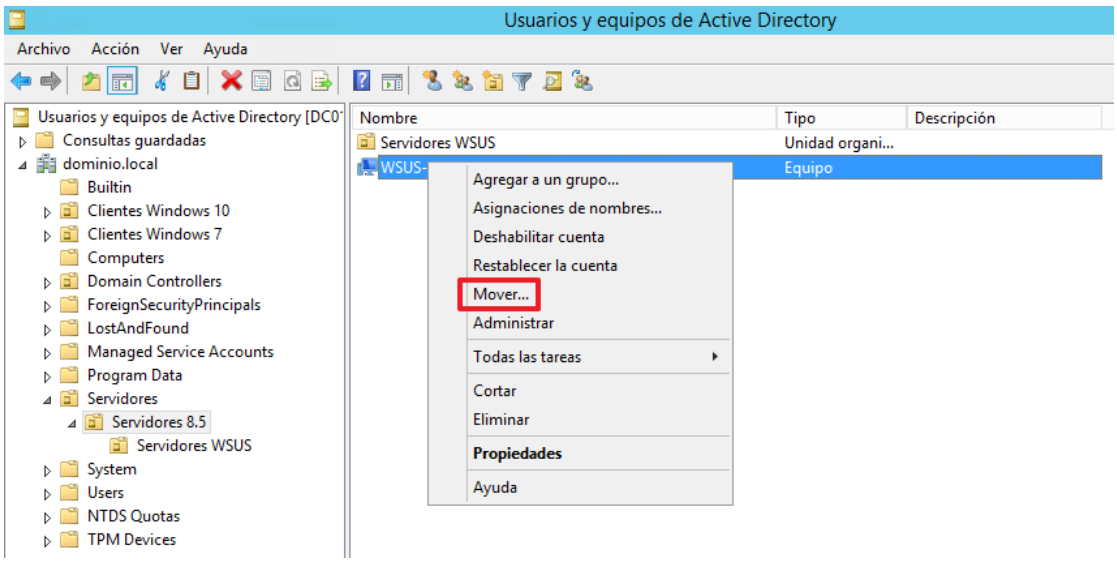
35.	Cierre la consola de “Administración de directivas de grupo”.
36.	Ejecute la consola Usuarios y equipos de Active Directory desde **“Inicio > Administrador del servidor > Herramientas > Usuarios y equipos de Active Directory”**.



Nota: Si inicia por primera vez la consola de “Administrador del Servidor” le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio “DOMINIO\SDT”.

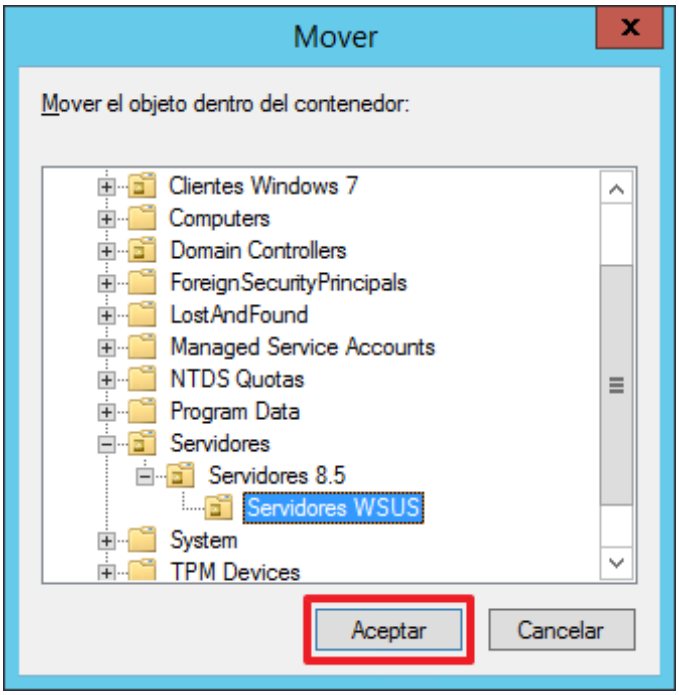
37.	En la consola, localice el objeto que representa el servidor en donde se instalarán los servicios de actualizaciones y muévalo desde su ubicación hasta la unidad organizativa **“Servidores WSUS”**.

Paso	Descripción
38.	Seleccione el servidor y con el botón derecho y haga clic en el menú **"Mover…"**.

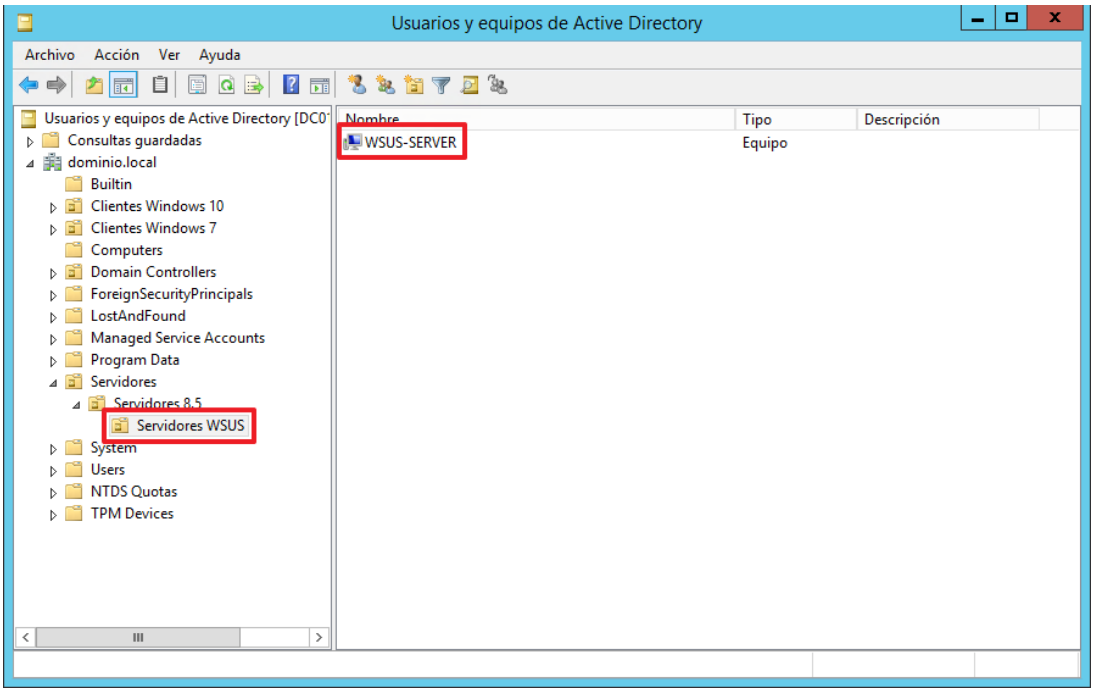


Nota: En este ejemplo se está utilizando un servidor con nombre "WSUS-Server". Es posible que en su organización se utilicen otros nombres de servidores.

39.	Seleccione la Unidad Organizativa **"Servidores / Servidores 8.5 / Servidores WSUS"** y haga clic en el botón **"Aceptar"**.



Paso	Descripción
40.	Compruebe que el equipo está en la unidad organizativa **"Servidores WSUS"**, tal y como se muestra a continuación.



41.	Será conveniente proceder a reiniciar el servidor que acaba de mover para que se le aplique correctamente la GPO y no haya problemas en la instalación del rol de Windows Server Update Services (WSUS) o bien ejecute un **gpudapte /force** mediante un símbolo de sistema. Antes de proceder a realizar la instalación del Rol Windows Server Update Services, asegúrese que la GPO que se acaba de crear está aplicando en el servidor adecuadamente.

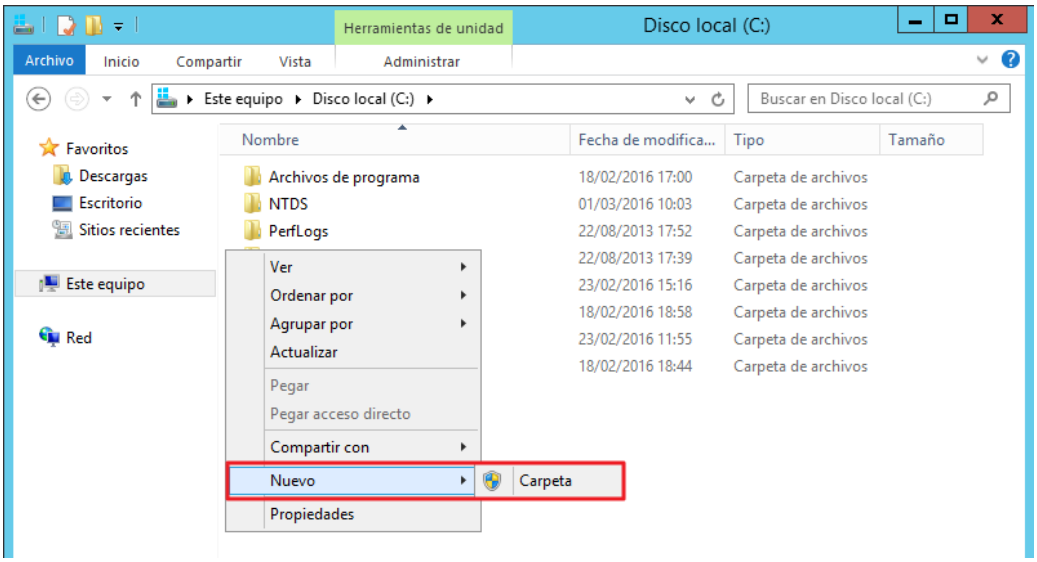
En este momento ya estará preparado el directorio activo para poder instalar el rol de Windows Server Update Services en el servidor correspondiente. Se volverán a aplicar directivas de grupo más adelante para realizar la configuración de los equipos cliente que estén enlazados con el servidor Windows Server Update Services.

2. INSTALACIÓN DE WINDOWS SERVER UPDATE SERVICES EN UN SERVIDOR MIEMBRO DEL DOMINIO

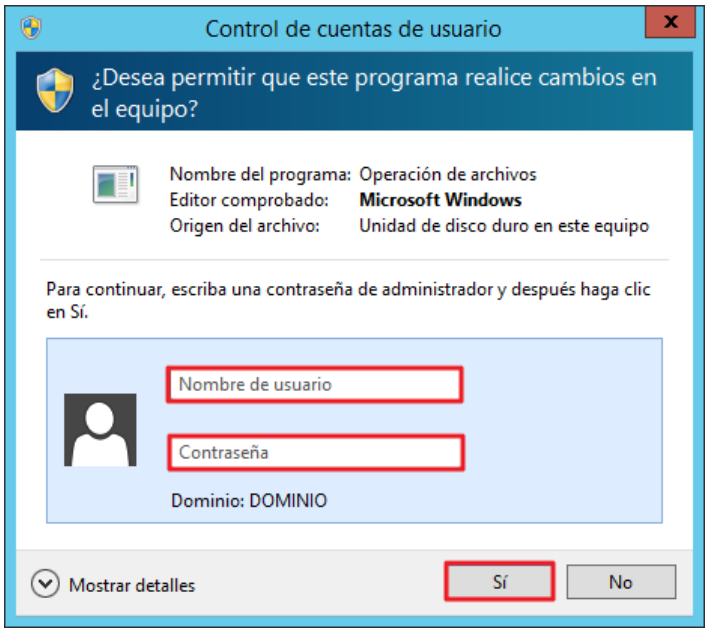
Los siguientes pasos describen el proceso de instalación del servidor de actualizaciones en un sistema Microsoft Windows Server 2012 R2. Se describe la instalación y configuración de una implementación de Windows Server Update Services para un entorno que no disponga de comunicación con el exterior. Las actualizaciones se importarán sobre este servidor y serán administradas por él mismo, el cual, las entregará a todos los equipos clientes que se encuentren enlazados al servidor WSUS y

estén habilitados para obtener las actualizaciones de un servidor de actualizaciones y no de Microsoft Update.

Nota: Es de requisito indispensable, que el equipo donde se vaya a instalar el rol de WSUS, contenga una partición o un disco duro nuevo con el objetivo de almacenar la base de datos que va a utilizar WSUS. Es muy importante que la letra de la unidad de la partición o del disco duro se le asigne la letra D:\. Para realizar esta operativa puede ser de gran ayuda la consola de "Administración de discos".
Todos los discos y particiones deberán formatearse utilizando el sistema de archivos NTFS, o cualquier otro que permita la aplicación de ACL´s.

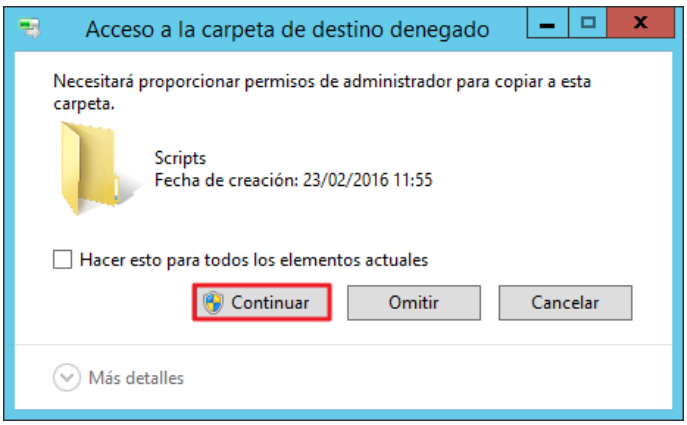
Paso	Descripción
42.	Si no lo ha hecho anteriormente, inicie sesión en el equipo en donde se va a instalar el servidor de actualizaciones. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
43.	Cree el directorio "Scripts" en la unidad C:\. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **"Nuevo > Carpeta"**. 

Paso	Descripción
44.	El “control de cuentas de usuario” le pedirá elevación de privilegios, para ello ingrese una cuenta “administrador del dominio”.



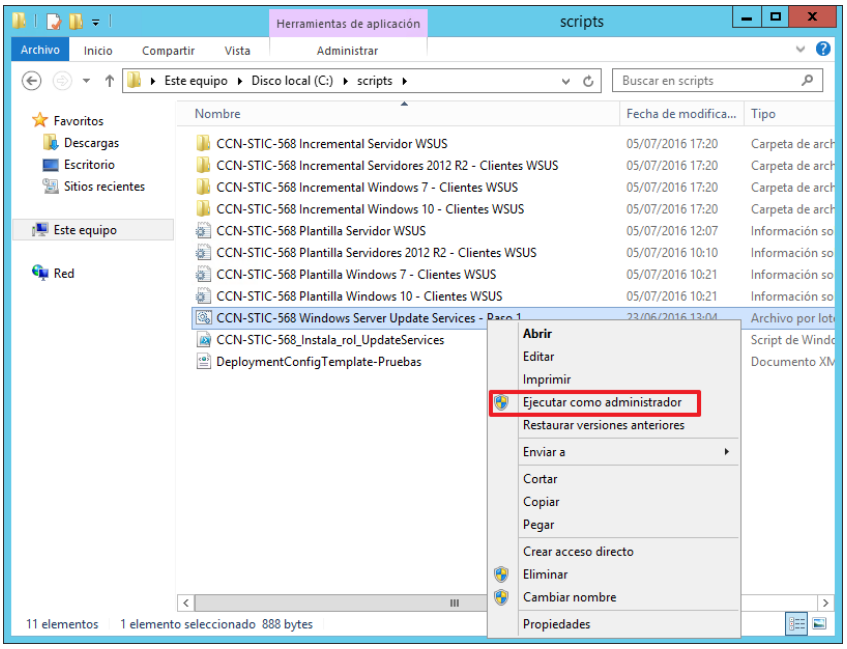
Nota: Para crear directorios en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administrador en el servidor.
En este ejemplo se utiliza la cuenta “DOMINIO\SDT”.

45.	Asigne el nombre **“Scripts”** al nuevo directorio.
46.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio **“C:\Scripts”**.

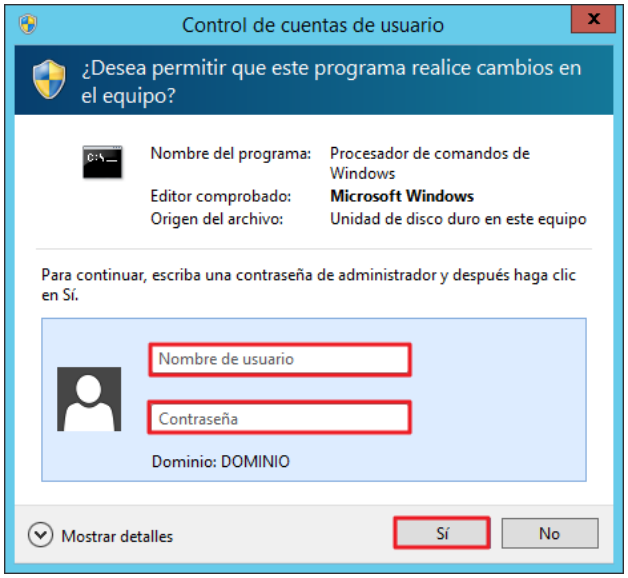


Nota: Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de una cuenta con permisos de administrador en el servidor.
En este ejemplo se utiliza la cuenta “DOMINIO\SDT”.

Paso	Descripción
47.	Acceda a la carpeta **"C:/Scripts"**.
48.	Con el botón derecho, seleccione el fichero denominado **"CCN-STIC-568 Windows Server Update Services – Paso 1.bat"** y haga clic en **"Ejecutar como administrador"**.

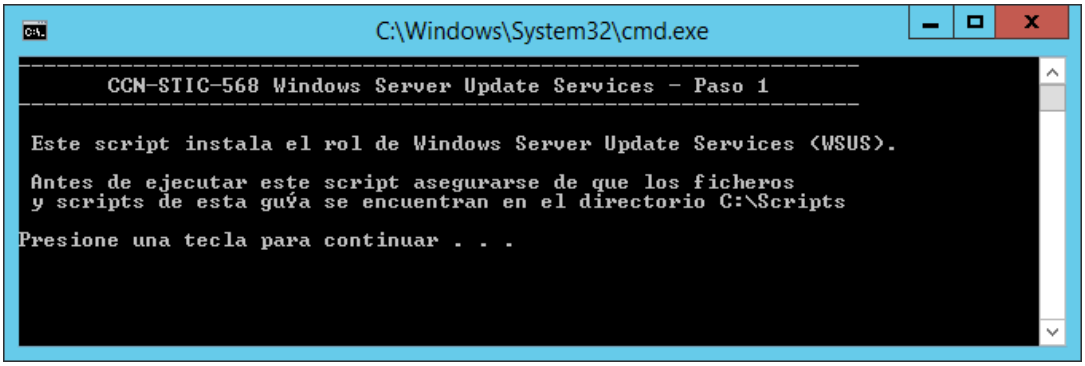


49.	El control de cuentas de usuario le solicitará las credenciales del administrador de dominio que se están utilizando para instalar el servidor de actualizaciones.

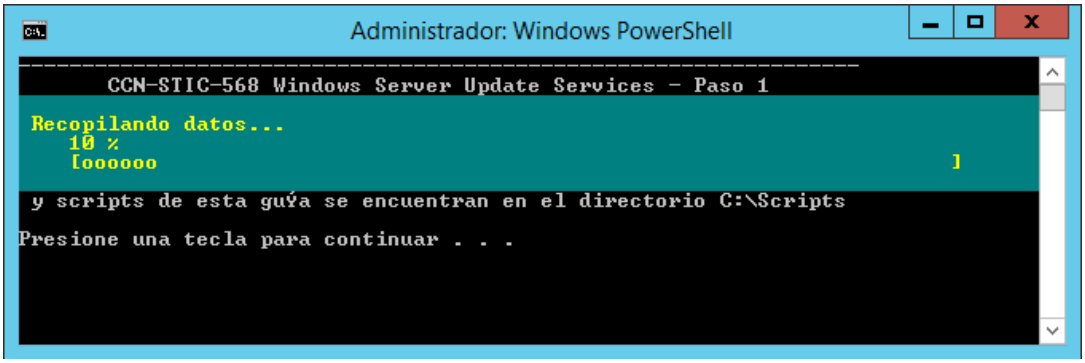


Nota: En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT" que pertenece al grupo "Usuarios de shells" del dominio.

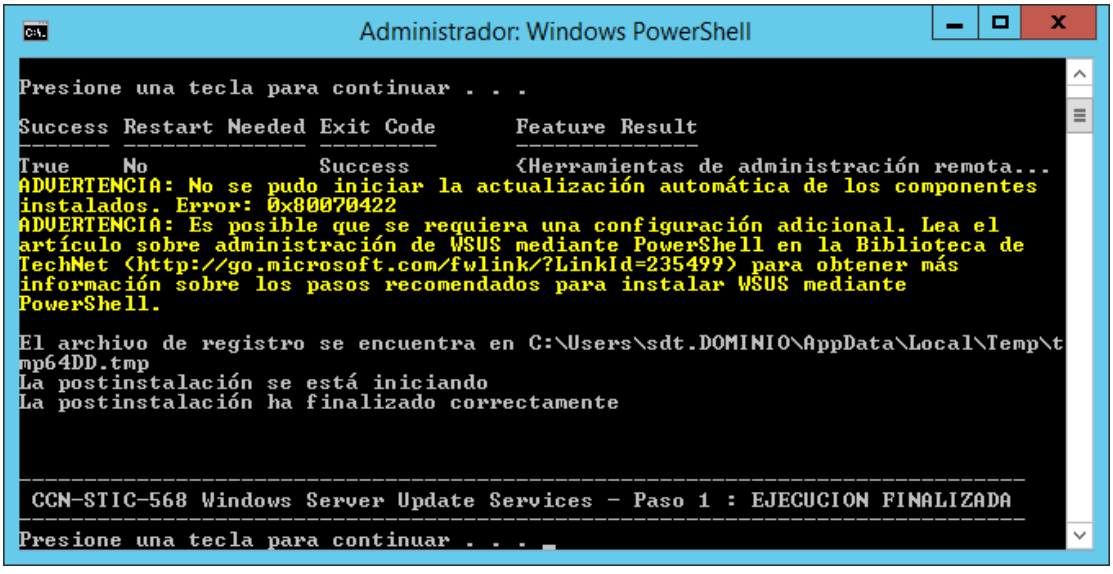
Paso	Descripción
50.	Aparecerá la siguiente pantalla.



51.	Pulse una tecla para iniciar el proceso de instalación y espere a que finalice.



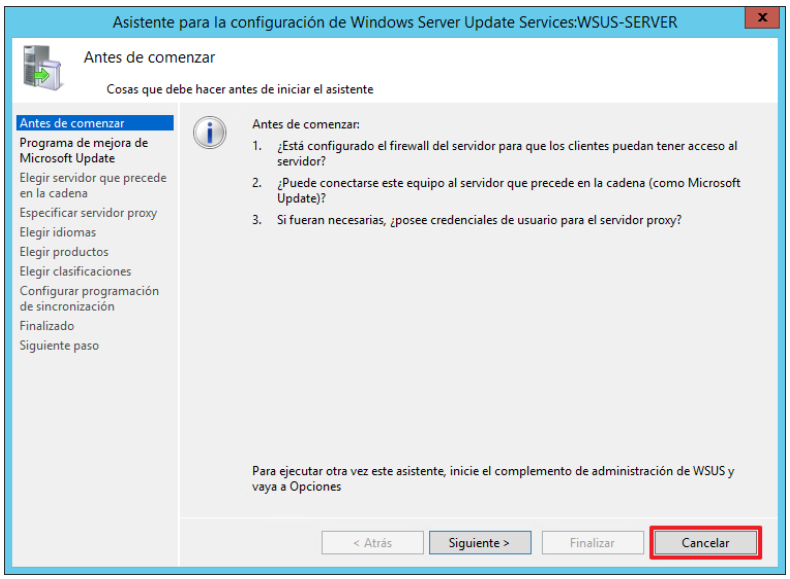
52.	Una vez instalado el rol de Windows Server Update Service, aparecerán dos advertencias indicando que no se pudo iniciar la actualización automática de los componentes instalados y que se requiere una post-instalación. Ignore estos mensajes. Pulse cualquier tecla para finalizar.



Paso	Descripción
53.	Ejecute la consola de Windows Server Update Service, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.

Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

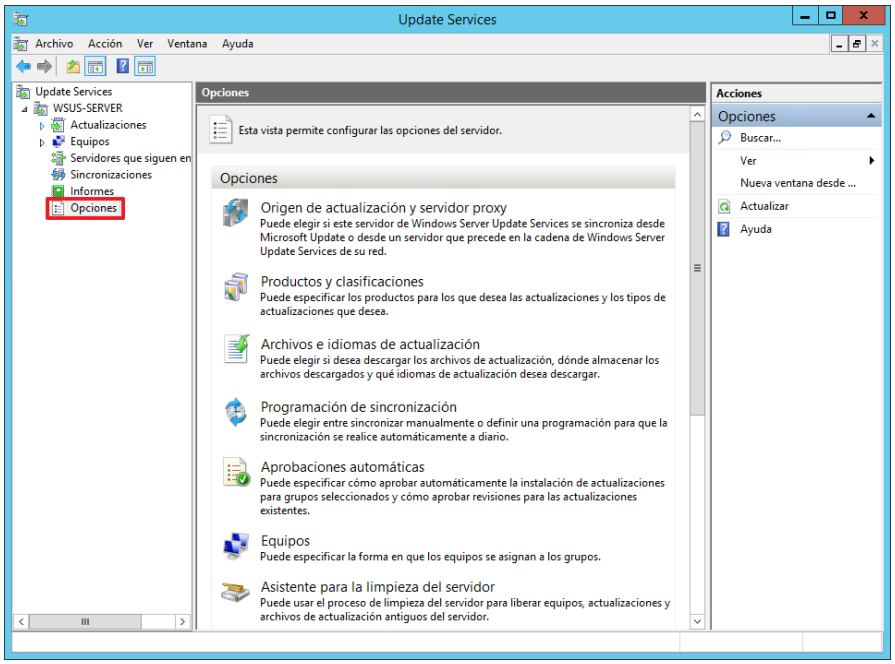
54.	En este momento se iniciará el "Asistente para la configuración de WSUS", pulse **"Cancelar"** en la ventana de **"Antes de comenzar"**.



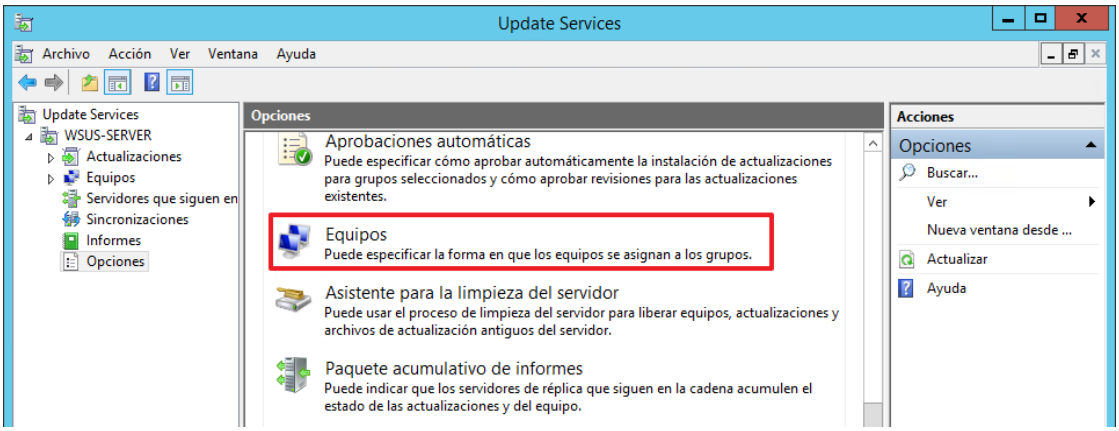
Nota: La decisión de cancelar el asistente de configuración de WSUS se debe a que para la implantación de la presente guía no es necesario ningún tipo de configuración que nos proporciona el asistente de WSUS.

Las configuraciones necesarias se realizarán en el presente punto y en el Anexo "TAREAS ADMINISTRATIVAS EN EL SERVIDOR RAÍZ WINDOWS SERVER UPDATE SERVICES."

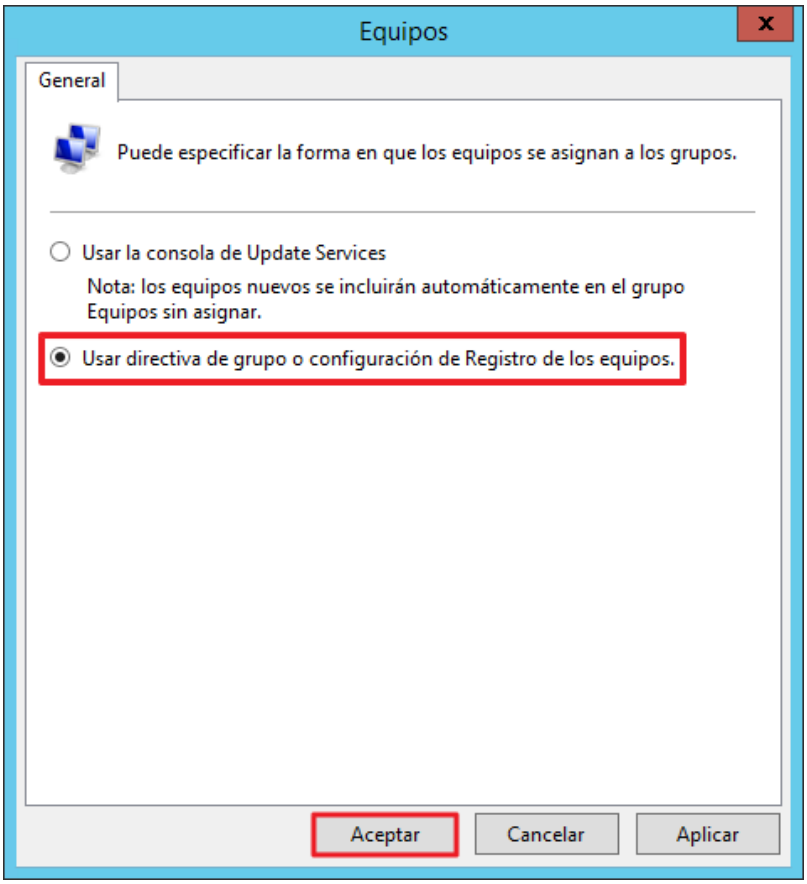
Paso	Descripción
55.	Se abrirá la consola de administración de Windows Server Update Services, diríjase en la columna de la izquierda a **"Update Services > <Su servidor WSUS> > Opciones".**



56.	En la pestaña "Opciones", pinche en **"Equipos"**.



Paso	Descripción
57.	Se abrirá una nueva ventana, deberá marcar la segunda opción: **"Usar directiva de grupo o configuración de Registro de los equipos".**



Pulse en **"Aceptar"** para guardar los cambios.

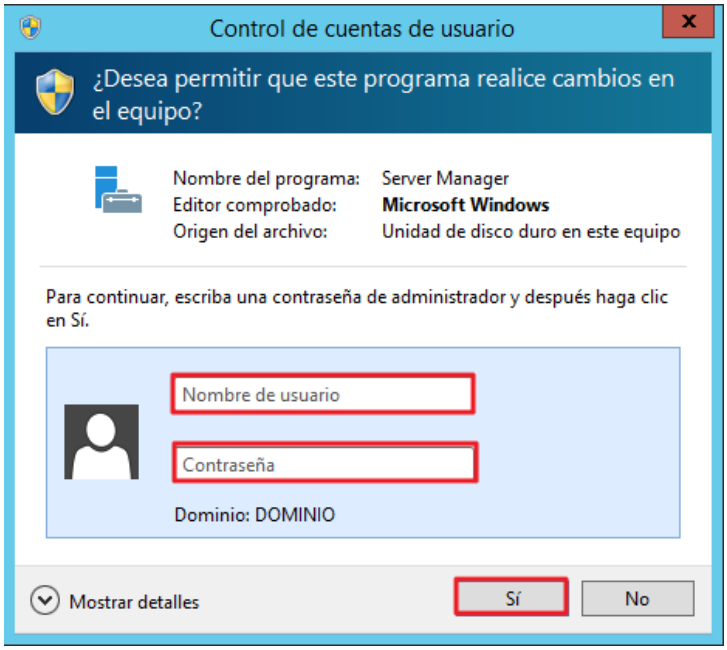
58.	Cierre la consola de Windows Server Update Services.

3. PROTEGER WSUS CON EL PROTOCOLO DE CAPA DE SOCKETS SEGUROS (SSL)

Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones que transmiten información de ida y vuelta, se encuentre cifrada y segura. Las aplicaciones que utilizan el protocolo SSL se encargan de enviar y recibir claves de cifrado con otras aplicaciones, de igual manera el protocolo controla la manera en que se cifran y descifran los datos enviados entre ambas. Para proteger la comunicación entre los clientes WSUS y el propio servidor de actualizaciones, el cifrado que se aplica en la comunicación entre ambos, consiste en cifrar los metadatos de las actualizaciones, pero no el contenido de las mismas. Por lo tanto, los metadatos cifrados viajan por el puerto 443 (HTTPS) y las actualizaciones por el puerto 80 (HTTP).

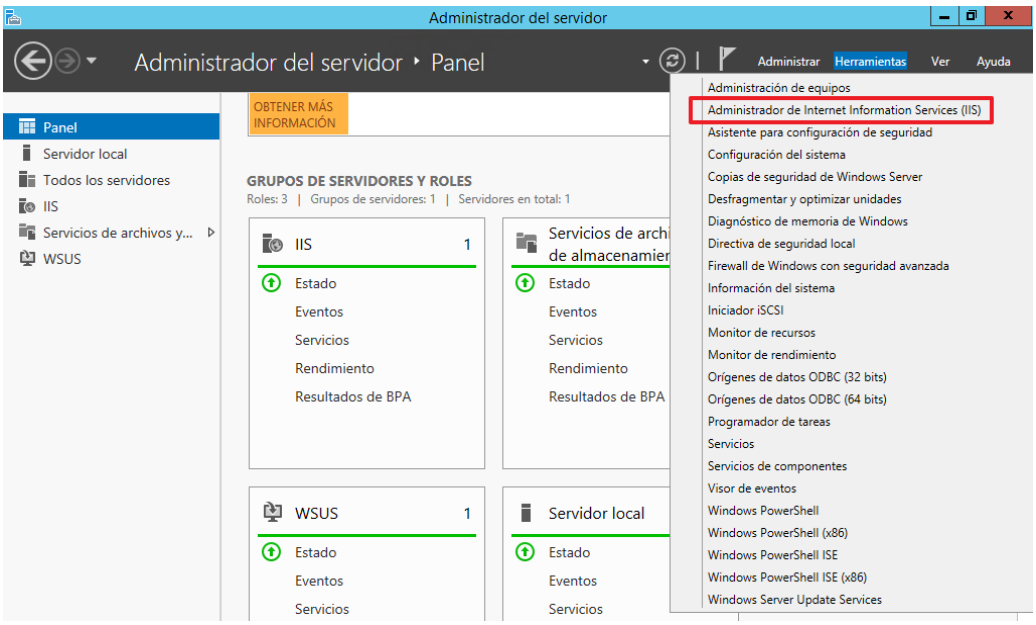
3.1. CONFIGURACIÓN DE SSL EN EL SERVIDOR RAÍZ DE WINDOWS SERVER UPDATE SERVICES

Los pasos que se describen a continuación, se realizan sobre el servidor Windows Server Update Services miembro del dominio y que tiene instalado un Servidor Web (IIS). Se detalla cómo configurar la administración WSUS para que requiera SSL en los "Sites" que se encuentra en la consola de Internet Information Services (IIS).

Paso	Descripción
59.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
60.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.  **Nota:** En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

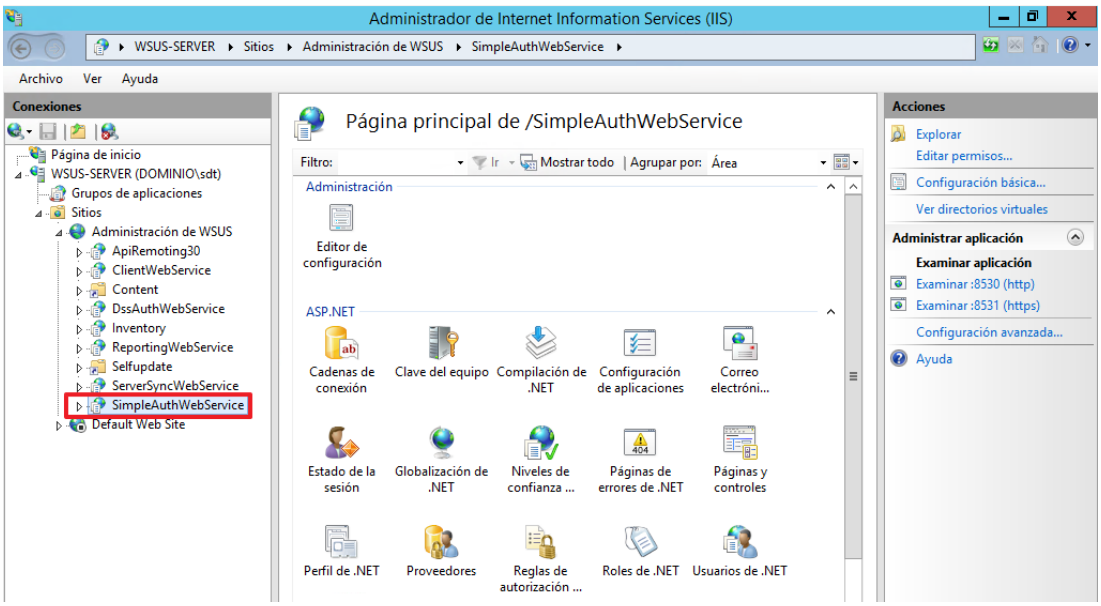
Paso	Descripción

61. Ejecute la consola de Administrador de Internet Information Services (IIS) desde el menú **"Inicio > Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)"**.

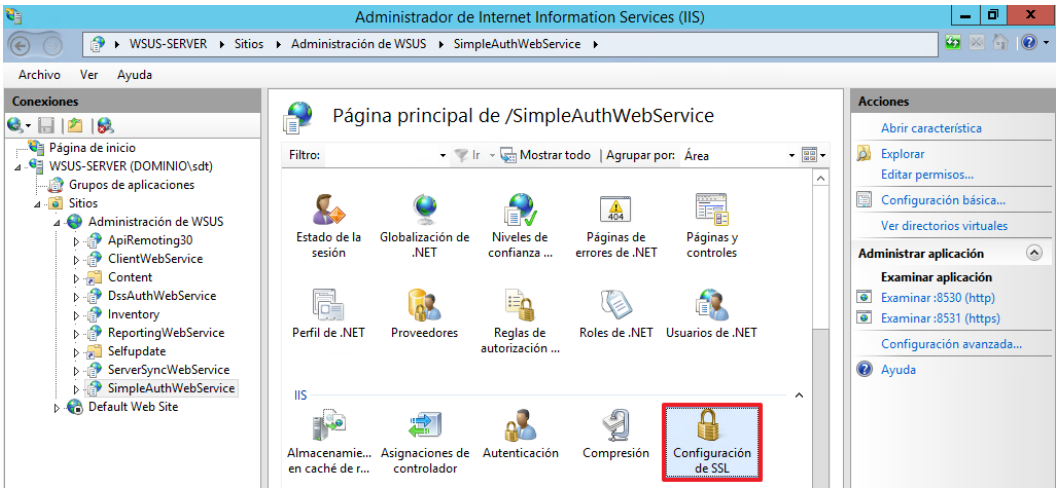


Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

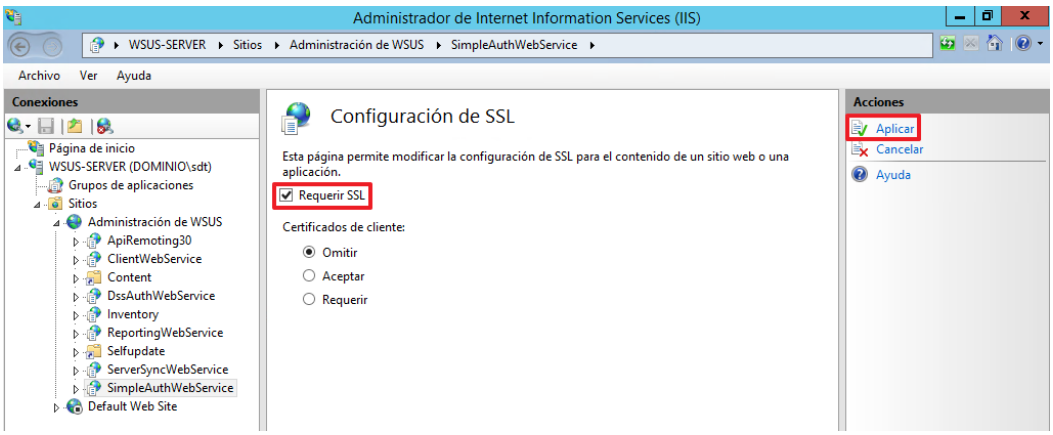
62. En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **"(Su servidor IIS) > Sitios > Administración de WSUS > SimpleAuthWebService"**



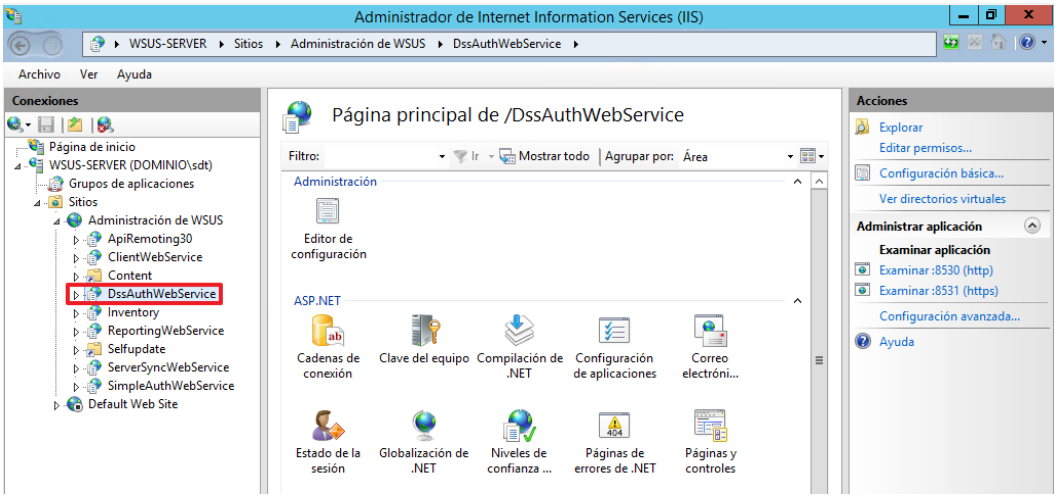
Paso	Descripción
63.	En la página principal de "/SimpleAuthWebService", haga doble clic sobre la característica **"Configuración SSL".**



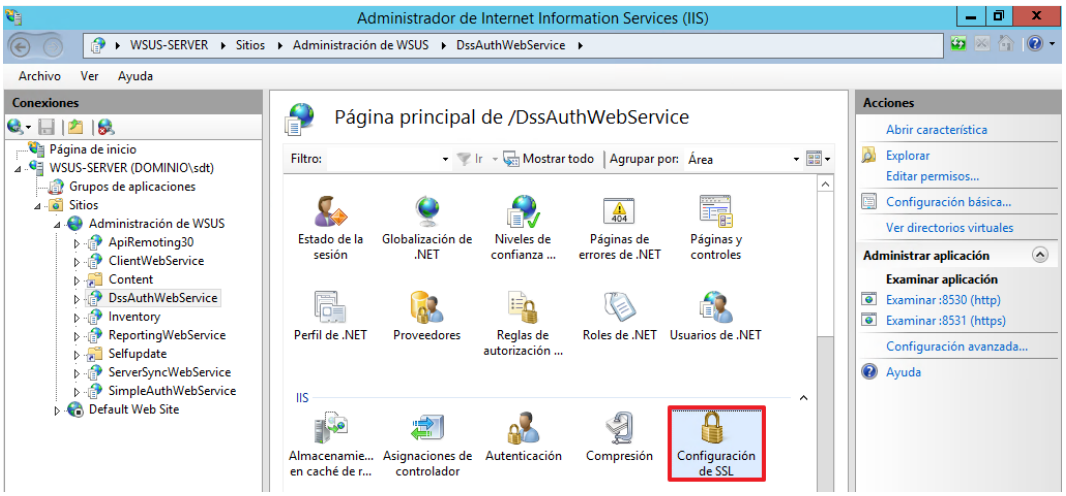
64.	Dentro de la característica "Configuración de SSL", debe habilitar la pestaña de **"Requerir SSL"**. A continuación, pinche en **"Aplicar"** para guardar los cambios.



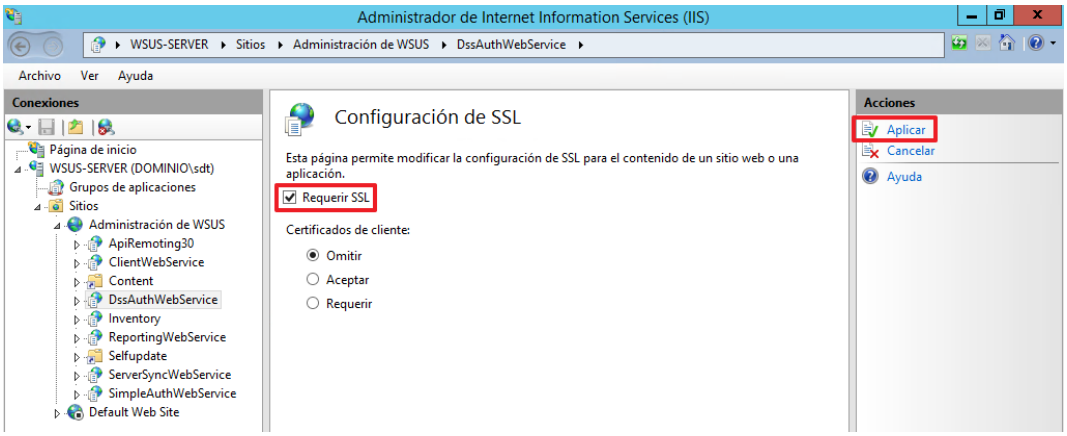
Paso	Descripción
65.	En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **"(Su servidor IIS) > Sitios > Administración de WSUS > DssAuthWebService"**



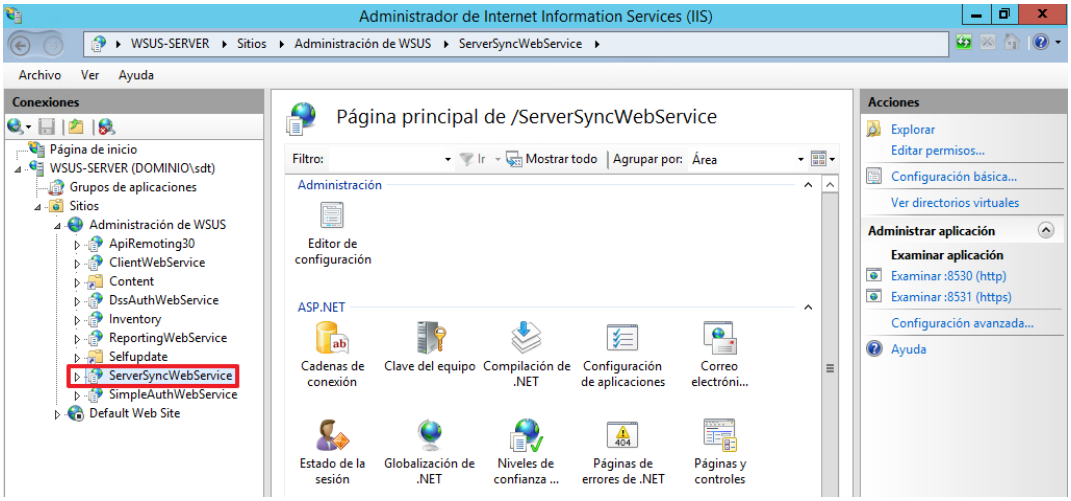
66.	En la página principal de "/DssAuthWebService", haga doble clic sobre la característica **"Configuración SSL".**



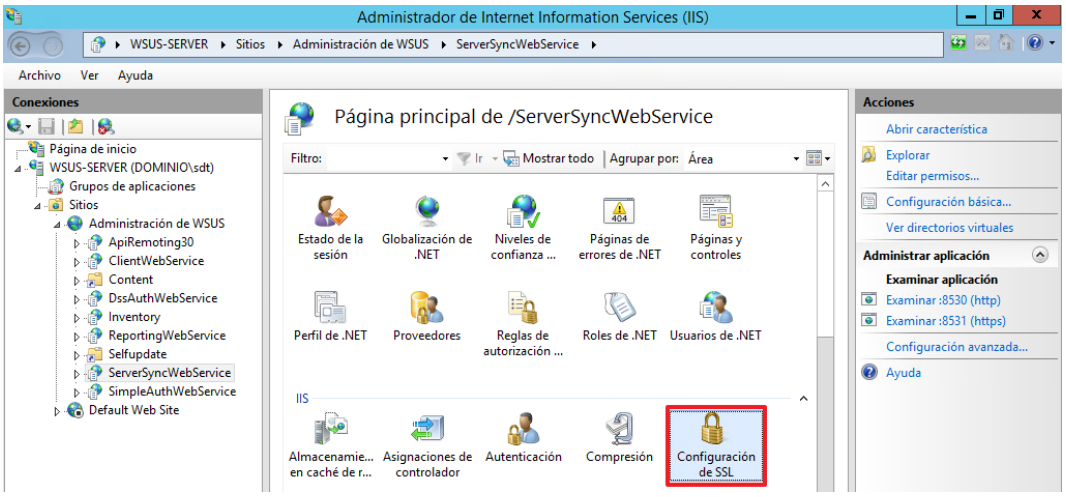
Paso	Descripción
67.	Dentro de la característica “Configuración de SSL”, debe habilitar la pestaña **“Requerir SSL”**. A continuación, pinche en **“Aplicar”** para guardar los cambios.



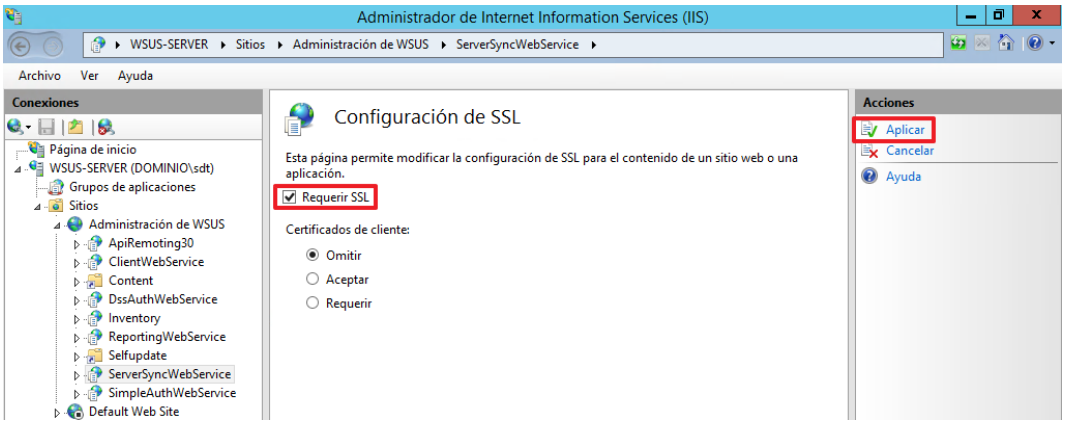
68.	En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **“(Su servidor IIS) > Sitios > Administración de WSUS > ServerSyncWebService”**



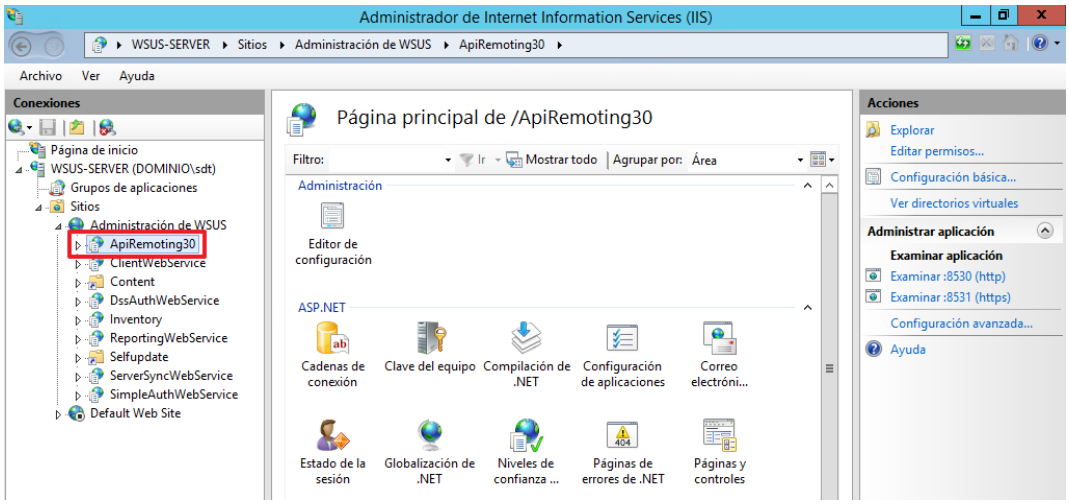
Paso	Descripción
69.	En la página principal de "/ServerSyncWebService", haga doble clic sobre la característica **"Configuración SSL".**



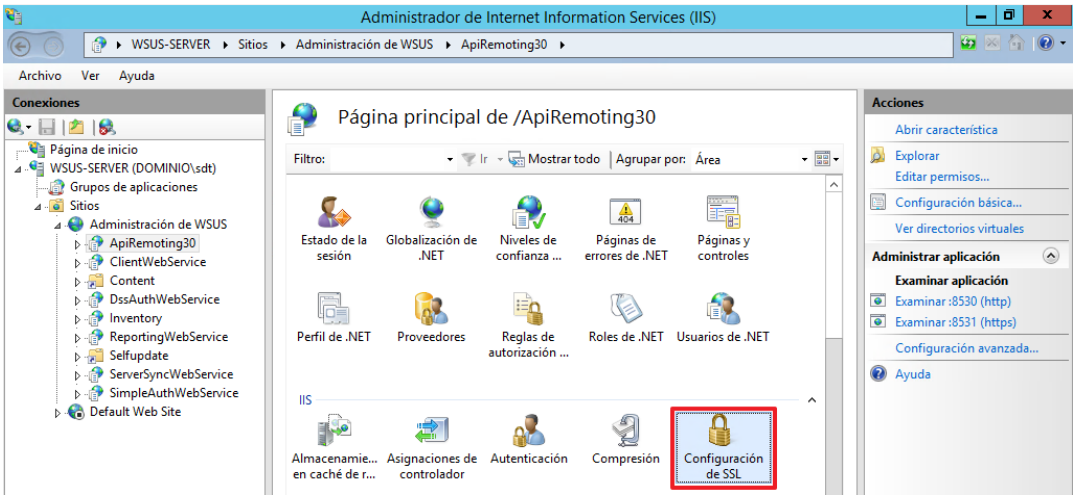
70.	Dentro de la característica "Configuración de SSL", debe habilitar la pestaña de **"Requerir SSL"**. A continuación, pinche en **"Aplicar"** para guardar los cambios.



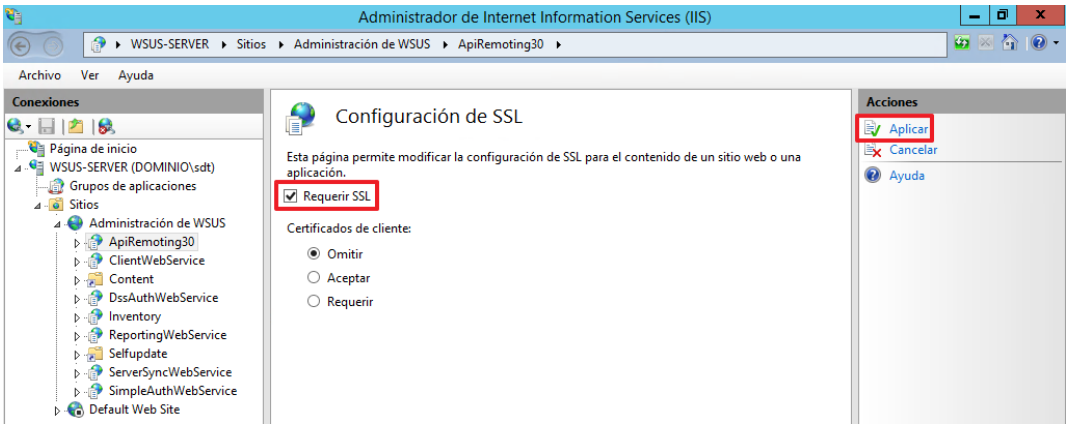
Paso	Descripción
71.	En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **"(Su servidor IIS) > Sitios > Administración de WSUS > ApiRemoting30".**



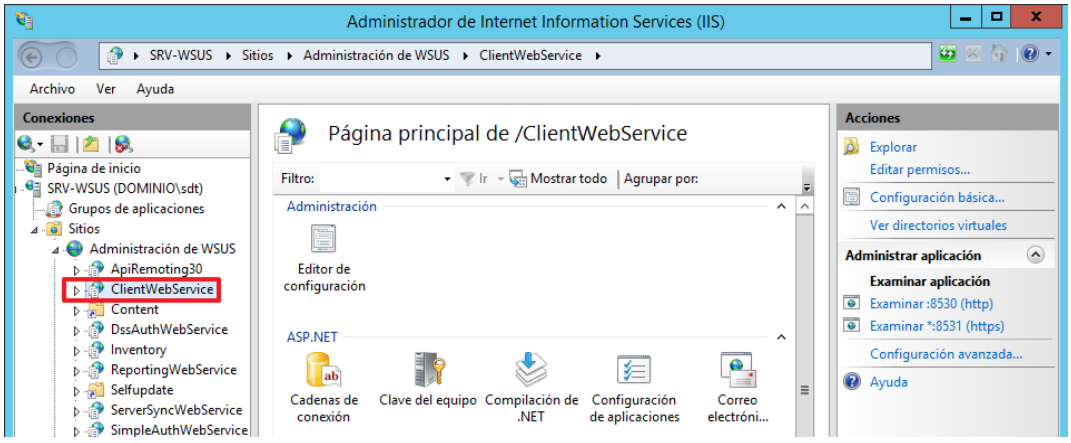
72.	En la página principal de "/ApiRemoting30", haga doble clic sobre la característica **"Configuración SSL".**



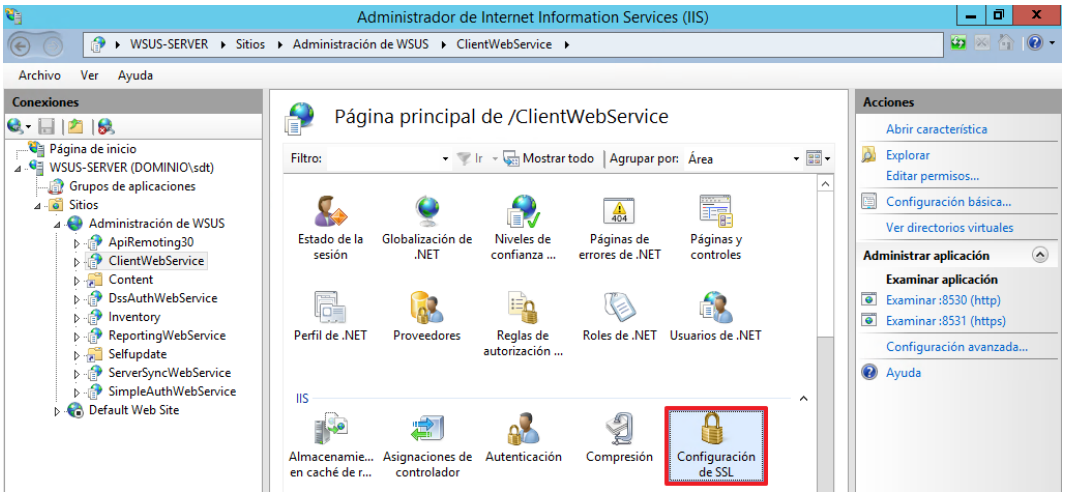
Paso	Descripción
73.	Dentro de la característica "Configuración de SSL", debe habilitar la pestaña de **"Requerir SSL".** A continuación, pinche en **"Aplicar"** para guardar los cambios.



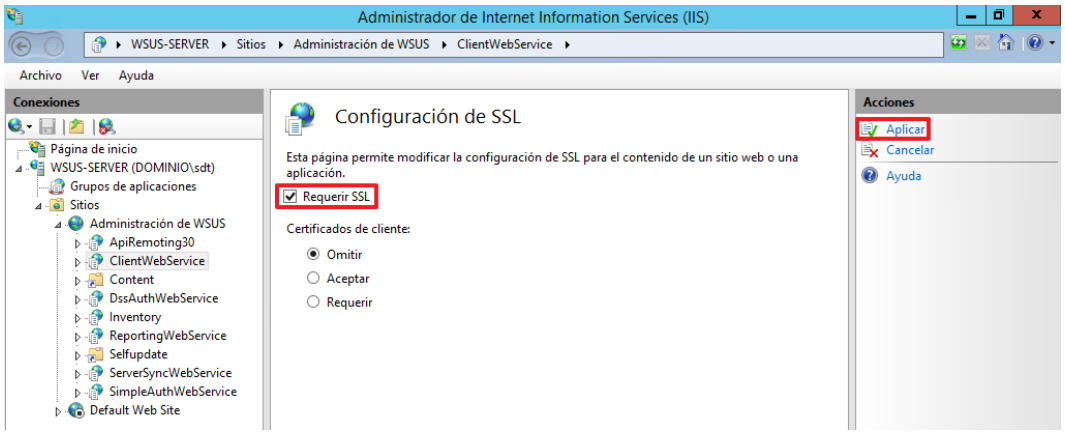
74.	En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **"(Su servidor IIS) > Sitios > Administración de WSUS > ClientWebService".**



Paso	Descripción
75.	En la página principal de "/ClientWebService", haga doble clic sobre la característica **"Configuración SSL".**

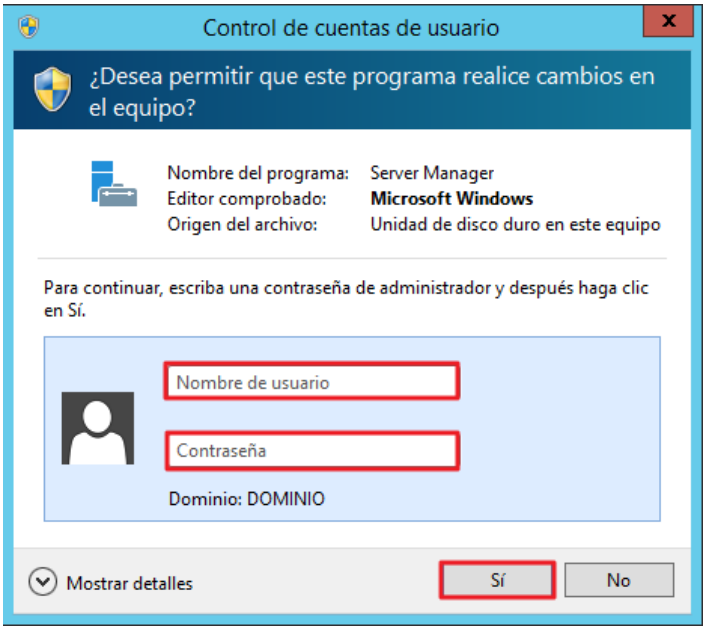


76.	Dentro de la característica "Configuración de SSL", debe habilitar la pestaña de **"Requerir SSL".** A continuación, pinche en **"Aplicar"** para guardar los cambios.

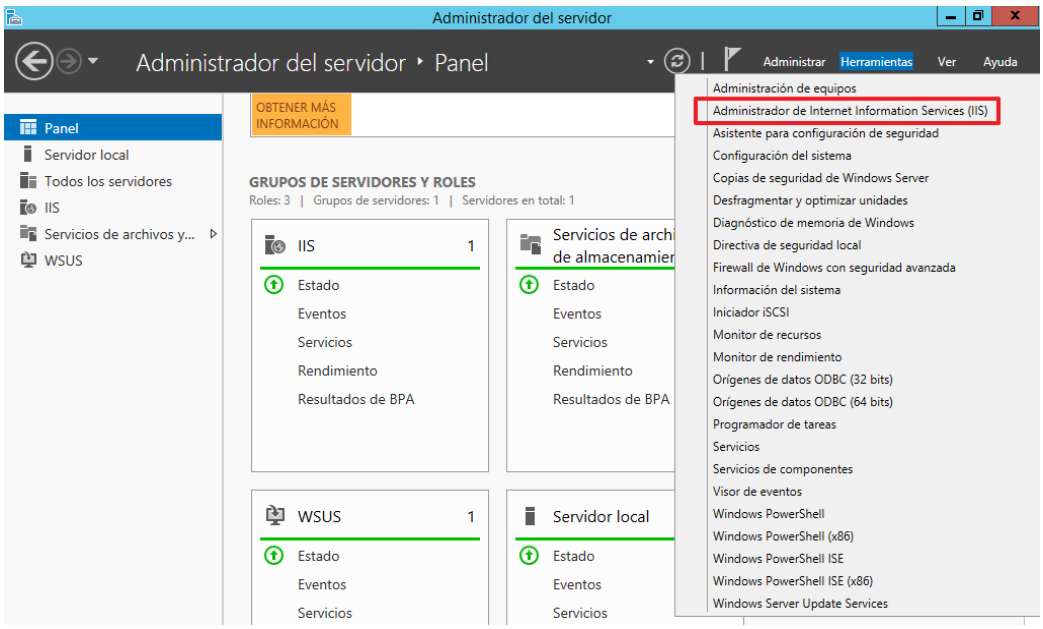


3.2. EMISIÓN DEL CERTIFICADO DE CONFIANZA Y EXPORTACIÓN DEL MISMO

Una vez que ha configurado los "Sites" de la administración de WSUS en el IIS para que requiera SSL, deberá generar un certificado autofirmado por el servidor de WSUS para que la comunicación con los equipos cliente sea efectiva y segura. Además, deberá exportarlo para facilitárselo a los equipos clientes del servidor de actualizaciones Windows Server Update Services.

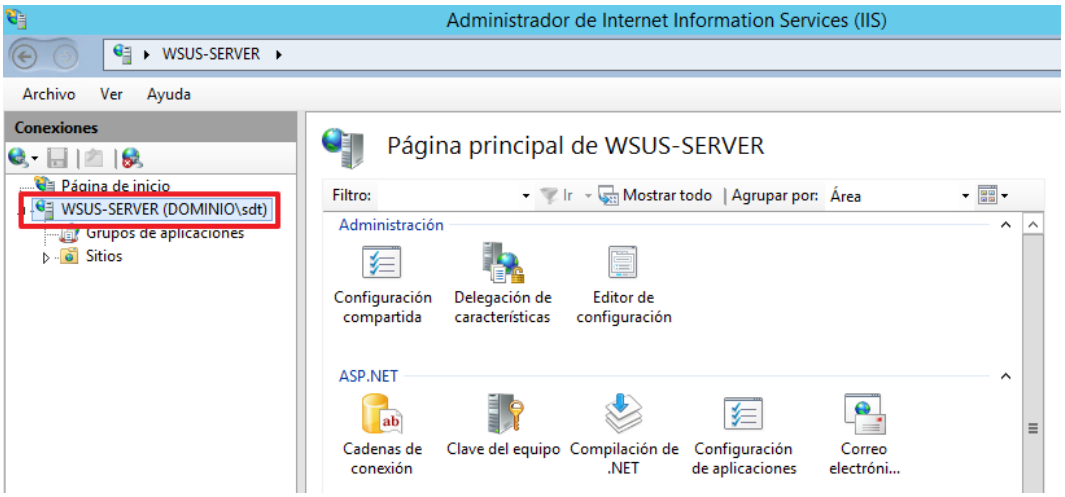
Paso	Descripción
77.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
78.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.  **Nota:** En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

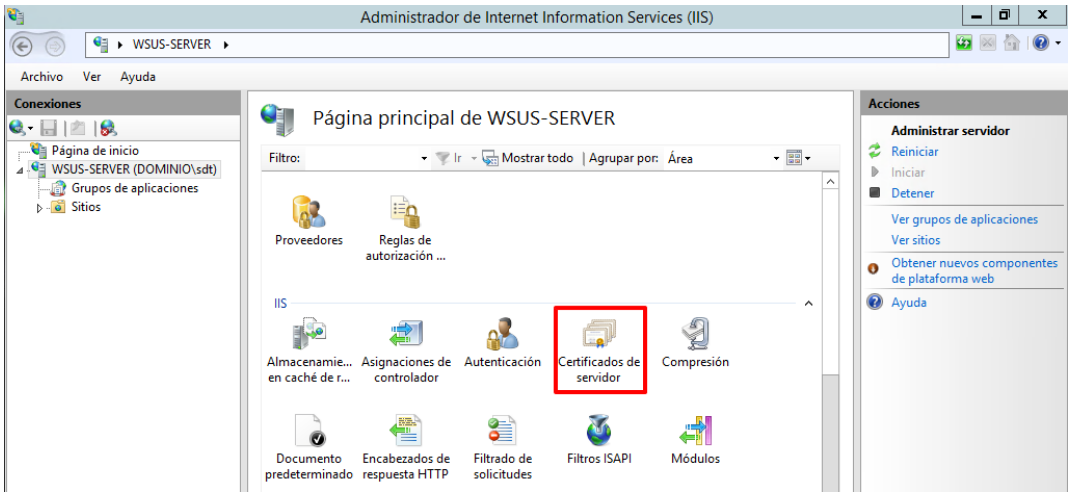
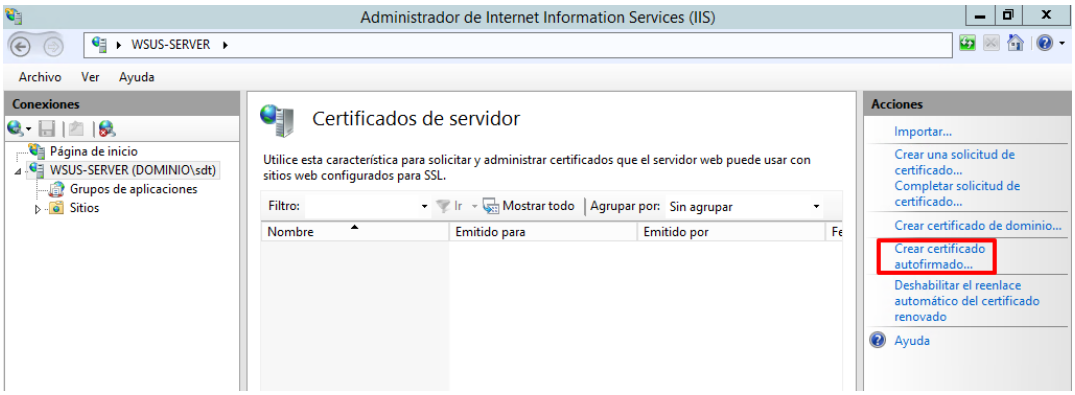
Paso	Descripción
79.	Ejecute la consola de Administrador de Internet Information Services (IIS) desde el menú **"Inicio > Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)"**.



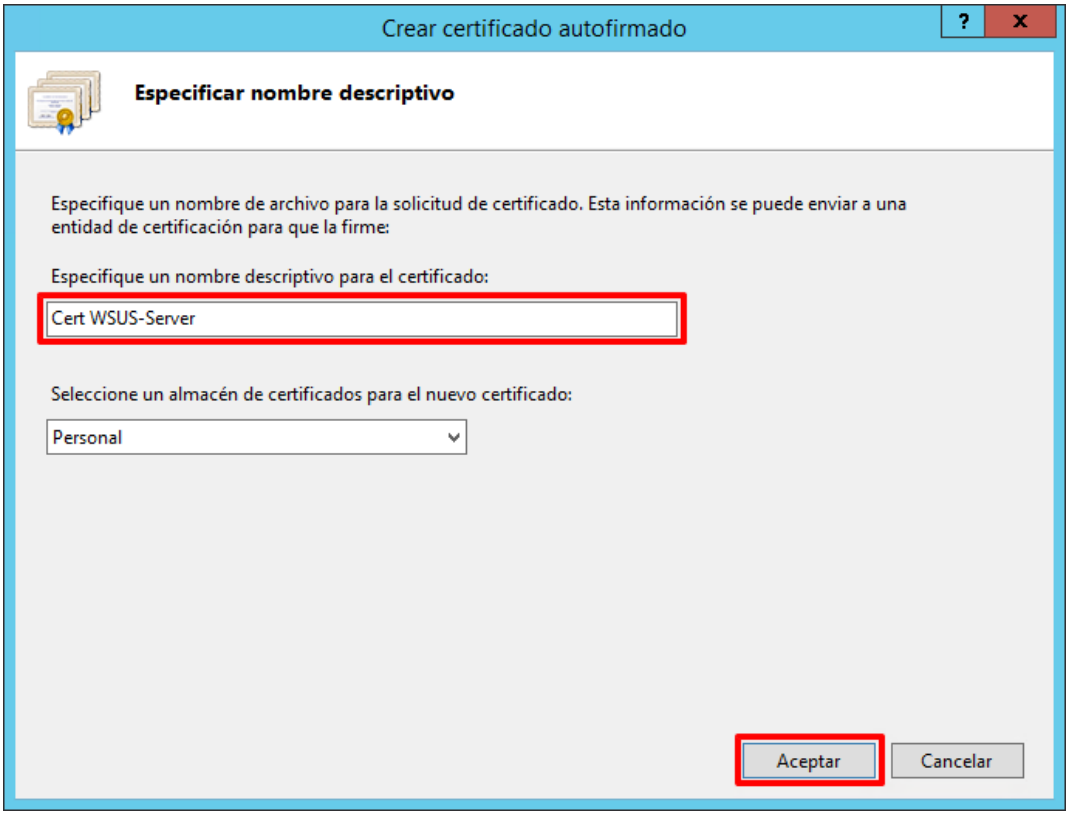
Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utilizará la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

80.	En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a **"Página de inicio > (Su servidor IIS)".**



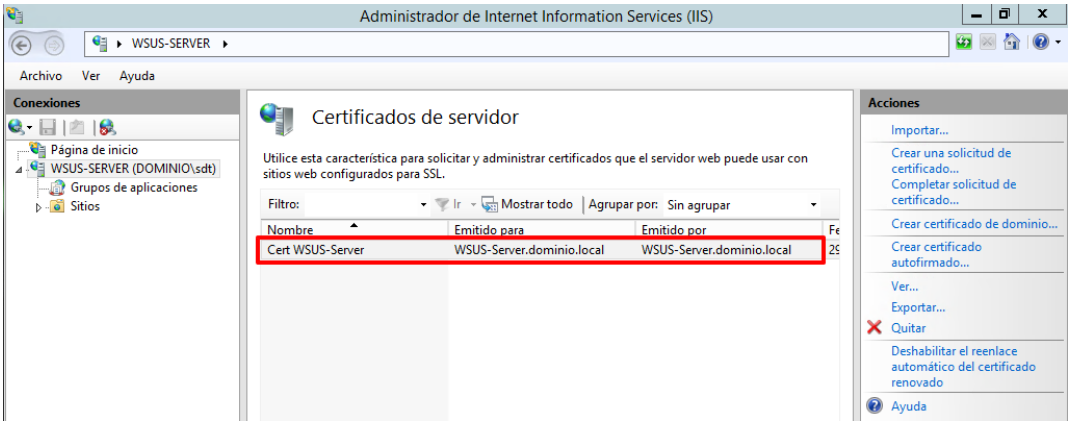
Paso	Descripción
81.	En la parte central de la consola, haga doble clic en **"Certificados de servidor".** 
82.	Dentro de "Certificados de servidor", en la columna de la derecha pulse sobre **"Crear certificado autofirmado…"** 

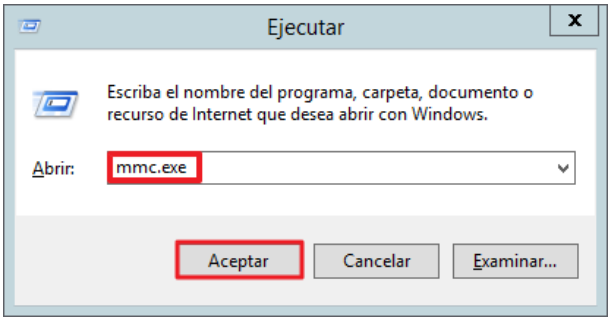
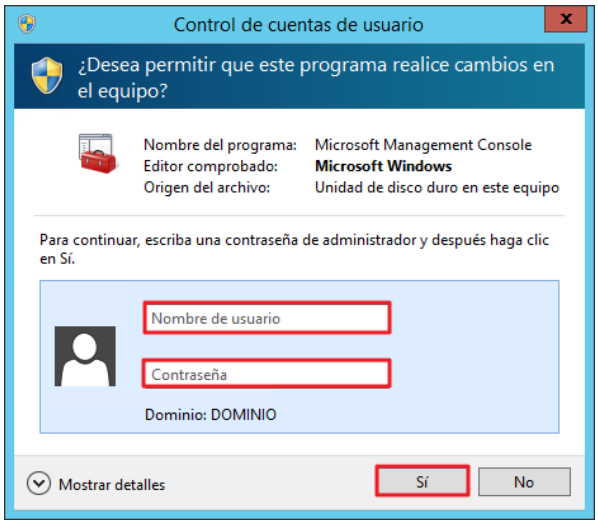
Paso	Descripción
83.	Se abrirá una ventana donde se indicará el nombre y el almacenamiento del certificado. Cuando haya proporcionado un nombre, pulse en **"Aceptar"** para continuar.



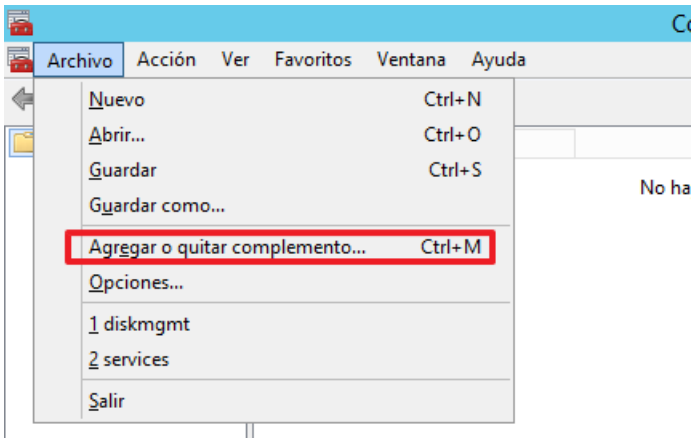
Nota: En este ejemplo se utiliza el nombre descriptivo como Cert WSUS-Sever, usted podrá elegir el nombre que más se adapte a su organización.

84.	Si todo salió correctamente, deberá existir dicho certificado en "Certificados del servidor". Tal y como se muestra en la siguiente imagen:

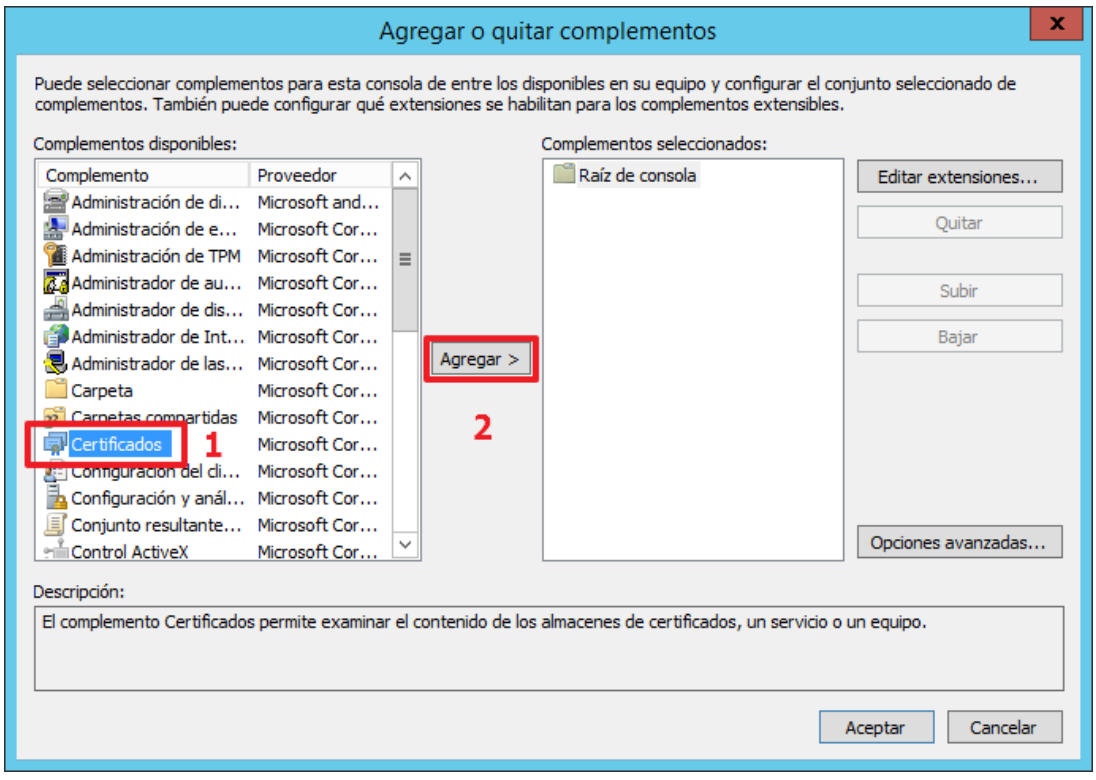


Paso	Descripción
85.	El paso descrito anteriormente, habrá generado un certificado de confianza, deberá comprobar que efectivamente se ha creado este certificado. Para ello, pulse la tecla **⊞ + R** y escriba **"MMC.EXE",** tal y como se muestra en la siguiente imagen:  Pulse **"Aceptar"** para abrir la consola.
86.	El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.  **Nota:** En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

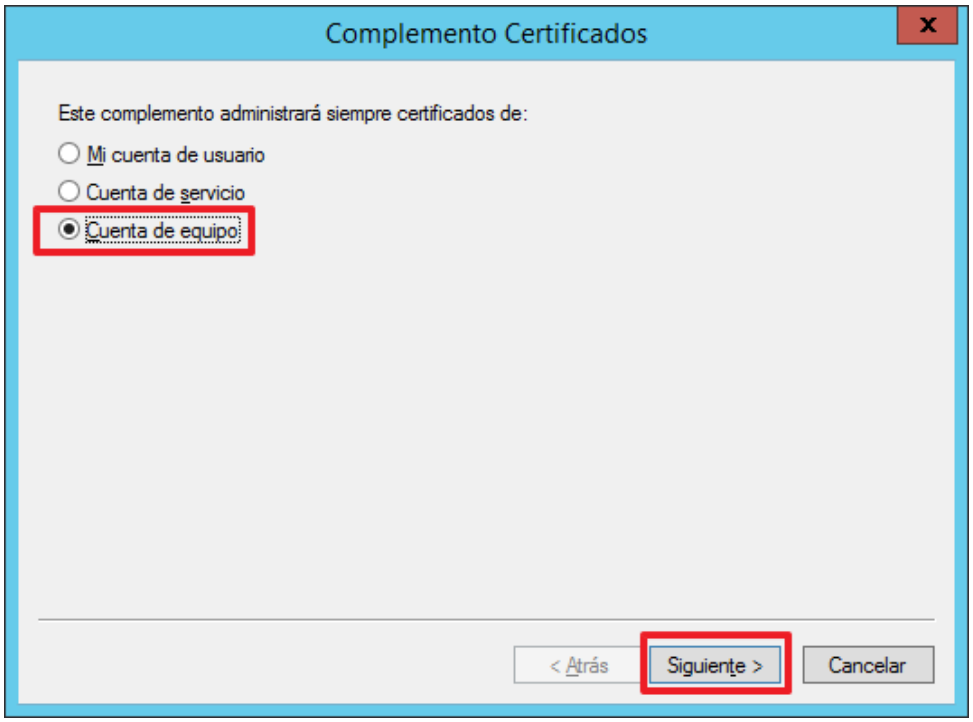
Paso	Descripción
87.	Se abrirá la consola MMC, seguidamente pinche en **"Archivo > Agregar o quitar complemento..."**.



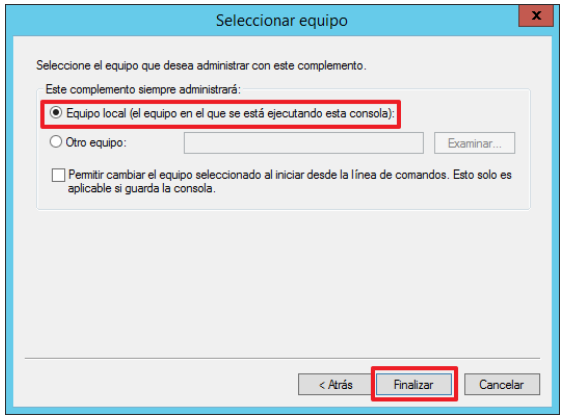
88.	En "Agregar o quitar complemento" seleccione **"Certificados"** y pulse en **"Agregar".**



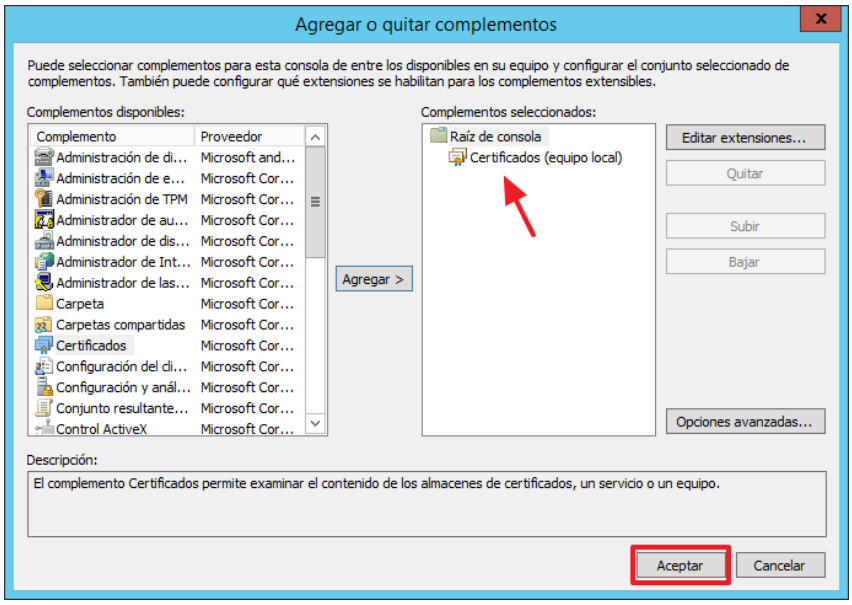
Paso	Descripción
89.	En la venta de "Complemento Certificados", seleccione **"Cuenta de equipo"** y pulse en **"Siguiente".**



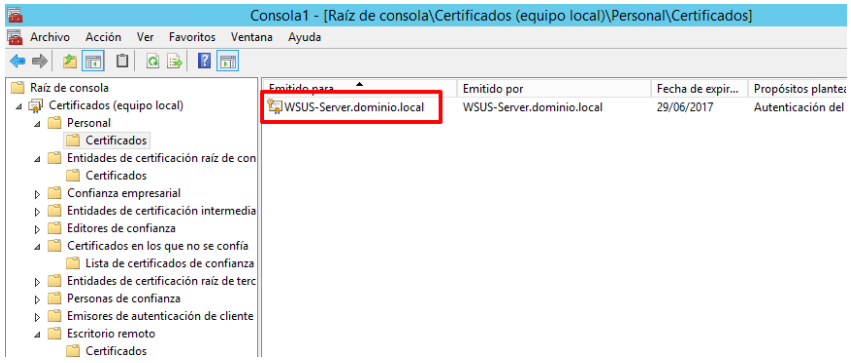
90.	Seleccione **"Equipo Local (el equipo en el que se está ejecutando esta consola)"** en la ventana siguiente, seguidamente pulse **"Finalizar".**



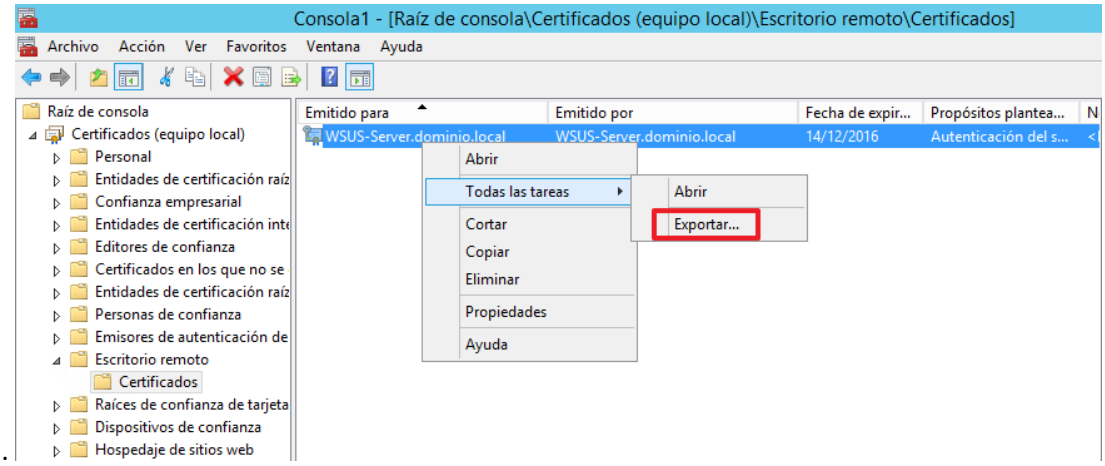
Paso	Descripción
91.	Pulse en **"Aceptar"** en la ventana de "Agregar o quitar complementos" para guardar los cambios.



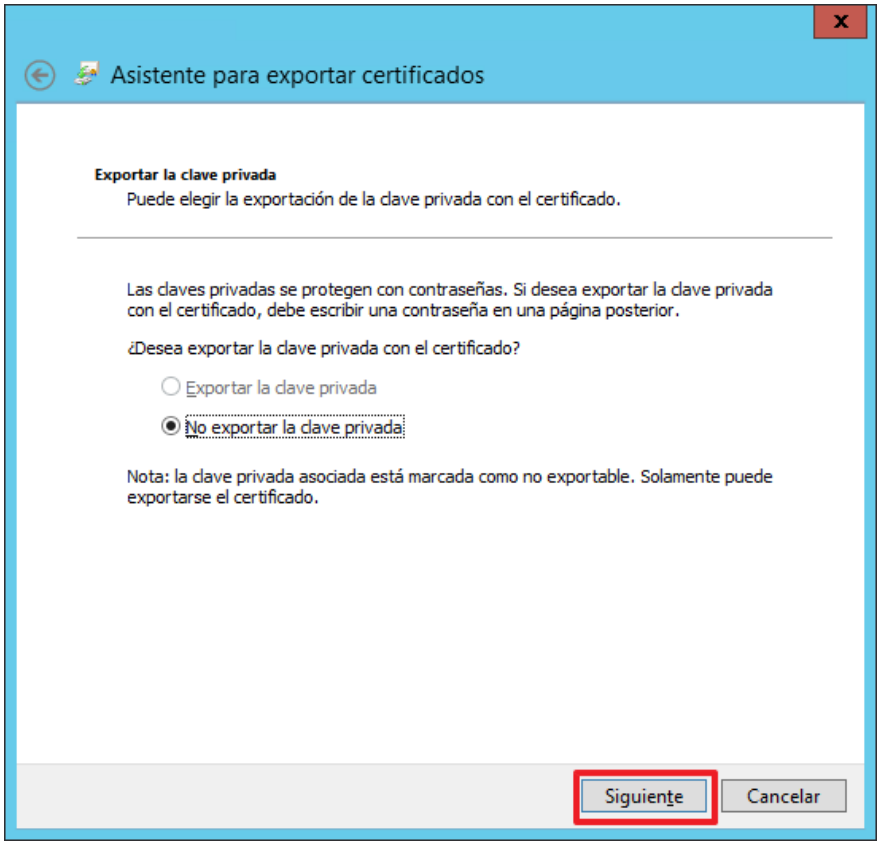
92.	En la consola MMC, en la parte izquierda sitúese en **"Certificados (equipo local) > Personal > Certificados"**, si todo se ha realizado correctamente, deberá existir el certificado generado anteriormente con el nombre FQDN del propio servidor WSUS.



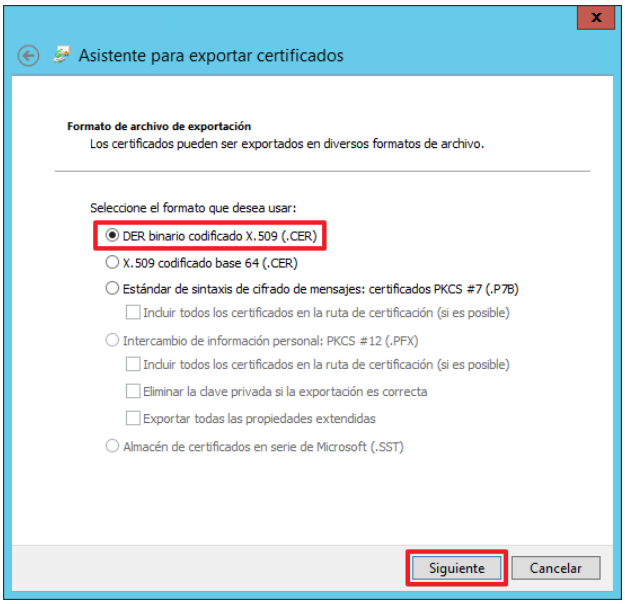
Paso	Descripción
93.	Para terminar, deberá exportar el certificado para proporcionarlo a la entidad certificadora raíz de confianza y a los equipos clientes del servidor WSUS, para ello, ubíquese en **"Raíz de consola > Certificados (equipo local) > Personal > Certificados"**, sobre el certificado, con el botón derecho, seleccione **"Todas las tareas > Exportar …"**



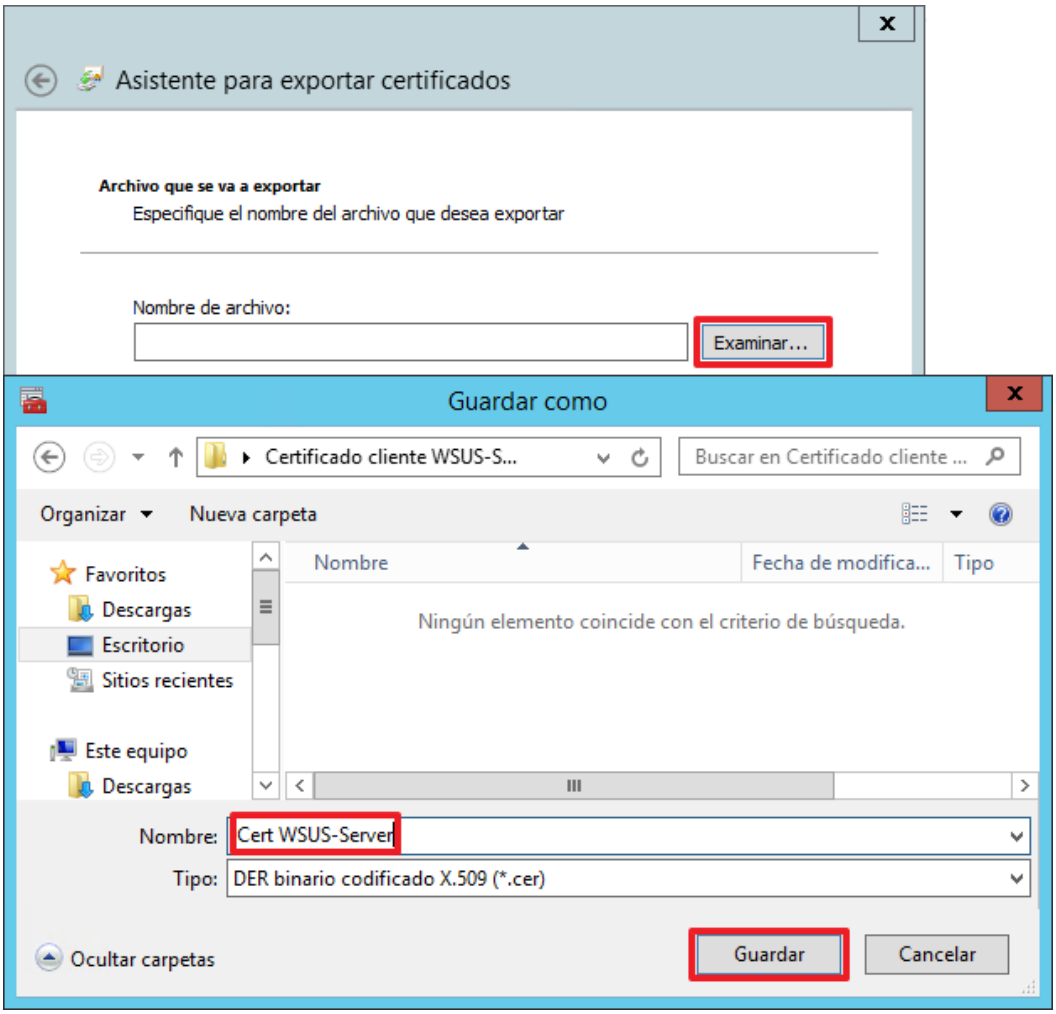
94.	Se abrirá el "Asistente para exportar certificados", pulse **"Siguiente"** para continuar.
95.	En "Exportar la clave privada", seleccione **"No exportar la clave privada"** y pulse en **"Siguiente".**



Paso	Descripción
96.	Para el formato de archivo de exportación, deje seleccionado **"DER binario codificado X.509 (.CER)"**, seguidamente pulse **"Siguiente".**



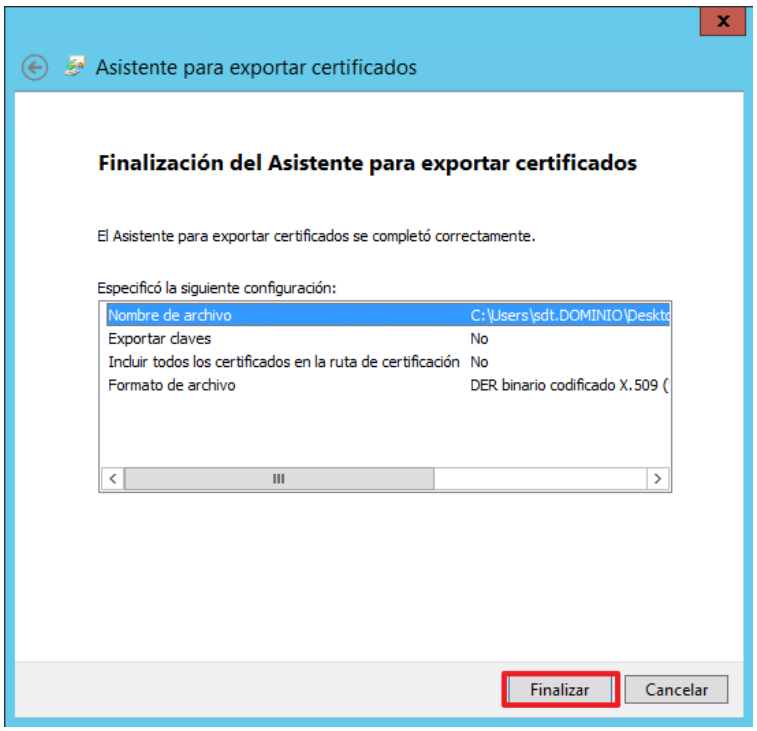
Paso	Descripción
97.	A continuación, pulse en **"Examinar",** e indique la ubicación y el nombre del certificado exportado y pulse en **"Guardar".**



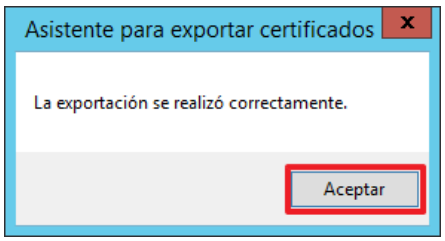
Nota: Para este ejemplo, se ha creado una carpeta en el escritorio llamada "Certificado cliente WSUS-Server" y se ha guardado el certificado con el nombre "Cert WSUS-Server". Usted debe decidir la ubicación y el nombre más adecuado para su organización.
Deberá almacenar el certificado en un sitio seguro y que no olvide, ya que volverá a utilizar el certificado exportado para asignarlo a una GPO que aplique a todos los equipos clientes del servidor WSUS.

98.	Pulse **"Siguiente"** para continuar con el asistente.

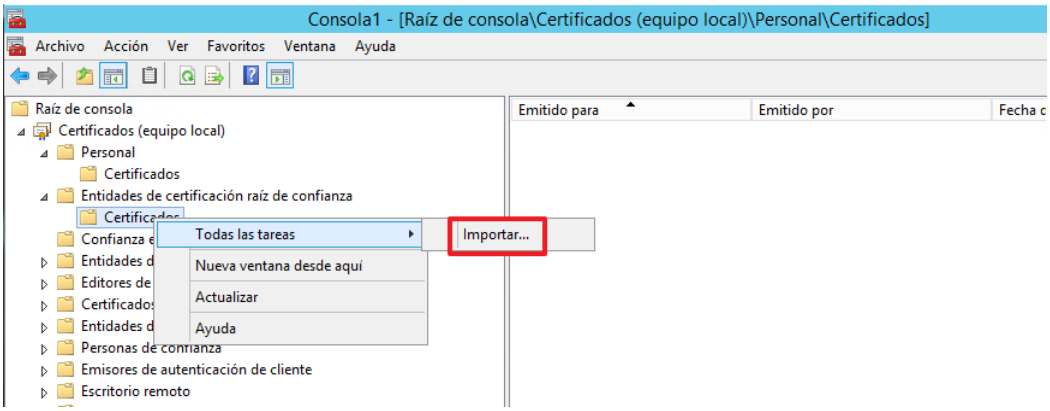
Paso	Descripción
99.	El asistente para exportar certificados mostrará un resumen de la configuración que usted ha facilitado, indicándole que la exportación se ha realizado correctamente. Pulse en **"Finalizar"** para terminar con la exportación.



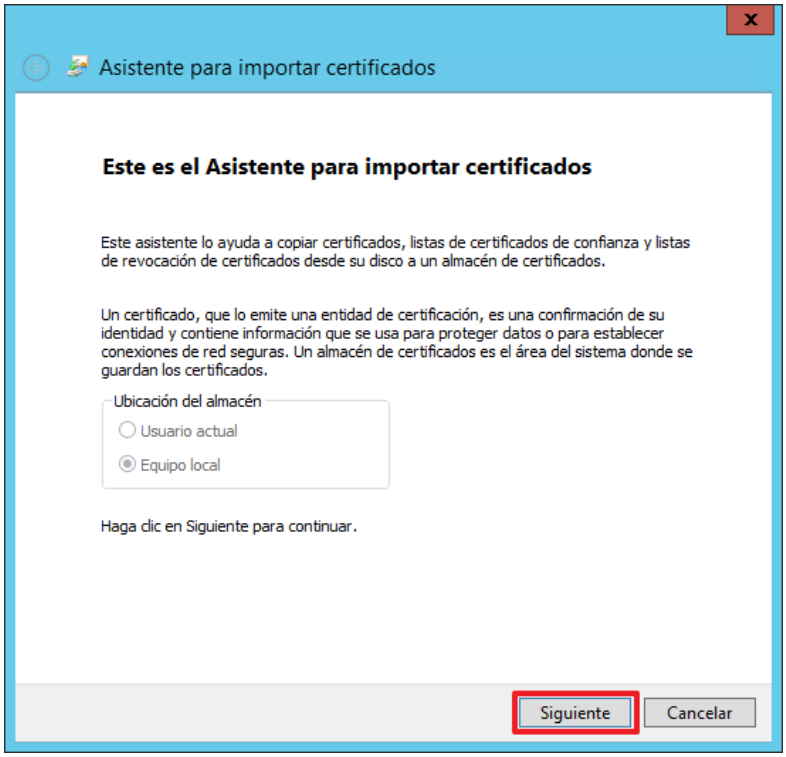
100.	El asistente notificará con un mensaje en pantalla que la exportación se realizó correctamente.



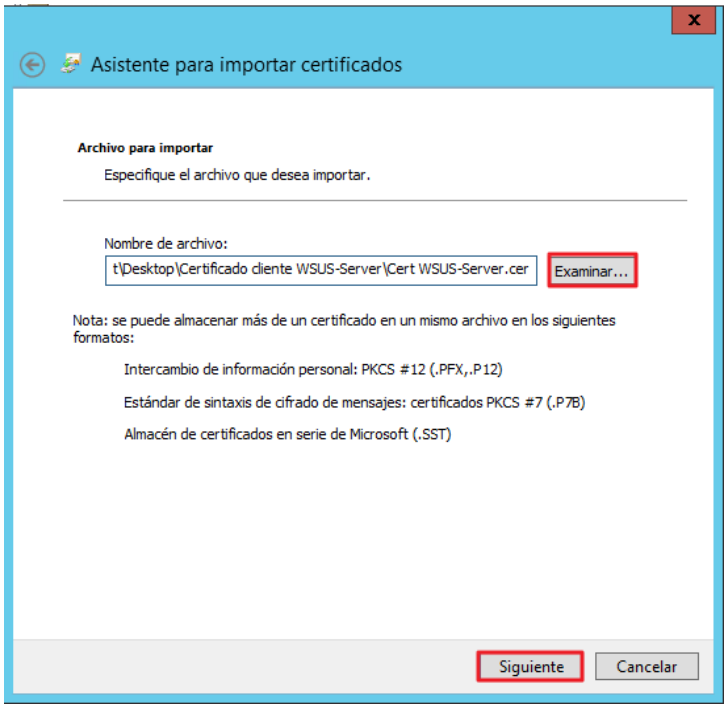
Paso	Descripción
101.	Una vez exportado el certificado, se deberá importarlo en “Entidades de certificación raíz de confianza > Certificados”, pulse con el botón derecho sobre **“Certificados > Todas las tareas > Importar”.**



102.	Se abrirá el asistente de importación de certificados, pulse “**Siguiente”** para continuar.

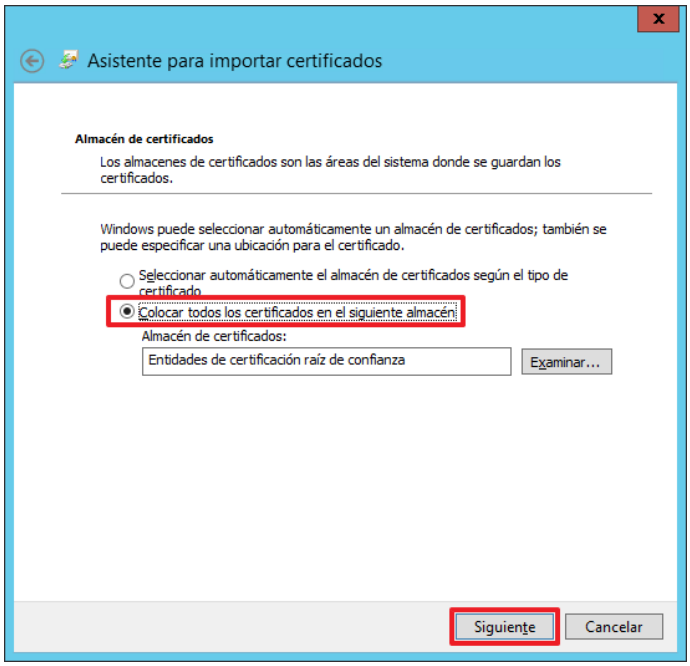


Paso	Descripción
103.	Importe el certificado que acaba de exportar, para ello, pulse en **"Examinar"** y selecciónelo.

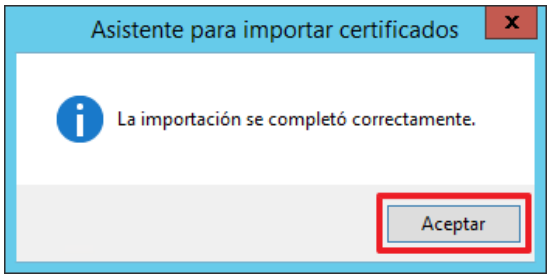
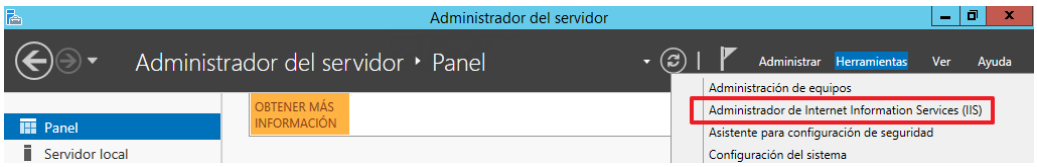


Pulse **"Siguiente"** para continuar.

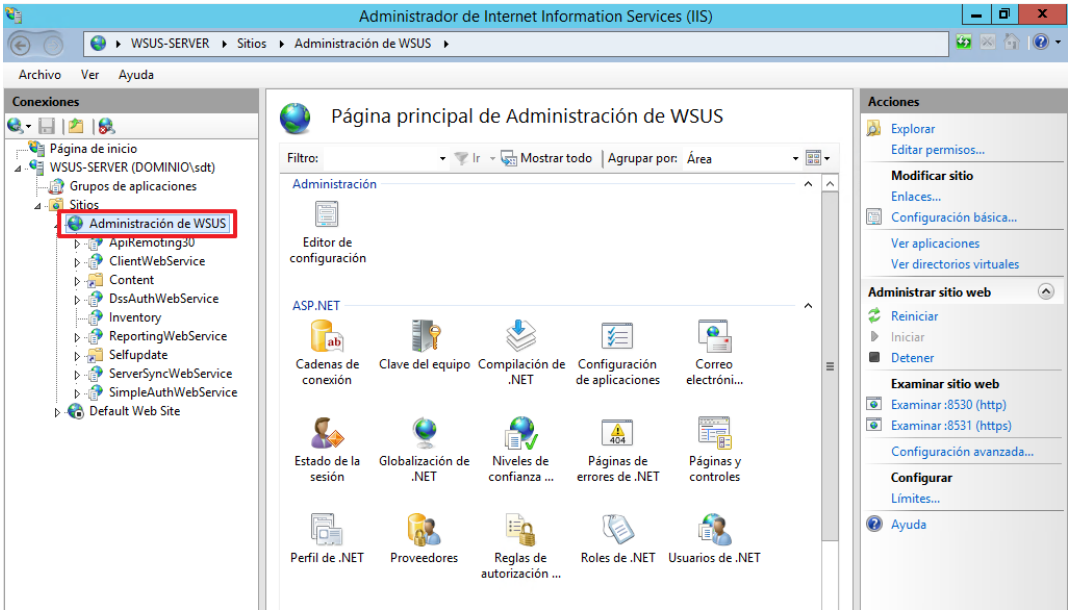
104.	Deje seleccionado **"Colocar todos los certificados en el siguiente almacén"** como almacén de certificados.



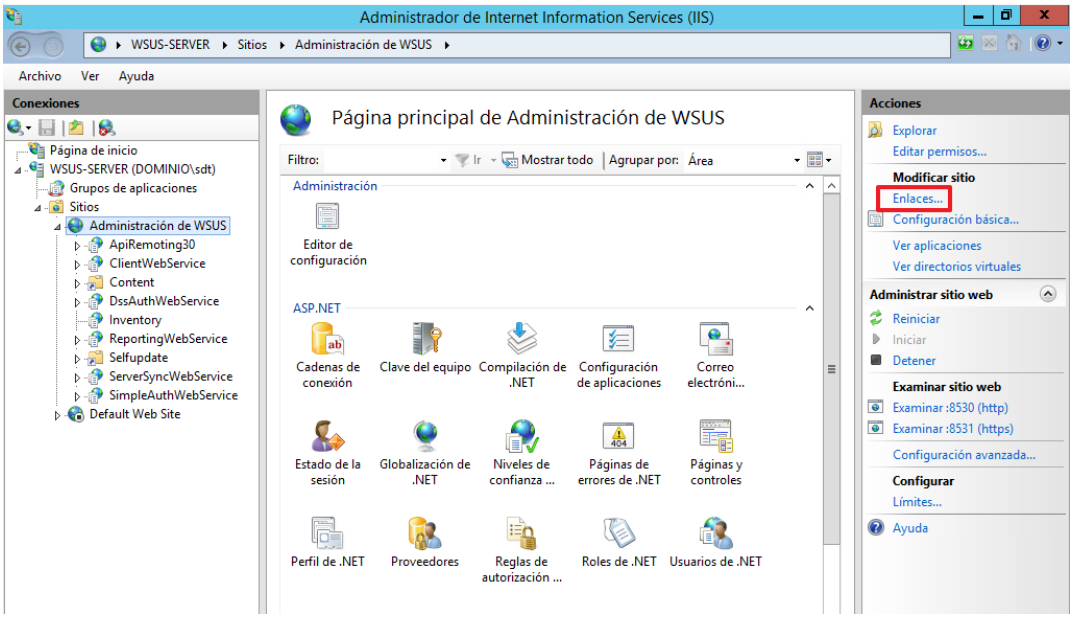
Pulse **"Siguiente"** para continuar.

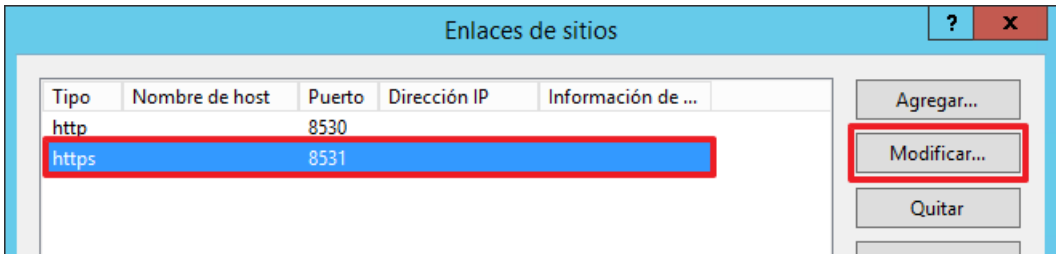
Paso	Descripción
105.	Pulse **"Finalizar"** para terminar con la importación.
106.	El asistente le notificará que la importación se ha realizado correctamente.  **Nota:** Puede darse el caso de que el propio certificado generado por IIS se almacene también en "Entidades de certificación raíz de confianza", si esto es así, elimínelo y seguidamente importe el certificado exportado.
107.	Ejecute la consola de Administrador de Internet Information Services (IIS) desde el menú **"Inicio > Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
108.	Dentro de la consola de IIS, sitúese en la parte izquierda en **"Página de inicio > <<su servidor WSUS>> > Sitios > Administración de WSUS"**.

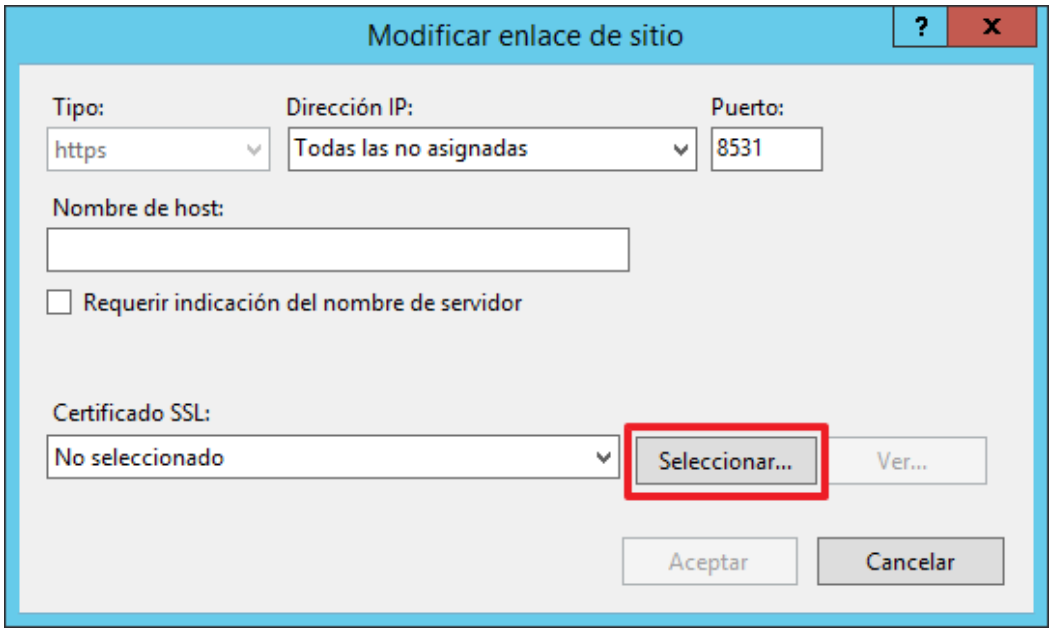


109.	Pinche sobre **"Enlaces"** que se encuentra en la parte da la derecha.

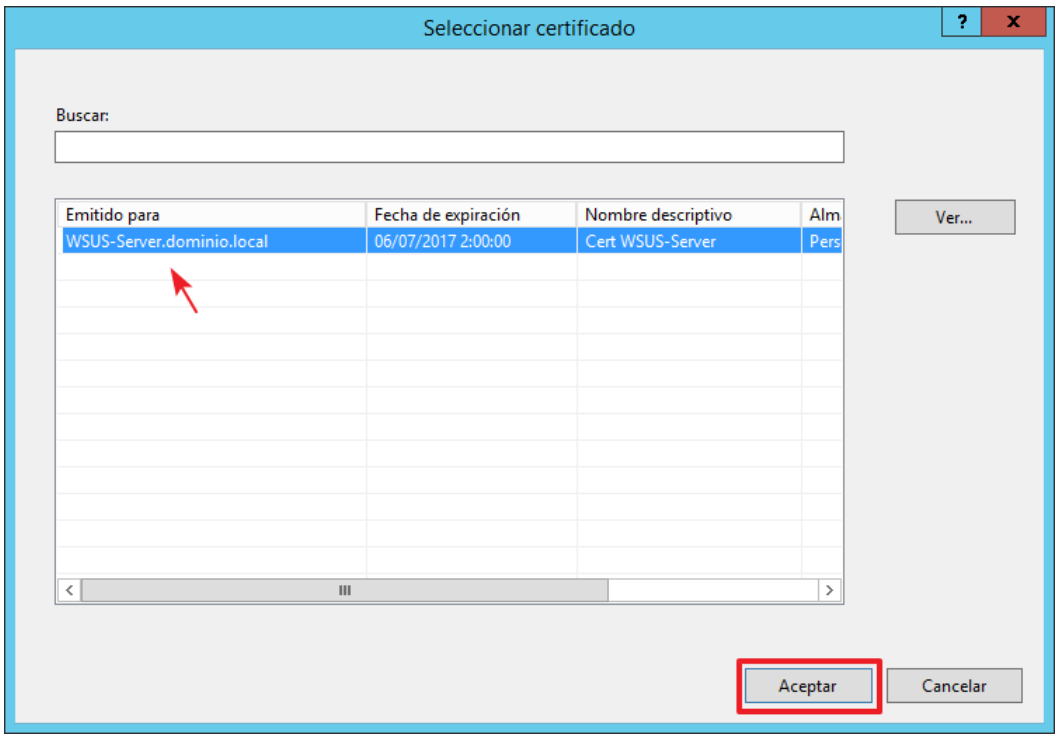


Paso	Descripción
110.	En el asistente de “Enlaces de sitios”, seleccione **HTTPS** y seguidamente pulse en **“Modificar…”.** 

Paso	Descripción
111.	En la siguiente ventana debe seleccionar el certificado exportado anteriormente, para ello, pulse sobre **"Seleccionar…".**



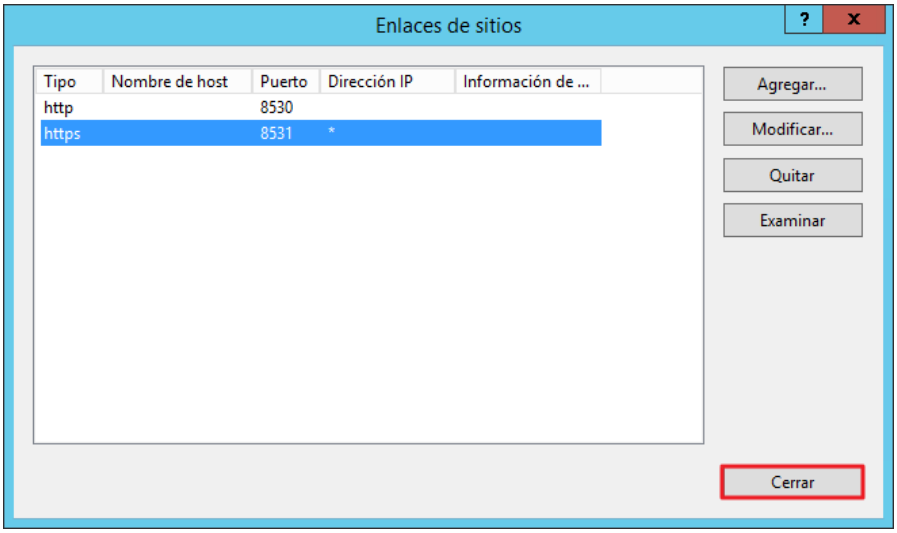
Seleccione el certificado y pulse **"Aceptar".**



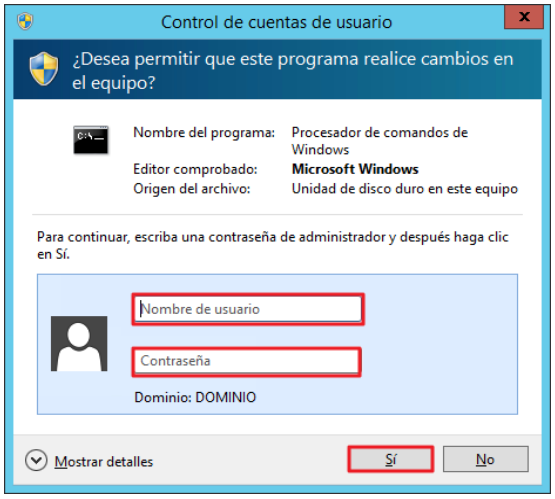
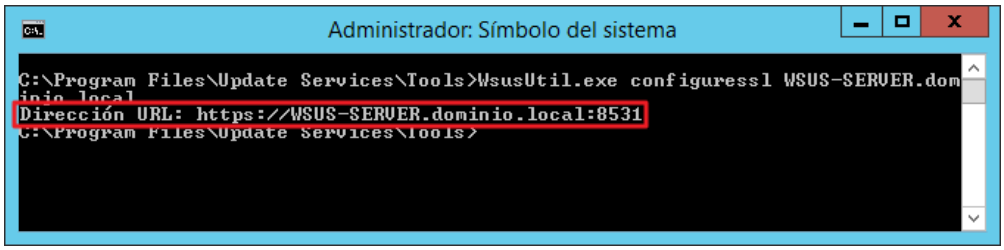
Nota: Si el asistente no es capaz de encontrar el certificado, puede intentar buscarlo con el nombre que le asigno al exportarlo. Si no encuentra dicho certificado, vuelva a realizar los pasos de emisión del certificado.

Paso	Descripción
112.	Pulse **"Aceptar"** para continuar.

113.	Cierre la venta de **"Enlaces de Sitios"**.



114.	Ejecute un **"Símbolo de sistema",** para ello pinche con el botón derecho sobre el **"Inicio"** y seleccione **"Símbolo del sistema (administrador)"**.

Paso	Descripción
115.	El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.  **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
116.	Sitúese en "C:\Program Files\Update Services\Tools\", seguidamente ejecute: **"wsusutil.exe < configuressl > <<su servidor WSUS.dominio.local>>"** y pulse **"Intro"**.  Se generará un enlace como el que se puede observar en la imagen.

Paso	Descripción
117.	Compruebe que la consola de Windows Server Update Service mantiene conexión con el propio servidor WSUS.

Nota: Cuando se configura SSL en el servidor WSUS, la consola Windows Server Update Services pierde comunicación con el servidor WSUS ya que la configuración ha cambiado. Si en este punto en la consola se le muestra algún error o no consigue enlazar en la consola el servidor WSUS, debería repasar el punto de 6.PROTEGER WSUS CON EL PROTOCOLO DE CAPA DE SOCKETS SEGUROS (SSL)

4. PREPARACIÓN DEL DIRECTORIO ACTIVO PARA LOS EQUIPOS CLIENTE DEL SERVIDOR WSUS.

Los pasos que se describen a continuación, se realizarán tanto en un Controlador de Dominio del dominio, como en el propio servidor Windows Server Update Services que pertenezca a dicho dominio. Sólo es necesario realizar este procedimiento una vez.

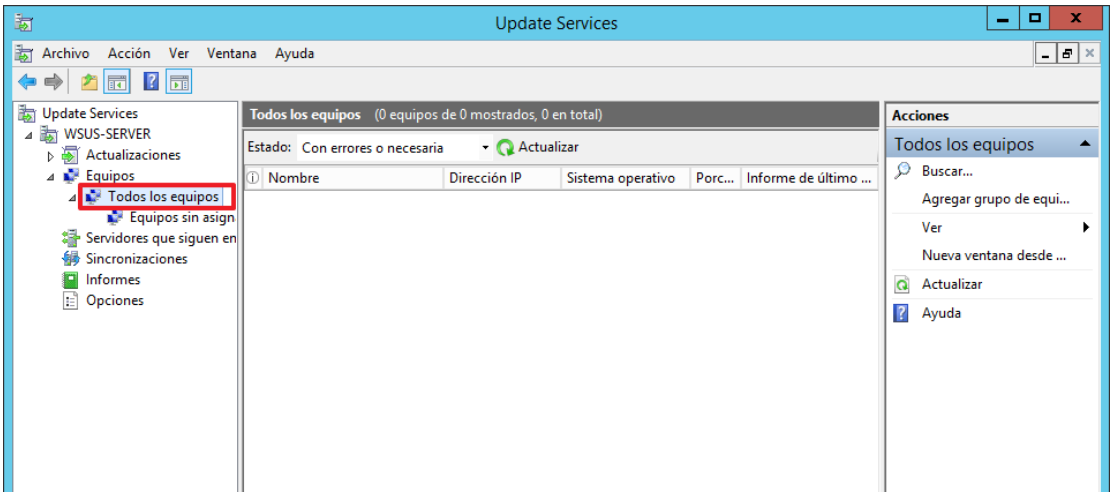
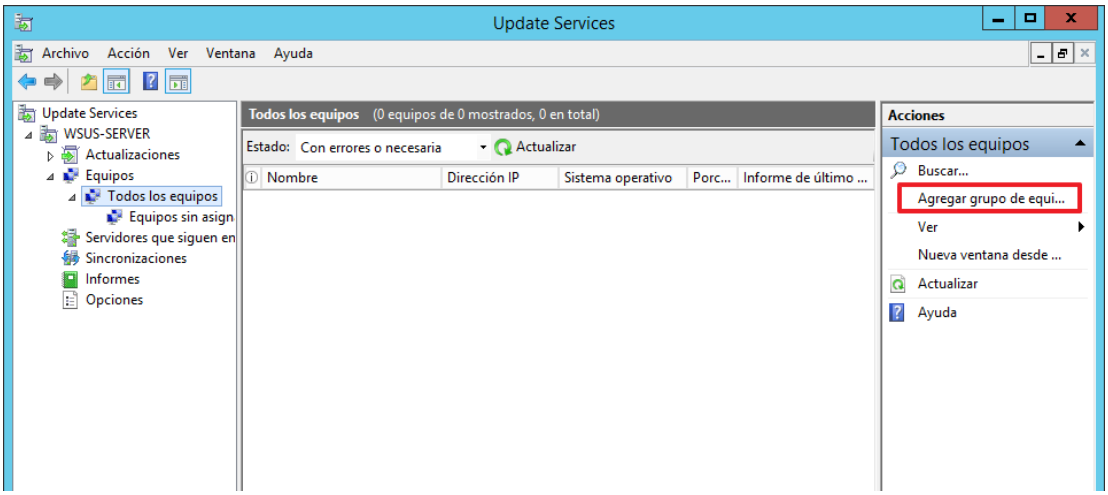
En el presente punto se detalla cómo gestionar los grupos de equipos desde la consola de WSUS. Esta gestión es necesaria para aplicar correctamente las directivas de grupo en los equipos clientes. Además, en este punto, se detalla el procedimiento para publicar un certificado de confianza mediante dichas directivas de grupo. Este procedimiento se aplicará a todos los equipos del dominio, para que puedan establecer comunicación con el servidor de actualizaciones WSUS, que ya fue configurado con SSL.

4.1. CONFIGURACIÓN DE LOS EQUIPOS CLIENTE WINDOWS 7

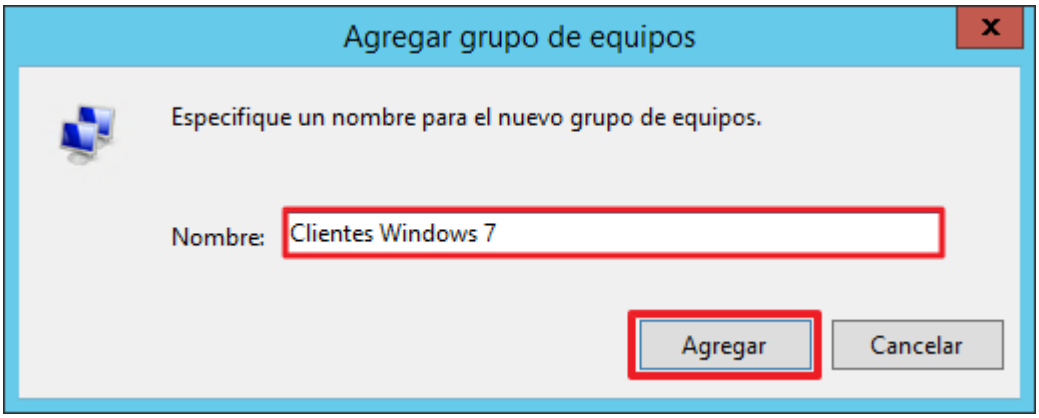
Antes de aplicar las GPO en el controlador de domino del dominio, se debe crear el grupo de equipos Windows 7 en la consola de WSUS. De esta forma, cuando la política “Habilitar destinatarios del lado cliente” se aplique a estos equipos, éstos quedarán asignados automáticamente al grupo que les corresponde.

Nota: Este apartado establece el procedimiento para utilizar un equipo cliente Windows 7 miembro del dominio como cliente del servicio WSUS. Si desea conectar un equipo cliente Windows 7 independiente (standalone) con el servicio WSUS, deberá aplicar los cambios en el registro que se indican en la URL https://technet.microsoft.com/en-us/library/cc720464(v=ws.10).aspx y realizar las modificaciones correspondientes en la configuración de comunicación entre ambos sistemas para permitir la conexión con el servicio.

Paso	Descripción
118.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
119.	Ejecute la consola de Windows Server Update Service, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor", ésta le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

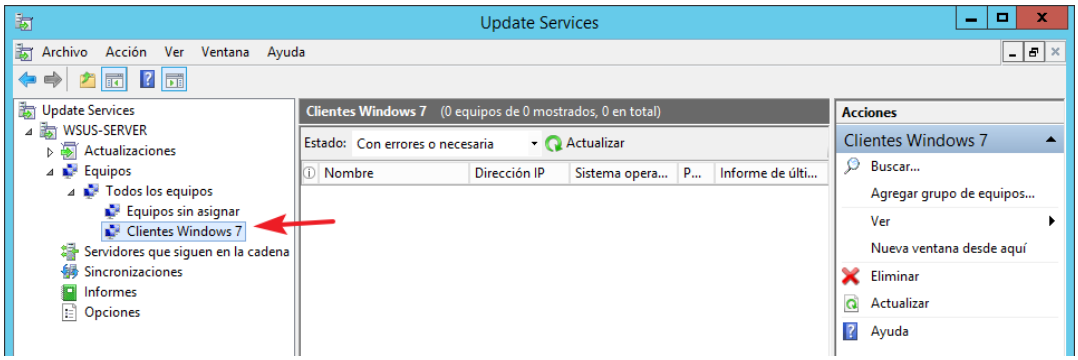
Paso	Descripción
120.	Dentro de la consola de Update Services, sitúese en la parte de la izquierda **"Update Services > <<Su servidor WSUS>> > Equipos > Todos los equipos".** 
121.	En la parte de la derecha, pinche en **"Agregar grupo de equipos…".** 

Paso	Descripción
122.	Se abrirá una ventana, donde se deberá indicar el nombre del grupo que se va a crear, añada **"Clientes Windows 7".**



Pulse en **"Agregar"** para terminar.

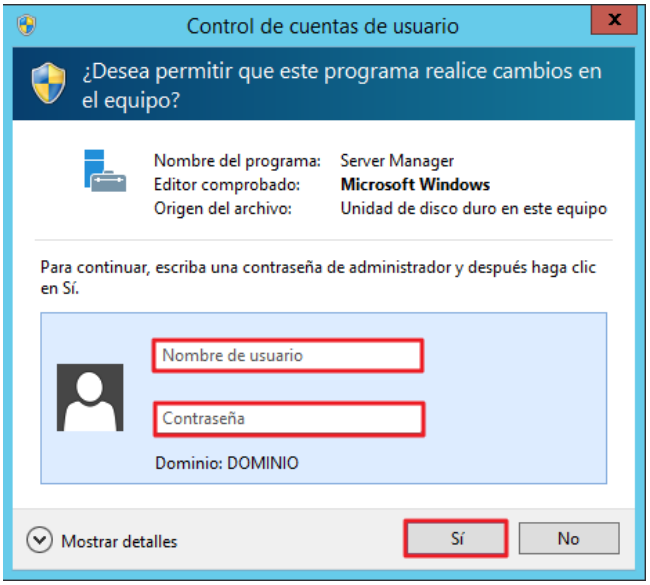
123.	Se habrá agregado este grupo en la pestaña de **"Equipos > Todos los equipos"**, tal y como se muestra en la siguiente imagen:



Una vez configurado en el servidor WSUS el grupo al que van pertenecer los equipos cliente Windows 7, ya se podrá aplicar la política en el Controlador de Dominio del dominio para que así los equipos ingresen automáticamente en el grupo al que correspondan.

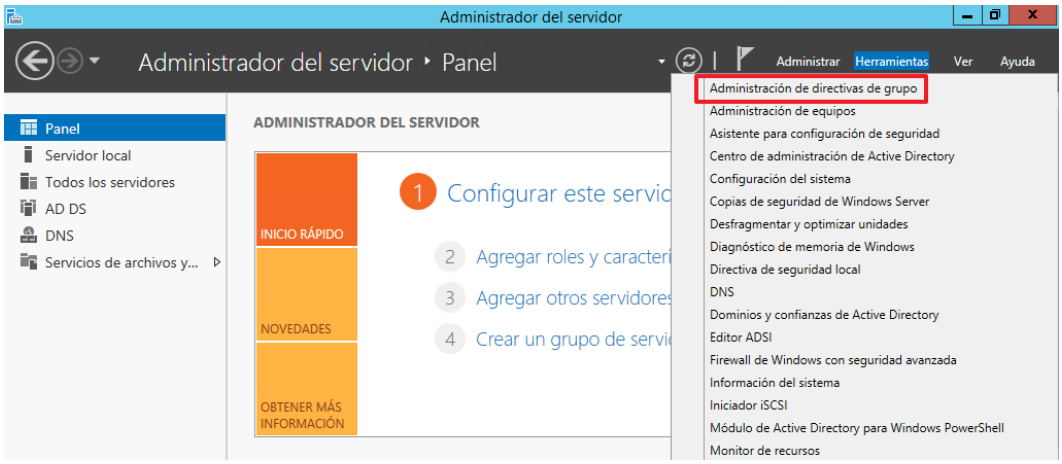
Paso	Descripción
124.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
125.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
126.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.



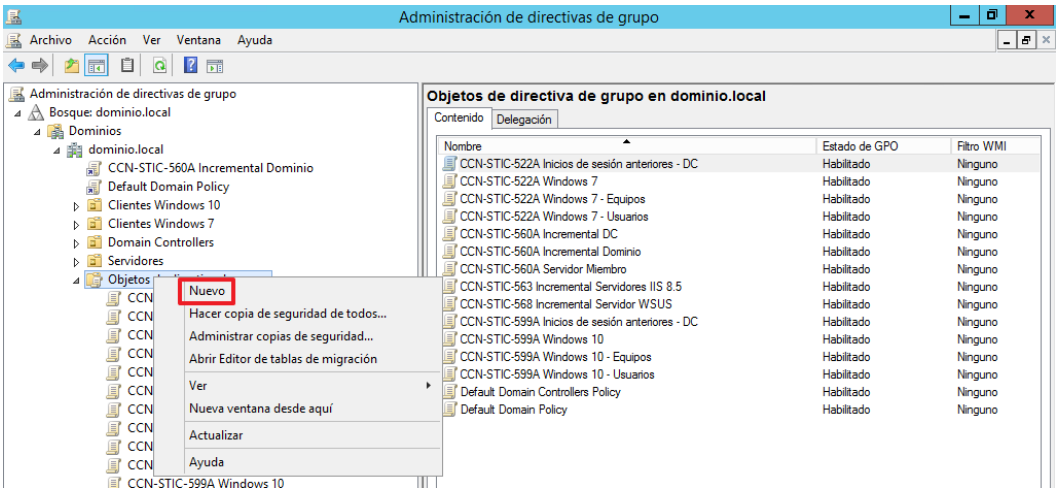
Nota: En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

127.	Ejecute la consola de Administración de directivas de grupo desde el menú **"Inicio > Administrador del servidor > Herramientas > Administración de directivas de grupo".**

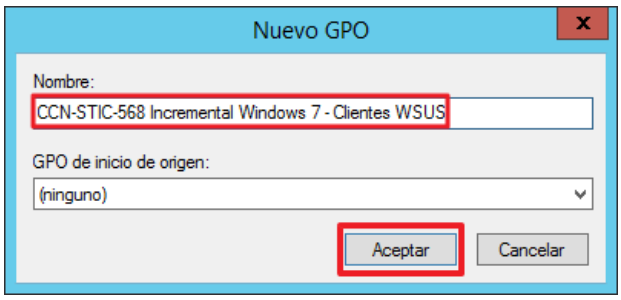


Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

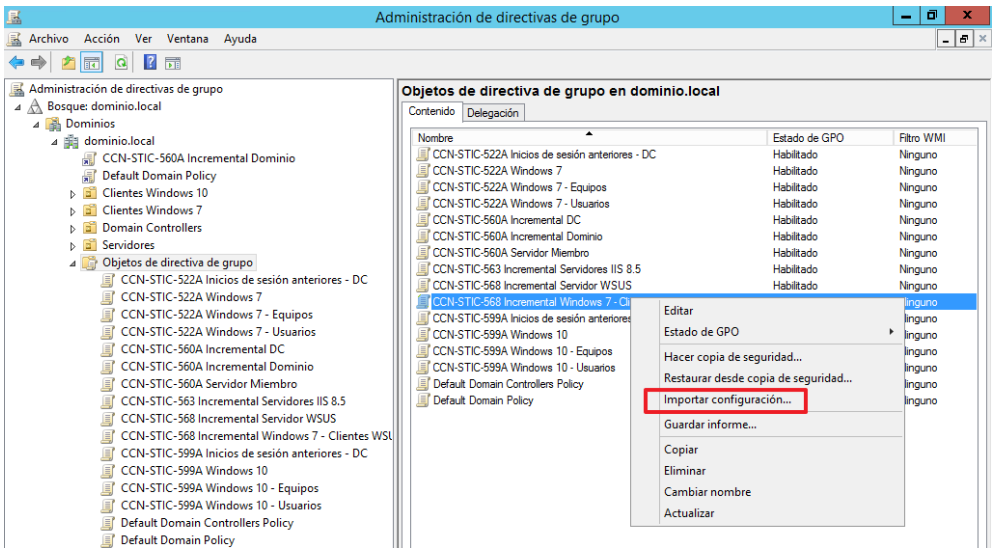
Paso	Descripción
128.	En la ventana de la izquierda sitúese sobre **"Objetos de directiva de grupo"** y con el botón derecho pulse sobre **"Nuevo"**.



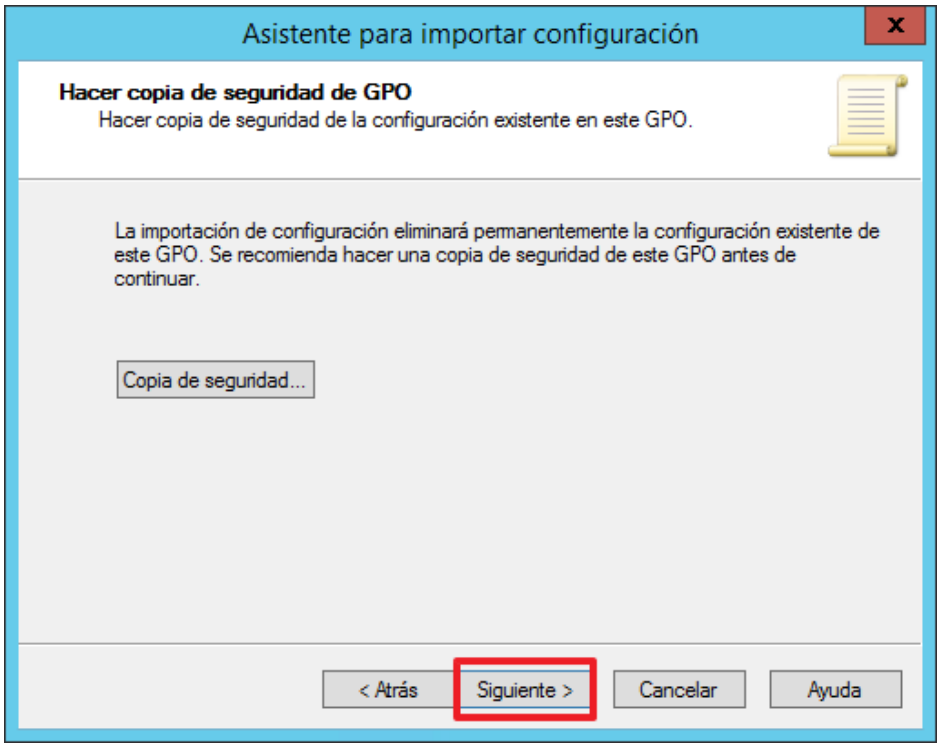
129.	Introduzca **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS"** como nombre de la nueva GPO que está creando. Pulse **"Aceptar".**



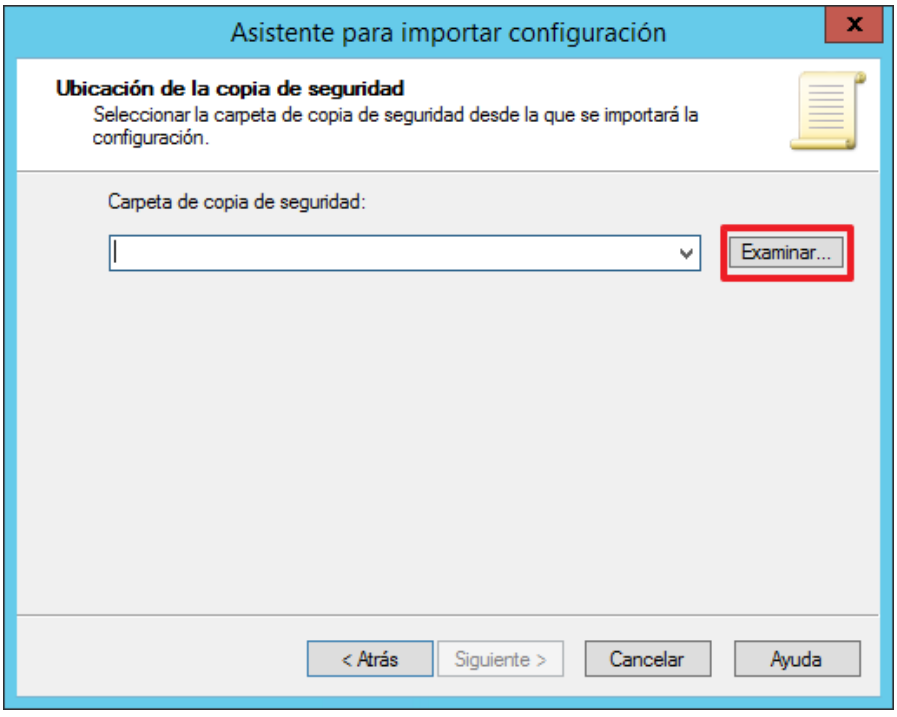
130.	Una vez creada la GPO, deberá importar la configuración. Para ello, sobre la política que acaba de crear, pulse botón derecho y pinche sobre **"Importar configuración…".**



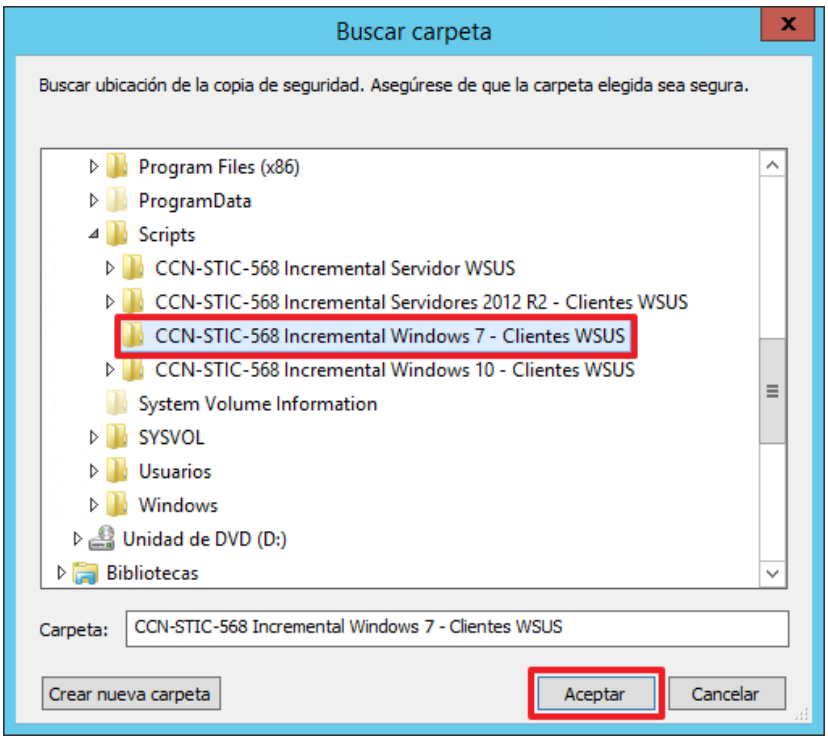
Paso	Descripción
131.	En el "Asistente para importar configuración", pulse **"Siguiente >"** para continuar.
132.	Omita realizar copia de seguridad y pulse **"Siguiente >".**



133.	Pulse en **"Examinar"**, sitúese en **"Este equipo > Disco local (C:) > Scripts".**

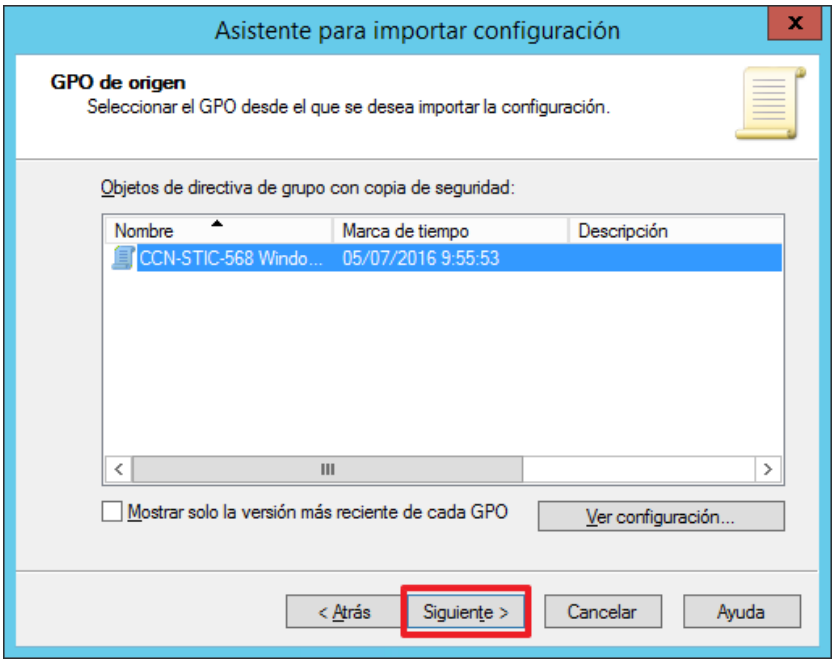


Paso	Descripción
134.	Seleccione **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS"** y pulse **"Aceptar".**

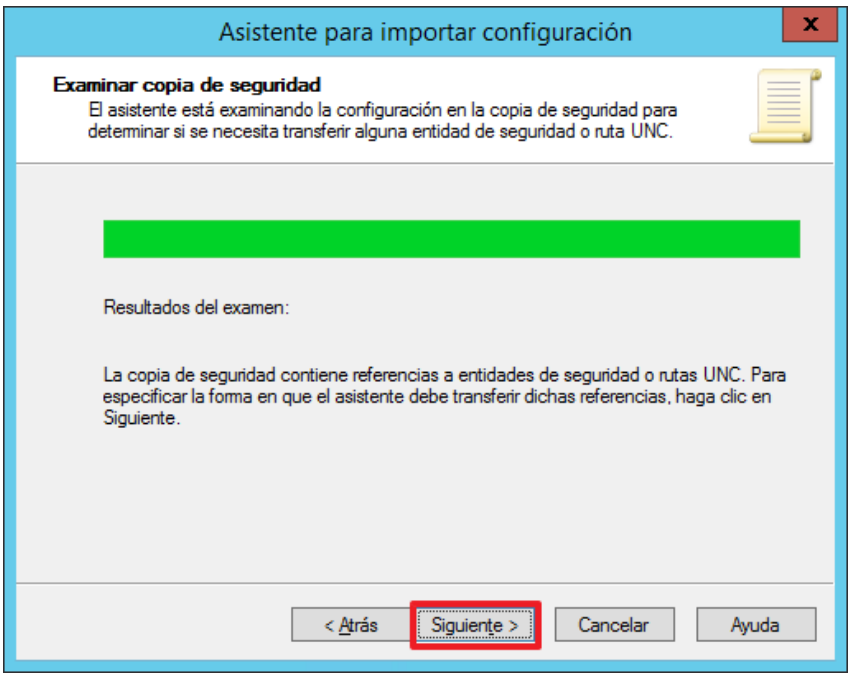


Después de pulsar "**Aceptar**", pulse **"Siguiente >"** en el asistente para continuar.

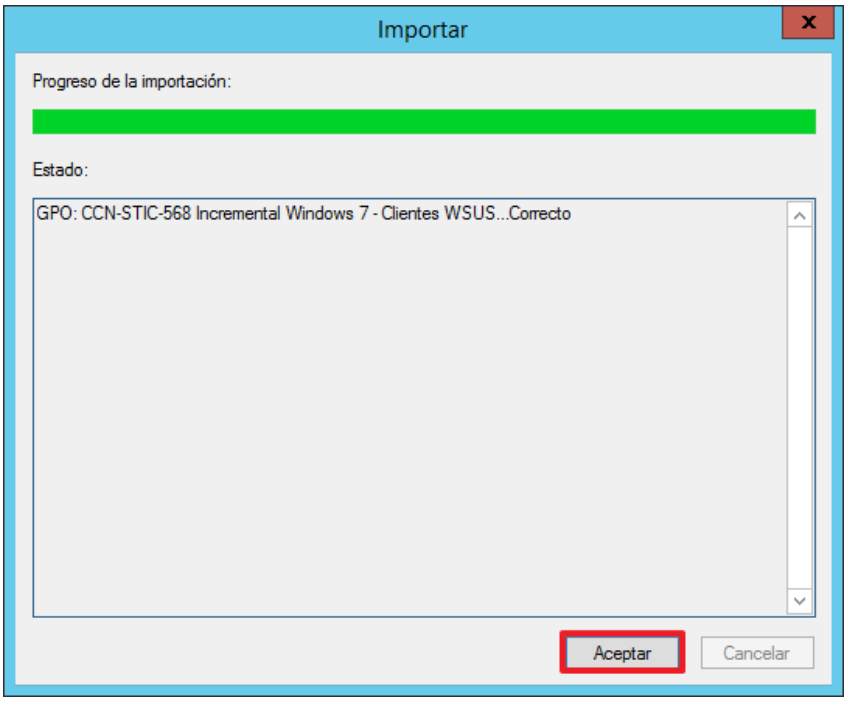
135.	Pulse **"Siguiente >".**



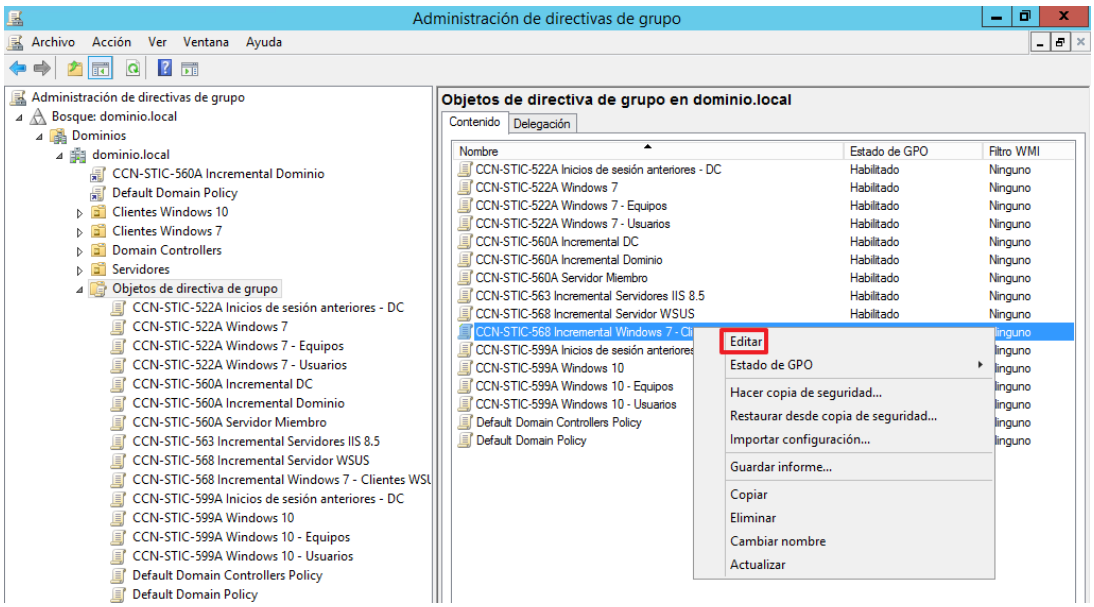
Paso	Descripción
136.	En “Examinar copia de seguridad”, pulse **“Siguiente >”**.



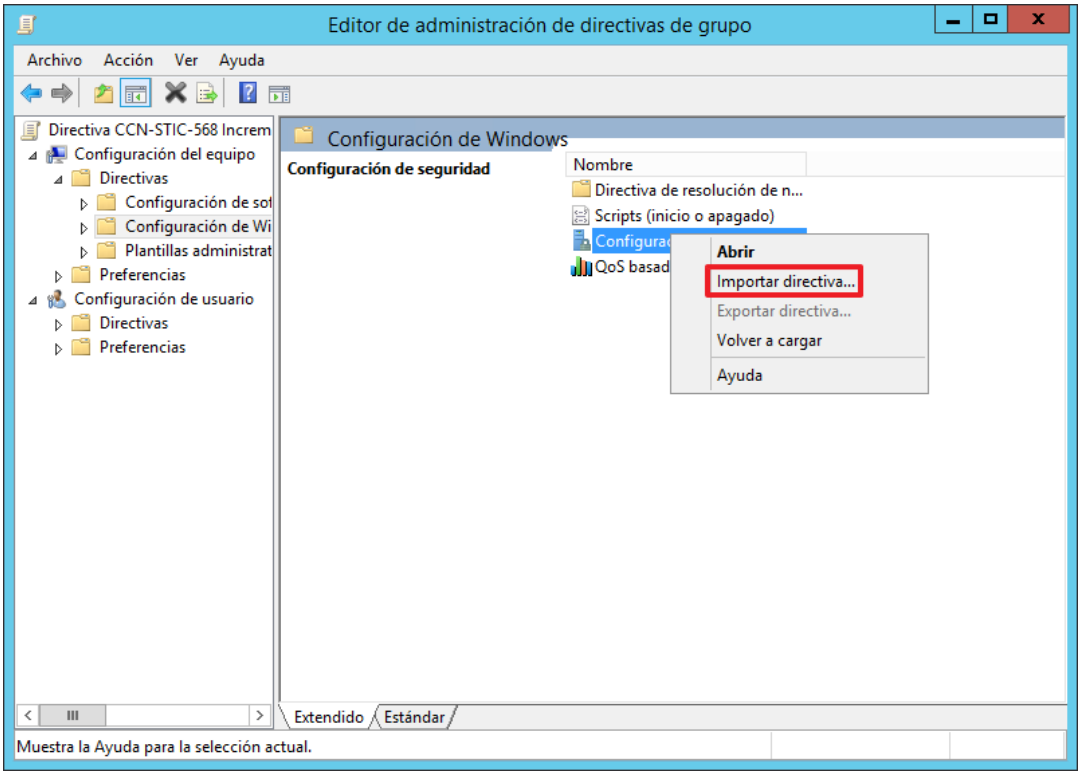
137.	Pulse **“Finalizar”** para terminar con la importación de configuración de la GPO.
138.	Pulse en **“Aceptar”** para guardar los cambios.



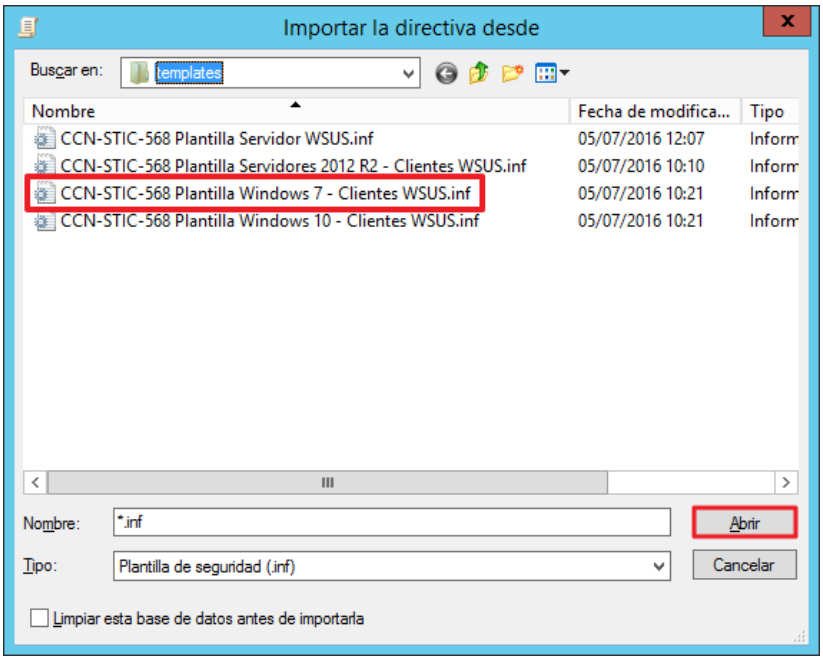
Paso	Descripción
139.	Una vez importada la configuración, debe realizar una serie de configuraciones en la propia GPO. Para ello, sobre la política **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS"**, pulse botón derecho y pinche sobre **"Editar".**



140.	Sitúese en **"Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad"** y sobre esté, pulse con el botón derecho y seleccione **"Importar directiva…".**

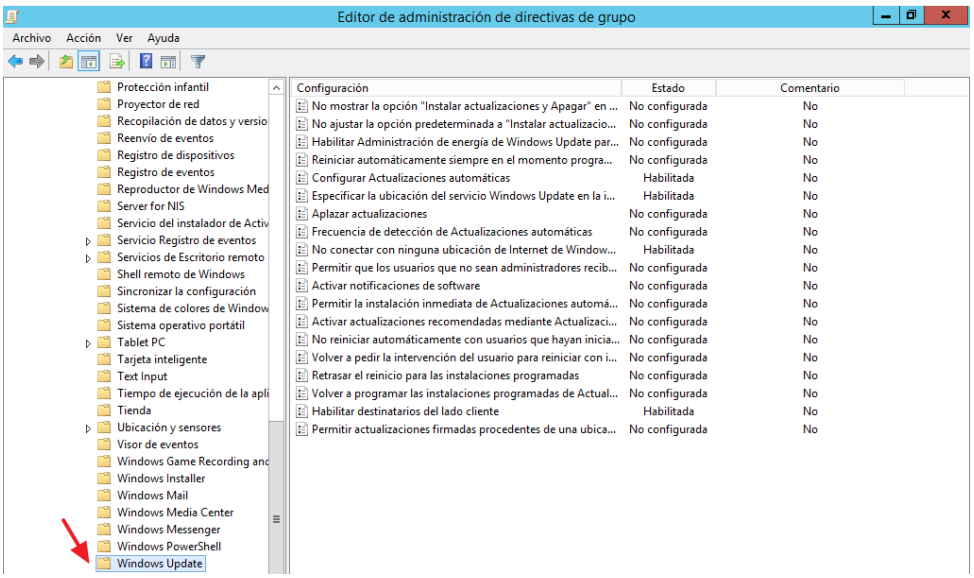


Paso	Descripción
141.	Desde C:\Windows\Security\templates, seleccione **"CCN-STIC-568 Plantilla Windows 7 – Clientes WSUS.inf".**

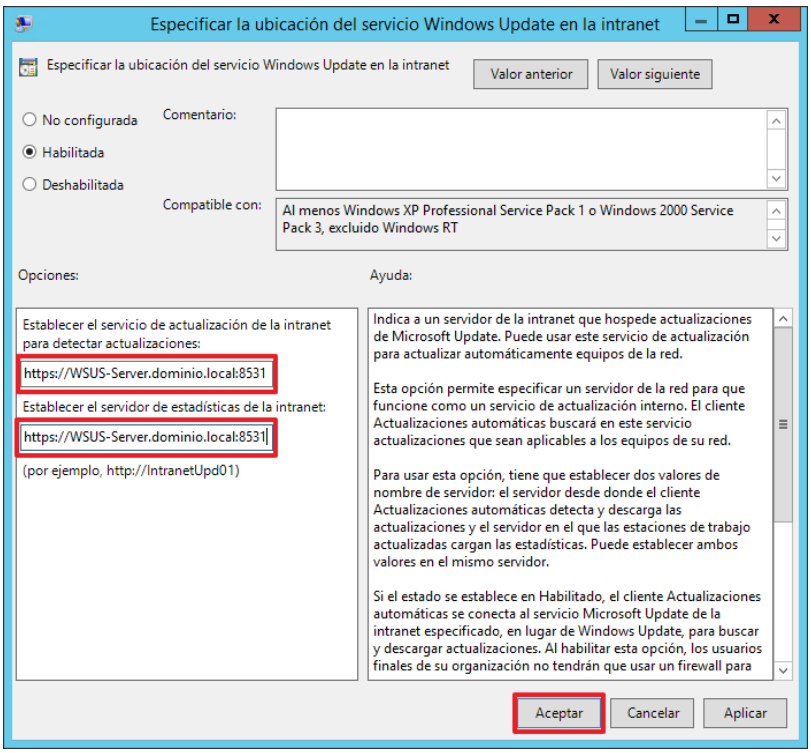


Pulse **"Abrir".**

142.	Seguidamente, sitúese en **"Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows Update".**



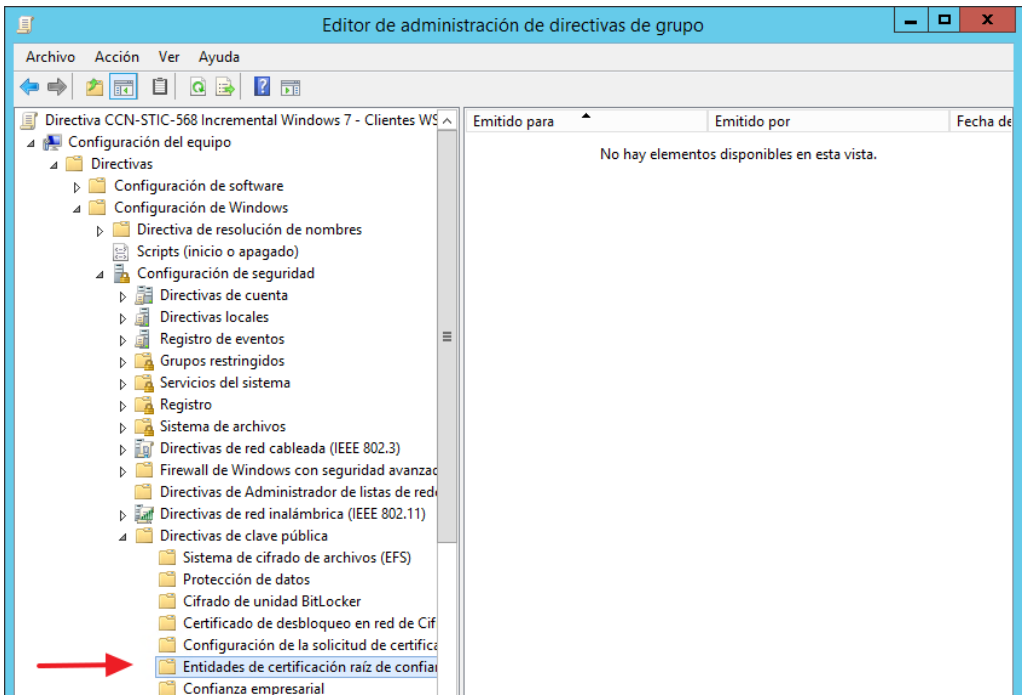
Paso	Descripción
143.	Haga doble clic sobre **"Especificar la ubicación del servicio Windows Update en la intranet"**, en la ventana opciones deberás introducir la ubicación del servidor WSUS. Tal y como se muestra en la siguiente imagen:



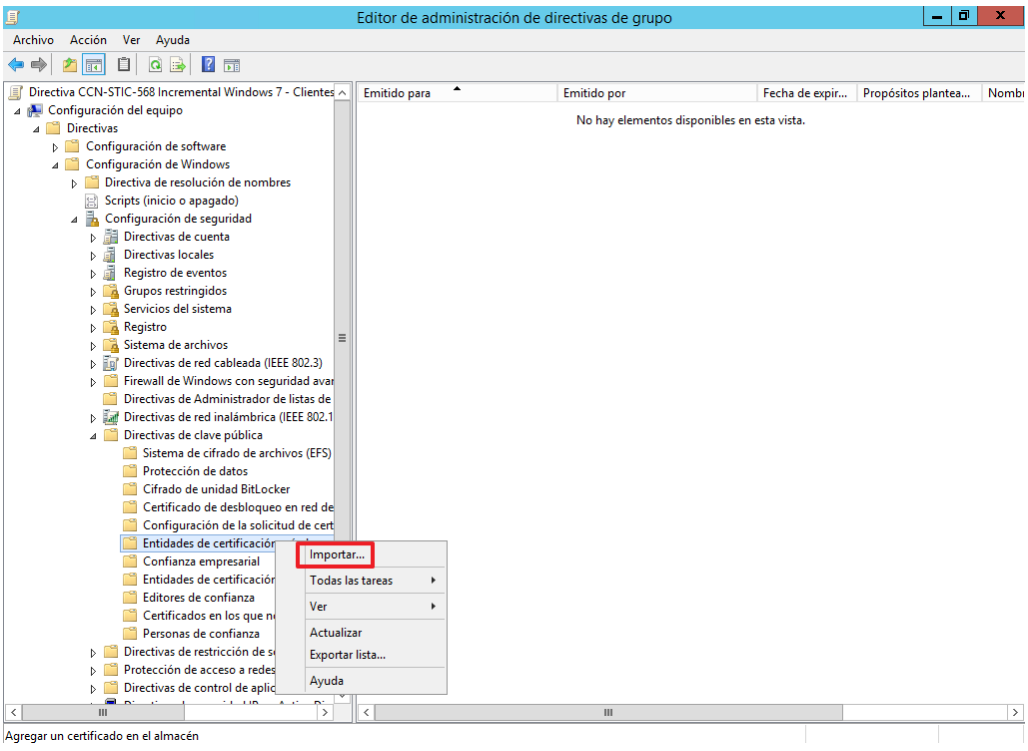
Pulse **"Aceptar"** para guardar los cambios.

Nota: Deberá introducir la dirección de su servidor WSUS (Nombre FQDN). Para este ejemplo se ha utilizado https://WSUS-Server.dominio.local:8531. Es muy importante tener en cuenta que debe introducir HTTPS y el puerto 8531, ya que la configuración SSL requiere de estos dos parámetros.

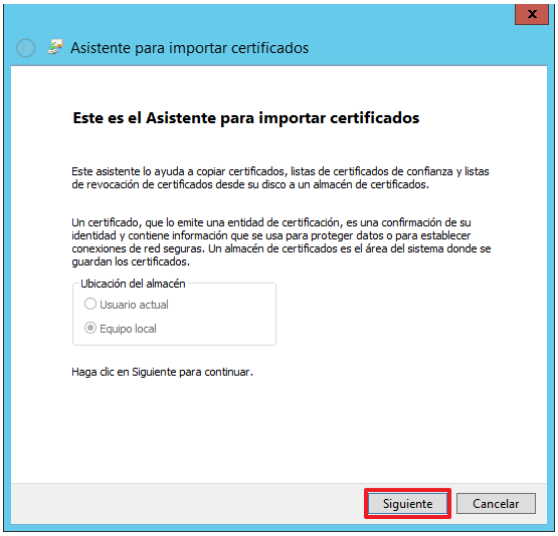
Paso	Descripción
144.	En el mismo "Editor de administración de directivas de grupo", diríjase a **"Configuración del equipo > Directivas > Configuración de seguridad > Directivas de clave pública > Entidades de certificación raíz de confianza".**



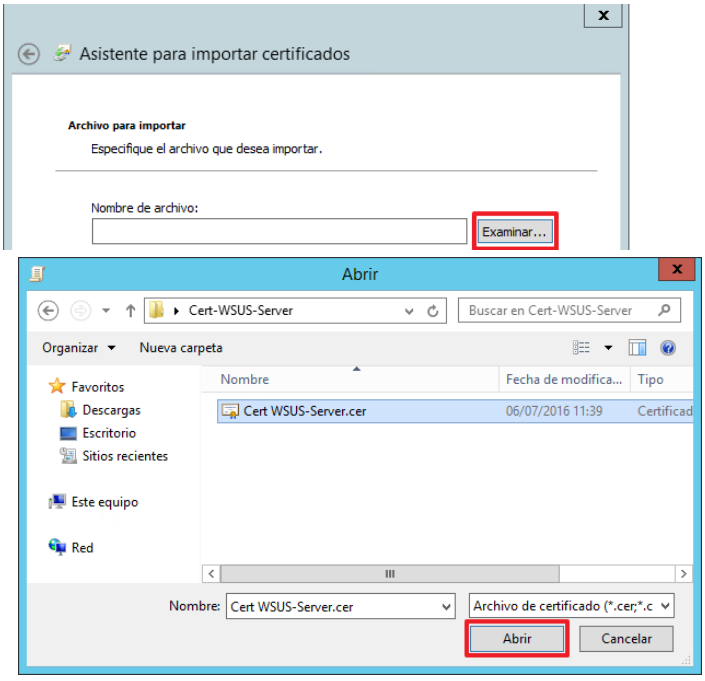
145.	Pulse sobre **"Entidades de certificación raíz de confianza"** con el botón derecho y seleccione **"Importar".**



Paso	Descripción
146.	Se abrirá el asistente de Importar certificados, pulse **"Siguiente"** para continuar.

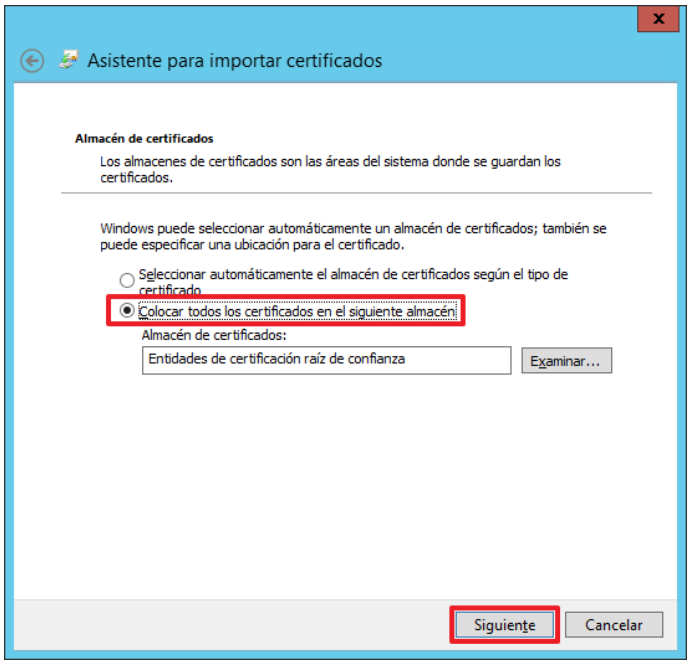
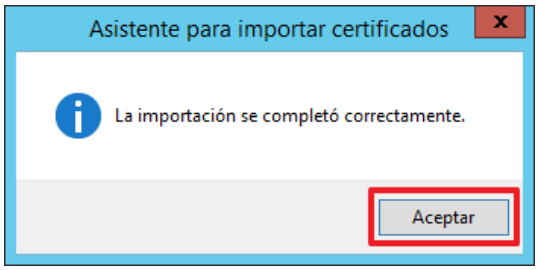


147.	Pulse sobre el botón **"Examinar"** y localice el certificado exportado anteriormente. Selecciónelo y pulse **"Abrir".**

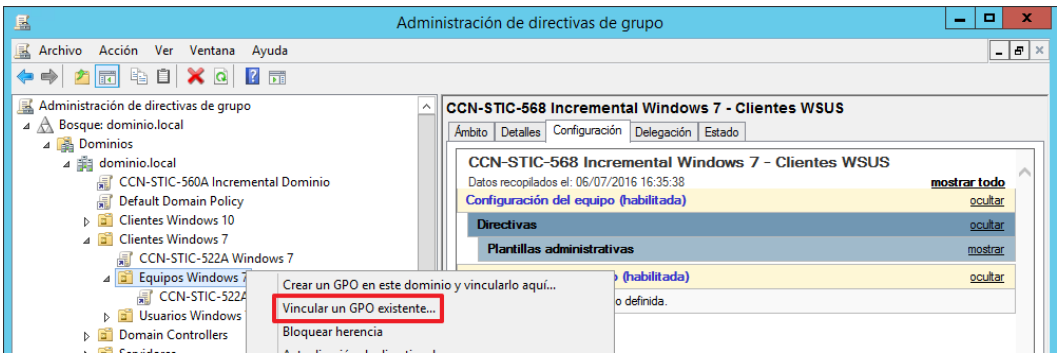


Pulse **"Siguiente"** para continuar.

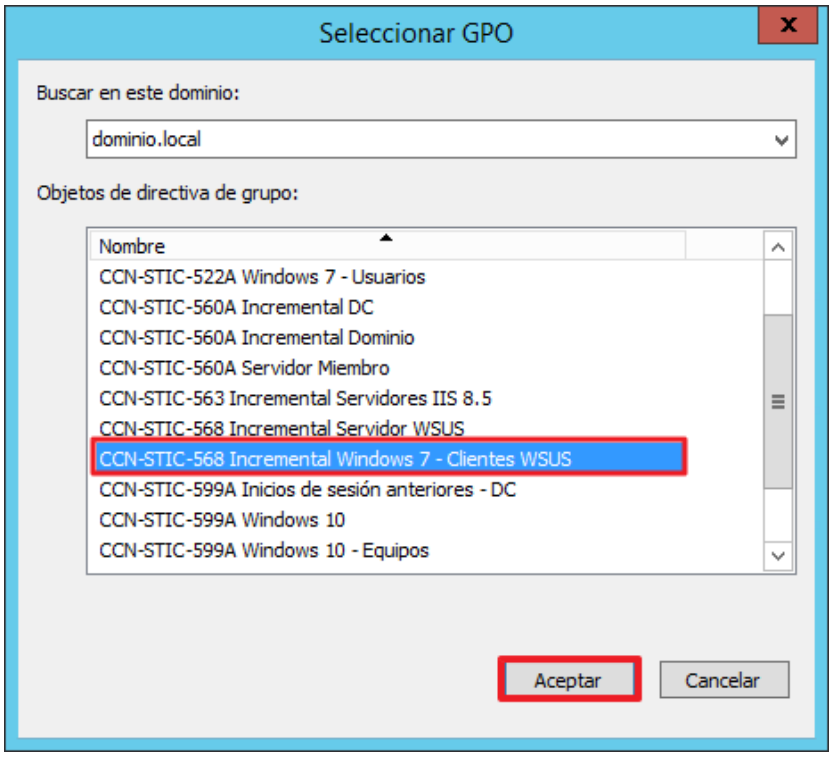
Nota: El certificado que debe importar es el mismo que ha exportado en el servidor WSUS, deberá encargarse de transportar el certificado hasta el servidor Controlador de domino del dominio para poder enlazarlo con las GPO de los clientes WSUS.
Si no realiza esto no podrá importar el certificado y por supuesto no podrá enlazar los equipos clientes con el servidor de Windows Server Update Services.

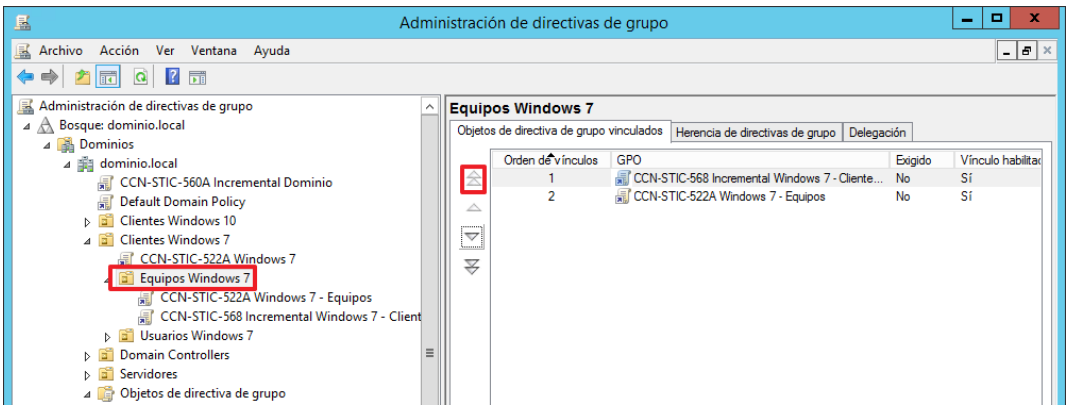
Paso	Descripción
148.	Deje seleccionado **“Colocar todos los certificados en el siguiente almacén”** como almacén de certificados.  Pulse **“Siguiente”** para continuar.
149.	Pulse **“Finalizar”** para terminar con la importación.
150.	El asistente le notificara que la importación se ha realizado correctamente. 
151.	Cierre el “Editor de administración de directivas de grupo”.

Paso	Descripción
152.	En la consola de "Administrador de directivas de grupo". En la parte de la izquierda, sobre **"<<Su dominio>> > Clientes Windows 7 > Equipos Windows 7"** piche con el botón derecho y seleccione **"Vincular una GPO existente...".**



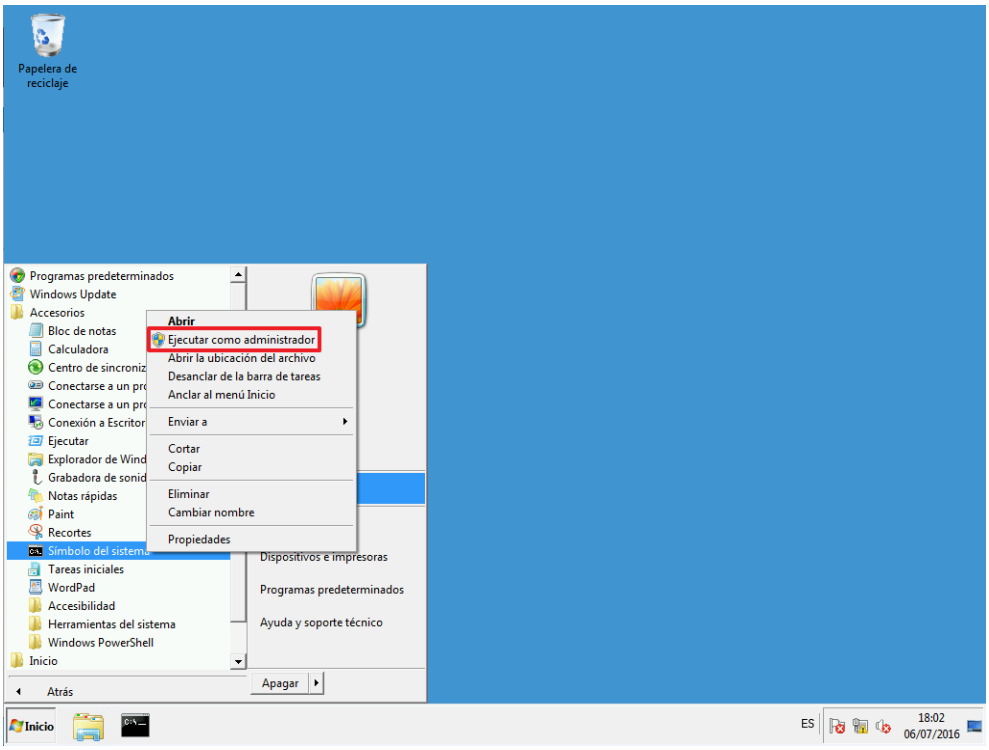
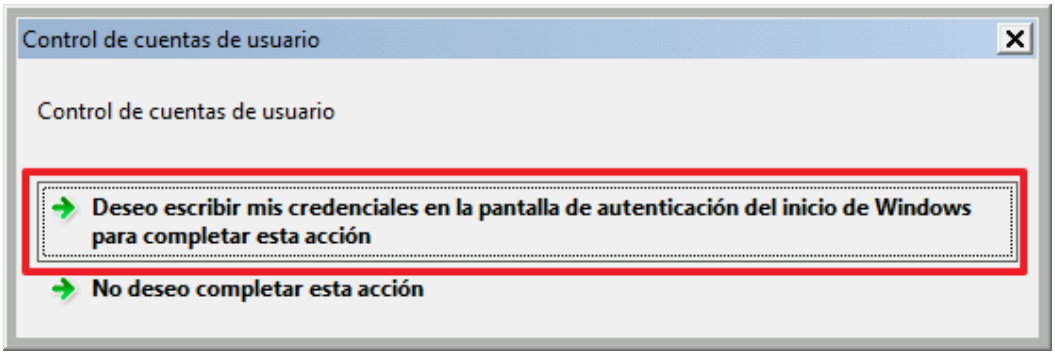
153.	Seleccione la GPO **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS"** y pulse **"Aceptar".**



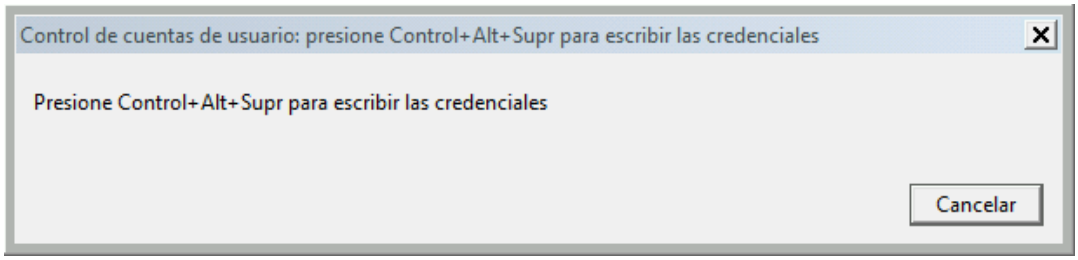
Paso	Descripción
154.	Seleccione la unidad organizativa **"Equipos Windows 7"**, situada en **"<<Su dominio>> > Clientes Windows 7 > Equipos Windows 7"** y en la parte de la derecha, establezca la GPO **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS"** en la posición 1. 

Una vez que ha realizado los pasos anteriores, ya estaría todo preparado para que Windows Server Update Services pueda detectar los equipos clientes Windows 7 que disponga en su infraestructura.

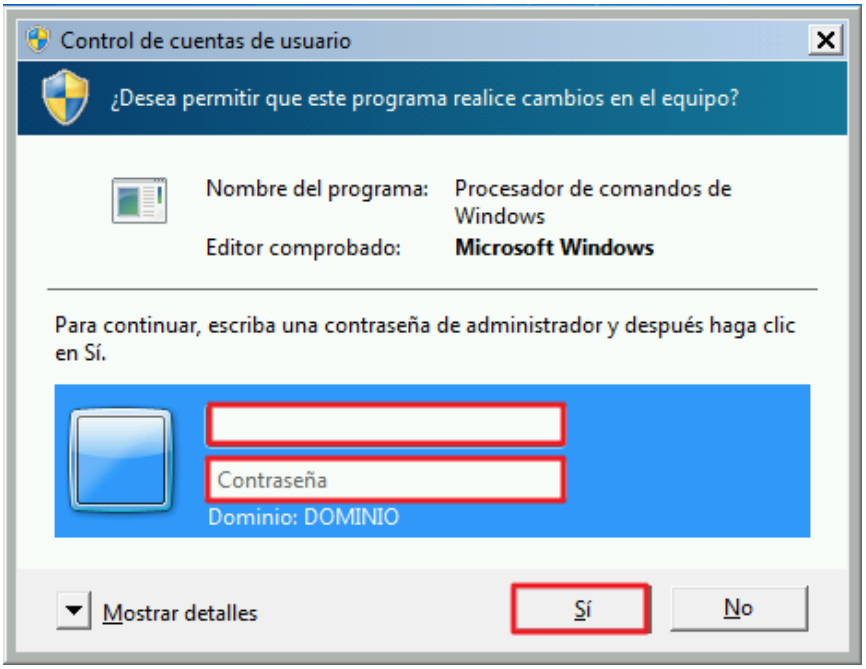
Paso	Descripción
155.	Inicie sesión en el equipo cliente Windows 7 con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
156.	Ejecute un **"Símbolo de sistema",** para ello vaya a **"Inicio > Todos los programas > Accesorios > Símbolo del sistema"** y con el botón derecho, seleccione **"Ejecutar como administrador".** 
157.	El control de cuentas de usuario le pedirá si quieres meter sus credenciales de administrador de domino, para ello, haga clic en **"Deseo escribir mis credenciales en la pantalla de autenticación… ".** 

Paso	Descripción
158.	Le pedirá que pulse **Control +Alt +Supr** para continuar.

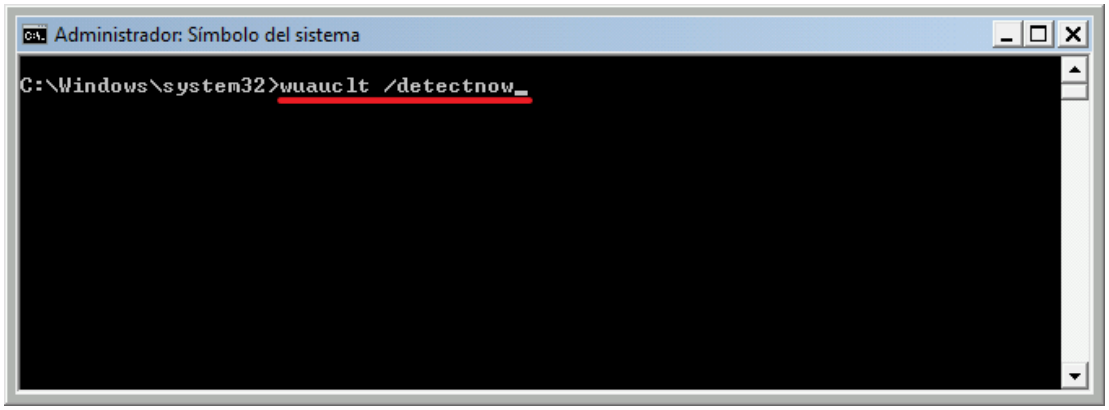


159. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.

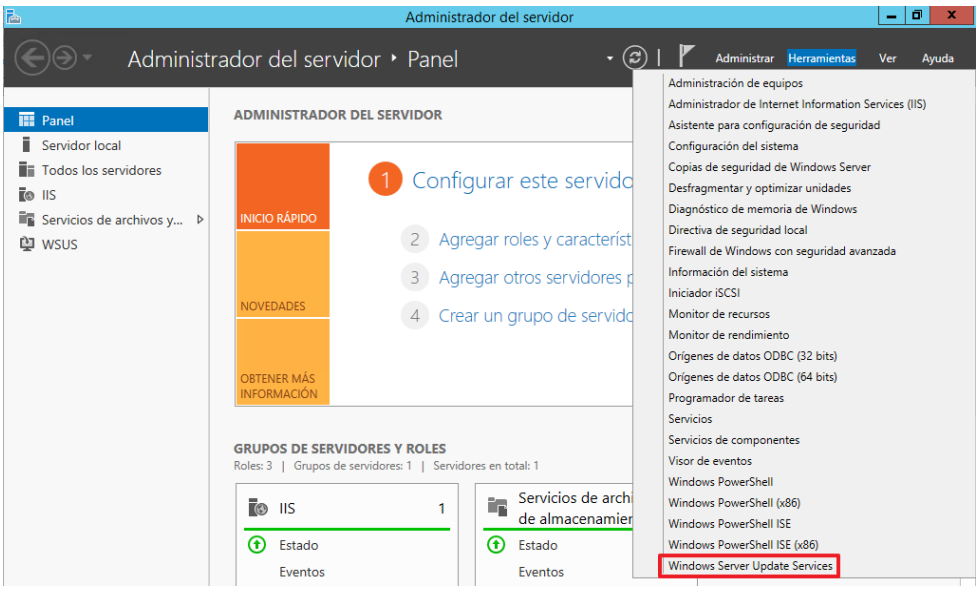


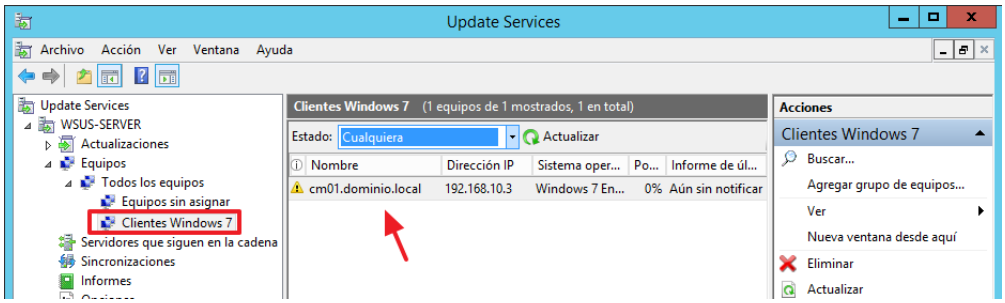
Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

160. Escriba el siguiente comando: **wuauclt /detectnow** y pulse **Intro.**



Una vez hecho esto el servidor Windows Server Update Services ya tendrá en cuenta el equipo Windows 7 que se acaba de enlazar. Siga los siguientes puntos para comprobar que la consola de WSUS es capaz de ver el equipo enlazado.

Paso	Descripción
161.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Service con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
162.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
163.	En la consola **"Update Services",** diríjase al grupo creado que pertenece a los equipos clientes de Windows 7. Si todo ha salido correctamente deberá encontrarse el equipo enlazado anteriormente. En la ventana central de la consola, debe situar la pestaña **"Estado"** en **"Cualquiera"** para que aparezca el equipo.  **Nota:** El tiempo que tarda WSUS en detectar en el equipo cliente una vez ejecutado el comando "wuauclt /detectnow", puede ser de varios minutos, esto dependerá de la velocidad de su red. Si después de un tiempo el equipo cliente no ha sido detectado por el servidor WSUS, vuelva a repasar los pasos anteriores para corroborar que ha realizado todos los pasos adecuadamente.

4.2. CONFIGURACIÓN DE LOS EQUIPOS CLIENTE WINDOWS 10

Antes de aplicar las GPO´s en el Controlador de Domino del dominio, se deberá crear el grupo de equipos Windows 10 en la consola de WSUS, para que cuando la política "Habilitar destinatarios del lado cliente" sea aplicada a estos equipos, éstos queden asignados automáticamente al grupo que les corresponde.

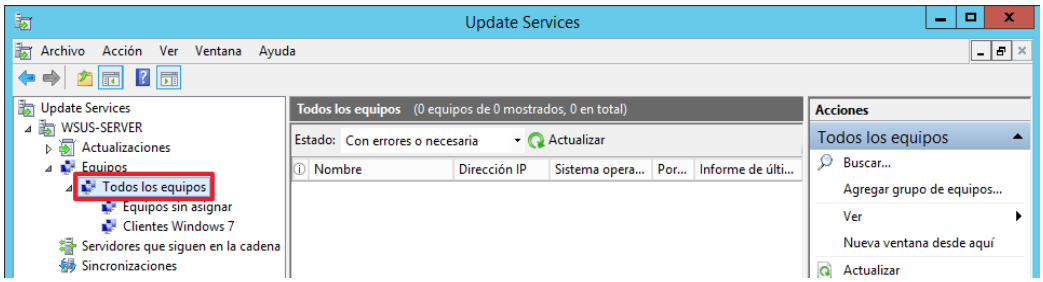
Nota: Este apartado establece el procedimiento para utilizar un equipo cliente Windows 10 miembro del dominio como cliente del servicio WSUS. Si desea conectar un equipo cliente Windows 10 independiente (standalone) con el servicio WSUS, deberá aplicar los cambios en el registro que se indican en la URL https://technet.microsoft.com/en-us/library/cc720464(v=ws.10).aspx y realizar las modificaciones correspondientes en la configuración de comunicación entre ambos sistemas para permitir la conexión con el servicio.

Paso	Descripción
164.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
165.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

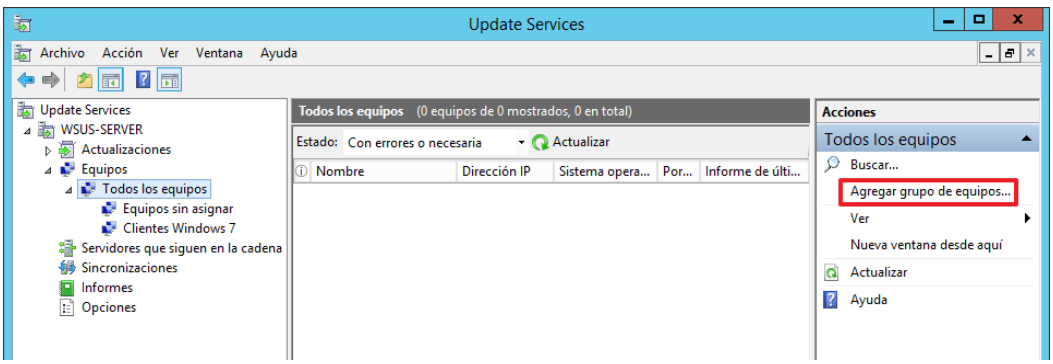
Paso	Descripción
166.	Ejecute la consola de Windows Server Update Service, desde **"Inicio > Administrador del servidor>Herramientas > Windows Server Update Services"**.

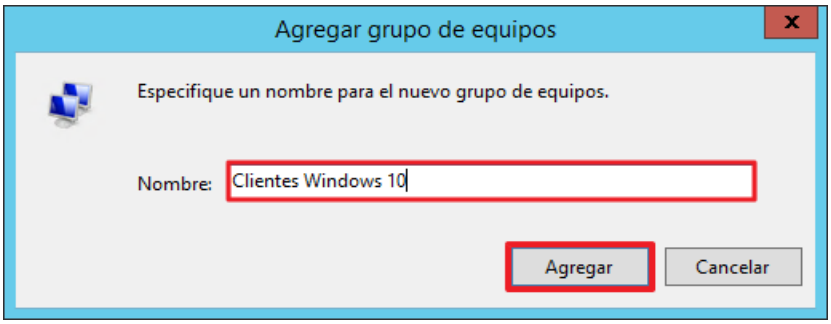
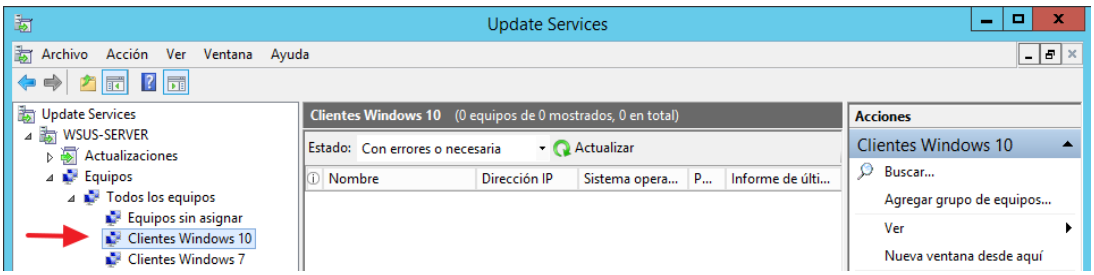
Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

167.	Dentro de la consola de Update Services, sitúese en la parte de la izquierda **"Update Services > <<Su servidor WSUS>> >Equipos > Todos los equipos".**



168.	En la parte de la derecha, pinche en **"Agregar grupo de equipos…".**

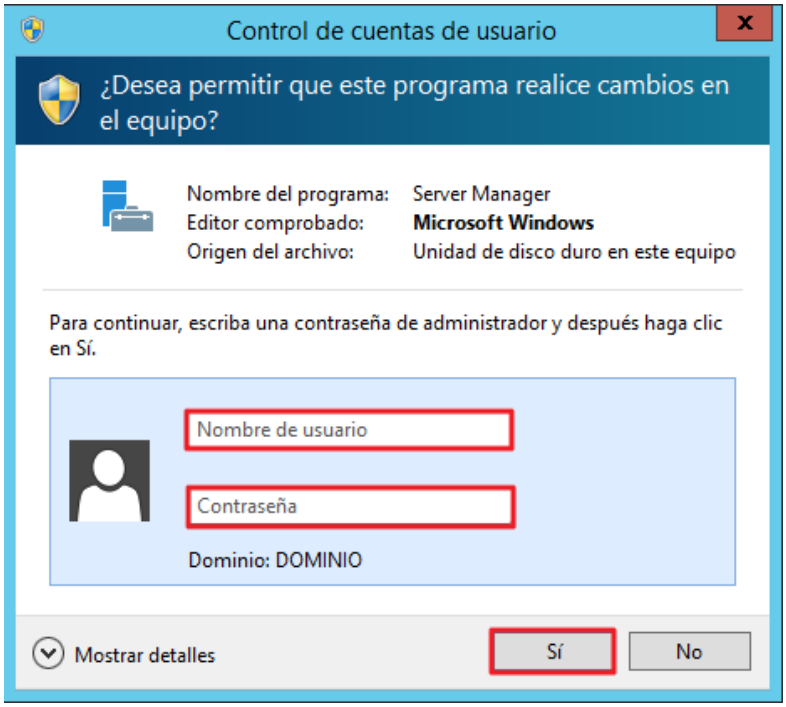


Paso	Descripción
169.	Se abrirá una ventana, donde se deberá indicar el nombre del grupo que se va a crear, añada **"Clientes Windows 10".**  Pulse en **"Agregar"** para terminar.
170.	Se habrá agregado este grupo en la pestaña de **"Equipos > Todos los equipos"**, tal y como se muestra en la siguiente imagen: 

Configurado ya el grupo al que van pertenecer los equipos cliente Windows 10 en el servidor WSUS, ya se podrá aplicar la política en el Controlador de Dominio del dominio para que los equipos ingresen automáticamente en el grupo al que correspondan.

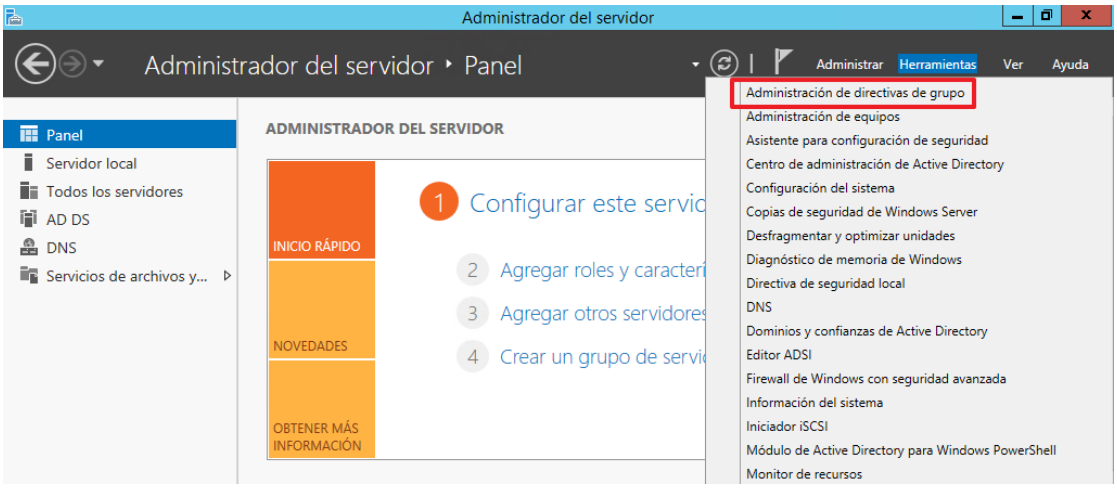
Paso	Descripción
171.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
172.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
173.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.



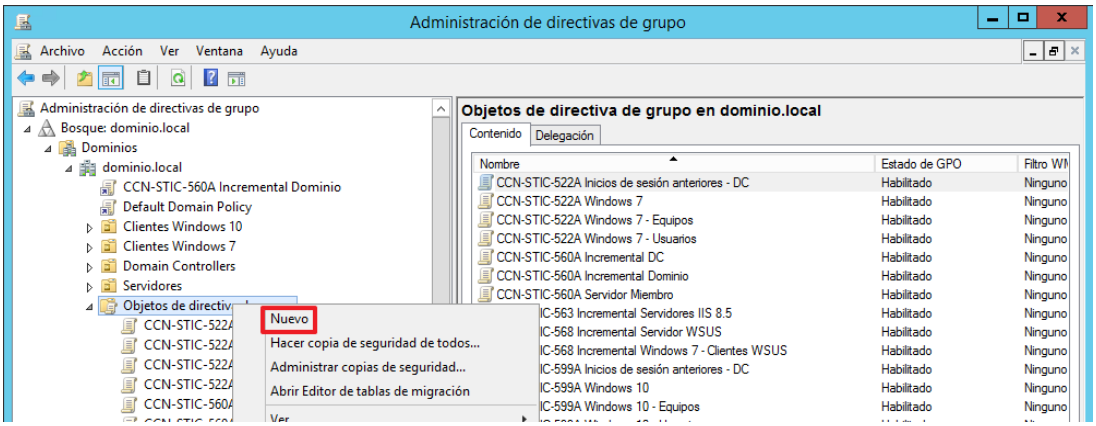
Nota: En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

174.	Ejecute la consola de Administración de directivas de grupo desde el menú **"Inicio > Administrador del servidor > Herramientas > Administración de directivas de grupo".**

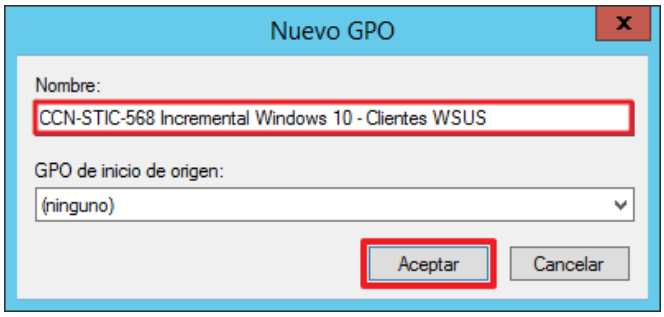


Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

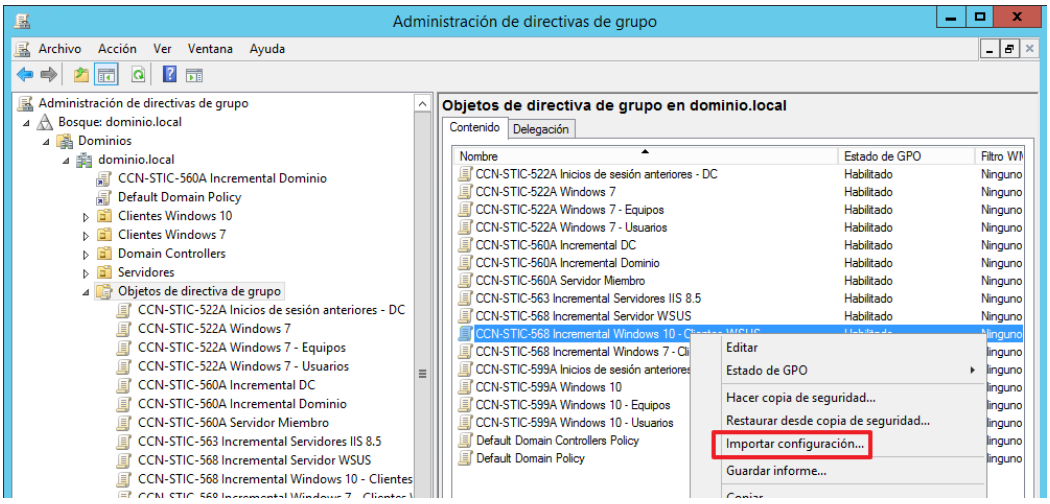
Paso	Descripción
175.	En la ventana de la izquierda sitúese sobre **"Objetos de directiva de grupo"** y con el botón derecho pulse sobre **"Nuevo"**.



176.	Introduzca **"CCN-STIC-568 Incremental Windows 10 – Clientes WSUS"** como nombre de la nueva GPO que está creando. Pulse **"Aceptar".**

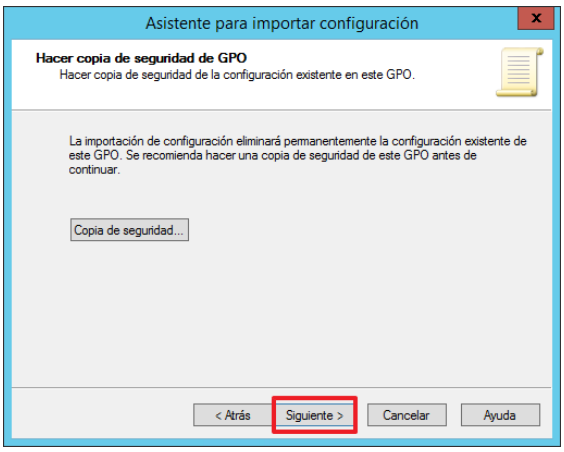


177.	Una vez creada la GPO, deberá importar la configuración. Para ello, sobre la política que acaba de crear, pulse botón derecho y pinche sobre **"Importar configuración…".**

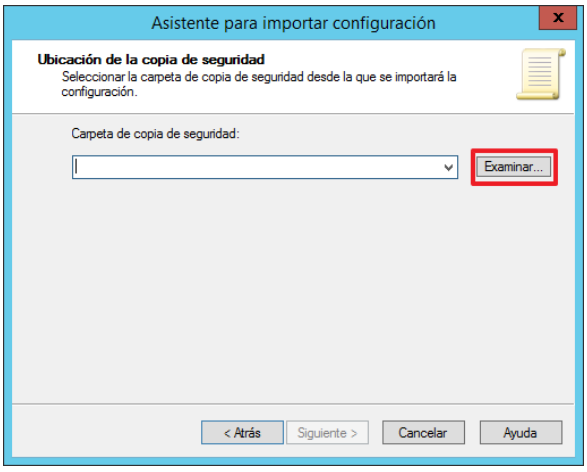


178.	En el "Asistente para importar configuración", pulse **"Siguiente >"** para continuar.

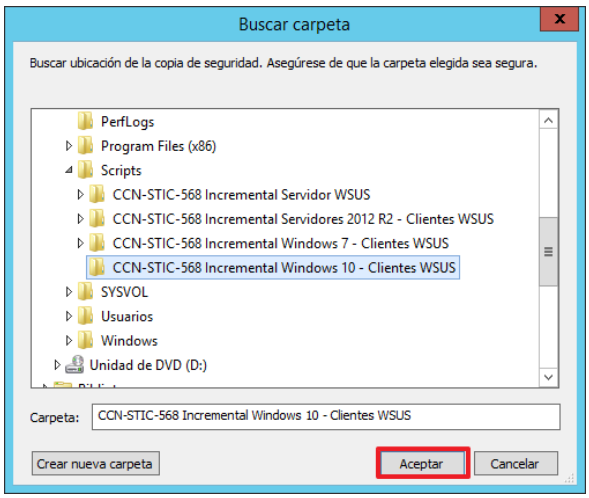
Paso	Descripción
179.	Omita realizar copia de seguridad y pulse **"Siguiente >".**



180.	Pulse en **"Examinar"**, sitúese en **"Este equipo > Disco local (C:) > Scripts"** y seleccione **"CCN-STIC-568 Incremental Windows 10 – Clientes WSUS".**

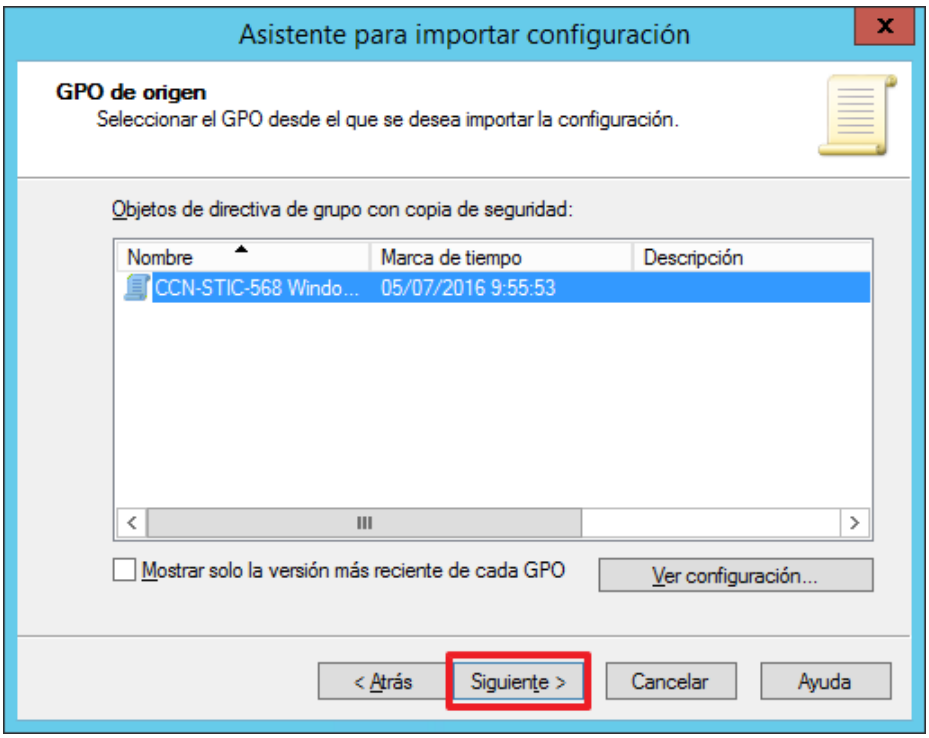


Pulse **"Aceptar".**

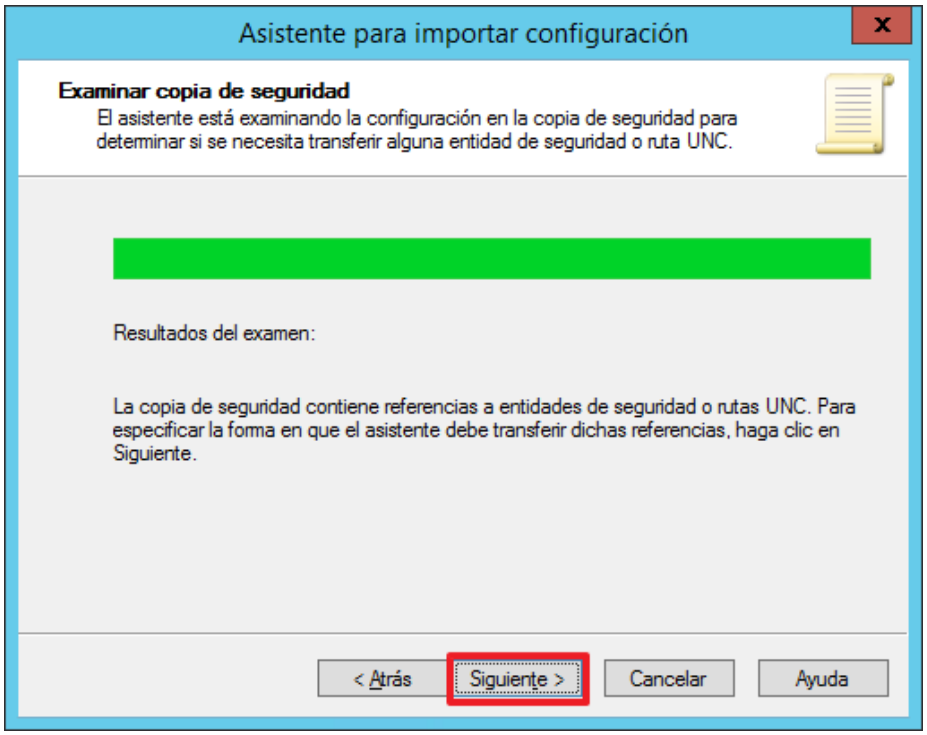


Pulse **"Siguiente >"** en el asistente para continuar.

Paso	Descripción
181.	Pulse **"Siguiente >".**

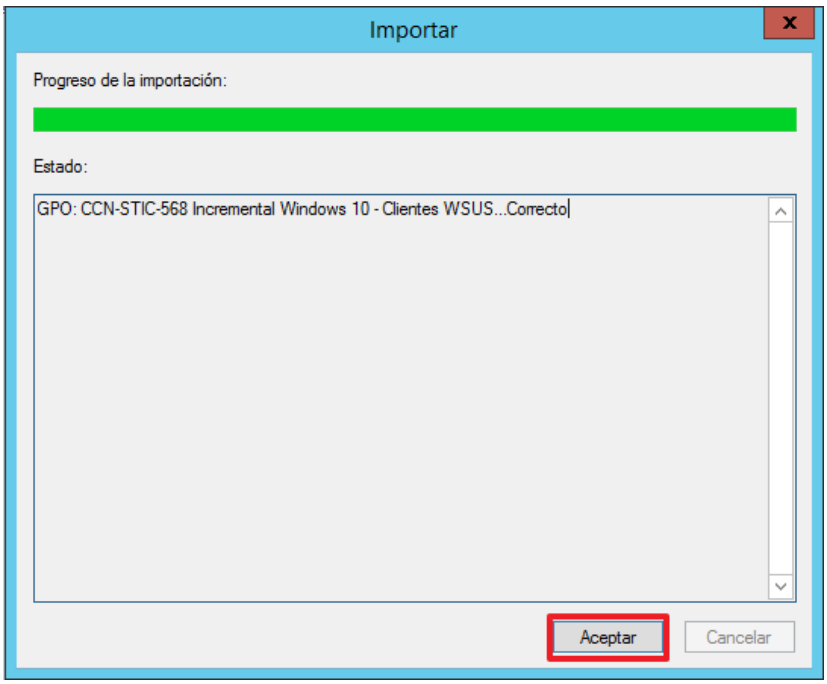


182.	Pulse **"Siguiente >"** en "Examinar copia de seguridad".

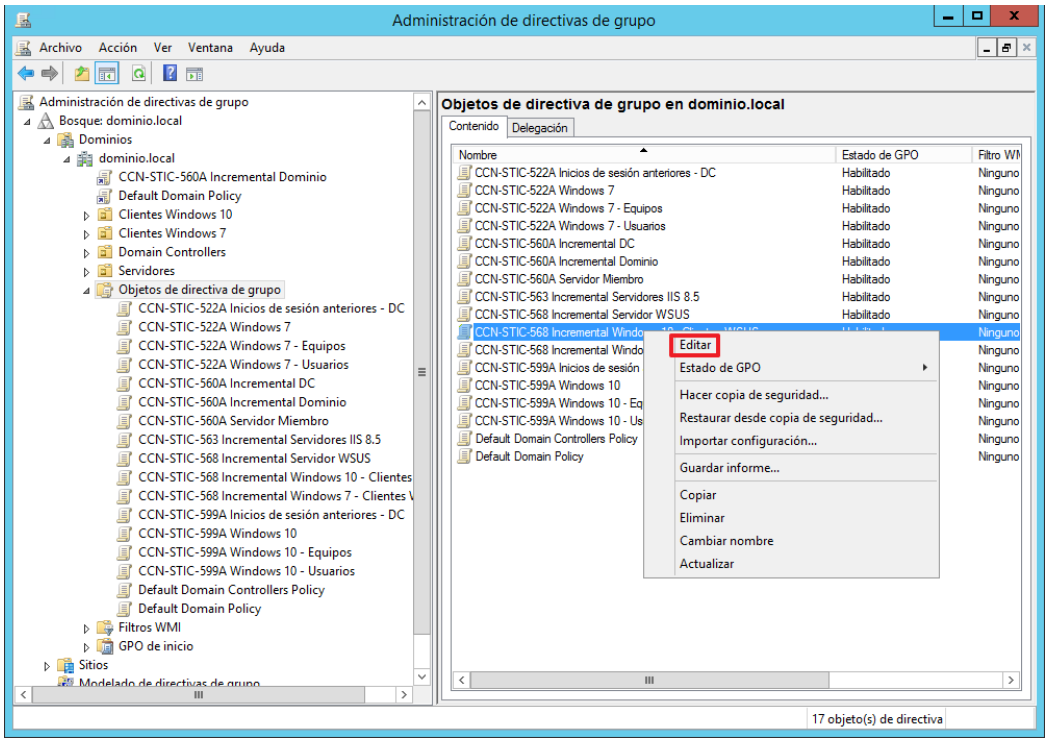


183.	Pulse **"Finalizar"** para finalizar la importación de configuración de la GPO.

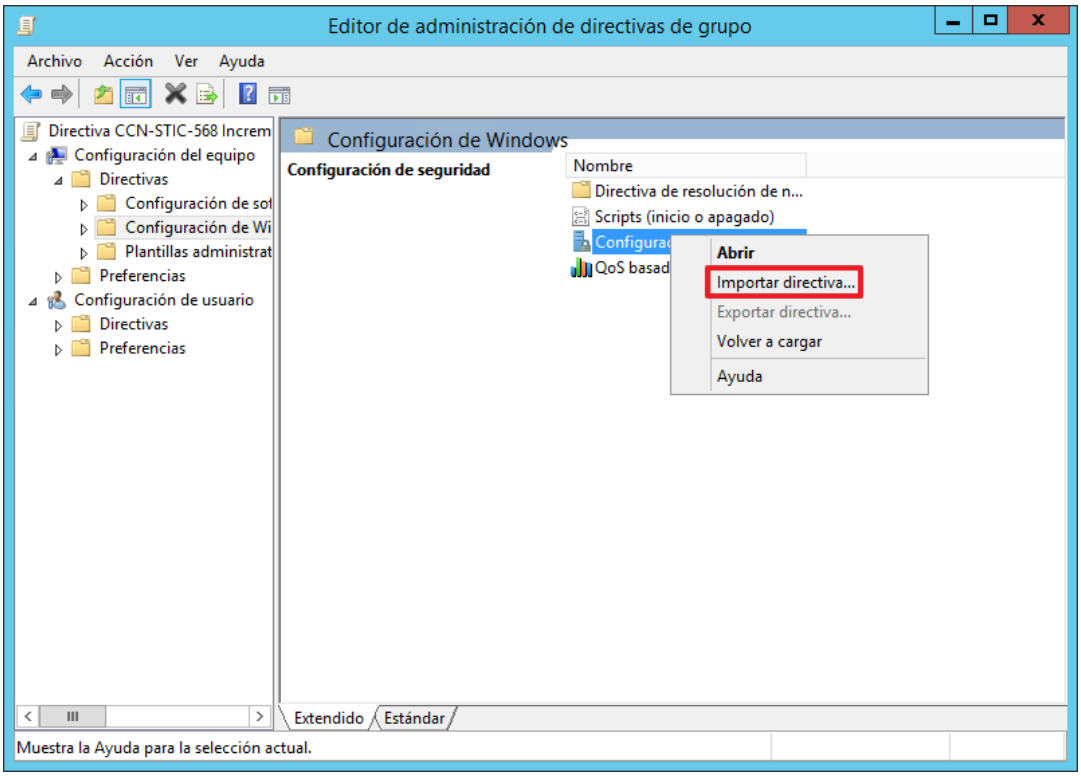
Paso	Descripción
184.	Pulse en “Aceptar” para guardar los cambios.



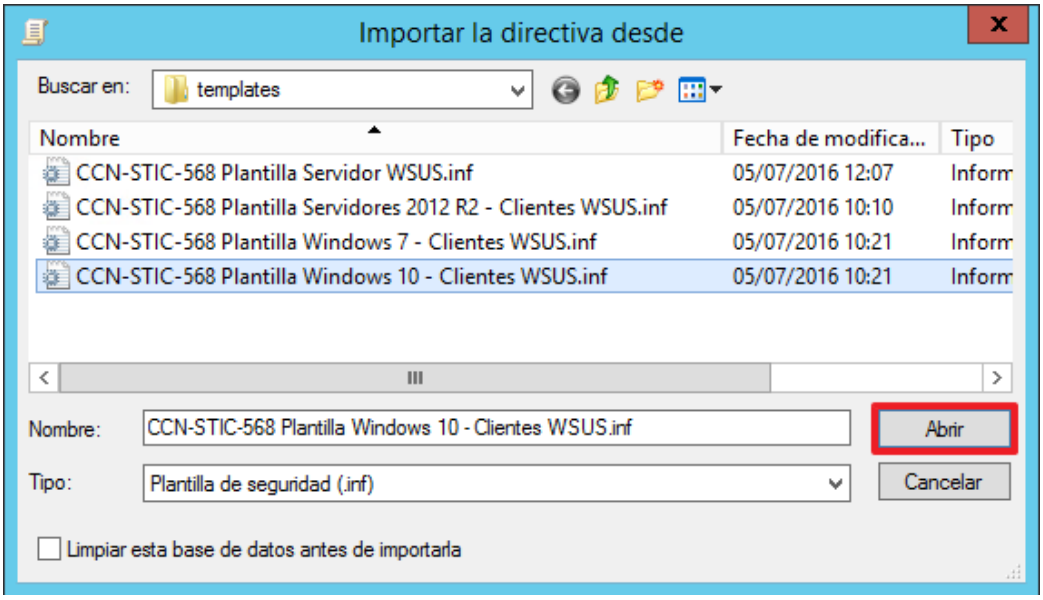
185. Una vez importada la configuración, deberá realizar una serie de configuraciones en la propia GPO. Para ello, sobre la política **“CCN-STIC-568 Incremental Windows 10 – Clientes WSUS”** pulse botón derecho y pinche sobre **“Editar”.**



Paso	Descripción
186.	Sitúese en **"Configuración del equipo > Directivas > Configuración de seguridad"** y sobre esté, pulse con el botón derecho y seleccione **"Importar directiva…".**

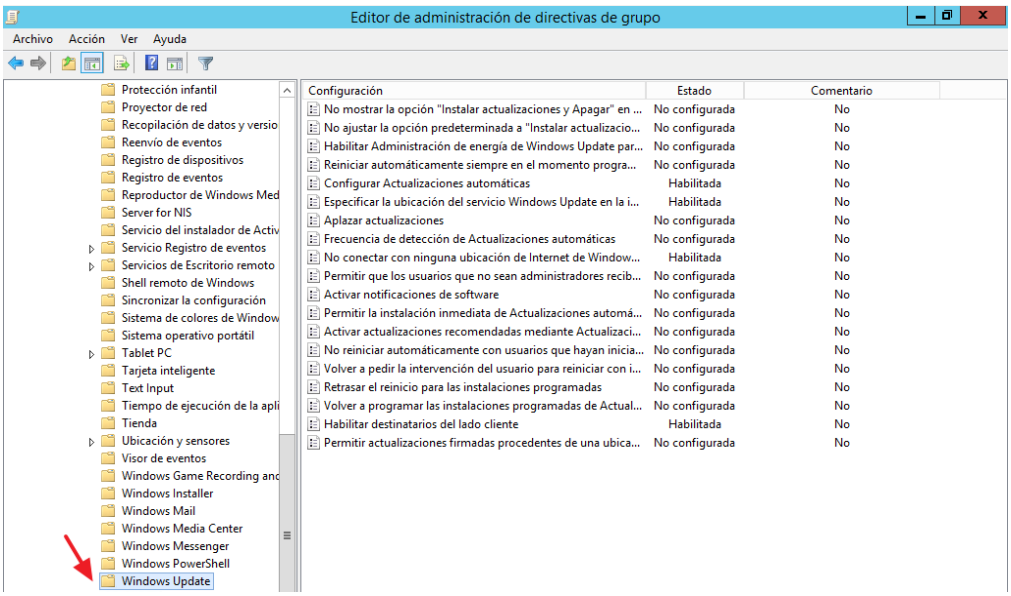


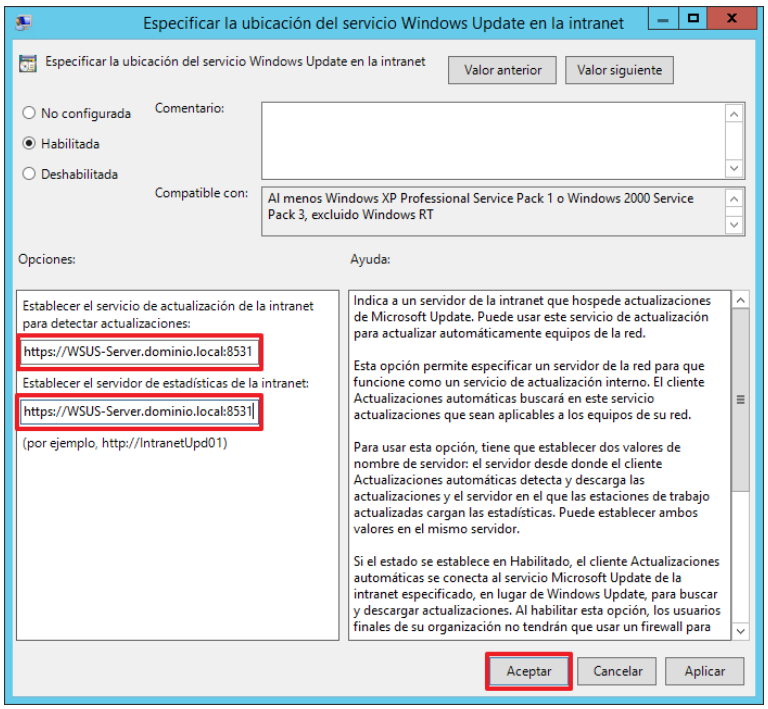
187.	Desde C:\Windows\Security\templates, seleccione **"CCN-STIC-568 Plantilla Windows 10 – Clientes WSUS.inf"**.



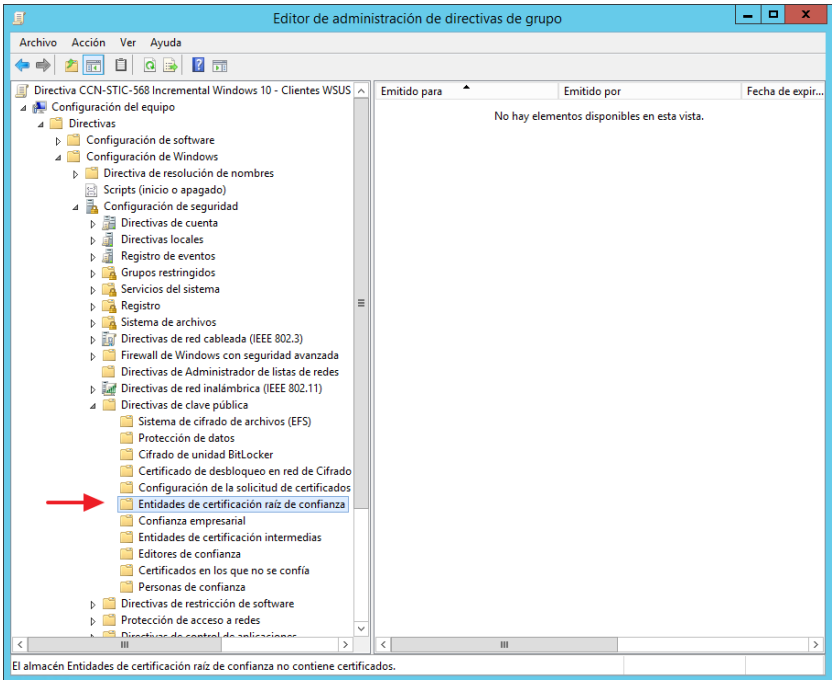
Pulse **"Abrir".**

Paso	Descripción
188.	Seguidamente, en **"Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows Update".**

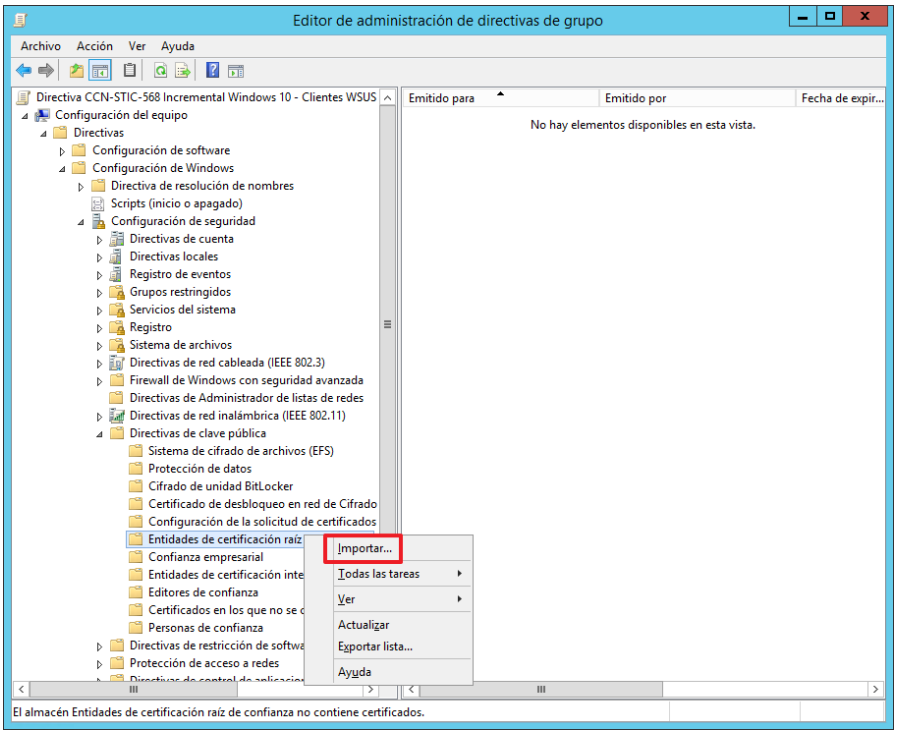


Paso	Descripción
189.	Haga doble clic sobre **"Especificar la ubicación del servicio Windows Update en la intranet"**, en la ventana opciones deberás introducir la ubicación del servidor WSUS. Tal y como se muestra en la siguiente imagen:  Pulse **"Aceptar"** para guardar los cambios. **Nota:** Deberá introducir la dirección de su servidor WSUS (Nombre FQDN). Para este ejemplo se ha utilizado https://WSUS-Server.dominio.local:8531. Es muy importante tener en cuenta que debe introducir HTTPS y el puerto 8531, ya que la configuración SSL requiere de estos dos parámetros.

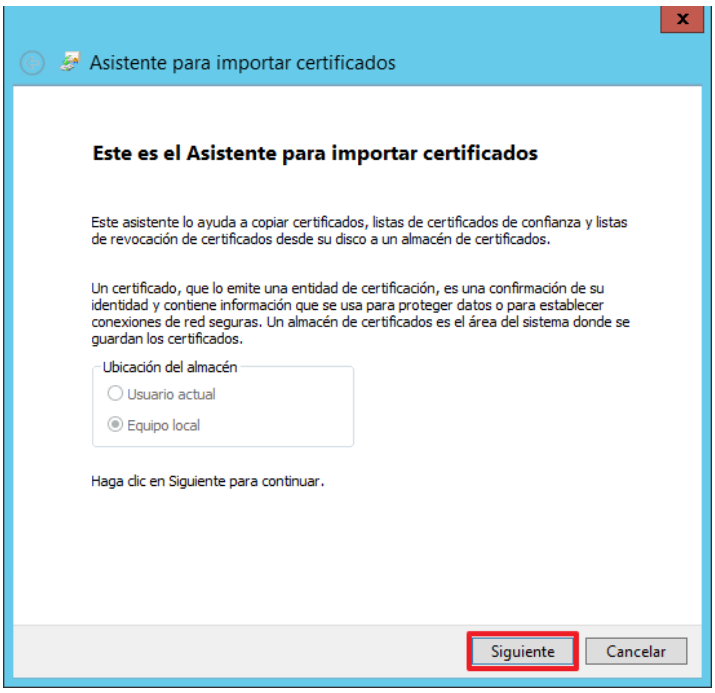
Paso	Descripción
190.	En el mismo "Editor de administración de directivas de grupo", diríjase a **"Configuración del equipo > Directivas > Configuración de seguridad > Directivas de clave pública > Entidades de certificación raíz de confianza".**



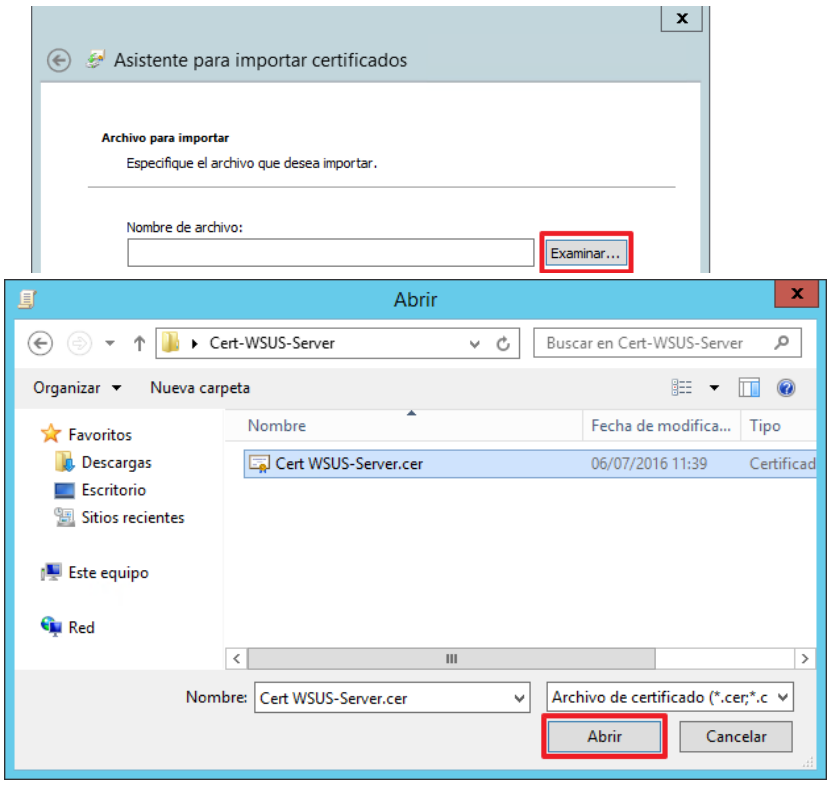
191.	Pulse sobre **"Entidades de certificación raíz de confianza"** con el botón derecho y seleccione **"Importar".**



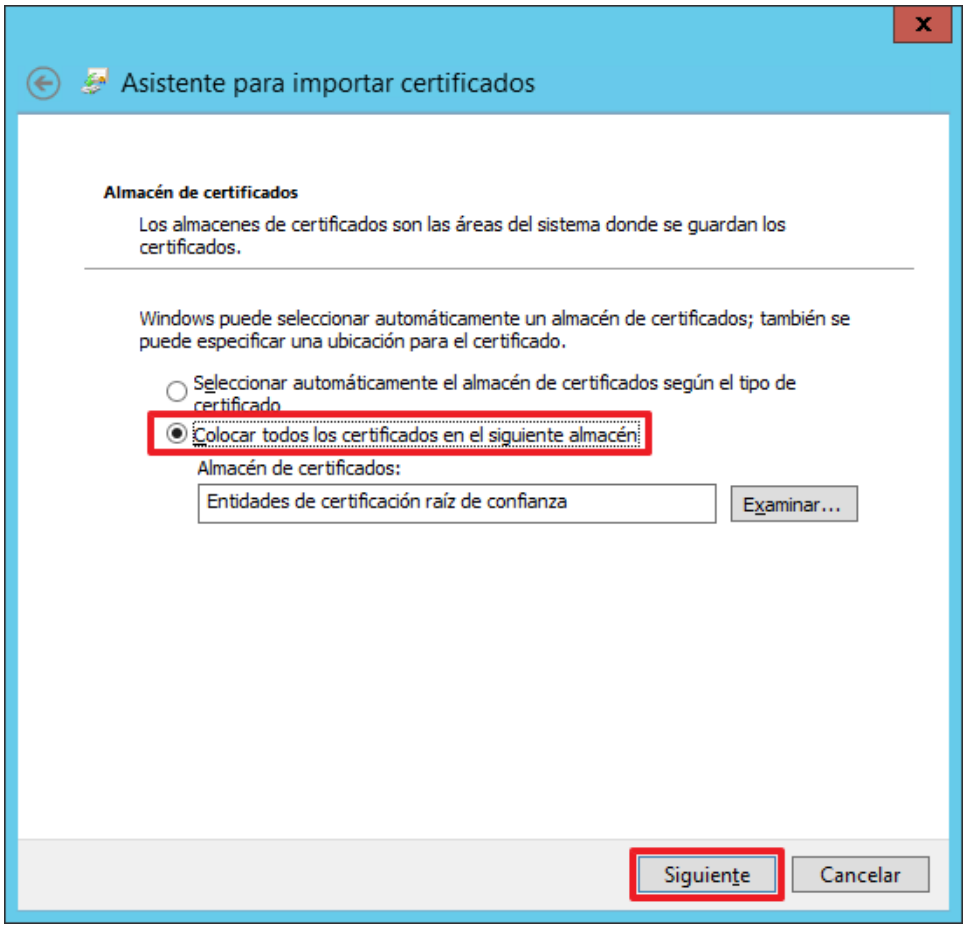
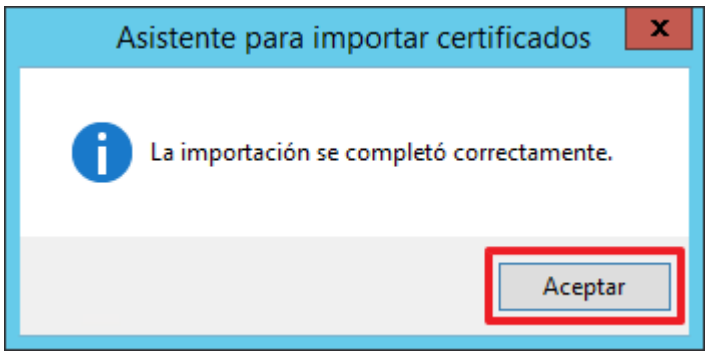
Paso	Descripción
192.	Se abrirá el asistente de Importar certificados, pulse **"Siguiente"** para continuar.



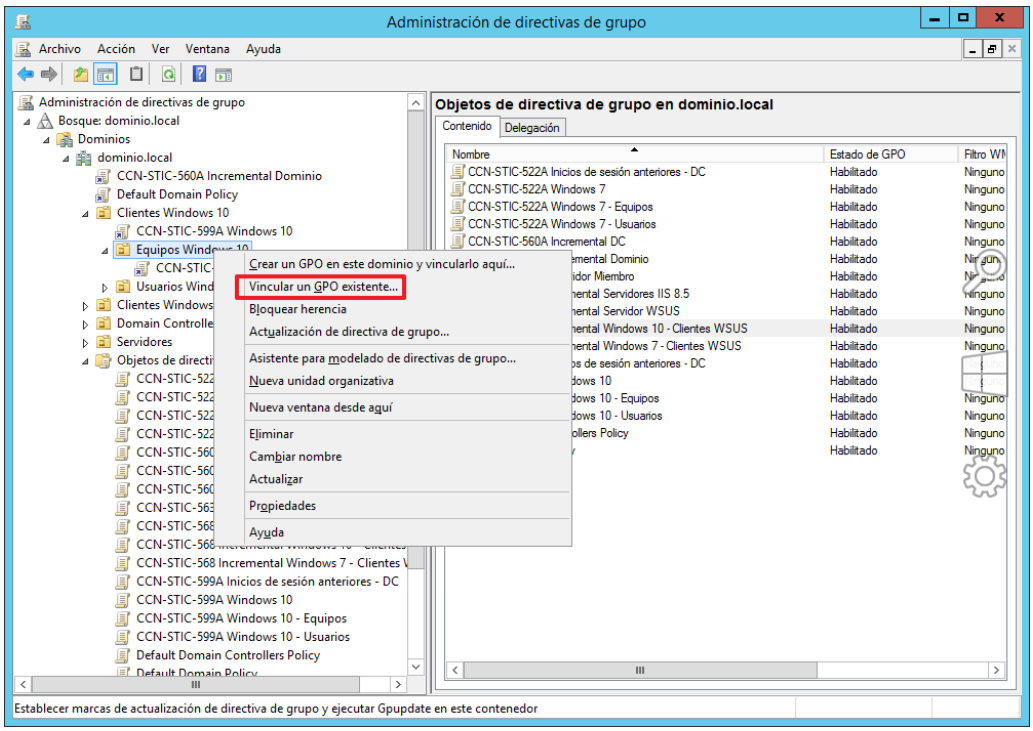
193.	Pulse sobre el botón **"Examinar"** y localice el certificado exportado anteriormente. Selecciónelo y pulse **"Abrir".**



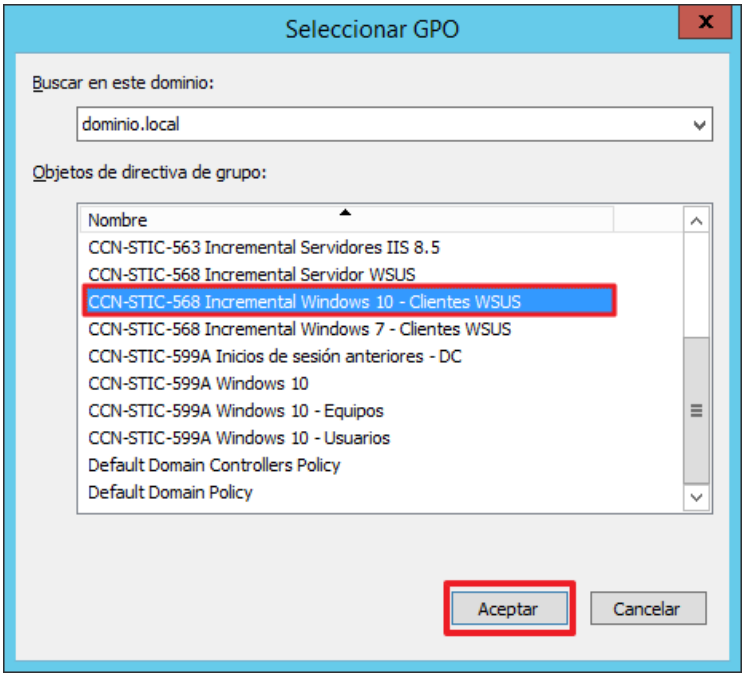
Pulse **"Siguiente"** para continuar.

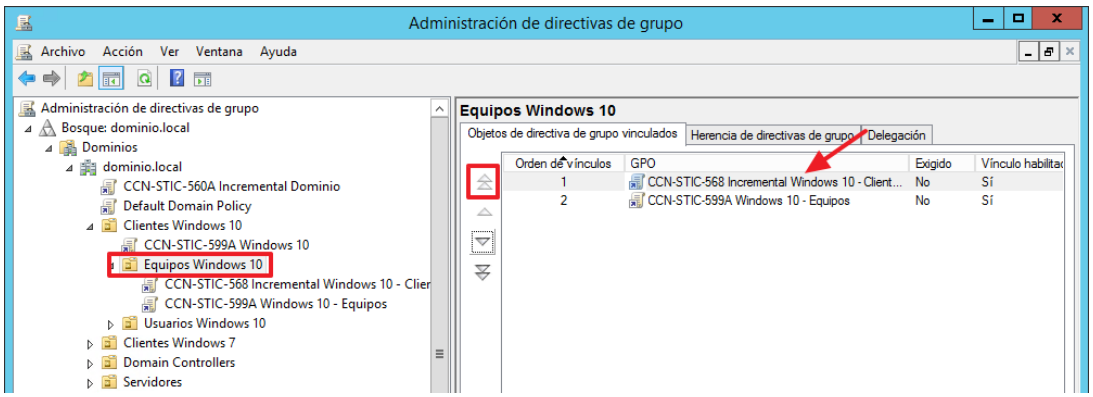
Paso	Descripción
194.	Deje seleccionado **"Colocar todos los certificados en el siguiente almacén"** como almacén de certificados.  Pulse **"Siguiente"** para continuar.
195.	Pulse **"Finalizar"** para terminar con la importación.
196.	El asistente le notificara que la importación se ha realizado correctamente. 
197.	Cierre el "Editor de administración de directivas de grupo".

Paso	Descripción
198.	En la consola de “Administrador de directivas de grupo”. En la parte de la izquierda, sobre **“<<Su dominio>> > Clientes Windows 10 > Equipos Windows 10”** piche con el botón derecho y seleccione **“Vincular una GPO existente…”.**



199.	Seleccione la GPO **“CCN-STIC-568 Incremental Windows 10 – Clientes WSUS”** y pulse **“Aceptar”.**

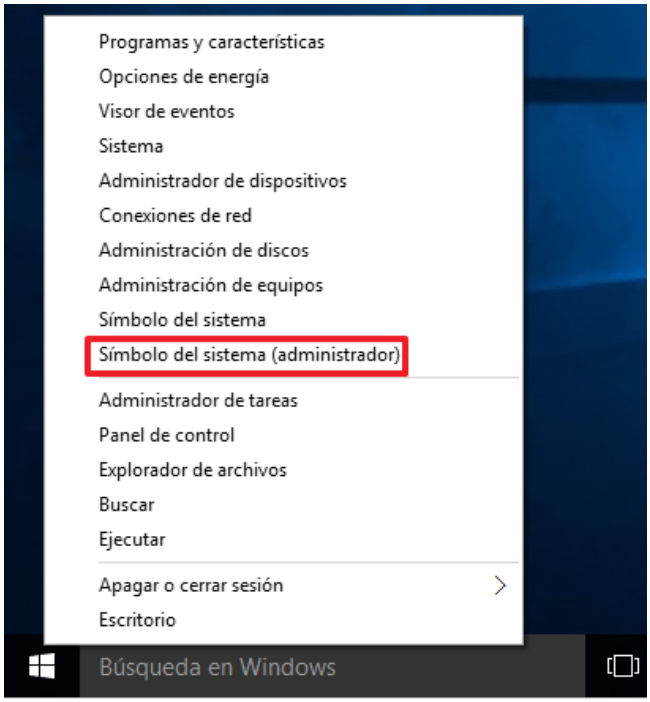


Paso	Descripción
200.	Seleccione la unidad organizativa **"Equipos Windows 10"**, situada en **"<<Su dominio>> > Clientes Windows 10 > Equipos Windows 10"** y en la parte de la derecha, establezca la GPO **"CCN-STIC-568 Incremental Windows 10 – Clientes WSUS"** en la posición 1. 

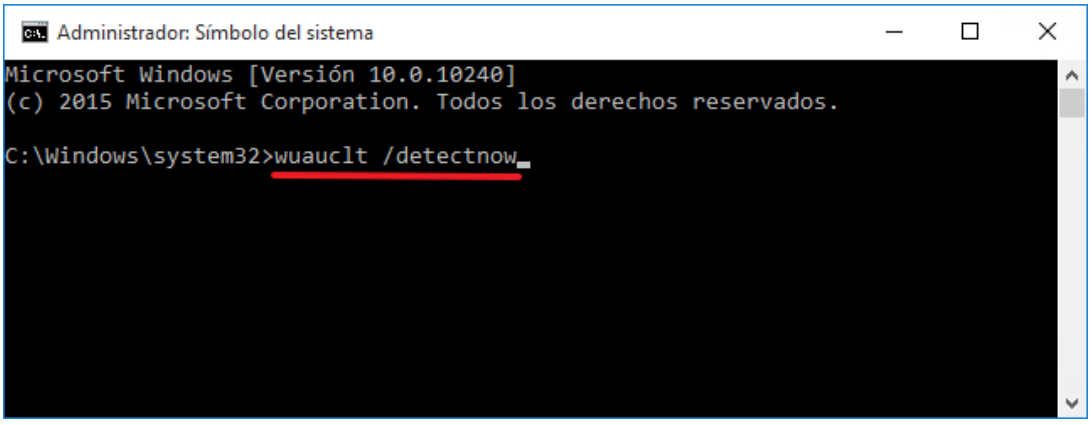
Una vez que ha realizado los pasos anteriores, ya estaría todo preparado para que Windows Server Update Services pueda detectar los equipos clientes Windows 10 que disponga en su infraestructura.

Paso	Descripción
201.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
202.	Inicie sesión en el equipo cliente Windows 10 con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
203.	Pulse con el botón derecho sobre el icono de **"Inicio"** y seleccione **"Símbolo del sistema (administrador)"**.

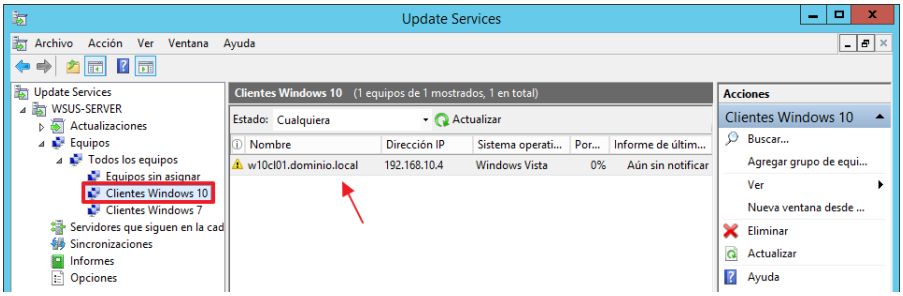


204.	Introduzca el siguiente comando: **wuauclt /detectnow**, seguidamente pulse **"Intro".**



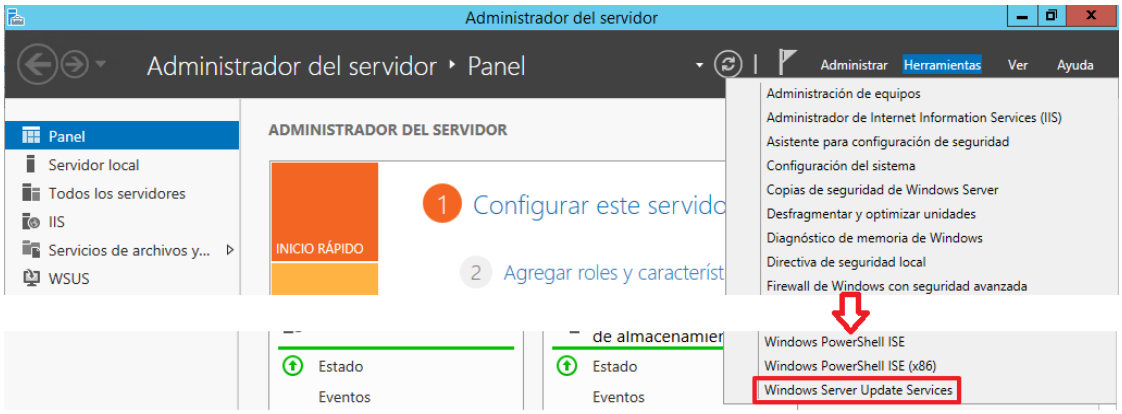
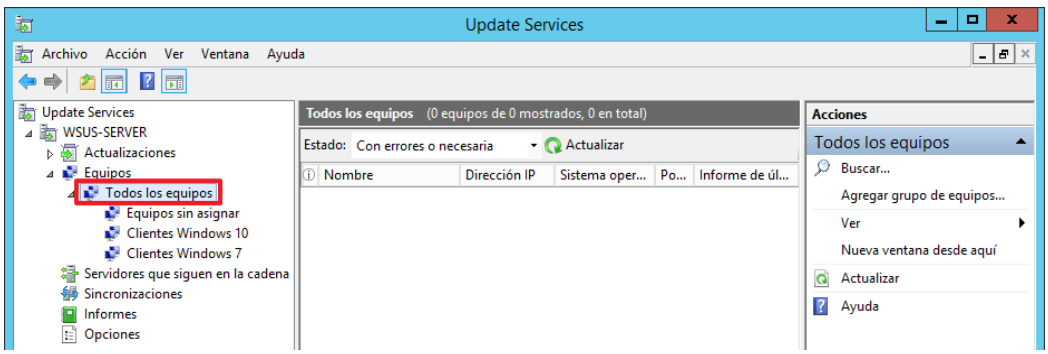
Una vez hecho esto el servidor Windows Server Update Services ya tendrá en cuenta el equipo Windows 10 que se acaba de enlazar. Siga los siguientes puntos para comprobar que la consola de WSUS es capaz de ver el equipo enlazado.

Paso	Descripción
205.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.

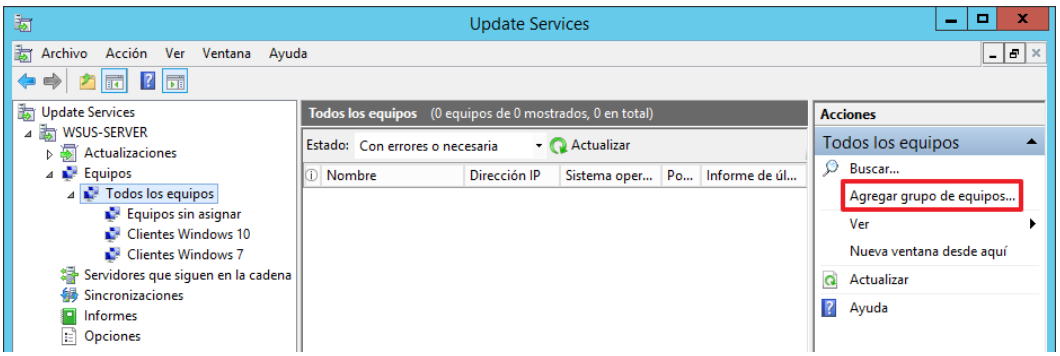
Paso	Descripción
206.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
207.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".
208.	En la consola **"Update Services",** diríjase al grupo creado que pertenece a los equipos clientes de Windows 10. Si todo ha salido correctamente deberá encontrarse el equipo enlazado anteriormente. En la ventana central de la consola, debe situar la pestaña **"Estado"** en **"Cualquiera"** para que aparezca el equipo.  **Nota:** El tiempo que tarda WSUS en detectar en el equipo cliente una vez ejecutado el comando "wuauclt /detectnow", puede ser de varios minutos, esto dependerá de la velocidad de su red. Si después de un tiempo el equipo cliente no ha sido detectado por el servidor WSUS, vuelva a repasar los pasos anteriores para corroborar que ha realizado todos los pasos adecuadamente.

4.3. CONFIGURACIÓN DE LOS EQUIPOS CLIENTE WINDOWS SERVER 2012 R2

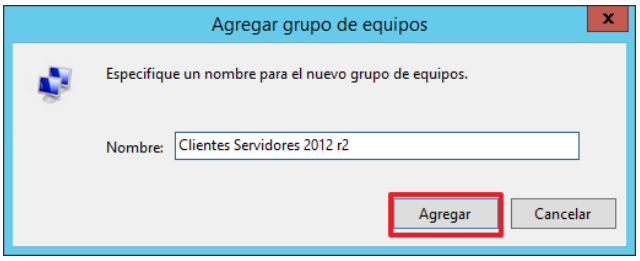
Antes de aplicar las GPO en el Controlador de Domino del dominio, se deberá crear el grupo de equipos Windows Server 2012 r2 en la consola de WSUS, para que cuando la política "Habilitar destinatarios del lado cliente" se aplique a estos equipos, se asignen automáticamente al grupo que les corresponde.

Paso	Descripción
209.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
210.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor>Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".
211.	Dentro de la consola de Update Services, sitúese en la parte de la izquierda **"Update Services > <<Su servidor WSUS>> > Equipos > Todos los equipos".** 

Paso	Descripción
212.	En la parte de la derecha, pinche en **"Agregar grupo de equipos…".**

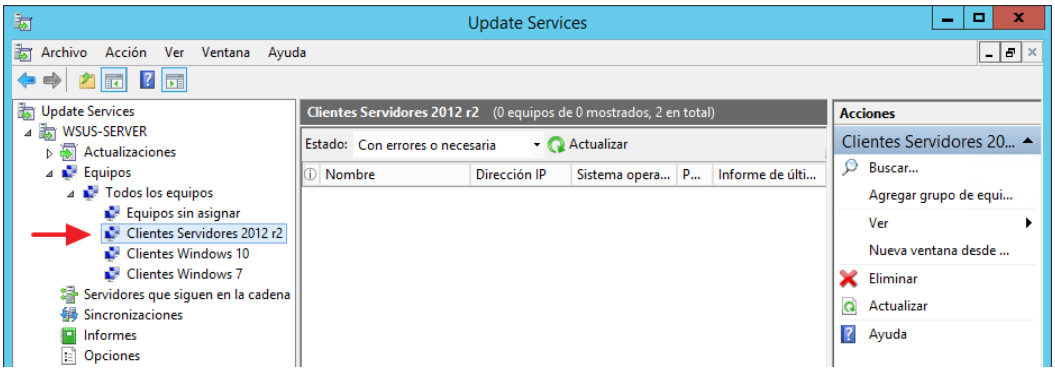


213.	Se abrirá una ventana, donde se deberá indicar el nombre del grupo que se va a crear, añada **"Clientes Servidor 2012 r2".**

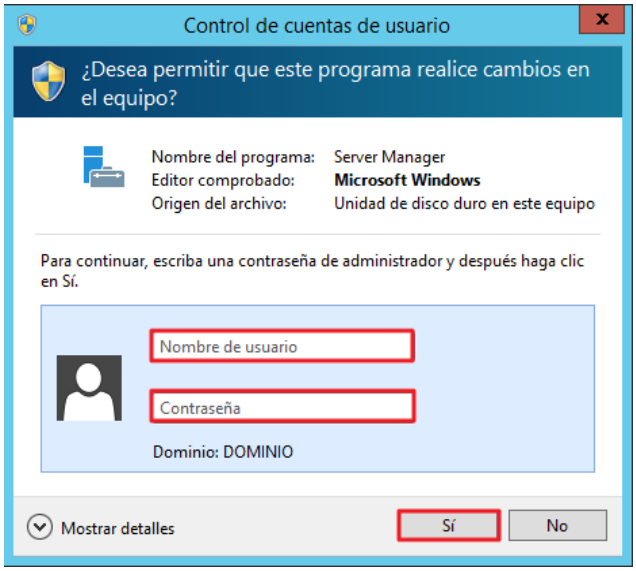
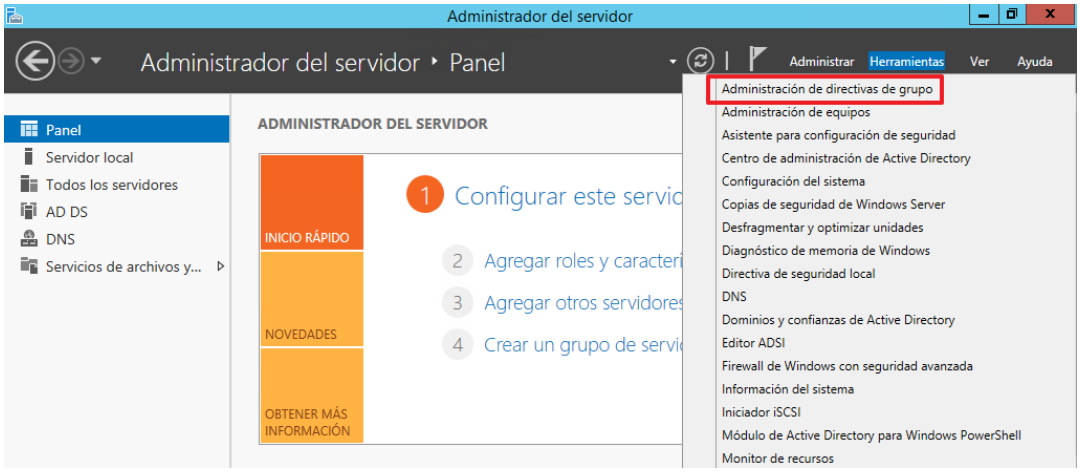


Pulse en **"Agregar"** para terminar.

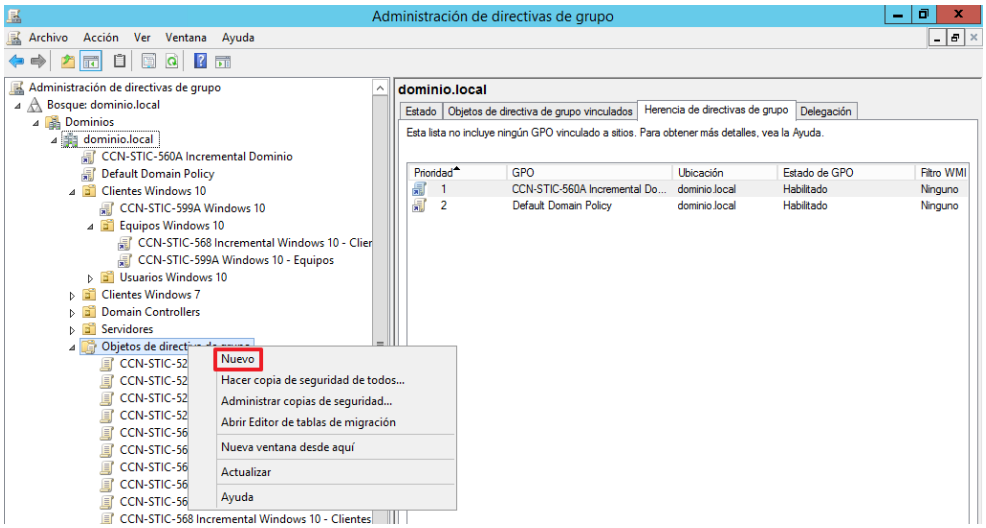
214.	Se habrá agregado este grupo en la pestaña de **"Equipos > Todos los equipos"**, tal y como se muestra en la siguiente imagen:



Configurado ya el grupo al que van pertenecer los equipos cliente Windows Server 2012 r2 en el servidor WSUS, ya se podrá aplicar la política en el Controlador de Dominio del dominio para que los equipos ingresen automáticamente en el grupo al que correspondan.

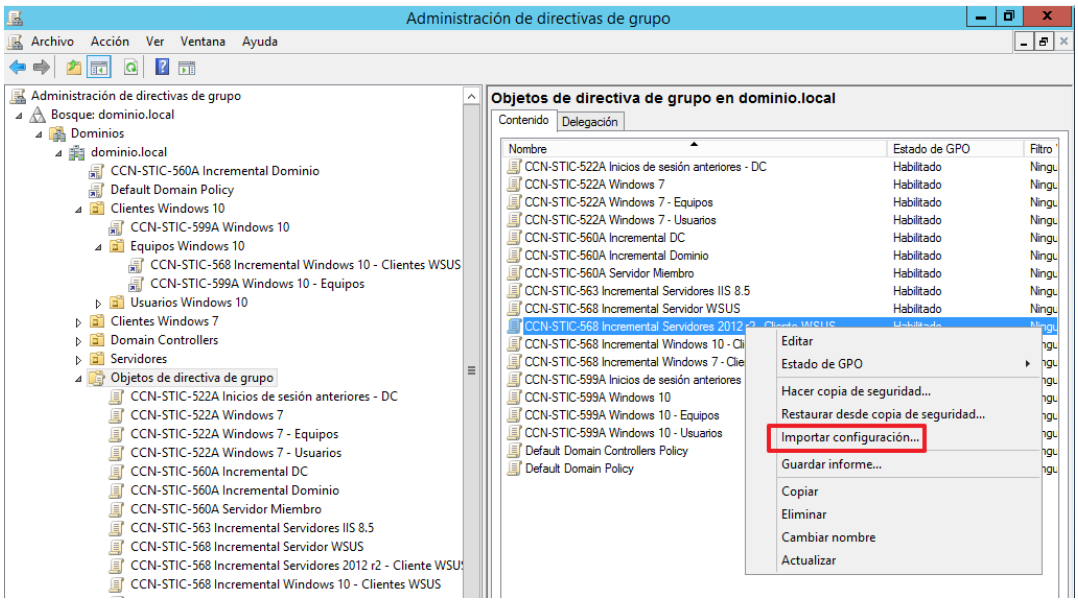
Paso	Descripción
215.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
216.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
217.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.  **Nota:** En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".
218.	Ejecute la consola de Administración de directivas de grupo desde el menú **"Inicio > Administrador del servidor > Herramientas > Administración de directivas de grupo".**  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
219.	En la ventana de la izquierda sitúese sobre **"Objetos de directiva de grupo"** y con el botón derecho pulse sobre **"Nuevo"**.

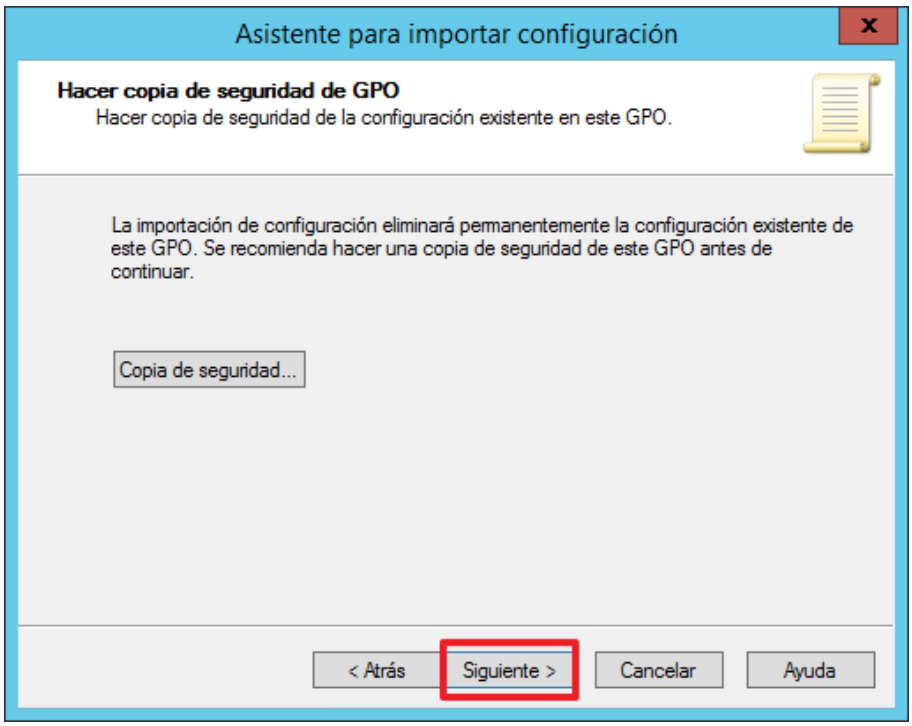


220.	Introduzca **"CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS"** como nombre de la nueva GPO que está creando. Pulse **"Aceptar".**

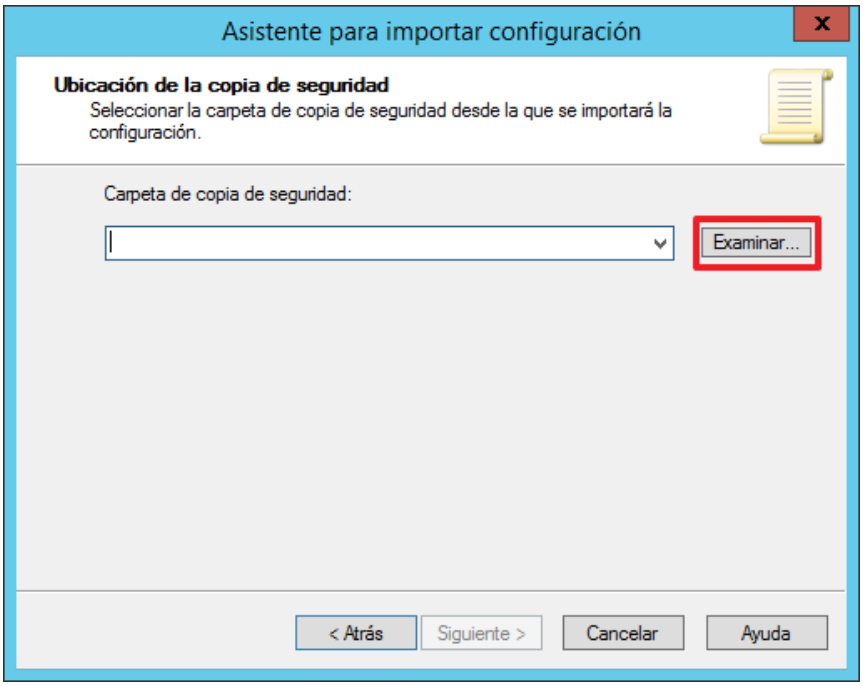
Paso	Descripción
221.	Una vez creada la GPO, deberá importar la configuración. Para ello, sobre la política que acaba de crear, pulse botón derecho y pinche sobre **"Importar configuración…".**



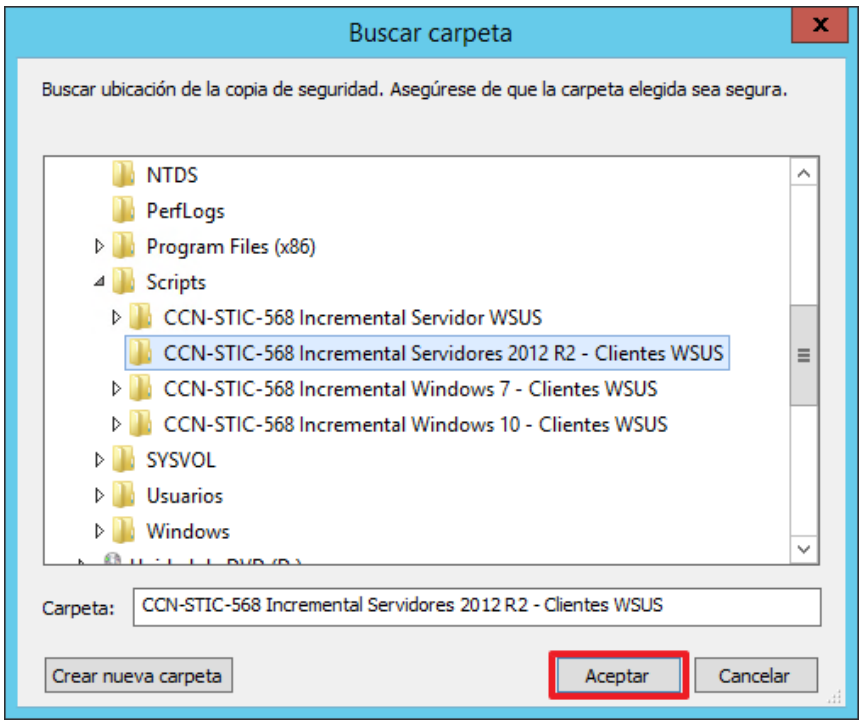
222.	En el "Asistente para importar configuración", pulse **"Siguiente >"** para continuar.
223.	Omita realizar copia de seguridad y pulse **"Siguiente >".**



Paso	Descripción
224.	Pulse en **"Examinar"**, sitúese en **"Este equipo > Disco local (C:) > Scripts"** y seleccione **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS".**

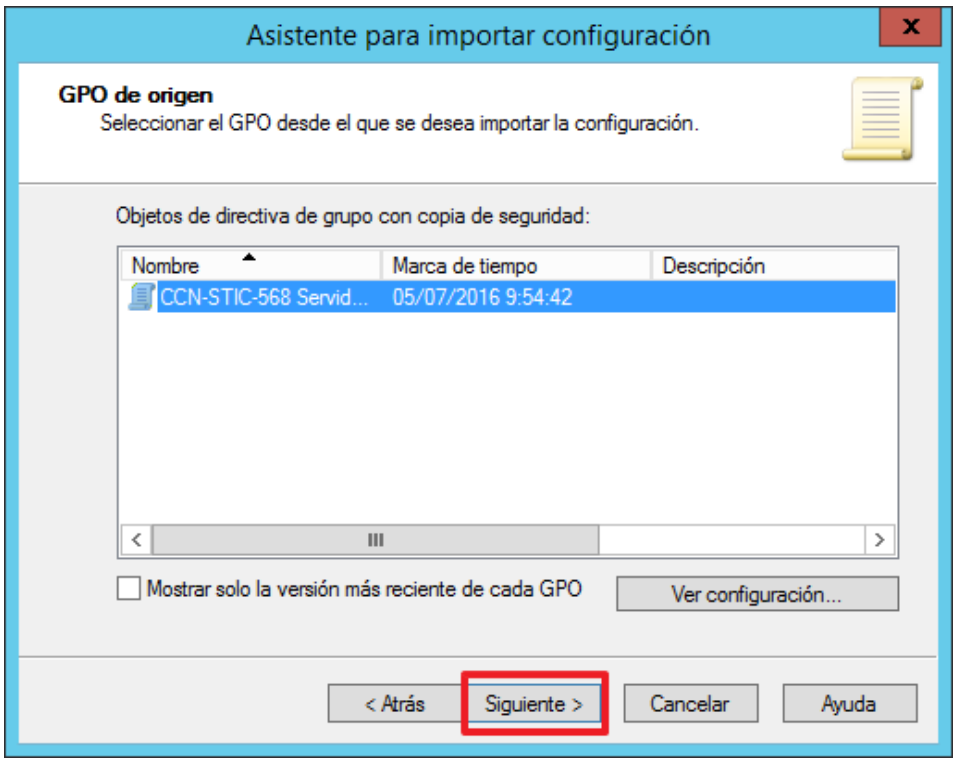


225.	Pulse **"Aceptar".**

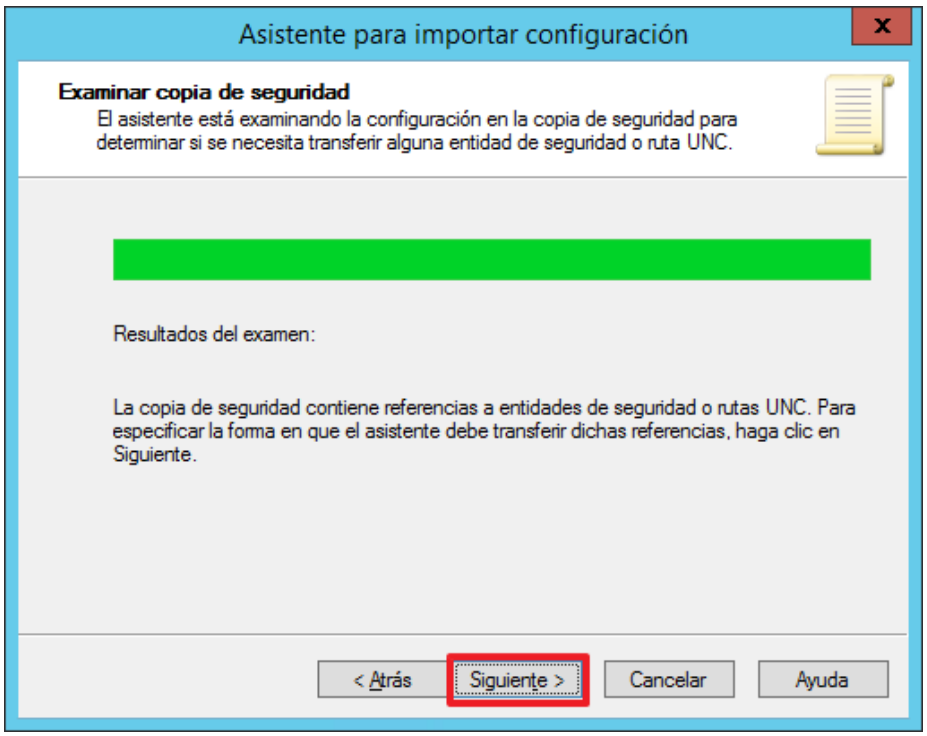


Pulse **"Siguiente >"** en el asistente para continuar.

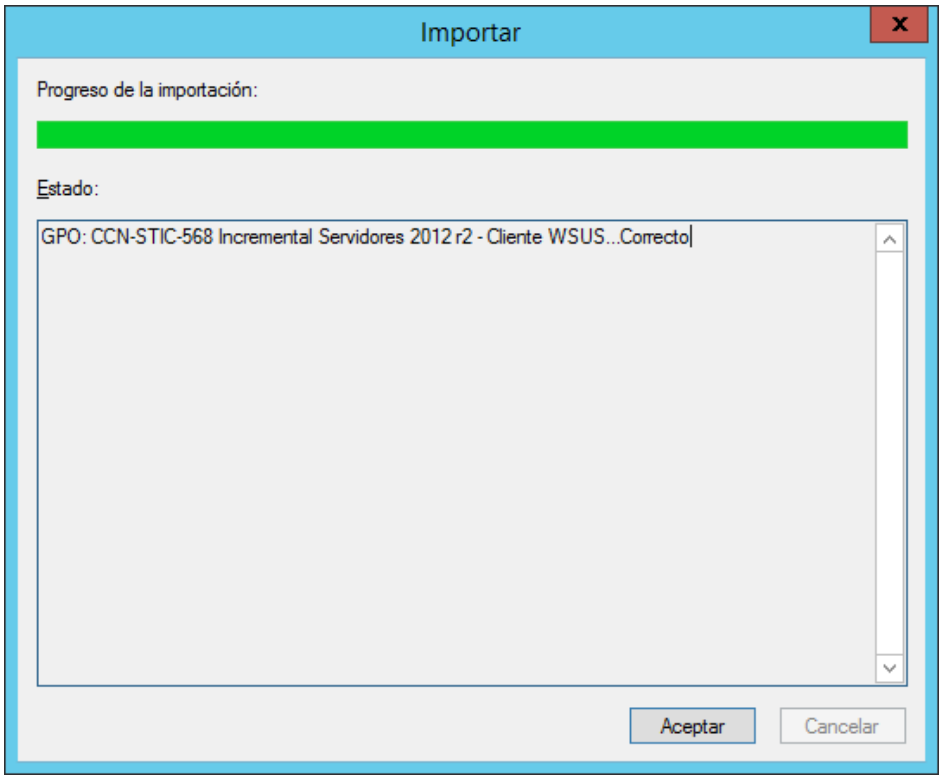
Paso	Descripción
226.	Pulse **"Siguiente >".**



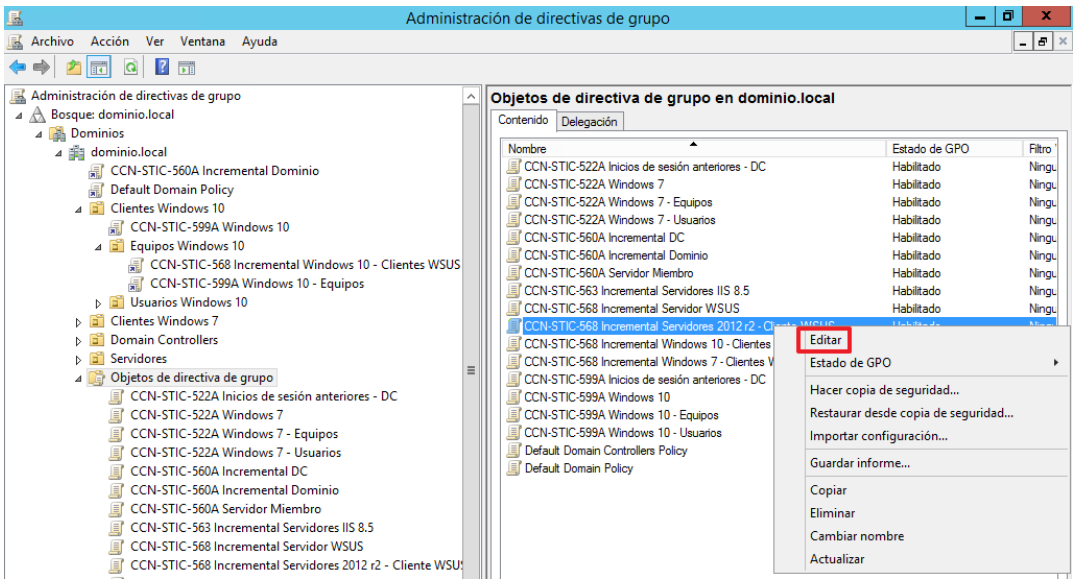
227.	Pulse **"Siguiente >"** en "Examinar copia de seguridad".



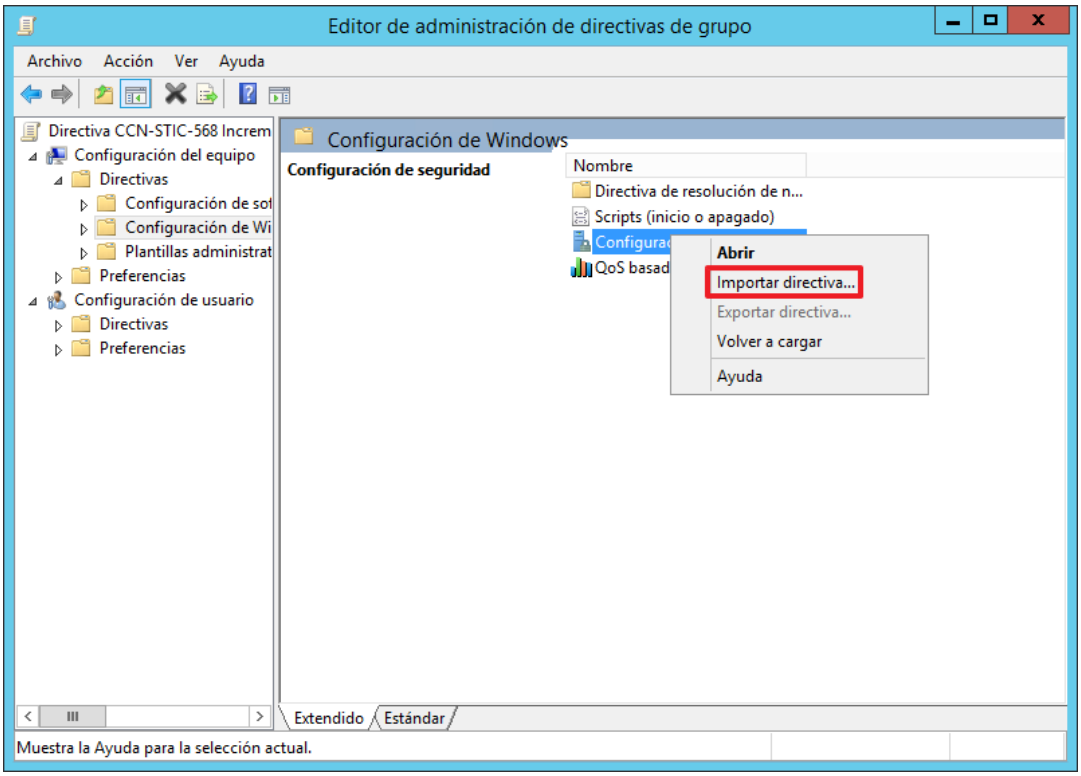
Paso	Descripción
228.	Pulse **"Finalizar"** para finalizar la importación de configuración de la GPO.
229.	Pulse en **"Aceptar"** para guardar los cambios.



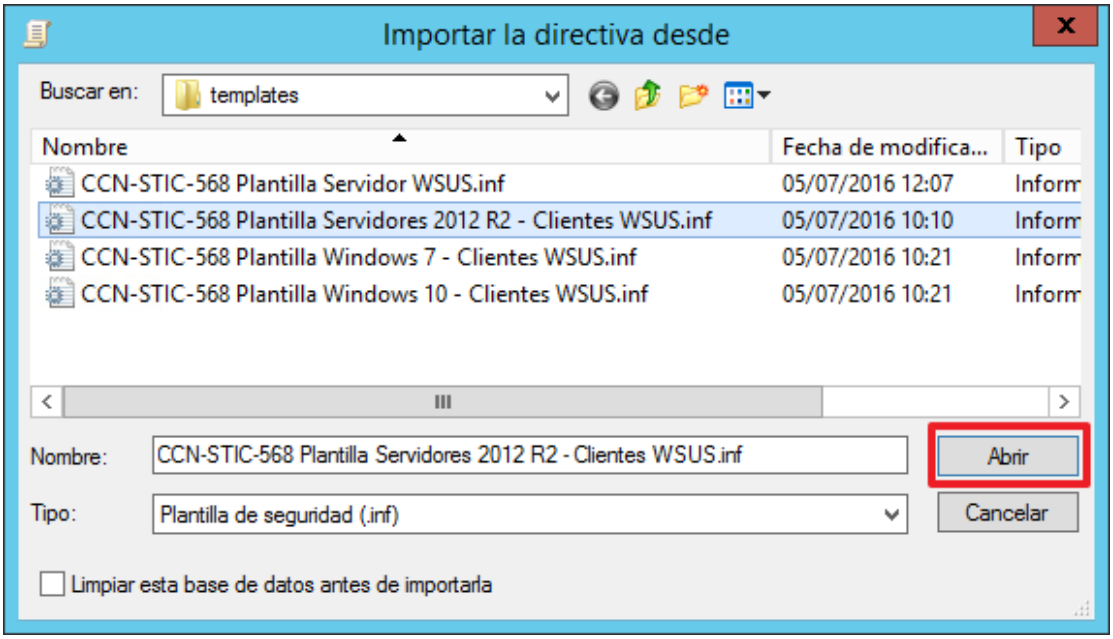
230.	Una vez importada la configuración, debe realizar una serie de configuraciones en la propia GPO. Para ello, sobre la política **"CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS"** pulse botón derecho y pinche sobre **"Editar".**



Paso	Descripción
231.	Sitúese en **"Configuración del equipo > Directivas > Configuración de seguridad"** y sobre esté, pulse con el botón derecho y seleccione **"Importar directiva…".**

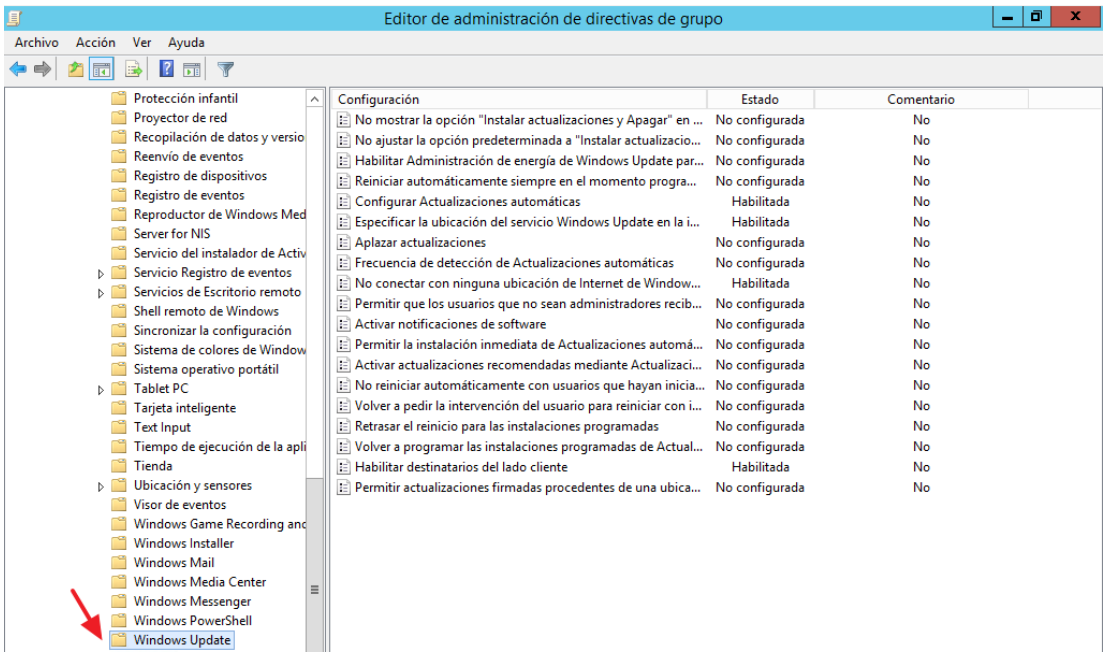


232.	Desde C:\Windows\Security\templates, seleccione **"CCN-STIC-568 Plantilla Windows 7 – Clientes WSUS.inf".**

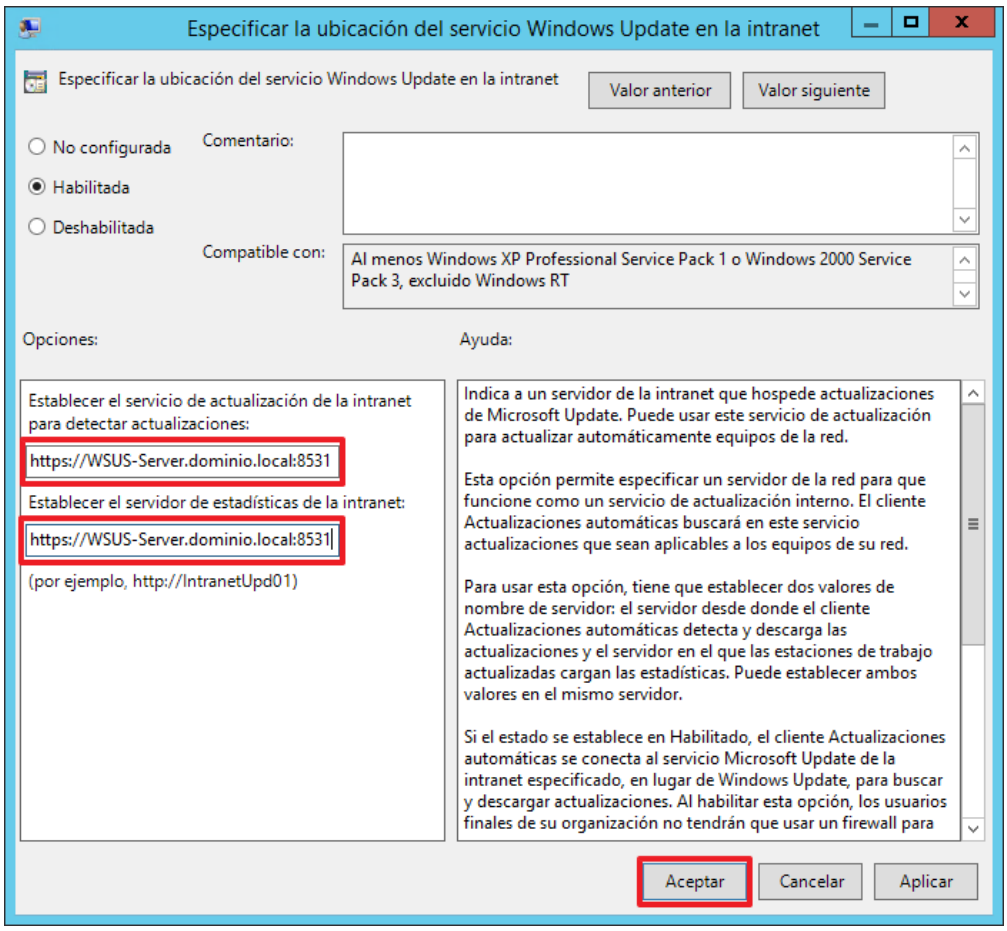


Pulse **"Abrir".**

Paso	Descripción
233.	Seguidamente, sitúese en **"Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows Update".**



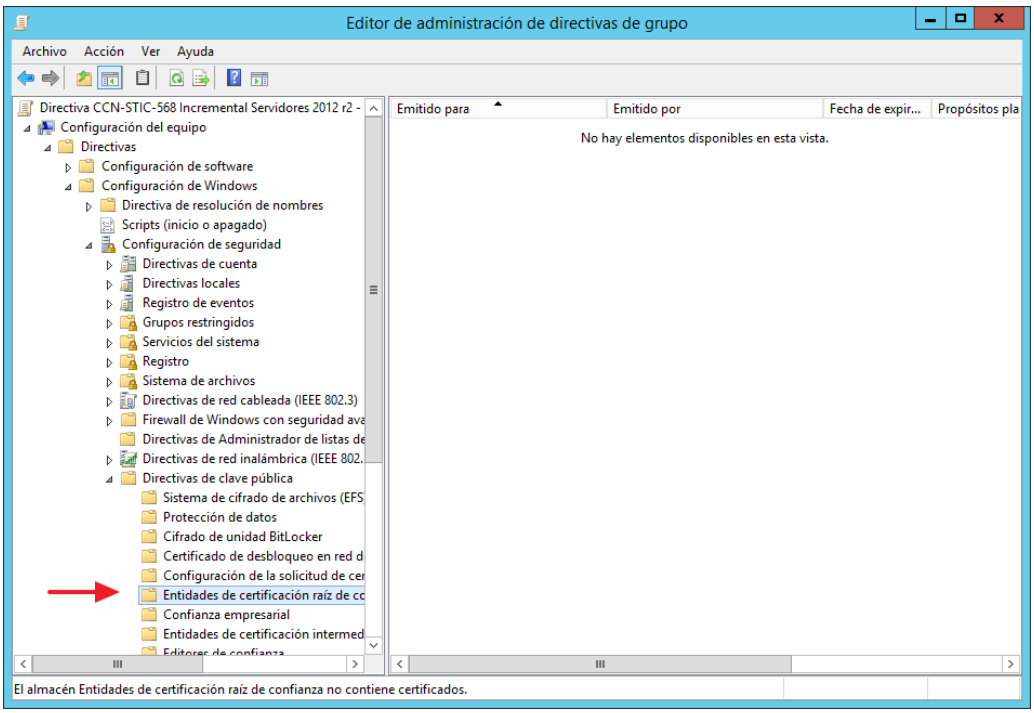
Paso	Descripción
234.	Haga doble clic sobre **"Especificar la ubicación del servicio Windows Update en la intranet"**, en la ventana opciones deberás introducir la ubicación del servidor WSUS. Tal y como se muestra en la siguiente imagen:



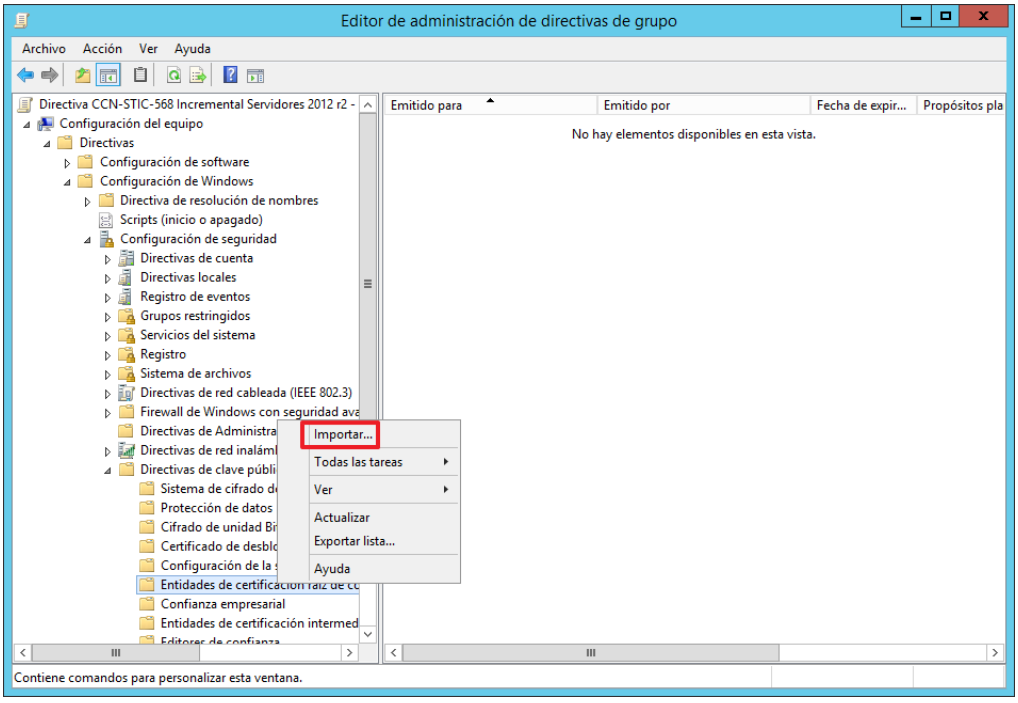
Pulse **"Aceptar"** para guardar los cambios.

Nota: Deberá introducir la dirección de su servidor WSUS (Nombre FQDN). Para este ejemplo se ha utilizado https://WSUS-Server.dominio.local:8531. Es muy importante tener en cuenta que debe introducir HTTPS y el puerto 8531, ya que la configuración SSL requiere de estos dos parámetros.

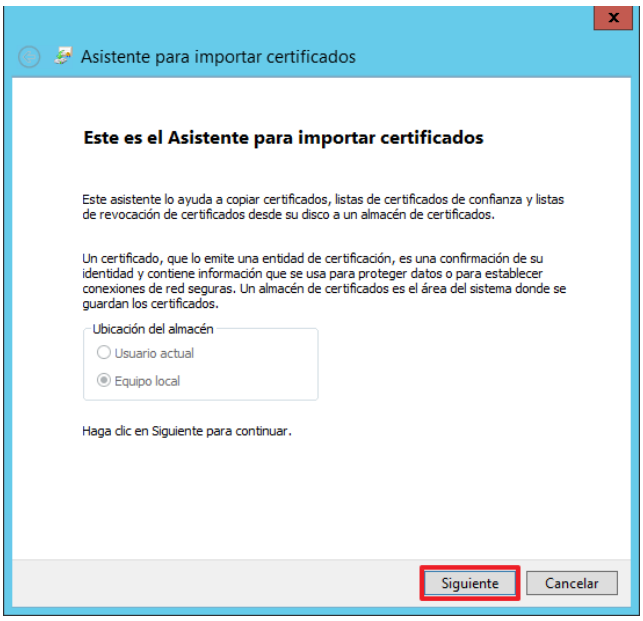
Paso	Descripción
235.	En el mismo "Editor de administración de directivas de grupo", diríjase a **"Configuración del equipo > Directivas > Configuración de seguridad > Directivas de clave pública > Entidades de certificación raíz de confianza".**



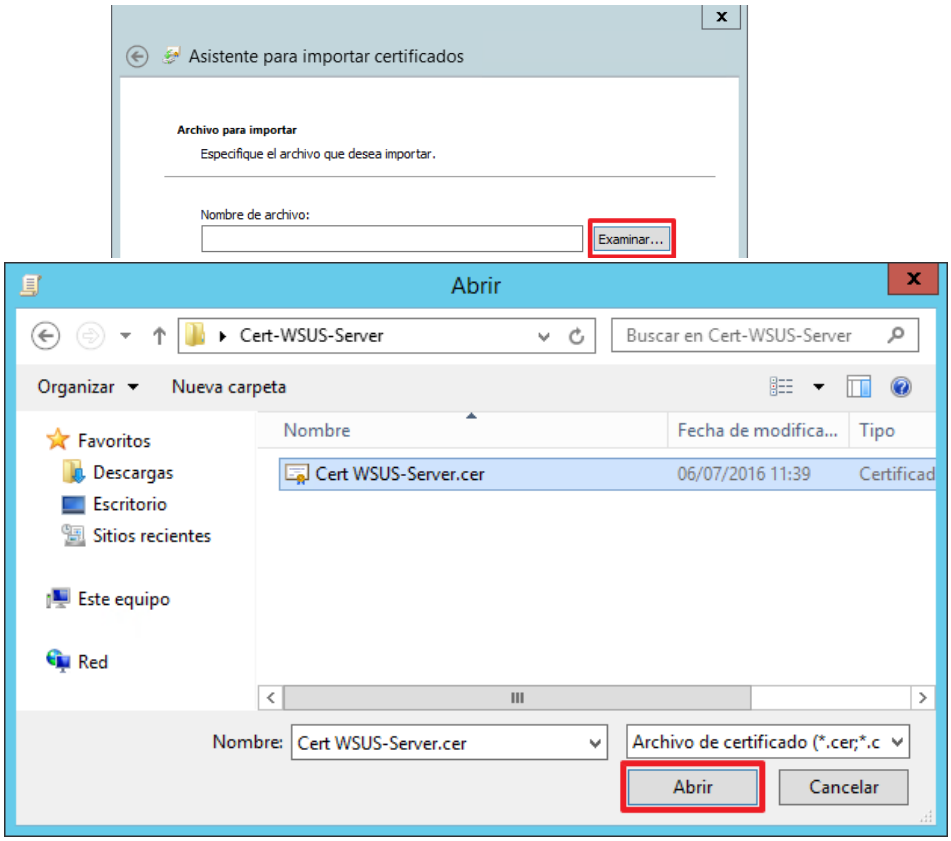
236.	Pulse sobre **"Entidades de certificación raíz de confianza"** con el botón derecho y seleccione **"Importar".**



Paso	Descripción
237.	Se abrirá el asistente para importar certificados, pulse **"Siguiente"** para continuar.

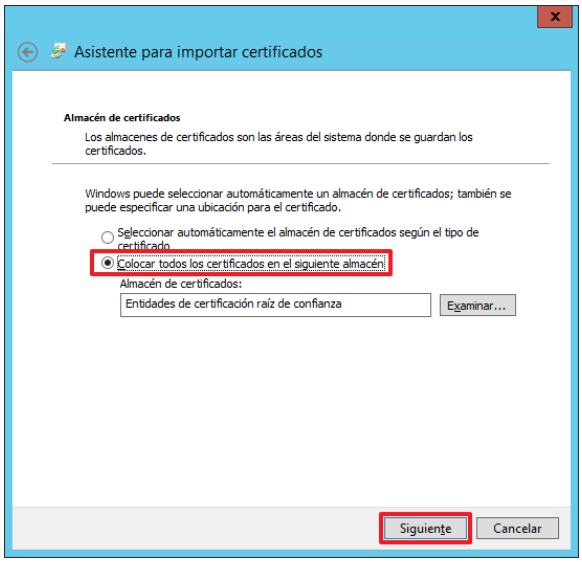
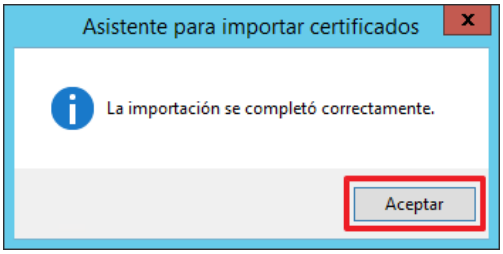


Paso	Descripción
238.	Pulse sobre el botón **"Examinar"** y localice el certificado exportado anteriormente. Selecciónelo y pulse **"Abrir".**

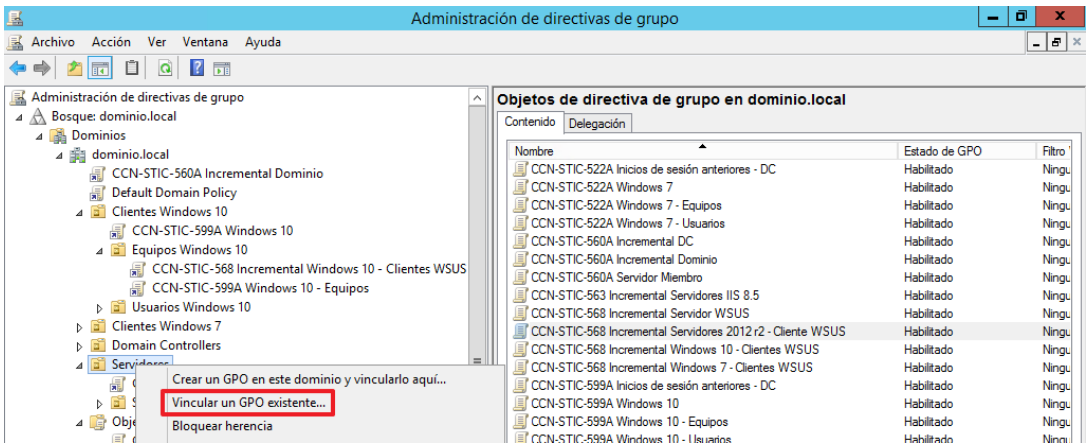


Pulse **"Siguiente"** para continuar.

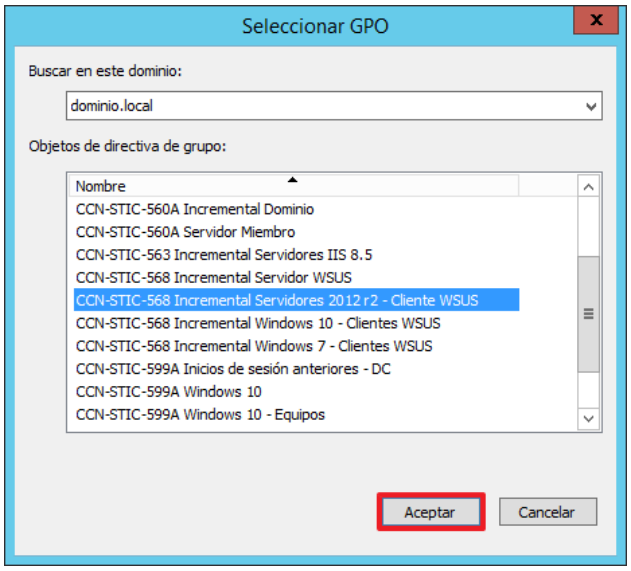
Nota: El certificado que debe importar es el mismo que ha exportado en el servidor WSUS, deberá encargarse de transportar el certificado hasta el servidor Controlador de Domino del dominio para poder enlazarlo con las GPO de los clientes WSUS.
Si no realiza esto no podrá importar el certificado y por supuesto no podrá enlazar los equipos clientes con el servidor de Windows Server Update Services.

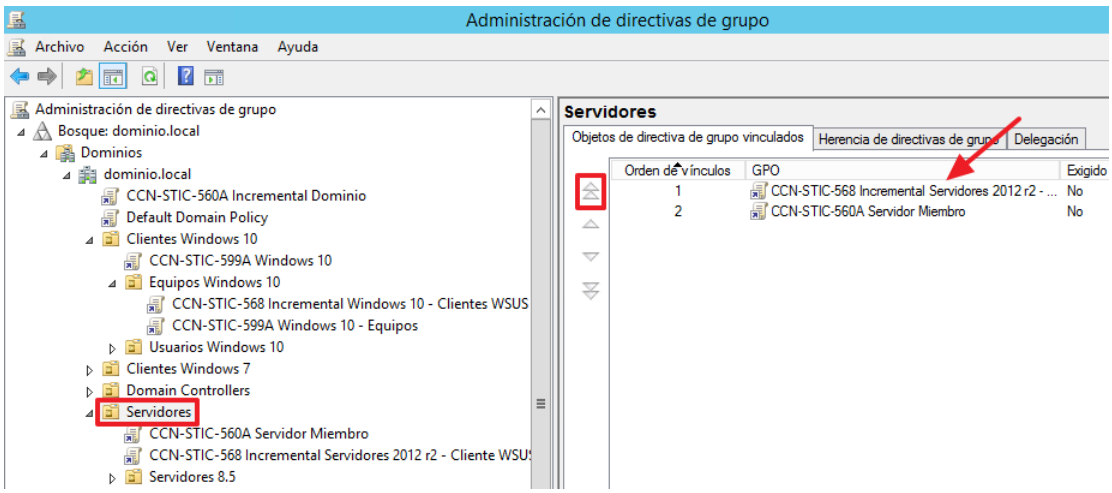
Paso	Descripción
239.	Deje seleccionado **“Colocar todos los certificados en el siguiente almacén”** como almacén de certificados.  Pulse **“Siguiente”** para continuar.
240.	Pulse **“Finalizar”** para terminar con la importación.
241.	El asistente le notificará que la importación se ha realizado correctamente. 
242.	Cierre el “Editor de administración de directivas de grupo”.

Paso	Descripción
243.	En la consola de "Administrador de directivas de grupo". En la parte de la izquierda, sobre **"<<Su dominio>> > Servidores"** pinche con el botón derecho y seleccione **"Vincular una GPO existente..."**.



244.	Seleccione la GPO **"CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS"** y pulse **"Aceptar"**.

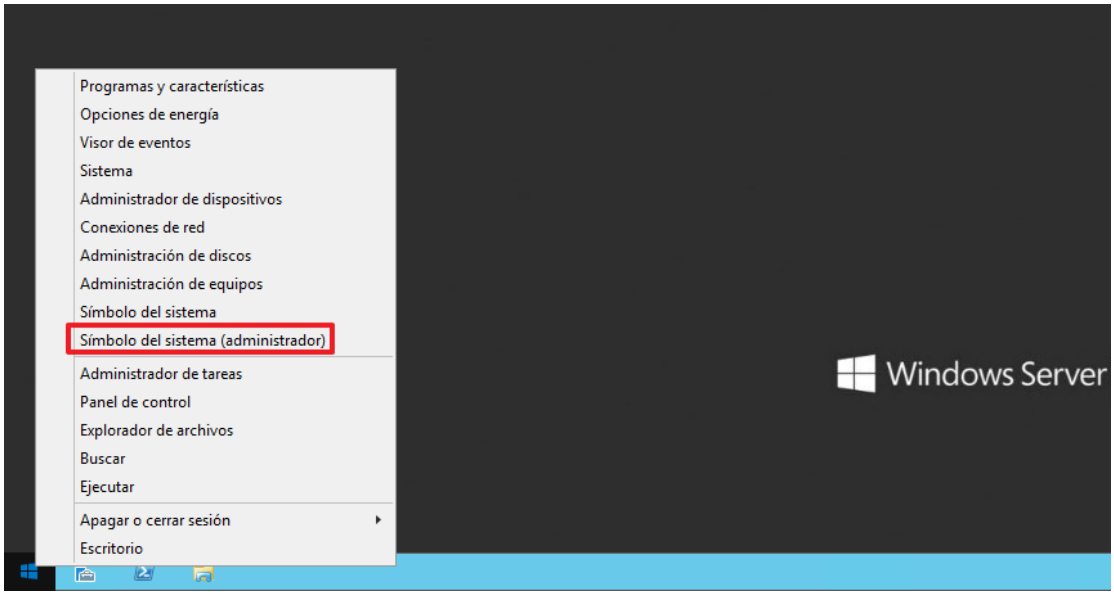


Paso	Descripción
245.	Seleccione la unidad organizativa **"Servidores"**, situada en **"<<Su dominio>> > Servidores"** y en la parte de la derecha, establezca la GPO **"CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS"** en la posición 1. 

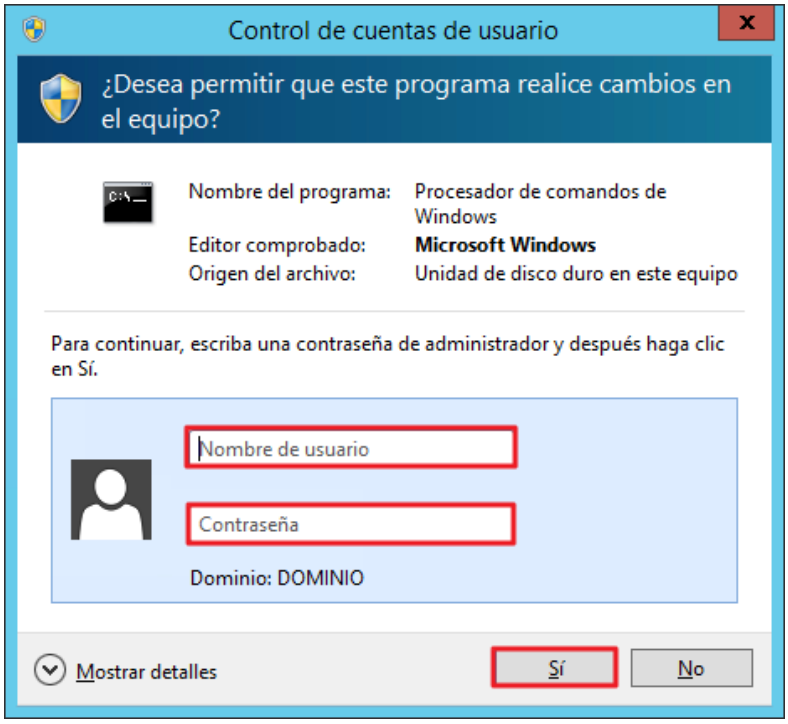
Una vez que ha realizado los pasos anteriores, ya estaría todo preparado para que Windows Server Update Services pueda detectar los equipos clientes Windows Server 2012 r2 que disponga en su infraestructura.

Paso	Descripción
246.	Inicie sesión en el equipo cliente Windows Server 2012 r2 con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
247.	Ejecute un **"Símbolo de sistema",** para ello pinche con el botón derecho sobre el **"Inicio"** y seleccione **"Símbolo del sistema (administrador)".**

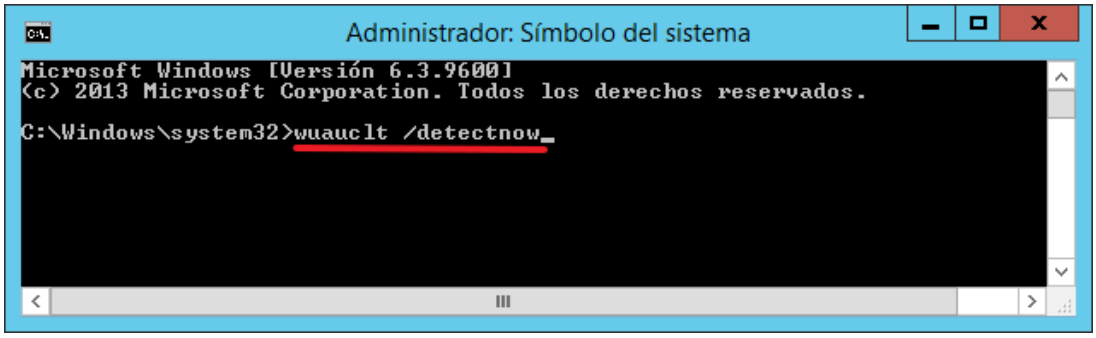


248.	El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.



Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
249.	Escriba el siguiente comando: **wuauclt /detectnow** y pulse **Intro.**



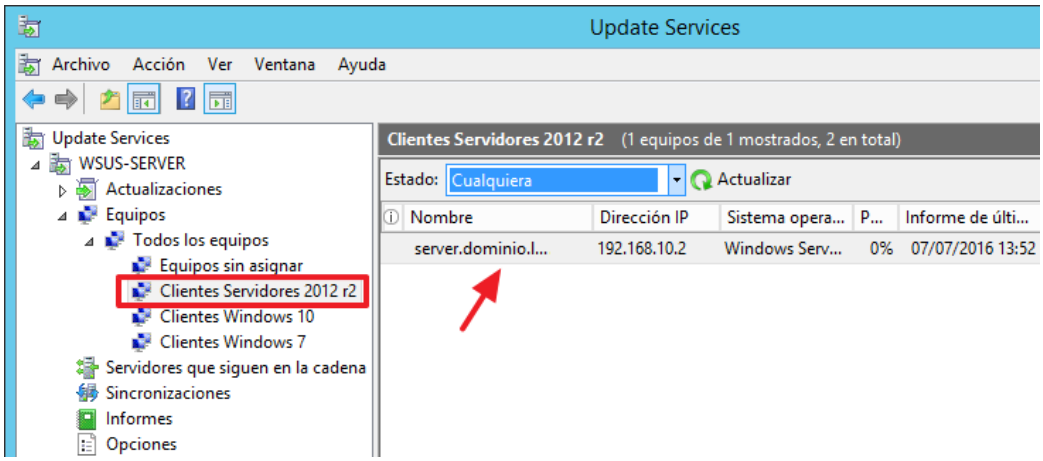
Una vez hecho esto, el servidor Windows Server Update Services ya tendrá en cuenta el equipo Windows Server 2012 r2 que se acaba de enlazar. Siga los siguientes puntos para comprobar que la consola de WSUS es capaz de ver el equipo enlazado.

Paso	Descripción
250.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio.

Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

251.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.

Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo, se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
252.	En la consola **"Update Services",** diríjase al grupo creado que pertenece a los equipos clientes de Windows Server 2012 r2. Si todo ha salido correctamente deberá encontrarse el equipo enlazado anteriormente. En la ventana central de la consola, debe situar la pestaña **"Estado"** en **"Cualquiera"** para que aparezca el equipo.  **Nota:** El tiempo que tarda WSUS en detectar en el equipo cliente una vez ejecutado el comando "wuauclt /detectnow", puede ser de varios minutos, esto dependerá de la velocidad de su red. Si después de un tiempo el equipo cliente no ha sido detectado por el servidor WSUS, vuelva a repasar los pasos anteriores para corroborar que ha realizado todos los pasos adecuadamente.

ANEXO G. TAREAS ADMINISTRATIVAS EN EL SERVIDOR RAÍZ DE WINDOWS SERVER UPDATE SERVICES

Este anexo se ha diseñado para ayudar a los operadores a administrar adecuadamente los servidores Windows Server Update Services implementados mediante esta guía de seguridad. La configuración de grupos de equipos, almacenamiento e importación de las actualizaciones en el servidor WSUS, gestión de las propias actualizaciones una vez importadas en el servidor, aprobación y rechazo de estás.

Para poder realizar estas tareas es necesario disponer del servidor Windows Server Update Services instalado correctamente siguiendo los pasos indicados en el Anexo F de esta misma guía.

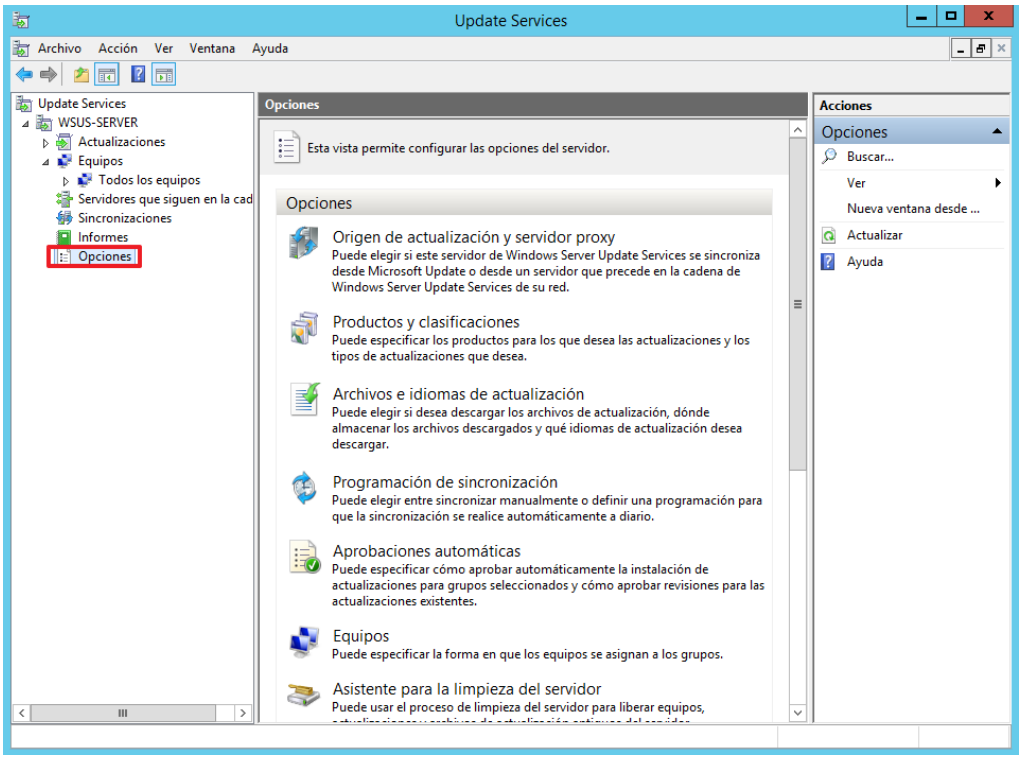
1. CONFIGURACIÓN Y ADMINISTRACIÓN DE WINDOWS SERVER UPDATE SERVICES

En el presente punto se describirán algunas tareas de configuración que son necesarias para proporcionar un funcionamiento adecuado al servidor Windows Server Update Services.

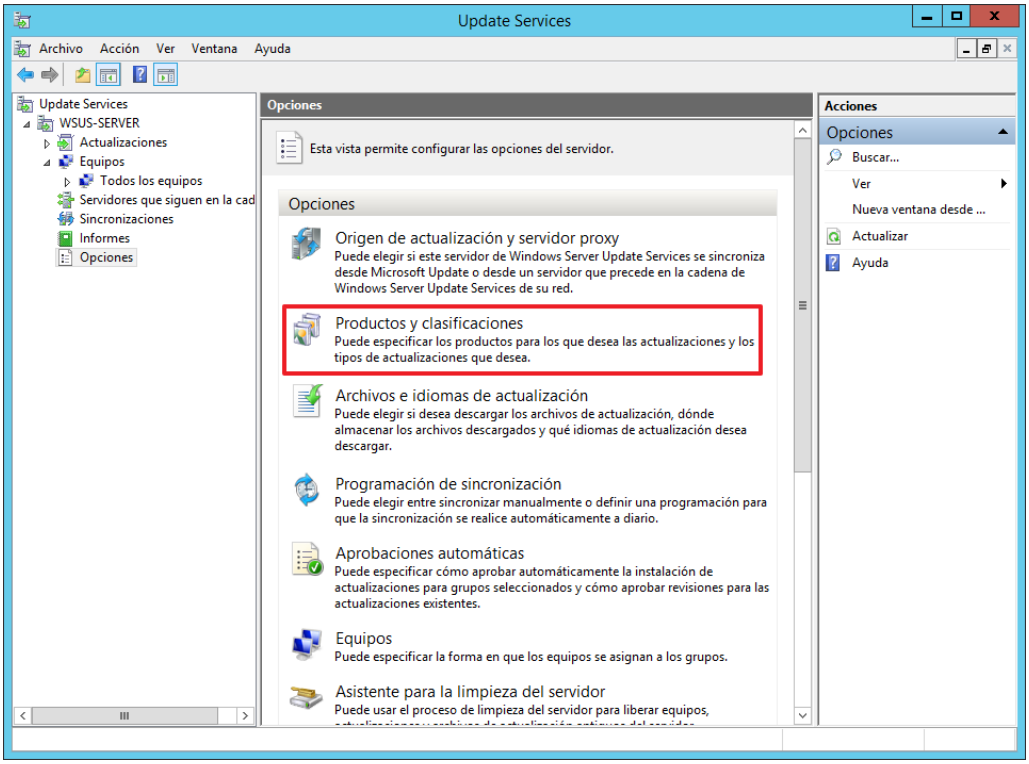
Paso	Descripción
1.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
2.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor>Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción

3. Dentro de la consola **"Update Services"**, en la parte de la izquierda, pinche en **"Opciones"**.



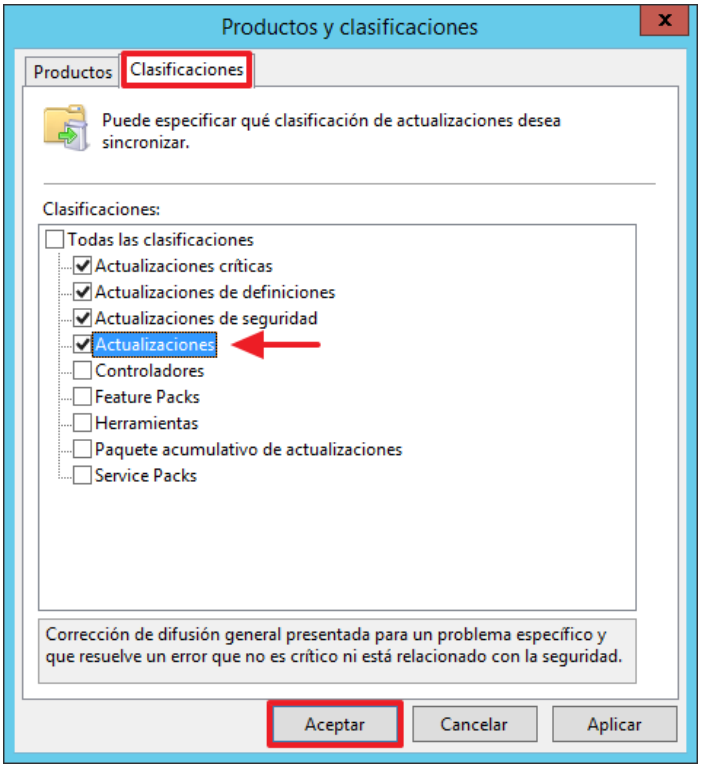
4. Seleccione **"Productos y clasificaciones".**



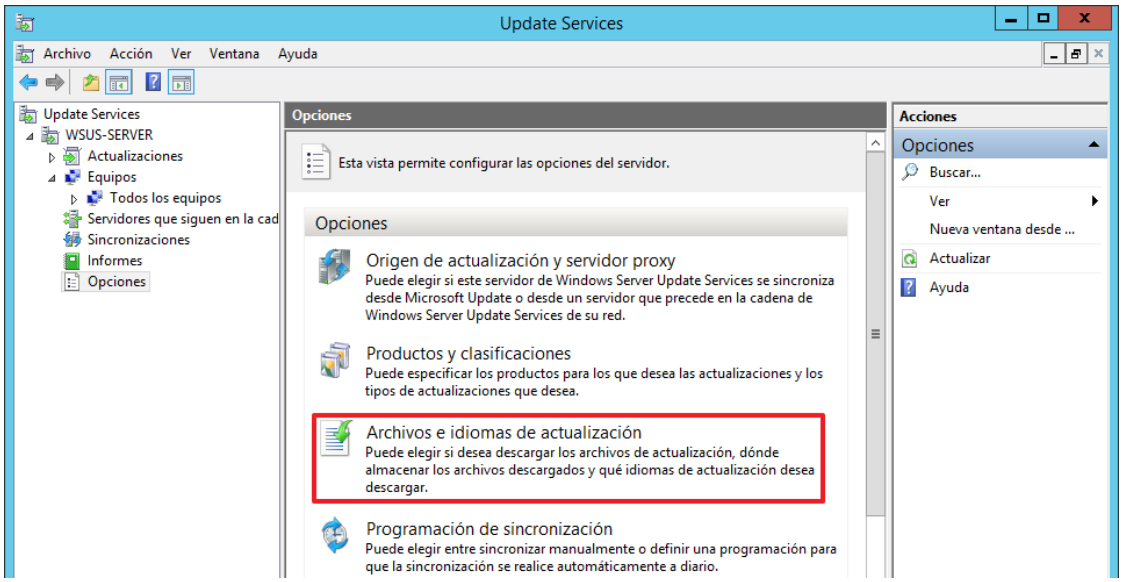
Paso	Descripción
5.	Se abrirá una ventana donde dispondrá de dos pestañas una de **"Productos"** y otra de **"Clasificaciones",** ubíquese en la pestaña **"Clasificaciones".**

Nota: Omita la configuración de la pestaña "Productos", ya que esta configuración se deberá realizar en el servidor WSUS que está destinado a realizar la descarga de actualizaciones. (Revise el **Anexo E. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR DE DESCARGAS DE ACTUALIZACIONES DE MICROSOFT UPDATE.**)

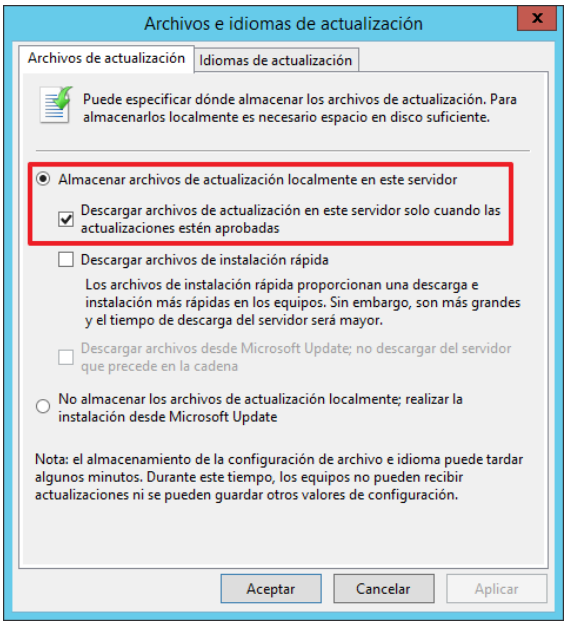
Marque la casilla "**Actualizaciones**". Pulse "**Aceptar**" para guardar los cambios.

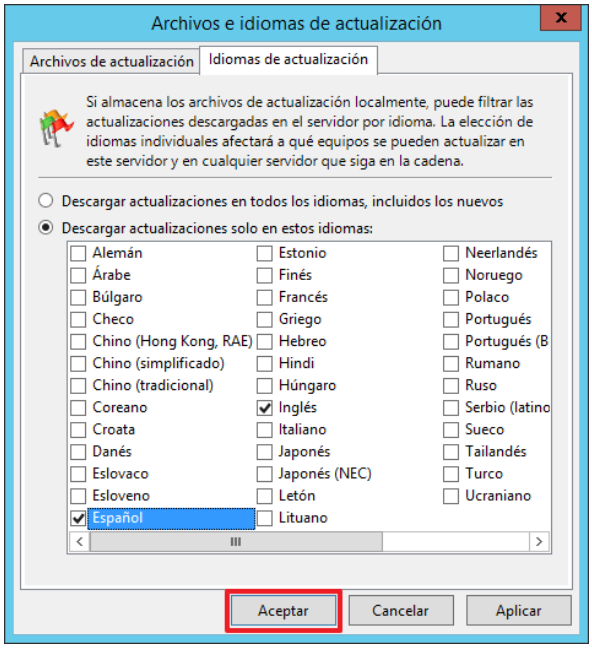


Paso	Descripción
6.	Manténgase en **“Opciones”,** y piche sobre **“Archivos e idiomas de actualización”.**

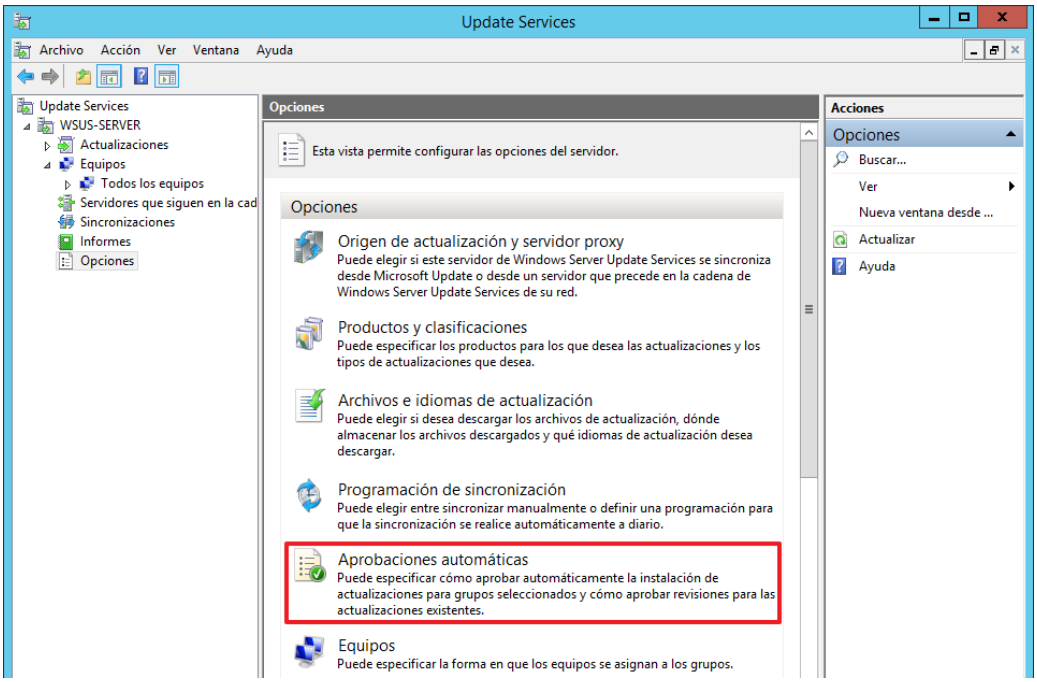


7.	En la ventana de “Archivos e idiomas de actualización”, seleccione primero la pestaña **“Archivos de actualización”.** Asegúrese de que se encuentra marcada la opción **“Almacenar archivos de actualizaciones localmente en este servidor > Descargar archivos de actualización en este servidor…”**.

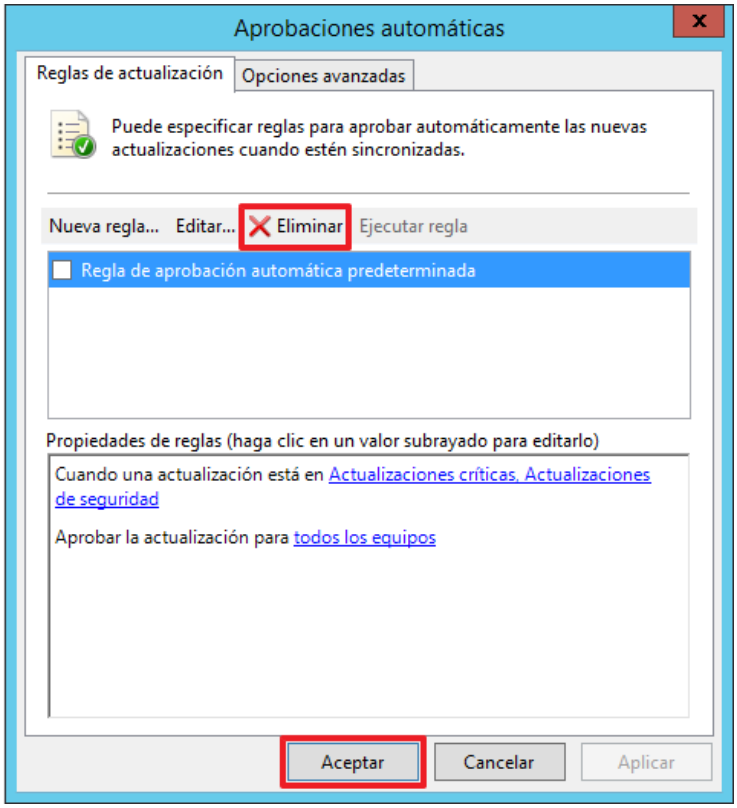


Paso	Descripción
8.	Continúe con la pestaña “Idiomas de actualización”. Seleccione **“Descargar actualizaciones solo en estos idiomas:”**. Pulse **“Aceptar”** en la ventana de advertencia. Seleccione **“Español”** y **“Inglés”.**  **Nota:** Para este ejemplo, se han seleccionado el idioma Español e Inglés, tenga en cuenta que esta configuración debe de ser idéntica a la que se encuentre en el servidor de descarga de actualizaciones, ya que, si esto no es así, podrá tener conflictos con las actualizaciones. Pulse **“Aceptar”** para guardar los cambios.

Paso	Descripción
9.	Entre en **“Aprobaciones automáticas”.**



Paso	Descripción
10.	En la pestaña **"Regla de actualización",** seleccione la regla predeterminada que ya existe y pulse sobre **"Eliminar".**



Pulse **"Aceptar"** para guardar los cambios.

2. CREACIÓN Y ADMINISTRACIÓN DE GRUPOS DE EQUIPOS

A continuación, se detalla cómo gestionar correctamente los grupos de equipos en el servidor Windows Server Update Services. Es conveniente tener una organización correcta de los equipos asociados al servidor, ya que esto ayudará a tener un control a la hora de aplicar las actualizaciones más organizadamente sobre los equipos clientes.

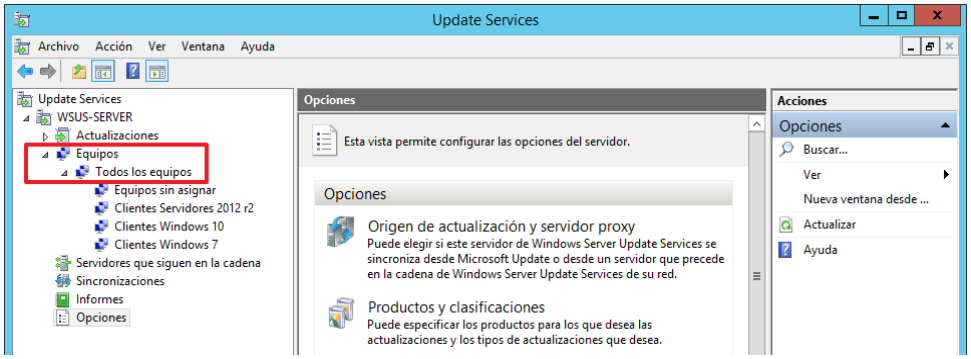
Además, gracias a la creación de grupos, podrá crear grupos de control a los que aplicar las actualizaciones antes de aplicarlas al resto de equipos de su organización y así evitar cualquier trastorno que puedan sufrir los equipos clientes.

Paso	Descripción
11.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio.
	Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

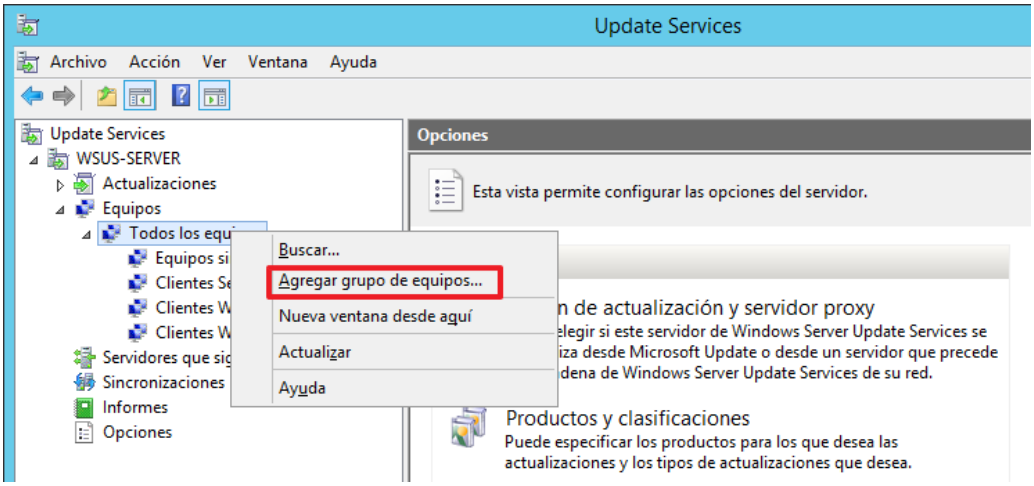
Paso	Descripción
12.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor>Herramientas > Windows Server Update Services"**.

Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

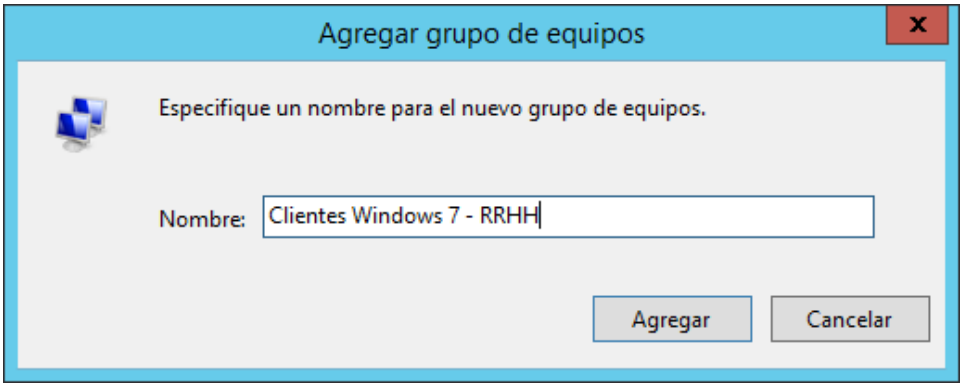
13.	Dentro de la consola **"Update Services",** despliegue la pestaña **"Equipos > Todos los equipos"** que se encuentra en la parte izquierda.



Paso	Descripción
14.	Para crear un grupo de equipos, pulse con el botón derecho sobre **"Todos los equipos"** y seleccione **"Agregar grupo de equipos…"**.

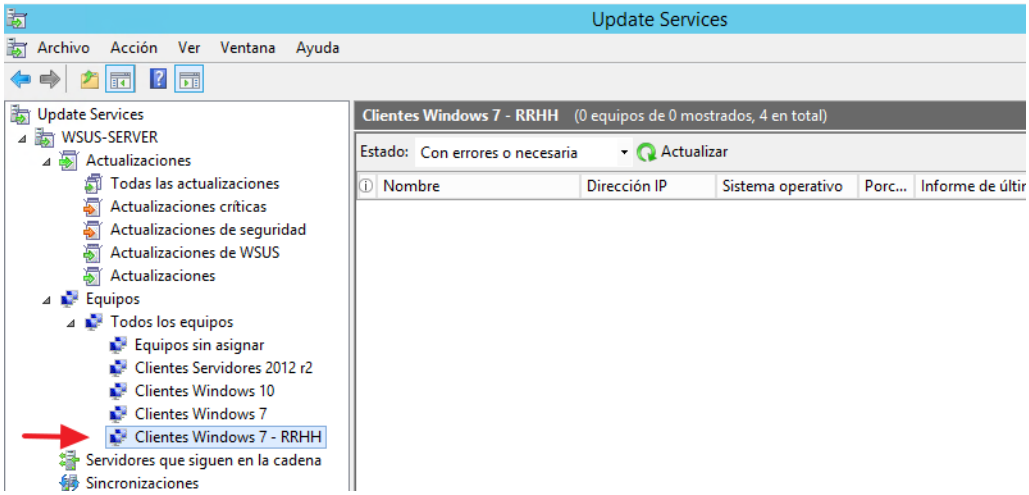


15.	Introduzca el nombre que quiera asignar al grupo que va a crear, a continuación **"Agregar".**

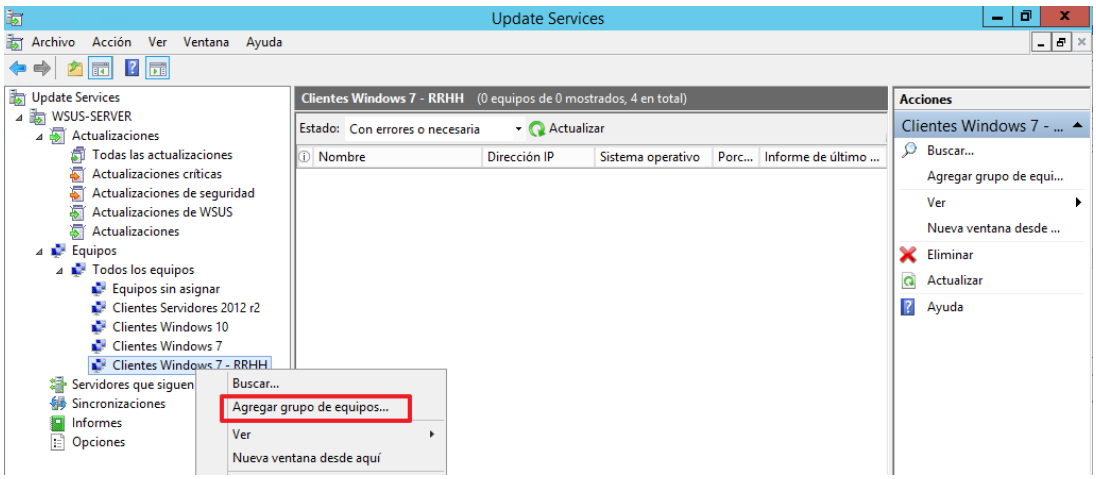


Nota: Para este ejemplo, se nombra el grupo como "Clientes Windows 7 - RRHH". Usted deberá asignar el que más se adecue a sus necesidades.

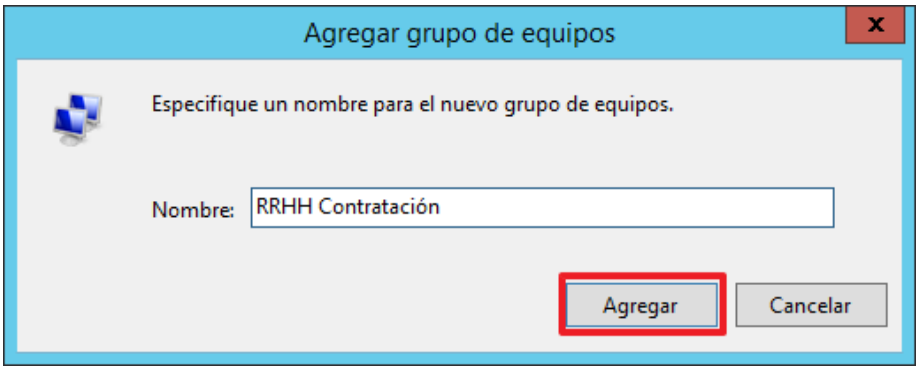
Paso	Descripción
16.	Observe que el grupo creado recientemente se agregó a la pestaña **"Todos los equipos"** en la consola **"Update Services".**



17.	Podrá crear grupos dentro de grupos ya creados, seleccione el grupo **"Clientes Windows 7 - RRHH"** y pulse sobre él, con el botón derecho, seleccione **"Agregar grupo de equipos…"**

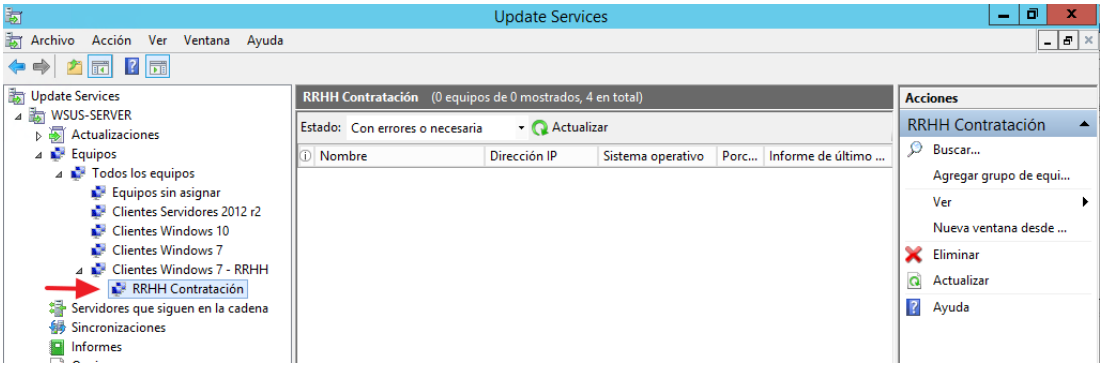


Paso	Descripción
18.	Introduzca un nombre para el grupo.



Nota: Para este ejemplo, se nombra el grupo como "RRHH Contratación". Usted deberá asignar el que más se adecue a sus necesidades.
No podrá asignar un nombre a un nuevo grupo que ya exista en la consola de "Update Service".

19.	Observe que el grupo creado recientemente se agregó a la pestaña **"Todos los equipos > Clientes Windows 7 – RRHH > RRHH Contratación"** en la consola **"Update Services".**

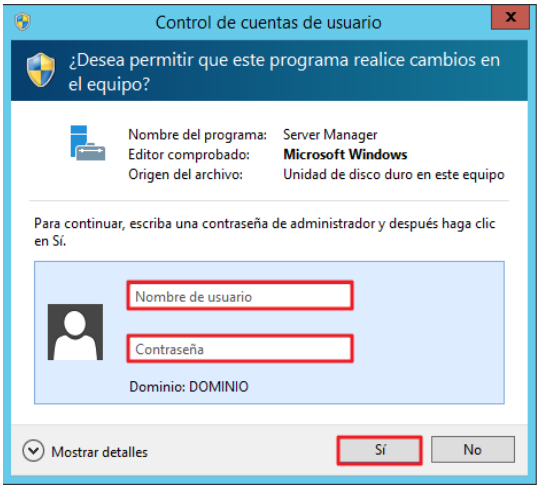


Podrá reubicar los equipos clientes enlazados con el servidor Windows Server Update Services desde la propia GPO que aplica a los diferentes clientes que existan en su infraestructura. Únicamente cambiando la configuración de la GPO podrá reubicar a que grupo de equipos deben pertenecer dichos equipos.

Los pasos que se describen a continuación, se realizarán en un Controlador de Dominio del dominio donde se realizará la implementación del servidor de actualizaciones. El paso que se describe a continuación, aplica igual para todos los equipos clientes de su infraestructura, solo tendrá que tener en cuenta la GPO correspondiente que aplique.

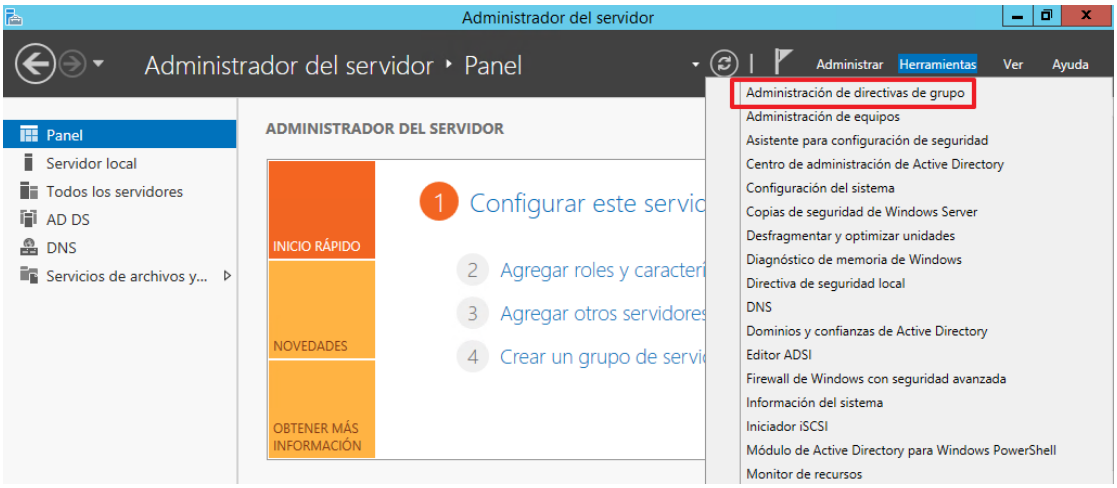
Paso	Descripción
20.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.
21.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
22.	Inicie el "Administrador del servidor" desde **"Inicio > Administrador del Servidor"**. El control de cuentas de usuario le solicitará las credenciales de un administrador del dominio.



Nota: En este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

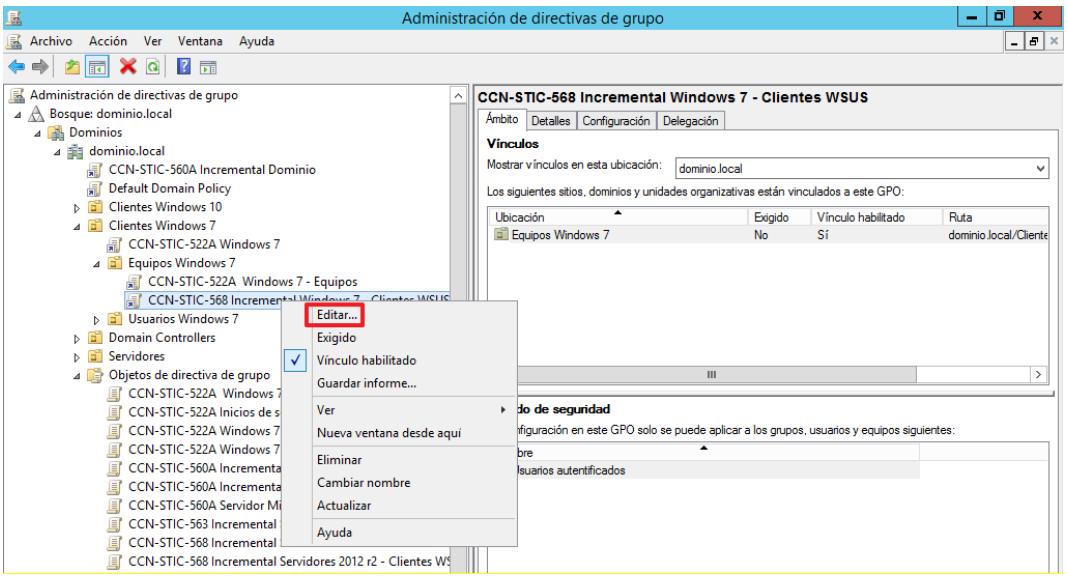
23.	Ejecute la consola de Administración de directivas de grupo desde el menú **"Inicio > Administrador del servidor > Herramientas > Administración de directivas de grupo".**



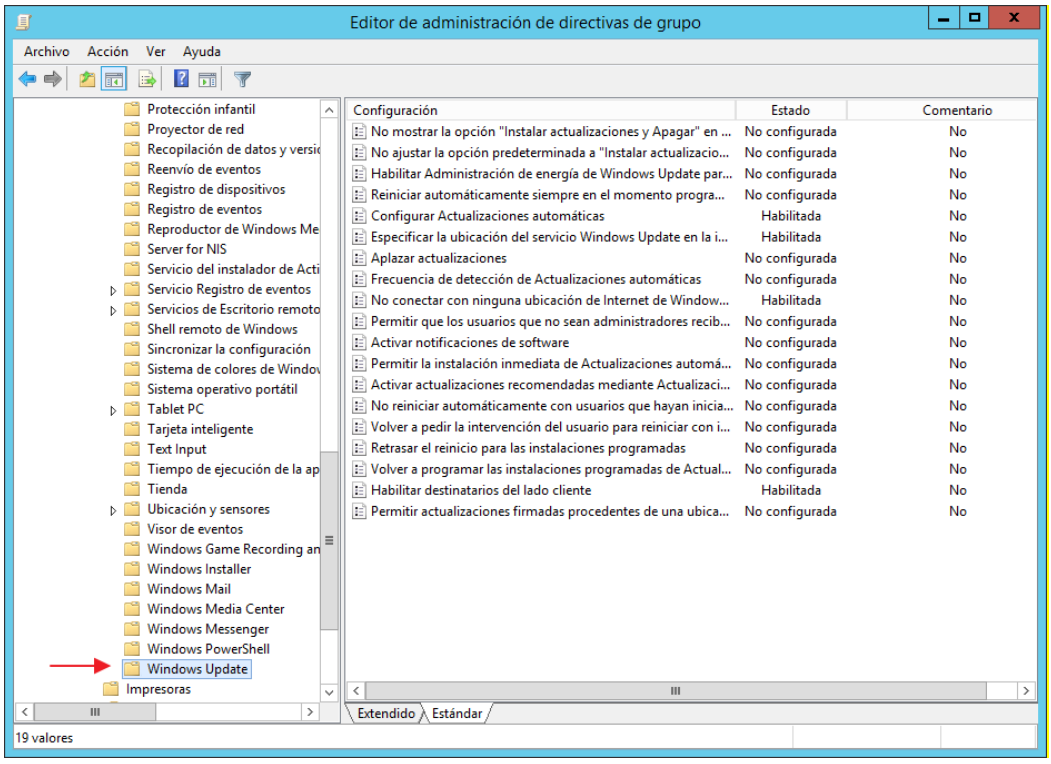
Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción

24. Diríjase a la unidad organizativa de **"Equipos Windows 7",** situada en **"<<Su dominio>> > Clientes Windows 7 > Equipos Windows 7".** Seleccione la unidad organizativa **"CCN-STIC-568 Incremental Windows 7 – Clientes WSUS",** pulse con el botón derecho y seleccione **"Editar".**

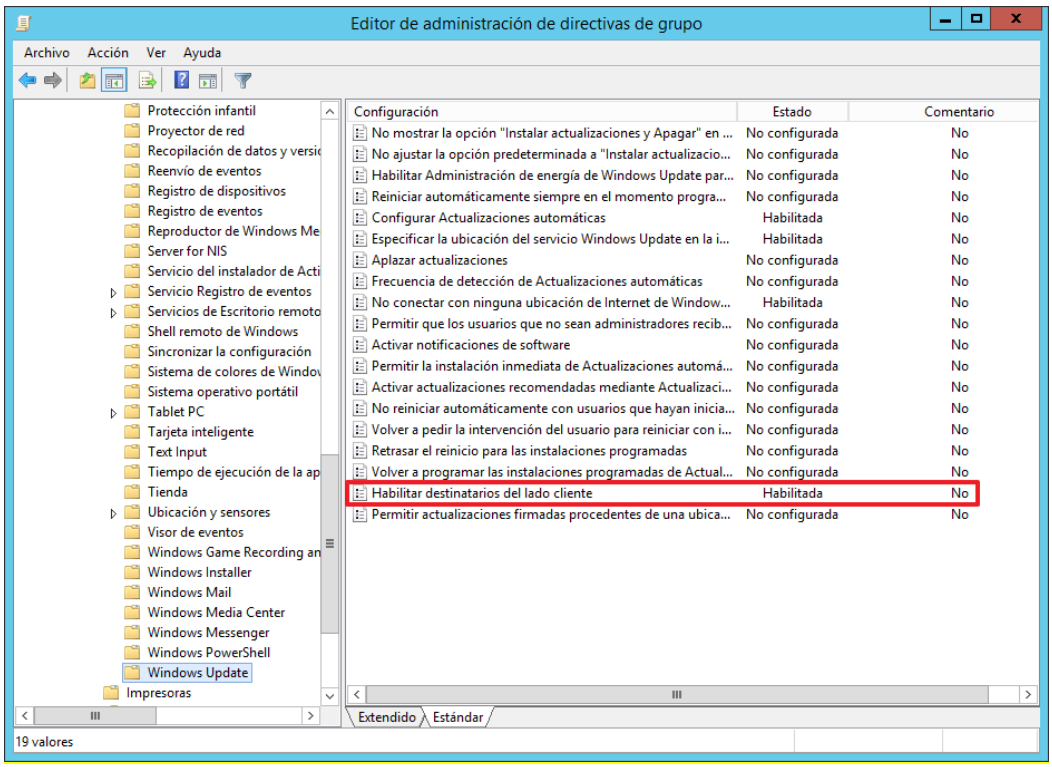


25. Dentro del "Editor de administración de directivas de grupo", sitúese en **"Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows Update"**

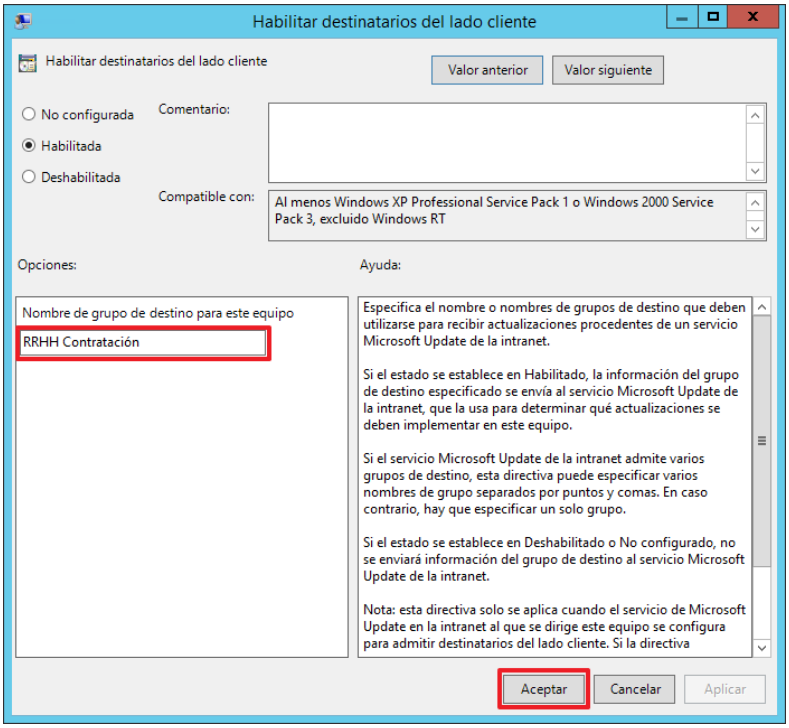


Paso	Descripción

26. Haga doble clic sobre la directiva “**Habilitar destinatarios del lado cliente”.**



27. Indique el nombre del grupo donde quiera reubicar el equipo o los equipos clientes.



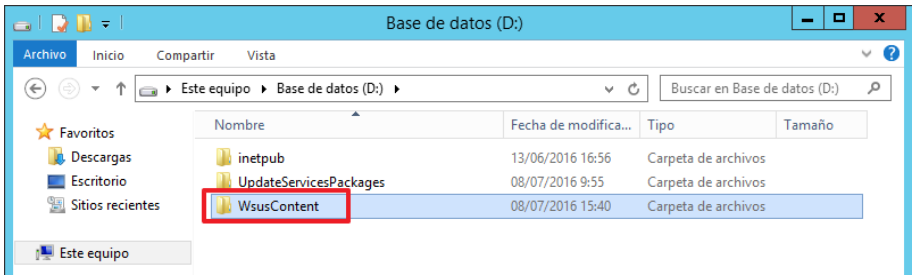
Pulse **“Aceptar”** para guardar los cambios.

3. ALMACENAMIENTO E IMPORTACIÓN DE ACTUALIZACIONES

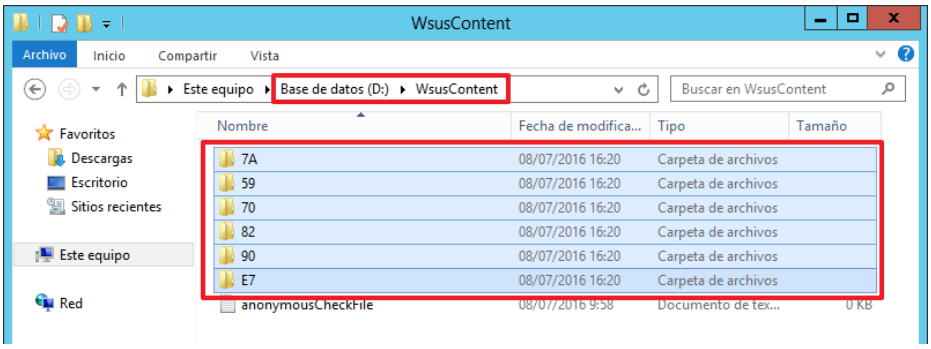
En el presente punto se detalla cómo integrar las actualizaciones descargadas por el servidor Windows Server Update Services, que se encuentra fuera de su red de dominio. Se trata de realizar una importación de todos los paquetes de actualizaciones en el servidor Windows Server Update Service Offline y almacenarlas en la base de datos adecuada y destinada para este fin.

Se detallarán dos tareas fundamentales para realizar este proceso, una será el volcado de los paquetes de actualizaciones y otra la importación de los metadatos necesarios para que el servidor WSUS interprete todos estos paquetes de actualizaciones almacenados en la base de datos.

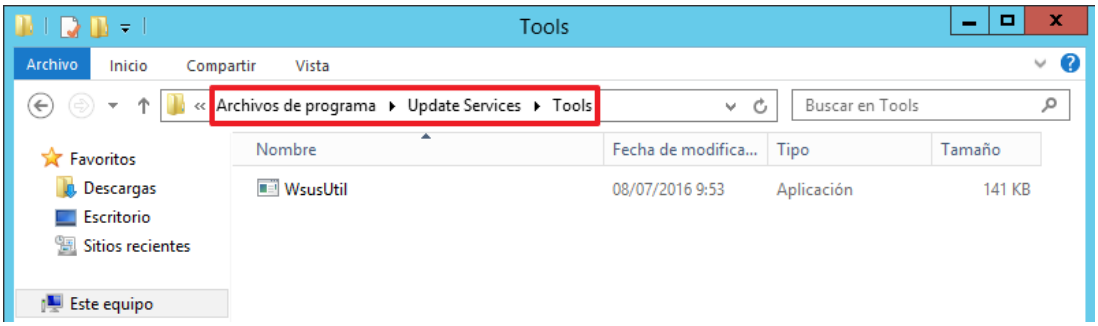
Nota: Recuerde que antes de introducir las actualizaciones descargadas de internet en sistemas de red clasificada, el dispositivo de almacenamiento que utilice para introducir éstas en la red, deberá pasar el análisis por el sistema de aduana con el que cuente su organización.
Para realizar este apartado, deberá tener las actualizaciones descargadas y los metadatos generados por el comando "WsusUtil.exe Export", deberá tener ambas cosas ubicadas en un almacenamiento externo disponible para poder copiar los paquetes de actualizaciones en el servidor Windows Server Update Service Offline.
Si no recuerda adecuadamente el proceso de descarga de actualizaciones desde el servidor Windows Server Update Services que se encuentra fuera de su red de dominio, visite el **ANEXO E. 3. DESCARGA Y EXPORTACIÓN DE ACTUALIZACIONES DESDE WINDOWS SERVER UPDATE SERVICES.**

Paso	Descripción
28.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
29.	Diríjase a la **unidad D:** que tenga en su servidor Windows Server Update Services, dentro de la carpeta **"WsusContent",** copie todos los paquetes de actualizaciones de los que disponga. 

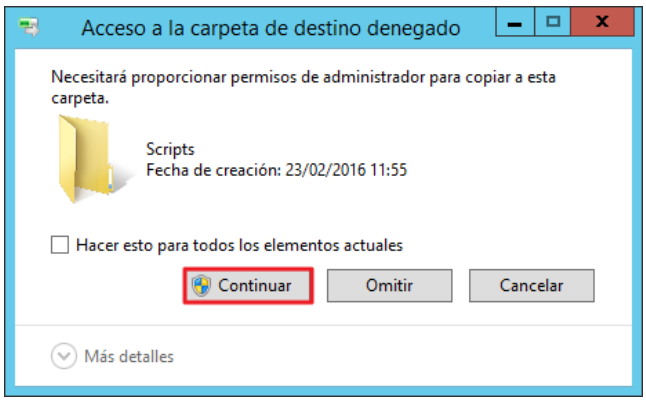
Paso	Descripción
30.	Dentro de la carpeta **"WsusContent"**, deben estar ubicados los paquetes de actualizaciones copiados anteriormente.



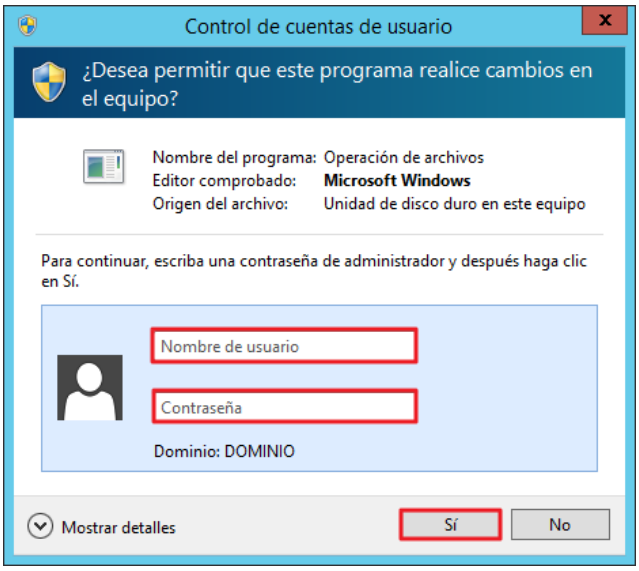
31.	Deberá copiar también los archivos **.cab** y **.log** generados en el proceso de exportación de estás actualizaciones. Deberá ubicarlos en **"C:\Archivos de programa\Update Service\Tools".**



Pulse **"Continuar".**

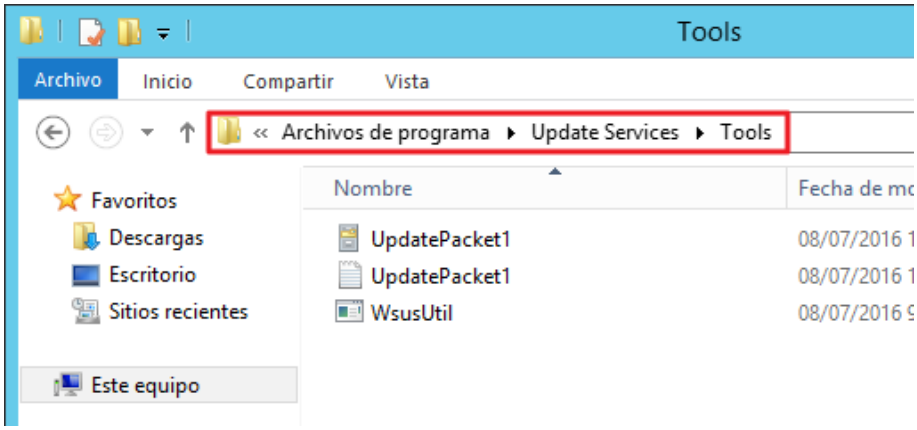


Paso	Descripción
32.	El **"control de cuentas de usuarios"** le pedirá elevación de privilegios, para ello ingrese una cuenta "administrador del dominio".

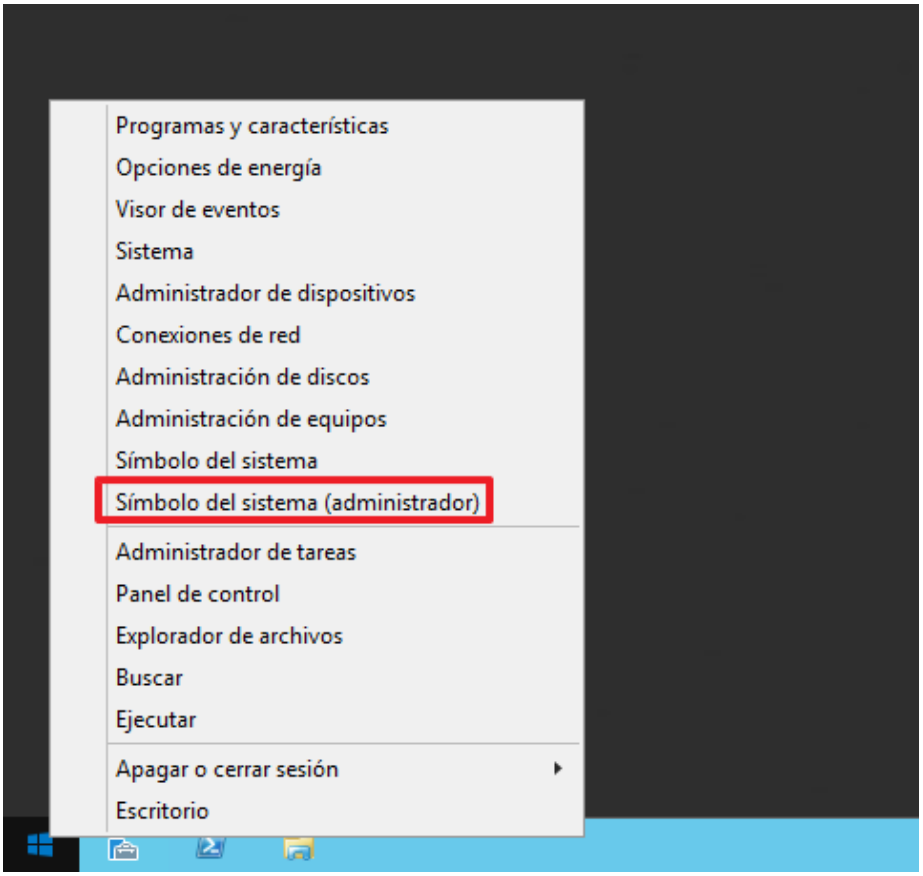


Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

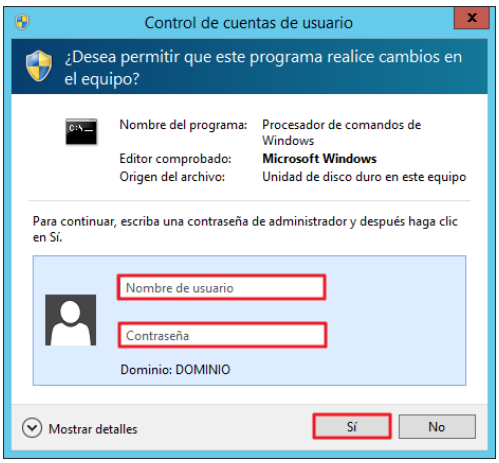
33.	Asegúrese de tener los archivos almacenados en la ubicación correcta.



Paso	Descripción
34.	Una vez que tenga almacenados los archivos en la ubicación correcta, deberá importar las actualizaciones, para ello, ejecute un **"Símbolo de sistema"**. Pulse con el botón derecho sobre **"Inicio"** y seleccione **"Símbolo de sistema (administrador)".**

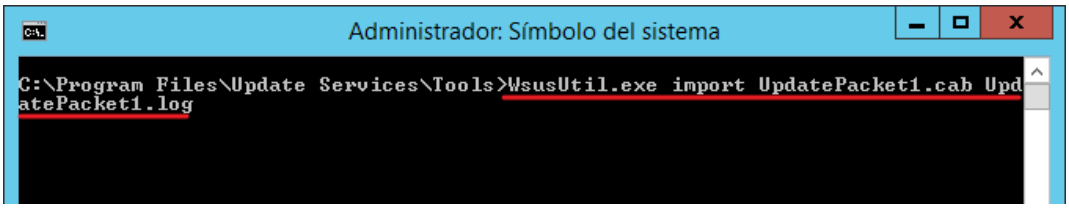


35.	El "control de cuentas de usuarios" le pedirá elevación de privilegios, para ello ingrese una cuenta "administrador del dominio".



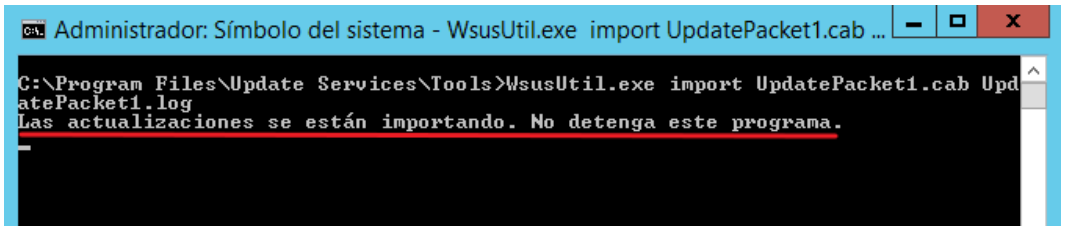
Nota: En este ejemplo se utiliza la cuenta "DOMINIO\SDT".

Paso	Descripción
36.	Ubíquese en **"C:\Archivos de programa\Update Services\Tools\",** ejecute el siguiente comando: **"WsusUtil.exe Import UpdatePacket1.cab UpdatePacket1.log"**

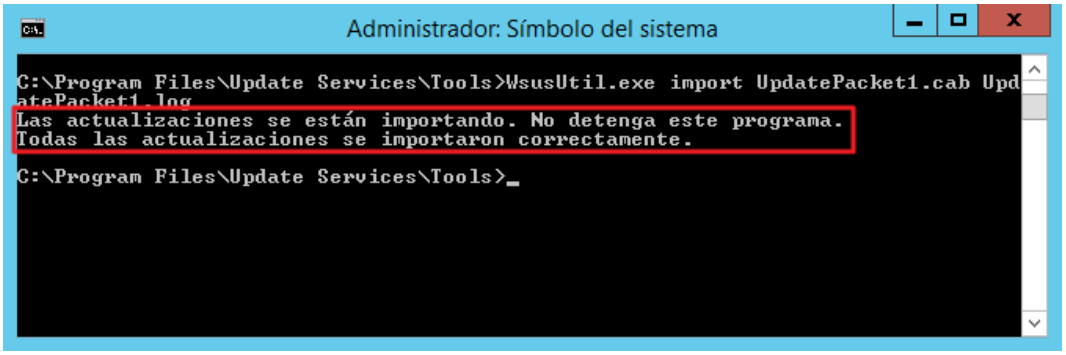


Nota: Para este ejemplo los archivos .cab y .log se han nombrado UpdatePacket1.cab y UpdatePacket1.log respectivamente.

37. WSUS empezará a importar las actualizaciones.

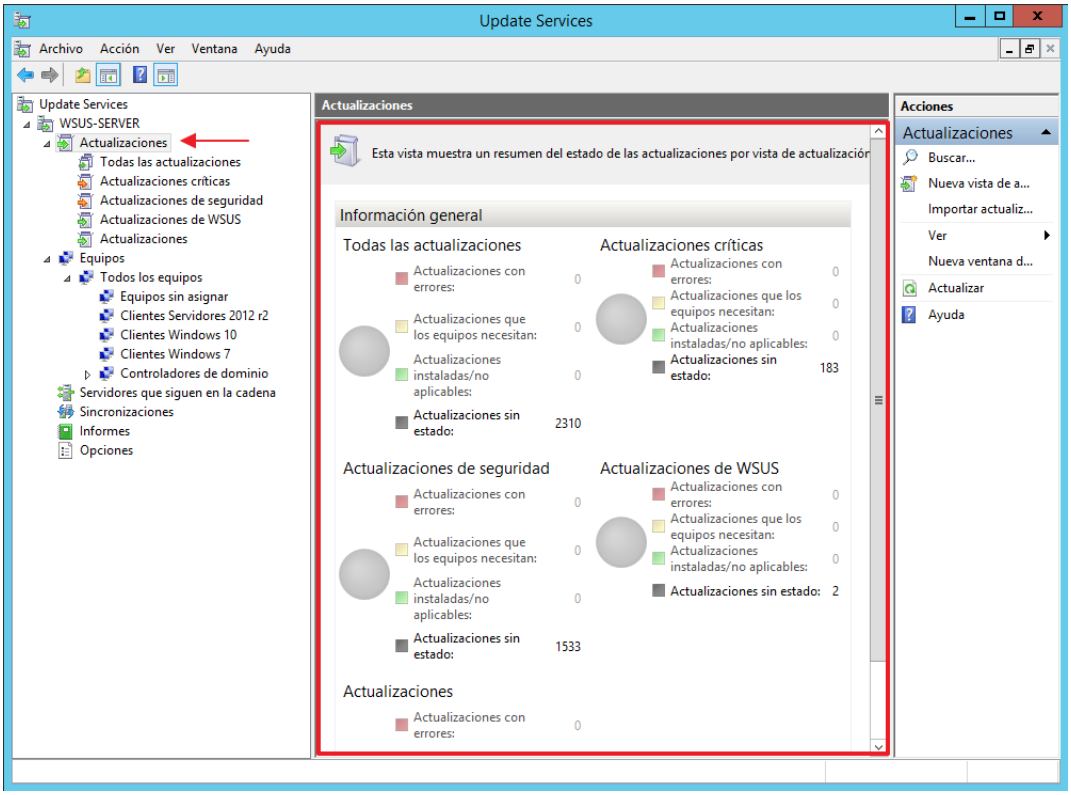


38. Cuando termine de importar, mostrará un mensaje en pantalla para confirmar la importación.



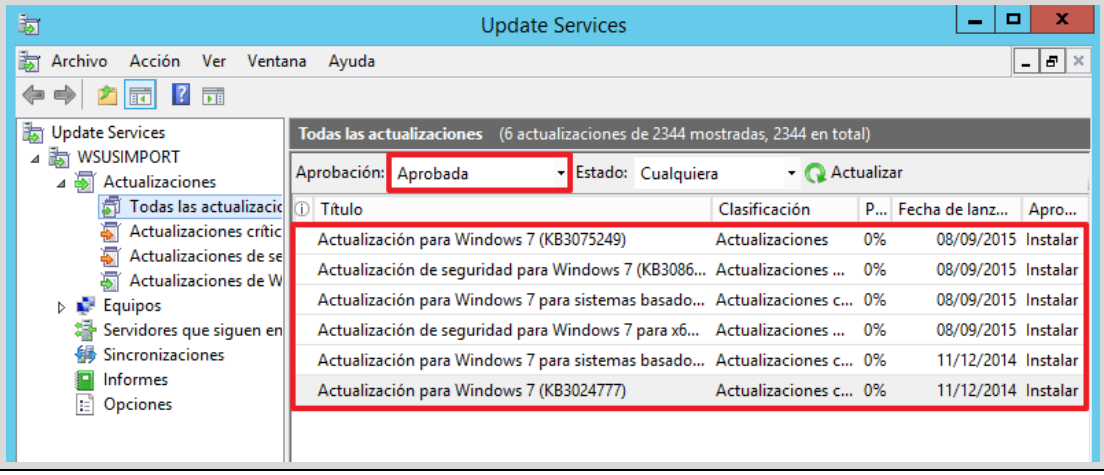
Cierre el **"Símbolo del sistema".**

Paso	Descripción
39.	Una vez que ha importado las actualizaciones, podrá observar éstas en la consola **"Update Services"**, sitúese en **"Actualizaciones"** que se encuentra en la parte izquierda. Visualizará que en la ventana central existe una información general de las actualizaciones y el estado que tendrán en el servidor WSUS.



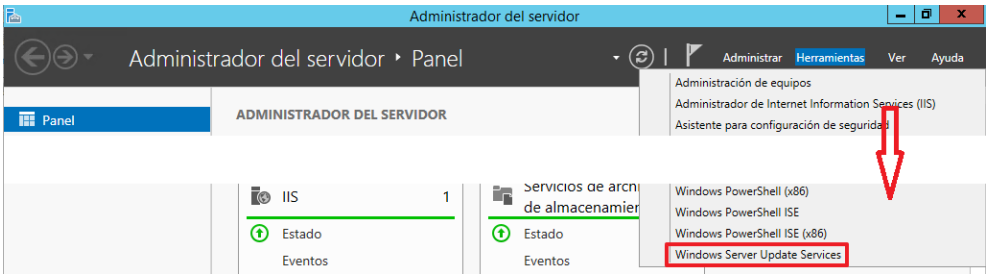
Nota: Es importante saber que, aunque se hayan importado un gran número de actualizaciones, solo podrá aplicar las que realmente se hayan descargado. Es decir, hasta que no apruebe las actualizaciones, estás no se descargarán en la base de datos. Por lo tanto, en el servidor WSUS fuera del dominio cuando sincroniza con Microsoft Update obtendrá un alto número de actualizaciones, pero se descargan las que hayan sido aprobadas. (Esto afectará en la importación)

Para este ejemplo, en el **ANEXO E. 3. DESCARGA Y EXPORTACIÓN DE ACTUALIZACIONES DESDE WINDOWS SERVER UPDATE SERVICES** se realiza una aprobación de seis paquetes de actualizaciones. Por lo que en el servidor WSUS dónde se han importado las actualizaciones, aparecerán todas las sincronizadas con Microsoft Update, pero solo aplicables seis.

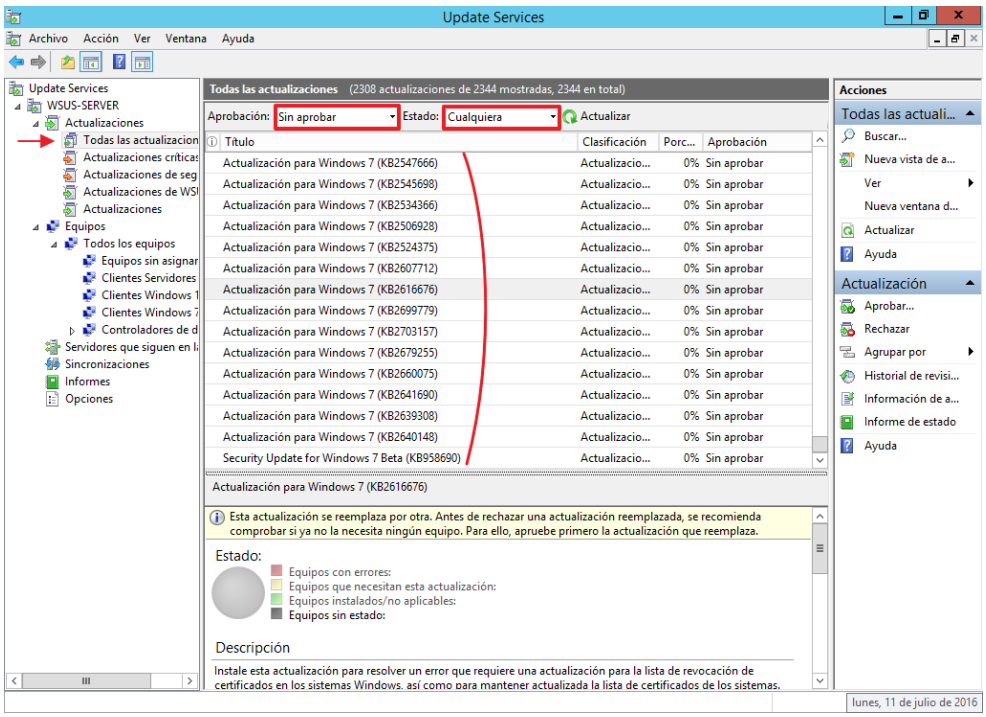


4. ADMINISTRACIÓN DE ACTUALIZACIONES

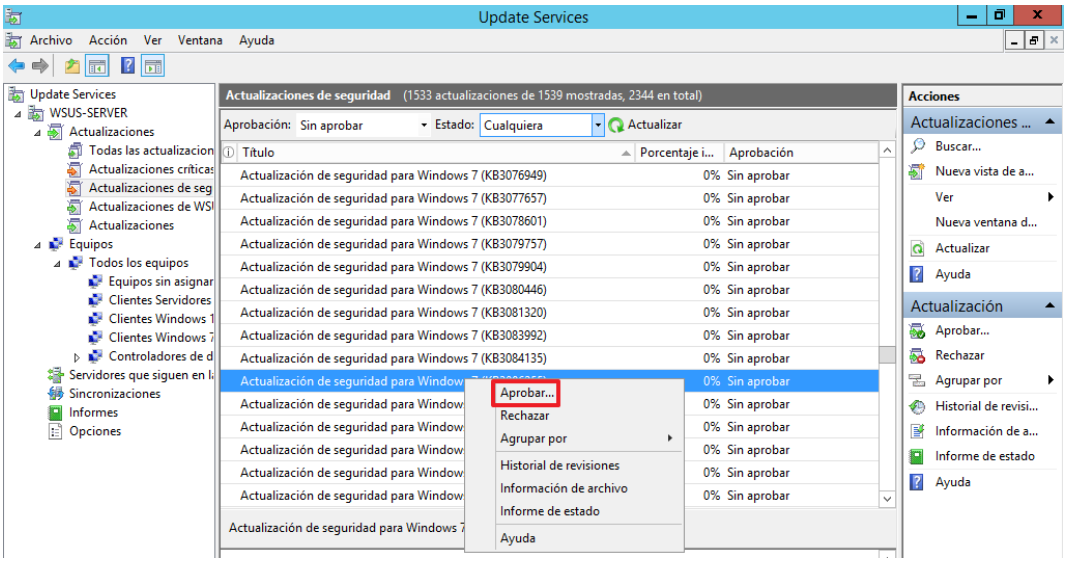
En el presente punto se detalla cómo administrar correctamente las actualizaciones importadas en el servidor Windows Server Update Services, que se encuentra dentro de su red de dominio. Se realizarán tareas de aprobación y rechazo de las actualizaciones, tareas de limpieza de los paquetes de actualizaciones y su instalación en los equipos clientes enlazados con el servidor WSUS.

Paso	Descripción
40.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta "DOMINIO\SDT".
41.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor>Herramientas > Windows Server Update Services"**.  **Nota:** Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

Paso	Descripción
42.	En la consola **"Update Services",** despliegue la pestaña **"Actualizaciones > Todas las actualizaciones"**. Podrá observar, que se encuentran todas las actualizaciones que se han importado.

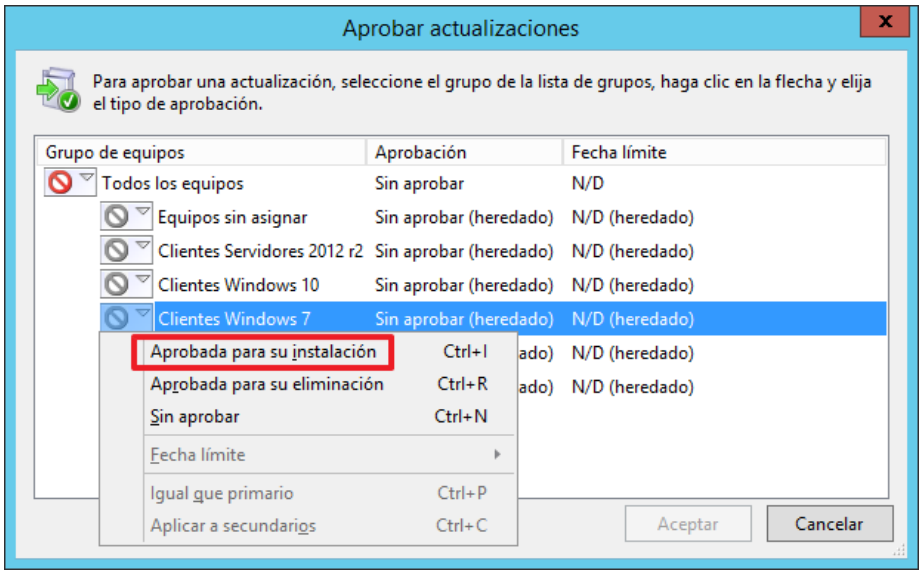


Paso	Descripción
43.	Para realizar una aprobación, pinche sobre una actualización y con el botón derecho seleccione **"Aprobar…"**.



Nota: Para este ejemplo se ha utilizado un paquete de actualización de seguridad, almacenado evidentemente en el grupo de "Actualizaciones de seguridad". Se realizarán más aprobaciones, para que se vea más delante de manera más clara, la instalación en el equipo cliente.
Si realiza la aprobación de una actualización, para la que no exista su archivo.cab en la base de datos de WSUS, ésta nunca llegará a descargarse.

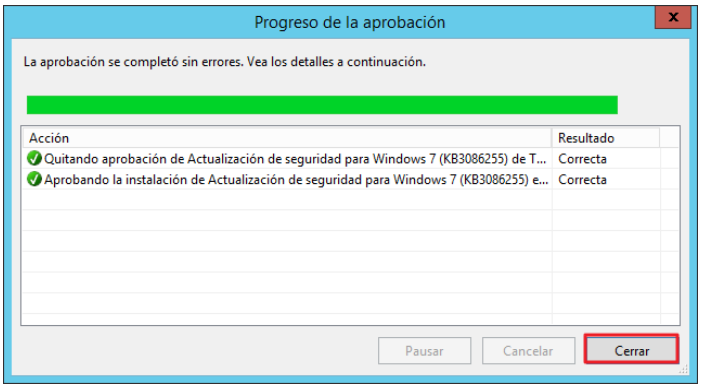
Paso	Descripción
44.	En la venta de **"Aprobar actualizaciones"** debe indicar los grupos para los que quiere aprobar está actualización. Seleccione un grupo y pulse sobre **"Aprobación para su instalación".**

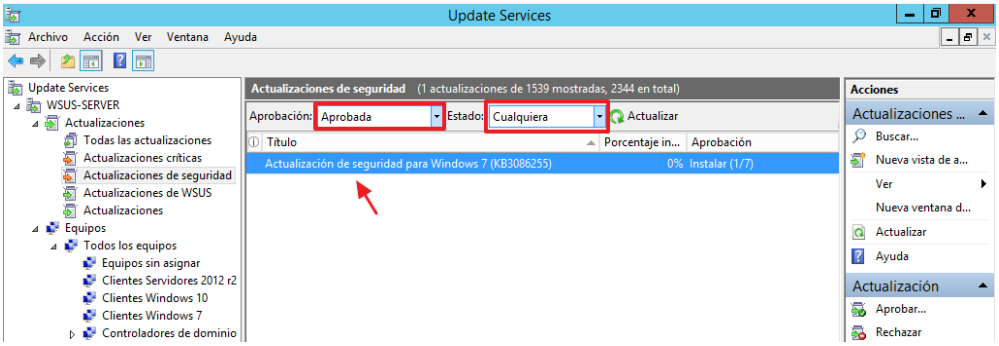
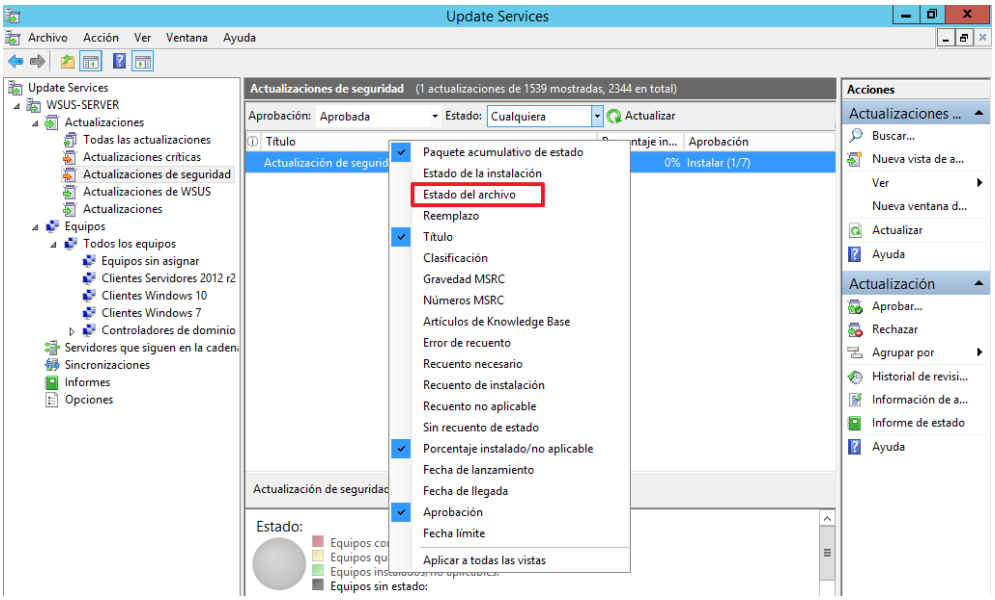


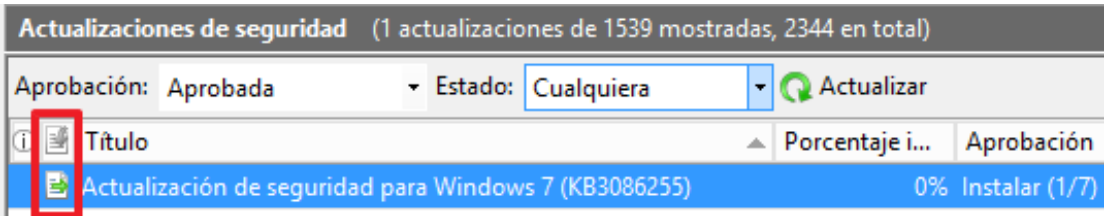
Pulse **"Aceptar".**

Nota: Para este ejemplo, se ha seleccionado la aprobación para los equipos cliente Windows 7, ya que el paquete de actualizaciones que se ha aprobado va dirigido a los sistemas Windows 7.

45.	Una vez que se haya completado la aprobación, pulse **"Cerrar".**



Paso	Descripción
46.	Para visualizar las actualizaciones aprobadas, deberá establecer las pestañas **"Aprobación"** y **"Estado"** de la siguiente manera. – Aprobación: Aprobada. – Estado: Cualquiera. Pulse en **"Actualizar"** para visualizar las actualizaciones aprobadas. 
47.	Sobre la barra de **"Título",** piche con el botón derecho y seleccione **"Estado de archivo"**. Esto comprobará si la actualización está lista para instalarse. 

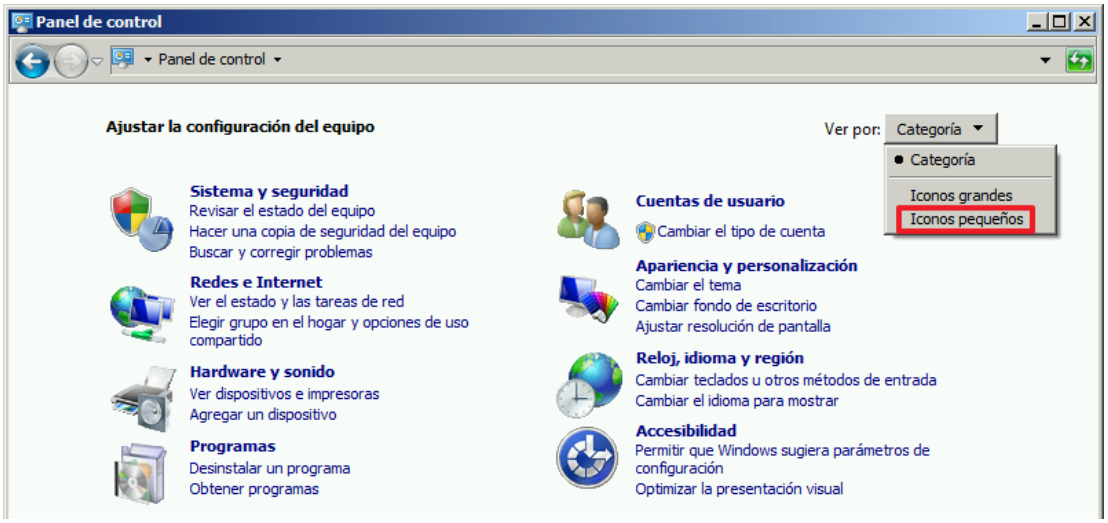
Paso	Descripción
48.	Se generará un icono nuevo que indicará si la actualización se está descargando o si ya está lista para su instalación.  **Nota:** Si la flecha verde está en horizontal, indica que las actualizaciones están descargadas y listas para la instalación. En cambio, si la flecha está en vertical, indica que la actualización no está descargada y por lo tanto, no está lista para su instalación.

Una vez que ya existan actualizaciones aprobadas, podrá instalar dichas actualizaciones a los equipos clientes. Si los equipos clientes están encendidos, estos comunicarán con el servidor WSUS a la hora que le indique la propia GPO, que aplica a los equipos clientes.

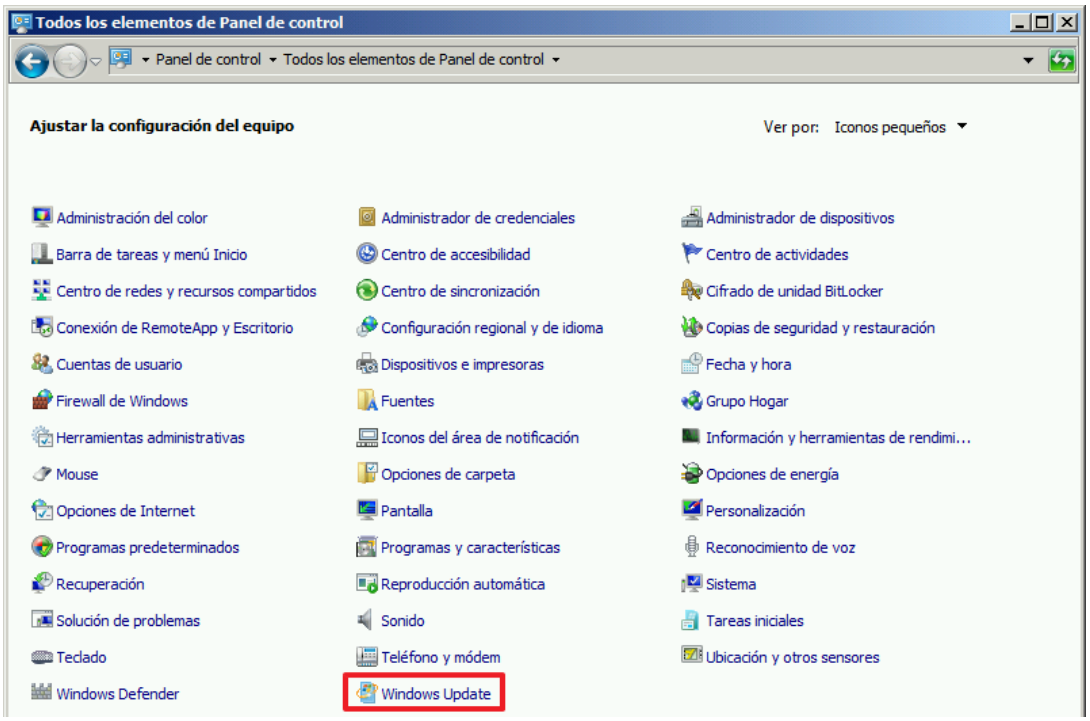
Podrá forzar manualmente que los equipos clientes detecten si tienen actualizaciones disponibles para instalar, mediante Windows Update. Antes de realizar esto, asegúrese de que las actualizaciones en el equipo son administradas por el propio servidor Windows Server Update Services.

Paso	Descripción
49.	Si no lo ha hecho antes, inicie sesión en uno de los clientes de WSUS con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. **Nota:** En este ejemplo se utiliza la cuenta “DOMINIO\SDT”.

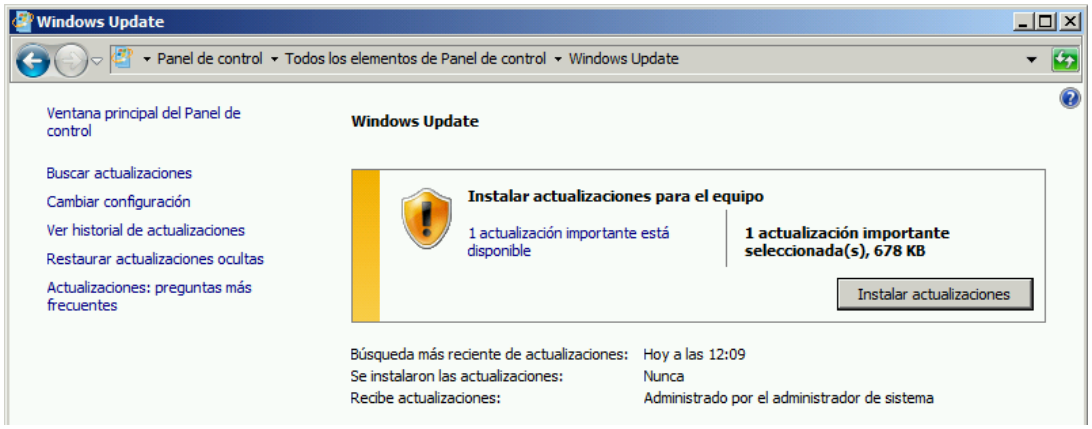
Paso	Descripción
50.	Abra **"Windows Update"**, para ello diríjase a **"Inicio > Panel de control "**. En la pestaña **"Ver por:"** seleccione **"Iconos pequeños"**.



51.	Haga clic sobre **"Windows Update"**.



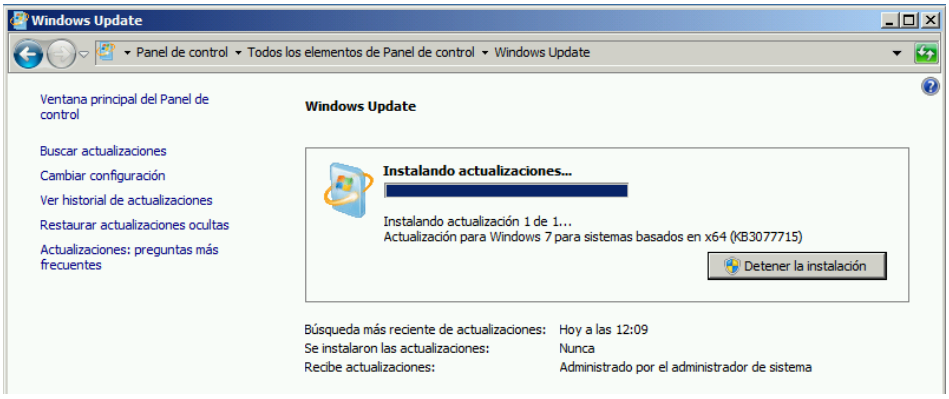
Paso	Descripción
52.	Podrá observar si existen actualizaciones para instalar en ese momento.



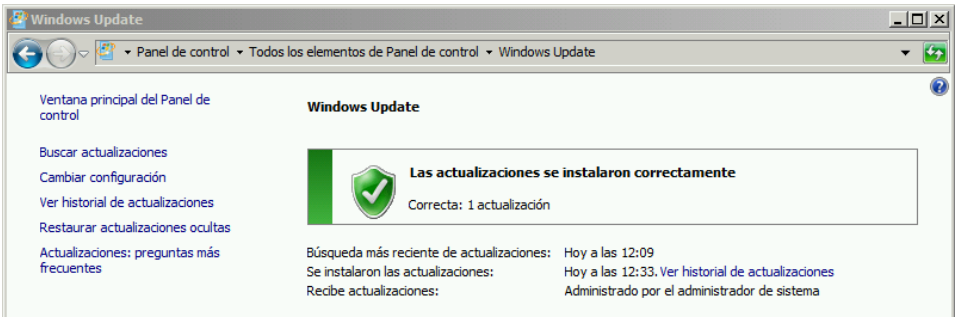
Pulse **"Instar actualizaciones"** para aplicar éstas al equipo cliente.

Nota: Puede forzar la instalación como en este ejemplo, puede esperar al próximo reinicio del equipo cliente para que aplique las actualizaciones. Si el equipo detecta que existen actualizaciones en el momento que el usuario está trabajando, lo notificará. Advertirá que las actualizaciones existen y deben aplicarse para el próximo reinicio del equipo.

Paso	Descripción
53.	Windows Update comenzará a instalar las actualizaciones.



Cuando haya terminado, Windows Update notificará que las actualizaciones se han aplicado correctamente.

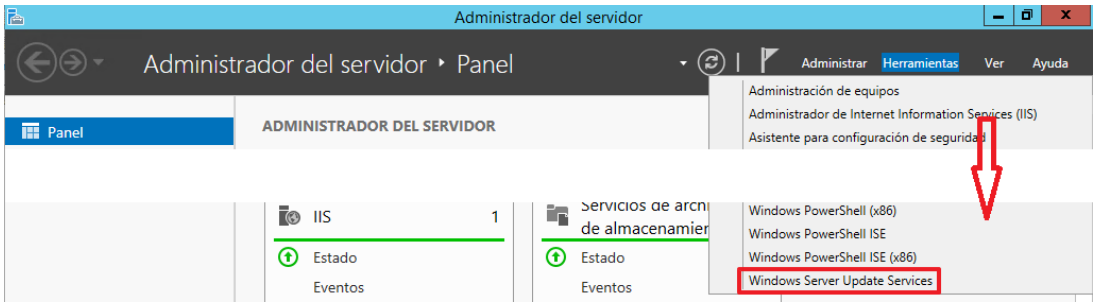


Nota: Dependiendo de las actualizaciones que se apliquen en el equipo, el sistema pedirá, si es necesario, reiniciar el equipo.

54.	Si no lo ha hecho antes, inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio.

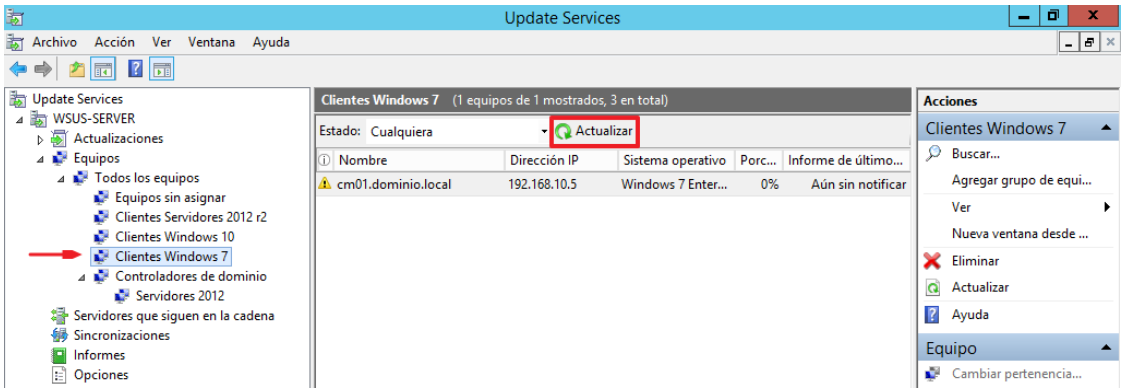
Nota: En este ejemplo se utiliza la cuenta “DOMINIO\SDT”.

Paso	Descripción
55.	Ejecute la consola de Windows Server Update Services, desde **"Inicio > Administrador del servidor > Herramientas > Windows Server Update Services"**.

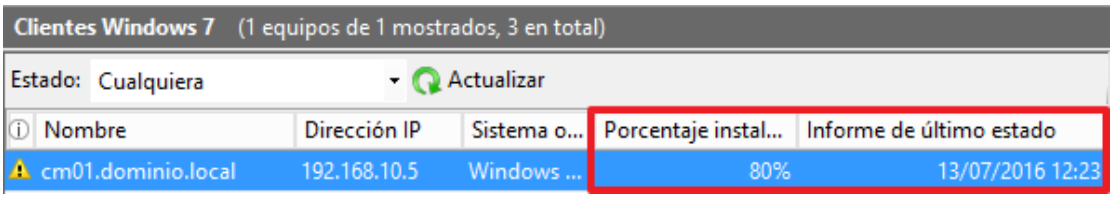


Nota: Si inicia por primera vez la consola de "Administrador del Servidor" le pedirá que introduzca credenciales, en este ejemplo se utiliza la cuenta con privilegios de administrador del dominio "DOMINIO\SDT".

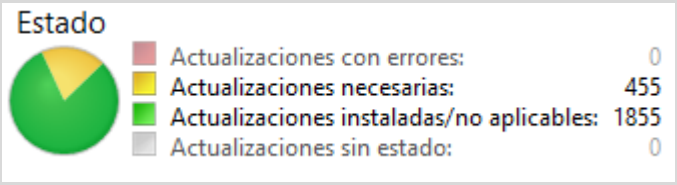
56.	En la consola de **"Update Services"**, despliegue el grupo de **"Clientes Windows 7"**. En la ventana central, pulse en **"Actualizar"**.



Paso	Descripción
57.	Podrá observar que las pestañas **"Porcentaje instalado…"** y **"Informe de último estado"** ha sido actualizado, ya que el equipo cliente logró instalar actualizaciones.



Nota: El "Porcentaje de Instalación" irá aumentando una vez que el equipo cliente aplique todas las actualizaciones disponibles que tiene el servidor WSUS.
Cuando el equipo contacta con WSUS, el propio servidor evalúa el estado del equipo cliente y verifica las actualizaciones que faltan. Como se puede observar en la siguiente imagen, se muestra el estado del equipo cliente con un diagrama, en el que se detallan los diferentes estados.



ANEXO H. LISTA DE COMPROBACIÓN DE LA CORRECTA INSTALACIÓN DEL SERVIDOR WINDOWS SERVER UPDATE SERVICES

Este anexo se ha diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad.

Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores WSUS que son miembros del dominio.

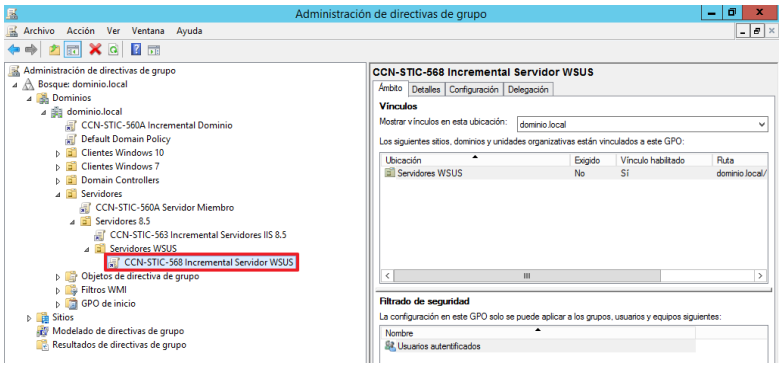
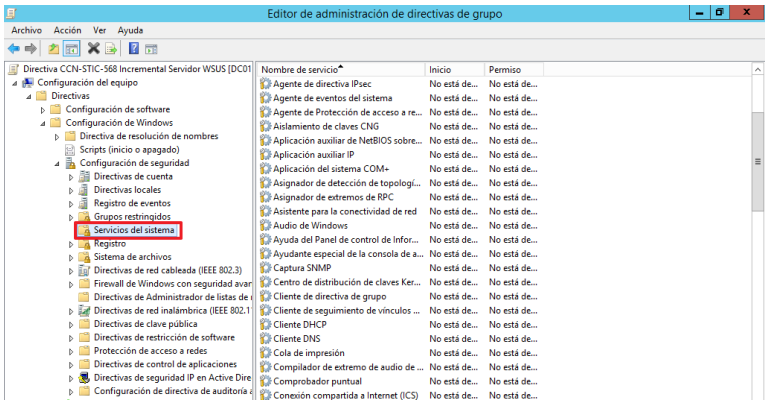
Nota: A la hora de seleccionar la cuenta de administrador hay que tener en consideración que, la cuenta de usuario de administrador por defecto, del dominio, se le ha denegado el derecho de acceso a los controladores de dominio a través de la red.

Posteriormente, se deberán realizar las comprobaciones en el propio servidor Windows Server Update Services, por lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles, si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios de administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

- En el controlador de dominio:
  - Usuarios y equipos de Active Directory (dsa.msc).
  - Administrador de directivas de grupo (gpmc.msc).
  - Editor de objetos de directiva de grupo (gpedit.msc).
- En el servidor WSUS:
  - Administrador de Windows (explorer.exe).
  - Servicios (services.msc).
  - Editor de objetos de directiva de grupo (gpedit.msc).

Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

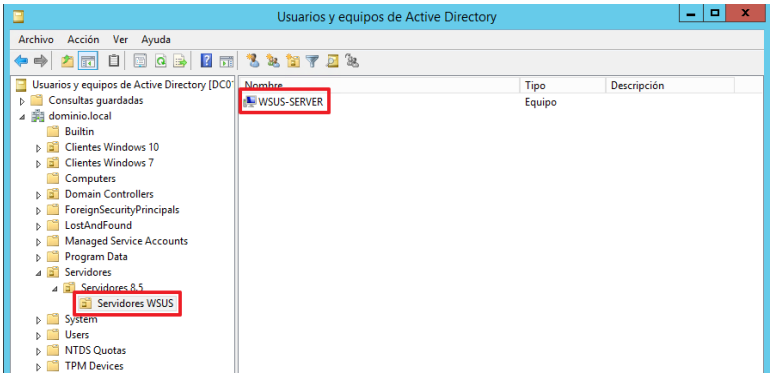
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva CCN-STIC-568 Incremental Servidor WSUS.		Utilice el Administrador de directivas de grupo **(Inicio → Herramientas administrativas → Administración de directivas de grupo)** y despliegue el menú en árbol hasta llegar a la unidad organizativa **"Servidores WSUS"** que se encuentra en la OU **"Servidores > Servidores 8.5"**. Verifique que está creada la política "CCN-STIC-568 Incremental Servidor WSUS". 
3. Verifique los servicios del sistema de la directiva CCN-STIC-568 Incremental Servidor WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Servidor WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes servicios de sistema habilitados dentro de: **Directiva CCN-STIC-568 Incremental Servidor WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema.** 

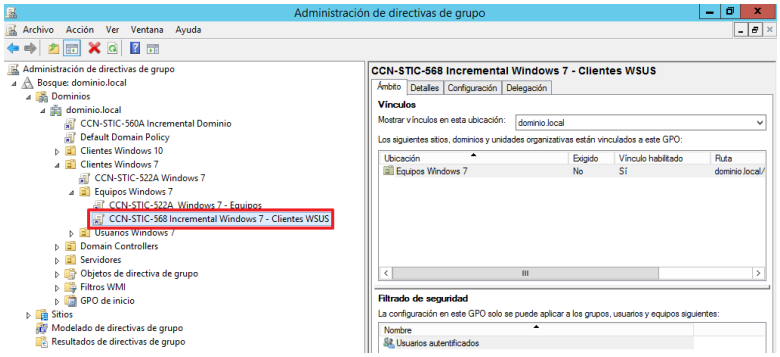
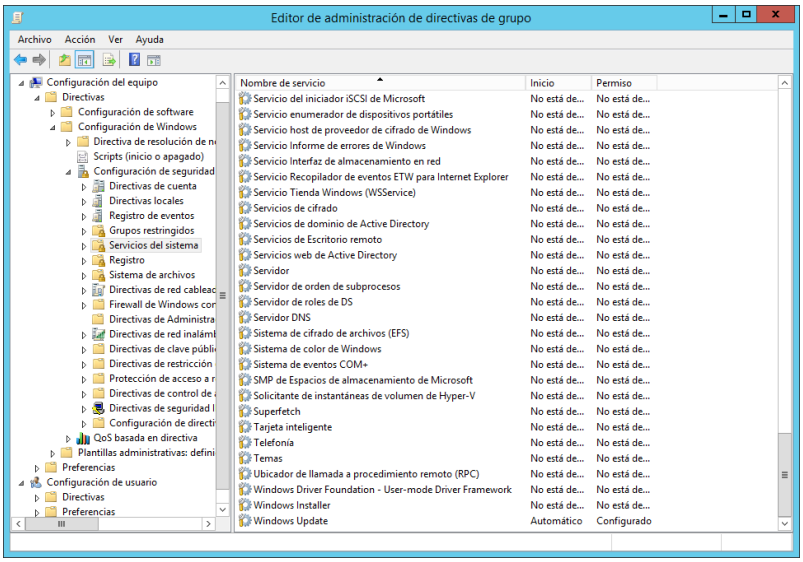
Comprobación	OK/NOK	Cómo hacerlo

Nombre de servicio	Inicio	OK/NOK
Administración remota de Windows (WS-Management)	Automático	
Servicio de transferencia inteligente en segundo plano (BITS)	Automático	
Servidor	Automático	
WsusService	Automático	
WsusCertServer	Automático	

4. Verifique que el servidor WSUS está dentro de la unidad organizativa "Servidores WSUS".

Utilice la herramienta Usuarios y equipos de Active Directory **(Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory)** y seleccione la unidad organizativa "Servidores WSUS". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores WSUS que se están asegurando.



Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que está creada la directiva CCN-STIC-568 Incremental Windows 7 – Clientes WSUS.		Utilice el Administrador de directivas de grupo **(Inicio → Herramientas administrativas → Administración de directivas de grupo)** y despliegue el menú en árbol hasta llegar a la unidad organizativa **"Equipos Windows 7"** que se encuentra en la OU **"Clientes Windows 7 > Equipos Windows 7"**. Verifique que está creada la política **"CCN-STIC-568 Incremental Windows 7- Clientes WSUS"**. 
6. Verifique los servicios del sistema de la directiva CCN-STIC-568 Incremental Windows 7 – Clientes WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 7 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes servicios del sistema habilitados dentro de: **Directiva CCN-STIC-568 Incremental Windows 7 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema.** 

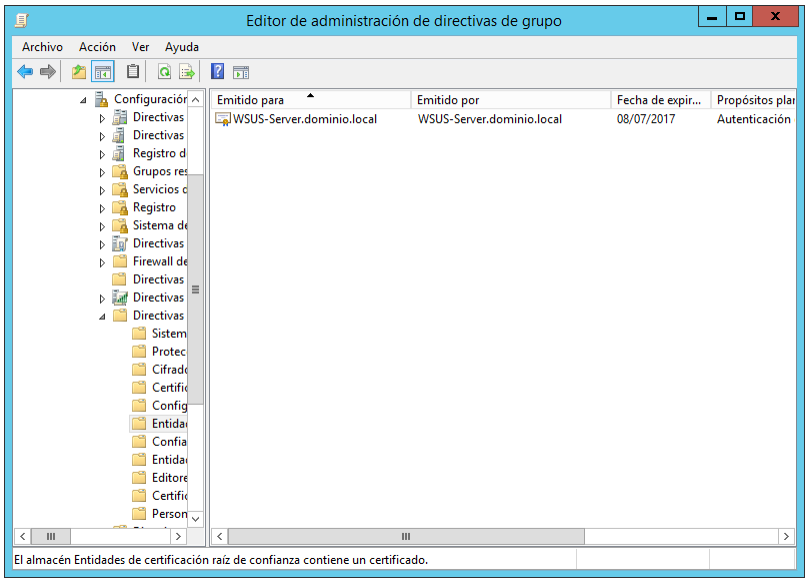
Comprobación	OK/NOK	Cómo hacerlo

Nombre de servicio	Inicio	OK/NOK
Windows Update	Automático	

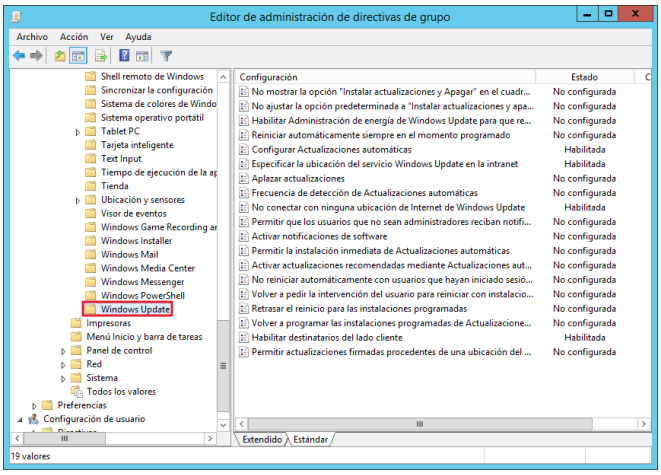
7. Verifique que el certificado se encuentra en la Entidad de certificación raíz de confianza de la directiva CCN-STIC-568 Incremental Windows 7 – Clientes WSUS.

Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 7 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene el certificado WSUS dentro de:

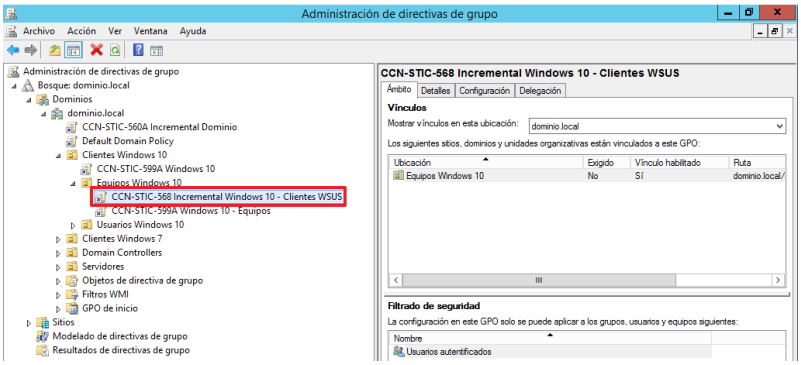
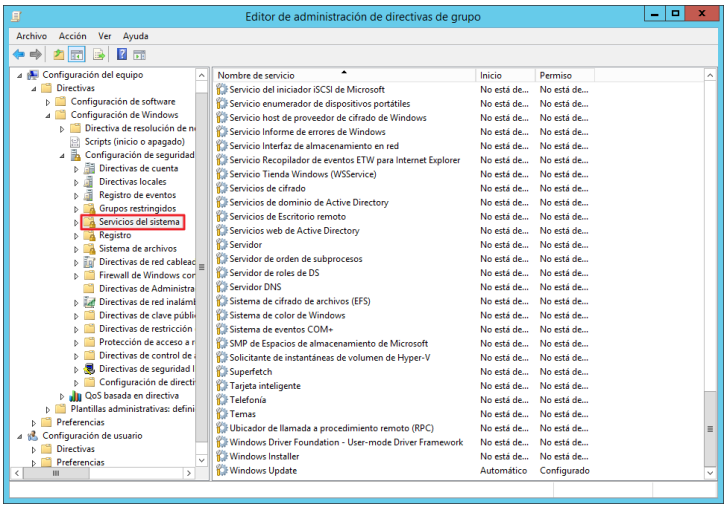
Directiva CCN-STIC-568 Incremental Windows 7 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de clave pública \ Entidad de certificación raíz de confianza.



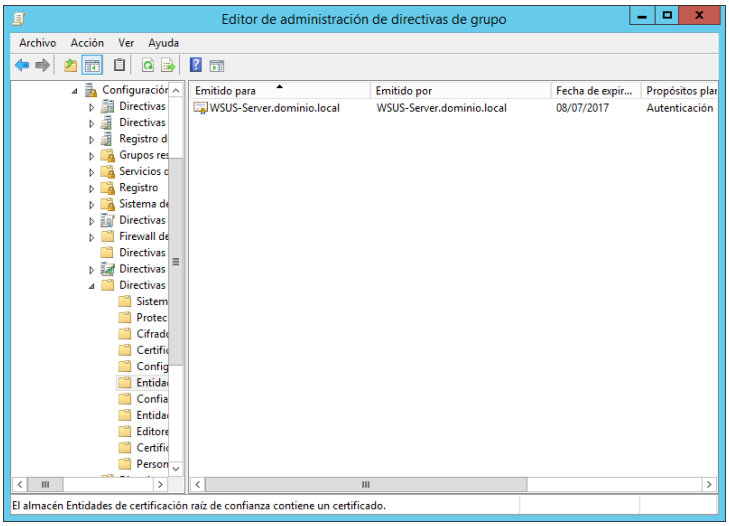
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique la configuración de Windows Update de la directiva CCN-STIC-568 Incremental Windows 7 – Clientes WSUS		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 7 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes valores en las directivas de Windows Update dentro de: **Directiva CCN-STIC-568 Incremental Windows 7 - Clientes WSUS \ Configuración del equipo \ Directivas \ Plantillas administrativas \ Componentes de Windows \ Windows Update.**



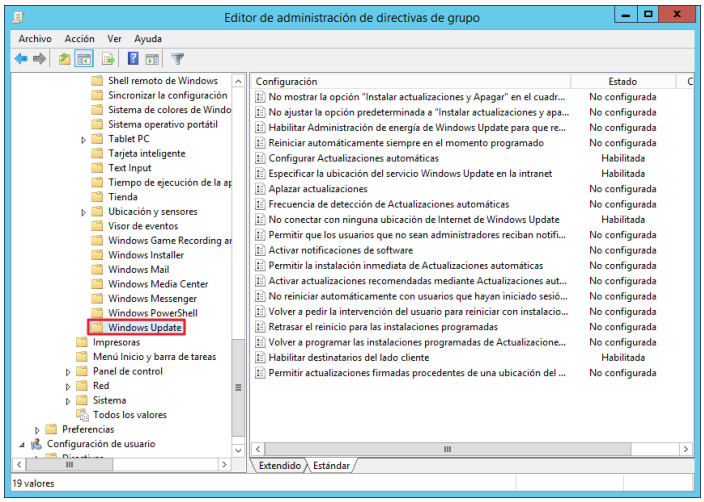
Configuración	Estado	OK/NOK
Configurar Actualizaciones automáticas	Habilitada	
Especificar la ubicación del servicio Windows Update en la intranet	Habilitada	
No conectar con ninguna ubicación de Internet de Windows Update	Habilitada	
Habilitar destinatarios del lado cliente	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique que está creada la directiva CCN-STIC-568 Incremental Windows 10 – Clientes WSUS.		Utilice el Administrador de directivas de grupo **(Inicio → Herramientas administrativas → Administración de directivas de grupo)** y despliegue el menú en árbol hasta llegar a la unidad organizativa **"Equipos Windows 10"** que se encuentra en la OU **"Clientes Windows 10 > Equipos Windows 10"**. Verifique que está creada la política **"CCN-STIC-568 Incremental Windows 10- Clientes WSUS"**. 
10. Verifique los servicios del sistema de la directiva CCN-STIC-568 Incremental Windows 10 – Clientes WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 10 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes servicios del sistema habilitados dentro de: **Directiva CCN-STIC-568 Incremental Windows 10 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema.** 

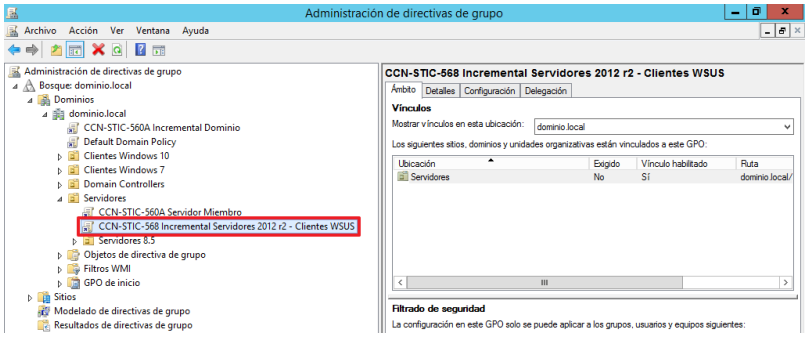
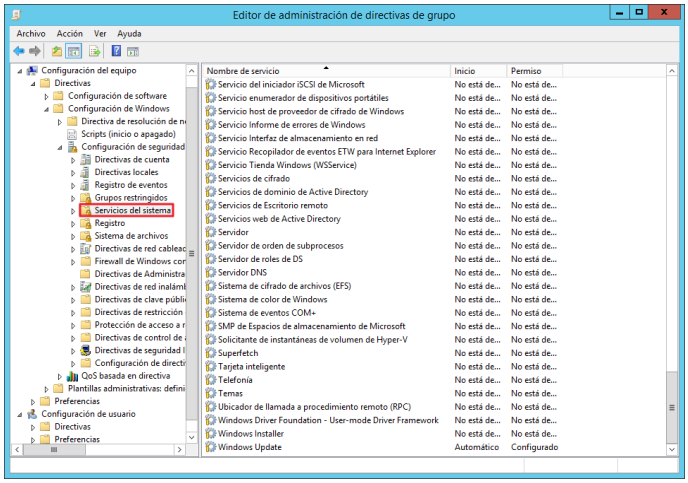
Nombre de servicio	Inicio	OK/NOK
Windows Update	Automático	

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique que el certificado se encuentra en la Entidad de certificación raíz de confianza de la directiva CCN-STIC-568 Incremental Windows 10 – Clientes WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 10 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene el certificado WSUS dentro de: **Directiva CCN-STIC-568 Incremental Windows 10 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de clave pública \ Entidad de certificación raíz de confianza.** 

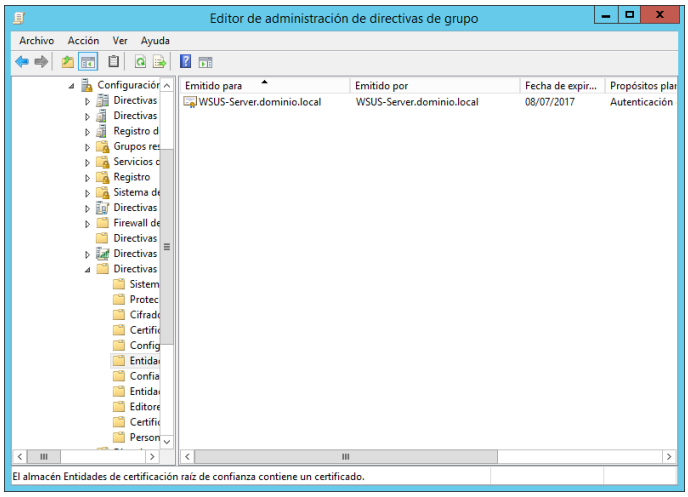
Comprobación	OK/NOK	Cómo hacerlo
12. Verifique la configuración de Windows Update de la directiva CCN-STIC-568 Incremental Windows 10 – Clientes WSUS		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Windows 10 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes valores en las directivas de Windows Update dentro de: **Directiva CCN-STIC-568 Incremental Windows 10 - Clientes WSUS \ Configuración del equipo \ Directivas \ Plantillas administrativas \ Componentes de Windows \ Windows Update.**



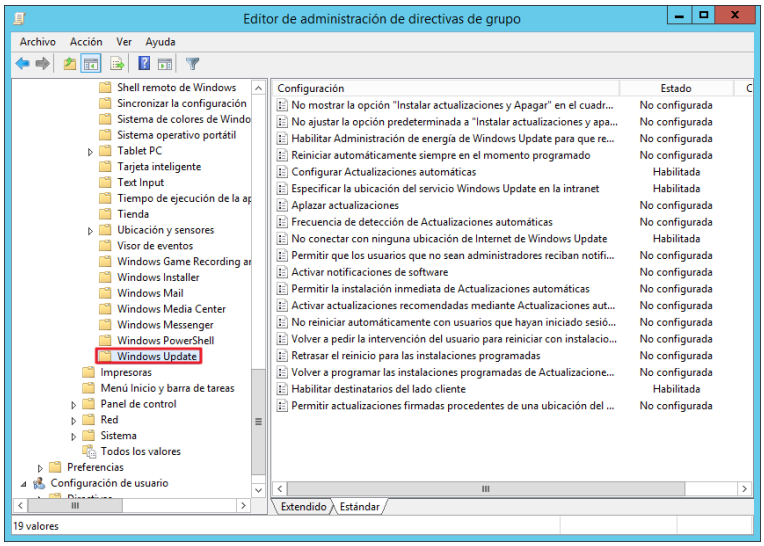
Configuración	Estado	OK/NOK
Configurar Actualizaciones automáticas	Habilitada	
Especificar la ubicación del servicio Windows Update en la intranet	Habilitada	
No conectar con ninguna ubicación de Internet de Windows Update	Habilitada	
Habilitar destinatarios del lado cliente	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo
13. Verifique que está creada la directiva CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS.		Utilice el Administrador de directivas de grupo **(Inicio → Herramientas administrativas → Administración de directivas de grupo)** y despliegue el menú en árbol hasta llegar a la unidad organizativa **"Servidores"**. Verifique que está creada la política **"CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS"**. 
14. Verifique los servicios del sistema de la directiva CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes servicios del sistema habilitados dentro de: **Directiva CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema.** 

Nombre de servicio	Inicio	OK/NOK
Windows Update	Automático	

Comprobación	OK/NOK	Cómo hacerlo
15. Verifique que el certificado se encuentra en la Entidad de certificación raíz de confianza de la directiva CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS.		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene el certificado WSUS dentro de: **Directiva CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de clave pública \ Entidad de certificación raíz de confianza.** 

Comprobación	OK/NOK	Cómo hacerlo
16. Verifique la configuración de Windows Update de la directiva CCN-STIC-568 Incremental Servidores 2012 r2 – Clientes WSUS		Utilizando el editor de directiva de grupo, haciendo clic derecho sobre la directiva **"CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS"** y seleccionando la opción **"Editar…"**, verifique que la directiva tiene los siguientes valores en las directivas de Windows Update dentro de: **Directiva CCN-STIC-568 Incremental Servidores 2012 r2 - Clientes WSUS \ Configuración del equipo \ Directivas \ Plantillas administrativas \ Componentes de Windows \ Windows Update.**
17. Inicie sesión en el servidor WSUS del dominio.		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.
18. Verifique que están instalados los componentes que se indican.		En el **"Administrador del Servidor"**, pulse sobre la opción **"Servidor Local"** del menú de la izquierda y diríjase a la parte final de la ventana principal, **"Roles y características"**, por medio del scroll lateral derecho.



Configuración	Estado	OK/NOK
Configurar Actualizaciones automáticas	Habilitada	
Especificar la ubicación del servicio Windows Update en la intranet	Habilitada	
No conectar con ninguna ubicación de Internet de Windows Update	Habilitada	
Habilitar destinatarios del lado cliente	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo

Componente	OK/NOK
Servicios de archivos y almacenamiento	
Windows Server Update Services	
Servidor web (IIS)	

19. Verifique que los servicios del sistema relacionados con el servidor WSUS están configurados correctamente.

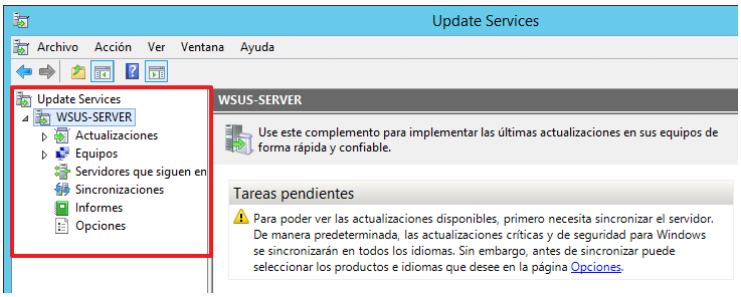
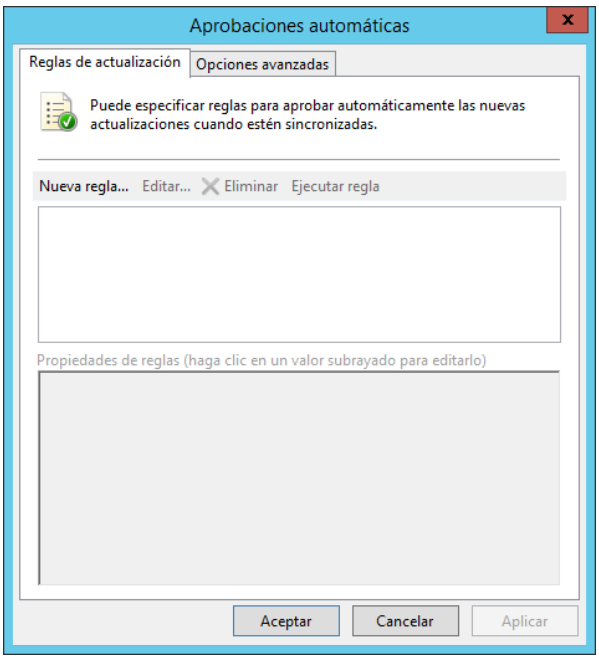
Ejecute el complemento Servicios (ejecutando **services.msc** desde, botón derecho sobre **Inicio → Ejecutar…**) y compruebe el tipo de inicio de los servicios.

Nombre de servicio	Inicio	OK/NOK
Administración remota de Windows (WS-Management)	Automático	
Servicio de transferencia inteligente en segundo plano (BITS)	Automático	
Servidor	Automático	
Servicio de WSUS	Automático	
WSUS Certificate Server	Automático	

20. Verifique las reglas de entrada del Firewall de Windows con seguridad avanzada.

Utilizando la herramienta de Firewall de Windows con seguridad avanzada, (botón derecho sobre **Inicio → Ejecutar → wf.msc**), verifique que existen las siguientes reglas de entrada y se encuentran habilitadas:

Regla de entrada	OK/NOK
WSUS (Port 8530)	
WSUS (Port 8531)	

Comprobación	OK/NOK	Cómo hacerlo
21. Verifique que la instalación del servidor WSUS se ha realizado correctamente .		Utilizando la consola de Windows Server Update Services (en el administrador del servidor, pulse sobre **"Herramientas > Windows Server Update Services"**), verifique que la consola se inicia y presenta el servidor local como un servidor Update Services.  **Nota:** En esta comprobación, el servidor se denomina "WSUS-SERVER". En su organización debe comprobar que aparece el nombre del servidor local de WSUS que está implementando.
22. Verifique las aprobaciones automáticas del servidor WSUS.		Utilizando la consola de Windows Server Update Services (en el **Administrador del servidor**, pulse sobre **"Herramientas > Windows Server Update Services"**), verifique que no existe alguna regla de aprobación automática en el servidor WSUS, vaya a **"Opciones > Aprobaciones automáticas".** 

Comprobación	OK/NOK	Cómo hacerlo
23. Verifique que la asignación de grupos de equipos está establecida por directiva de grupo.		Utilizando la consola de Windows Server Update Services (en el **Administrador del servidor**, pulse sobre **"Herramientas > Windows Server Update Services"**), verifique que la asignación de grupo de equipos se administra por directiva de grupo, vaya a **"Opciones > Equipos".**