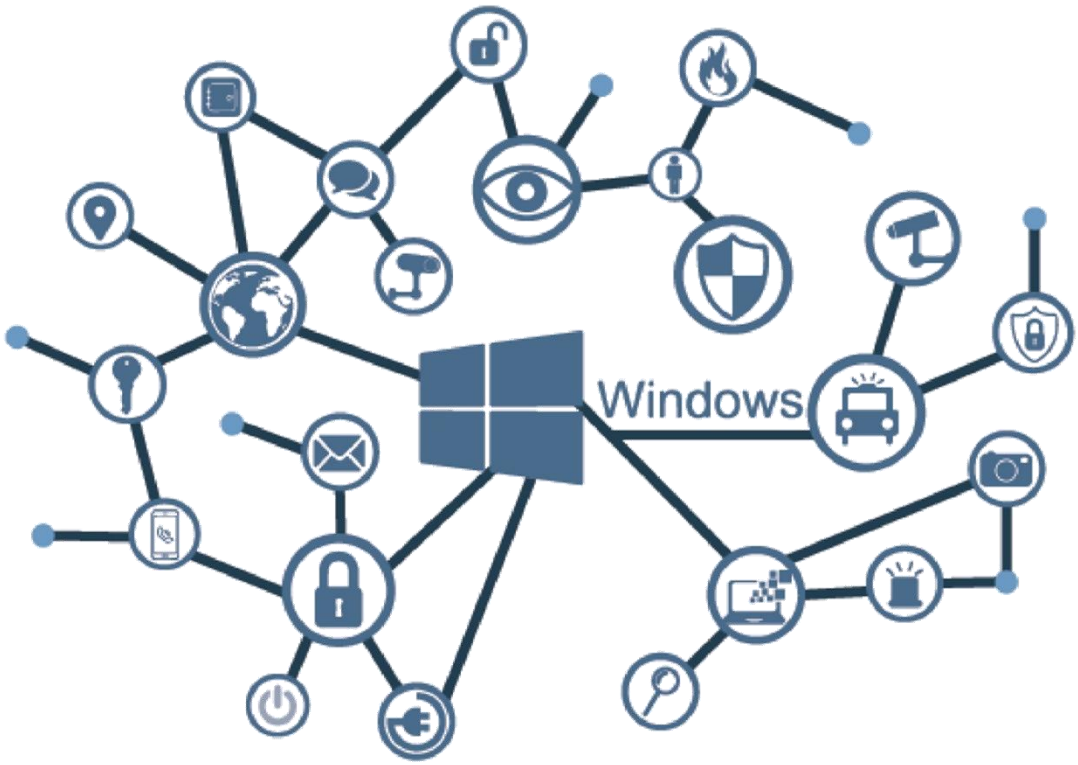
centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 568A25

# APLICACIÓN DE SEGURIDAD SOBRE WINDOWS SERVER UPDATE SERVICES (WSUS)




ENERO 2026

MINISTERIO DE DEFENSA

Edita:

centro criptológico nacional



centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.27 16:53:04 +01'00'

Fecha de Edición: enero de 2026

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

# INDICE

# 1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el **Centro Criptológico Nacional (en adelante, CCN)** para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC-500), siendo de aplicación para la administración pública en el cumplimiento del **Esquema Nacional de Seguridad** (en adelante, ENS) y, de igual modo, de obligado cumplimiento para los sistemas que manejen **Información Clasificada** de ámbito NACIONAL tal y como se expone en el "Artículo 2" del propio ENS. Esto último sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa de aplicación. De igual modo se aplica a los sistemas de información de las entidades del sector privado cuando, según el ENS, "de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público".

La **serie CCN-STIC-500** se ha diseñado de manera incremental. Así, dependiendo del sistema operativo, los productos que implemente y los servicios que ofrezca, se aplicarán consecutivamente varias de estas guías para asegurar en su totalidad todos los elementos del sistema de información. En este sentido, se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno para un servidor miembro de dominio con Microsoft Windows Server 2025, en el que se instale Microsoft WSUS, el cual requiere la instalación del rol **Windows Server Update Services**, deberán aplicarse las guías técnicas más recientes publicadas en el portal web del CCN-CERT:

a) Guía CCN-STIC-570A25 en el servidor miembro con Windows Server 2025.

b) Guía CCN-STIC-574A25 sobre Internet Information Services (IIS), para la configuración segura del servicio.

c) Guía CCN-STIC-568A25 sobre Microsoft WSUS, aplicable al servidor que alojará el servicio de WSUS.

**Nota:** actualmente, las guías Microsoft publicadas en la serie **800** están orientadas a servicios en la nube adaptados al ENS. Para el despliegue en infraestructura propia, las guías aplicables se encuentran en la serie **500**, que recoge la documentación más actualizada para estos escenarios.

## 2. OBJETO

El propósito de esta guía de seguridad es proporcionar los elementos y directrices para aplicar y garantizar la seguridad en equipos que implementen el aplicativo **Windows Server Update Services** en un entorno de dominio.

La configuración que se aplica a través de la presente guía establece las restricciones necesarias para minimizar la superficie de ataque y posibles riesgos asociados a la implementación de este servicio. En algunos casos, y dependiendo de la funcionalidad asociada al servidor, podría ser necesario modificar la configuración planteada en la presente guía.

Así, se entenderá que la implementación del servicio **Windows Server Update Services**, dependerá de las necesidades peculiares y servicios prestados por la entidad que lo aplica. Consecuentemente, aquellas plantillas y guías de seguridad generadas recogerán aquellas pautas generales de seguridad que permitan el cumplimiento de los requisitos y estándares mínimos de seguridad establecidos en el ENS, así como aquellas condiciones que, según la normativa nacional de aplicación, se requieran para el manejo de Información Clasificada.

La definición de las medidas de seguridad asociadas a la presente guía se basan, principalmente, en las necesidades técnicas recogidas en el "Anexo II: Medidas de Seguridad", así como aquellas disposiciones establecidas por el CCN en la Instrucción Técnica de Seguridad de las TIC (CCN-STIC-301) y otras normativas nacionales de aplicación, que permitan una aproximación al Marco Moderno de Seguridad.

Este marco de aplicación basa sus pilares fundamentales en los siguientes objetivos:

- Las medidas a adoptar estarán condicionadas no solo por la normativa aplicable y el presente documento, sino también por el análisis de riesgos preceptivo de cada escenario (Sistema de Información Clasificada, en adelante, CIS), la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca utilizando la Declaración de Aplicabilidad Técnica o Perfil de Cumplimiento Técnico Específico (en adelante, PCTE) como elemento fundamental sobre el que vertebrar la seguridad. Se tomará de igual modo en cuenta el Perfil de Cumplimiento Específico (en adelante, PCE) aplicable al conjunto del organismo y sus sistemas de información.
- El PCTE y las medidas establecidas por medio del presente documento cumplen los requisitos técnicos para que los sistemas TIC se adapten a cualquier CLASIFICACIÓN DE LA INFORMACIÓN tomando en consideración la categorización de los sistemas definida en el ENS.
- Las guías se revisarán y se actualizarán según las nuevas amenazas, avances tecnológicos y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.

La configuración planteada se ha diseñado para adaptarse a las características específicas de cada entorno, en función de las necesidades de este, pero garantizando el cumplimiento de los requisitos mínimos de seguridad definidos bajo el PCTE. En caso de no poder aplicar los requisitos mencionados, estos deberán ser compensados por medio de medidas técnicas complementarias (vigilancia) y/o compensatorias.

Para la elaboración de esta guía, se ha realizado una revisión exhaustiva de las distintas configuraciones de seguridad disponibles en los sistemas operativos Windows Server, alineándolas y clasificándolas en función de los requisitos definidos por las normativas aplicables.

De esta forma, se pretende dar mayor coherencia al conjunto de medidas resultantes, siendo necesario implementar únicamente aquellas que realmente son de aplicación según el tipo de sistema de información y datos que maneja.

## 3. ALCANCE

La presente guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de Microsoft Windows Server Update Services en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración.

El escenario en el cual está basada la guía CCN-STIC-568A25 tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo (en adelante, AD).

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2025.

d) Un controlador de dominio basado en Windows Server 2025.

e) Un servidor miembro del dominio basado en Windows Server 2025.

f) Un servidor independiente con conexión a Internet basado en Windows Server 2025.

Este documento incluye:

a) Mecanismos para la implementación de la solución. Se incorporan mecanismos para la implementación de la solución de forma automatizada.

b) Mecanismos para la aplicación de configuraciones. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

c) Descripción de la seguridad en Microsoft Windows Server Update Services. Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Microsoft WSUS.

d) Guía paso a paso. Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor con Microsoft Windows Server Update Services.

# 4. DESCRIPCIÓN DE USO DE ESTA GUÍA

Para comprender la presente guía de seguridad, es fundamental explicar el proceso que describe y los recursos que se ponen a disposición para garantizar una implementación segura y conforme a las buenas prácticas. Este proceso se compone de las fases que se describen a continuación.

- **Configuración de seguridad sobre AD DS:** Las configuraciones de seguridad del servicio y de los componentes necesarios del sistema se modifican por medio de objetos de política de grupo (GPO). Dicha configuración está desarrollada en el anexo *ANEXO A.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES WSUS MIEMBROS DE DOMINIO SOBRE WINDOWS SERVER 2025.*
- **Configuraciones adicionales de seguridad:** Las configuraciones adicionales de seguridad hacen referencia a algunos ajustes que no se pueden realizar mediante aplicación de objetos de política de grupo. Dicha configuración está desarrollada en el anexo *ANEXO A.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD.*

## 4.1. REQUISITOS PREVIOS PARA WINDOWS SERVER UPDATE SERVICES

Antes de aplicar las medidas descritas en esta guía, es necesario que el servidor disponga de un sistema operativo compatible. Windows Server Update Services (WSUS) se encuentra integrado como rol nativo en Windows Server 2025, en las ediciones que permiten la instalación de roles y características de servidor. El sistema debe estar correctamente instalado y actualizado, con una configuración básica funcional que incluya los siguientes elementos:

- Nombre de equipo.
- Resolución DNS.
- Sincronización horaria.
- Conectividad de red.

Asimismo, el servidor debe contar con recursos hardware suficientes para soportar el servicio web y las aplicaciones que se vayan a alojar, así como con la configuración de red y seguridad necesaria. Esto incluye la disponibilidad de los puertos requeridos (habitualmente HTTP y HTTPS), las correspondientes reglas de cortafuegos y, en caso de utilizar comunicaciones cifradas, la disponibilidad de certificados digitales válidos o acceso a la infraestructura de certificación.

# 5. PERFILADO DE CUMPLIMIENTO TÉCNICO

Antes de aplicar cualquier medida de seguridad específica sobre **Microsoft Windows Server Update Services,** es necesario implementar las medidas técnicas definidas por el ENS o ampliando el alcance del PCTE para entornos que manejan **Información Clasificada** mediante los requisitos de seguridad recogidos en la guía **CCN-STIC-570A25 Perfilado de Seguridad para Windows Server (DC o MS).**

Estas medidas, refuerzan la seguridad del Sistema Operativo Windows Server, proporcionando una base sólida y verificable sobre la que desplegar Exchange.

Por tanto, el perfil de aplicabilidad base, podrá ser:

a) ENS.

b) Difusión Limitada.

c) Información Clasificada.

Con el objetivo de facilitar la implementación de la configuración de seguridad definida bajo el presente documento, en la próxima tabla se recoge aquella agrupación de medidas de seguridad dependientes del grado de clasificación de la información y la categoría del sistema.

| | | CLASIFICACIÓN DE LA INFORMACIÓN/PERFIL | | |
|---|---|---|---|---|
| | | ENS | DIFUSIÓN LIMITADA | INFORMACIÓN CLASIFICADA |
| CATEGORÍA DEL SISTEMA DE INFORMACIÓN | BÁSICA | ✓ | ✗ | ✗ |
| | MEDIA | ✓ | ✗ | ✗ |
| | ALTA | ✓ | ✗ | ✗ |
| | DIFUSIÓN LIMITADA | ✗ | ✓ | ✗ |
| | CONFIDENCIAL<br>RESERVADO<br>SECRETO | ✗ | ✗ | ✓ |

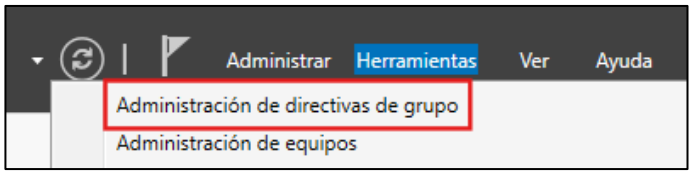
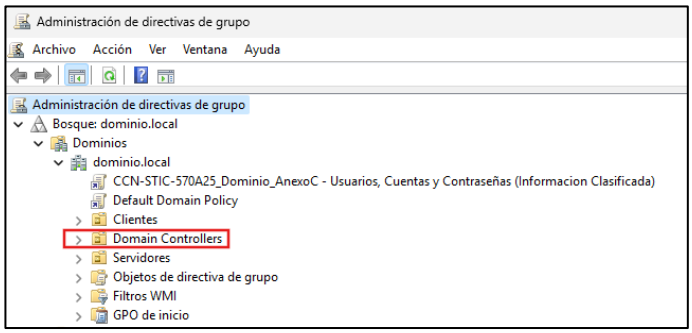
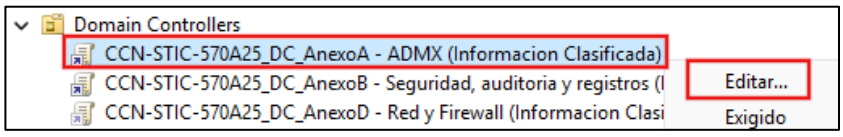
En los apartados siguientes se desarrollarán los controles específicos aplicables a Microsoft Windows Server Update Services, explicando su implementación técnica y las consideraciones específicas para entornos clasificados o de uso oficial. Solo tras aplicar estas medidas se procederá a la aplicación de seguridad específica de Microsoft Windows Server Update Services, garantizando una protección integral y alineada con la normativa vigente.

**Nota:** es posible obtener información sobre la interpretación de lo anteriormente comentado en el "Anexo II. Medidas de Seguridad" del ENS relativo a definición de medidas de seguridad.
- https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

# ANEXO A. APLICACIÓN DE SEGURIDAD SOBRE WINDOWS SERVER UPDATE SERVICES (WSUS)

## ANEXO A.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES WSUS MIEMBROS DE DOMINIO SOBRE WINDOWS SERVER 2025

### ANEXO A.1.1. PASO A PASO DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE EL DOMINIO

| Paso | Descripción |
|---|---|
| 1. | Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un Controlador de Dominio. |
| 2. | En el "Administrador del servidor", haga clic en "Herramientas" en la barra superior y seleccione "Administración de directivas de grupo".<br>  <br>*Ilustración 1 - Administración de directivas de grupo* |
| 3. | Despliegue en el panel izquierdo hasta llegar a la OU "Domain Controllers".<br>  <br>*Ilustración 2 - OU Domain Controllers* |
| 4. | Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO "CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)", y seleccione "Editar".<br>  <br>*Ilustración 3 - Edición de ADMX 570A25* |

| | |
|---|---|
| 5. | En el panel “Editor de administración de directivas de grupo”, despliegue la lista siguiendo la siguiente ruta: “**Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell**”. Haga clic sobre “Windows PowerShell” para consultar las políticas que aplica. |
| 6. | Haga doble clic sobre la política “Activar la ejecución de scripts”. |
| 7. | En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”. |
| 8. | Reinicie el controlador de dominio para que se aplique la configuración correctamente. |

| Configuración | Estado | Comentario |
|---|---|---|
| Activar registro de módulos | Habilitada | No |
| Activar el registro de bloque de script de PowerShell | Habilitada | No |
| Activar la ejecución de scripts | Habilitada | No |
| Activar la transcripción de PowerShell | Habilitada | No |
| Establecer la ruta de acceso de origen de Update-Help | No configurada | No |

*Ilustración 4 - Políticas de PowerShell*

c

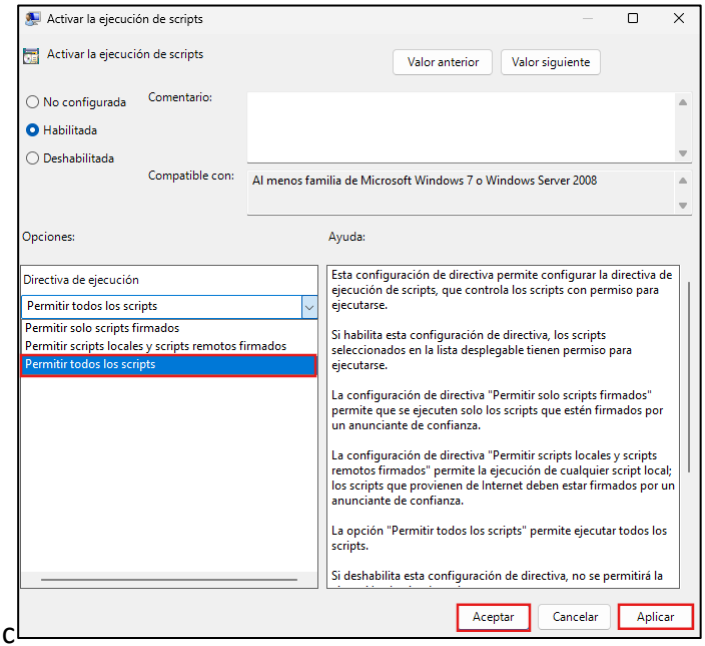
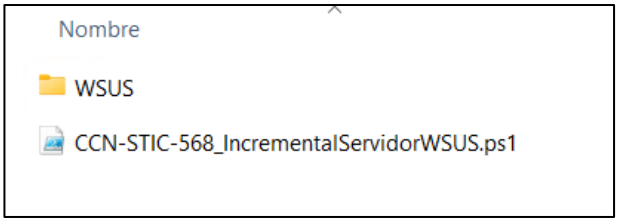
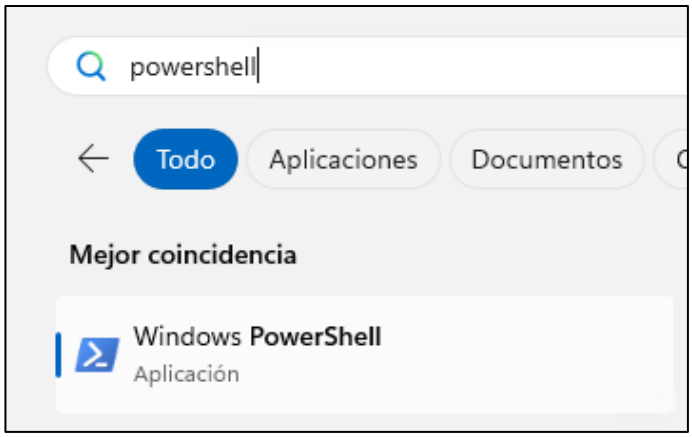
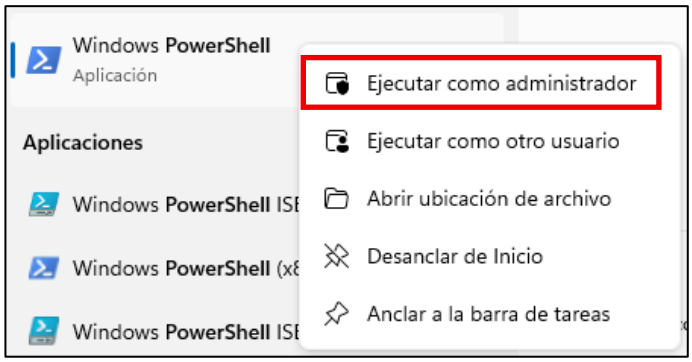
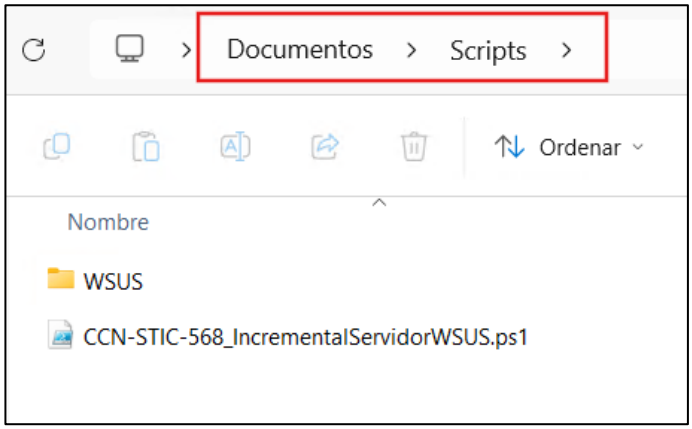
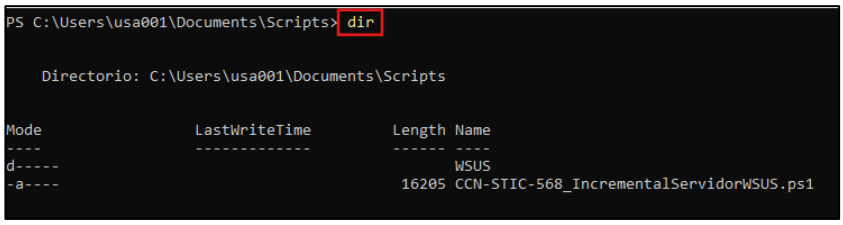
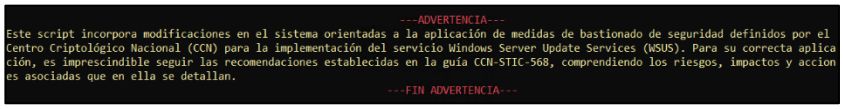
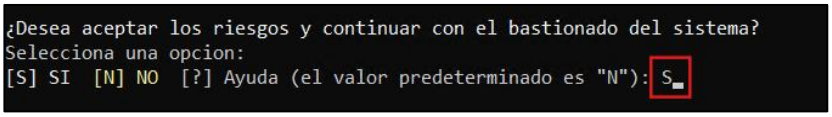
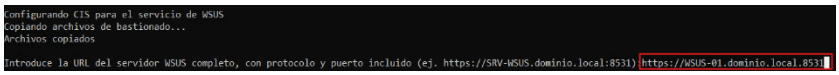



*Ilustración 5 - Selección de "Permitir todos los scripts"*

| | |
|---|---|
| 9. | Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta.<br>Verifique que en su interior se encuentran los siguientes archivos:<br>- Directorio: WSUS<br>- Fichero: CCN-STIC-568_IncrementalServidorWSUS.ps1<br>  <br>*Ilustración 6 - Copia de ficheros necesarios*<br>**Nota:** Adicionalmente, es necesario haber aplicado con anterioridad la guía CCN-STIC-574A25 Aplicación de seguridad sobre Microsoft Internet Information Services (IIS) 10. |
| 10. | Sobre la barra de búsqueda, escriba “PowerShell”:<br>  <br>*Ilustración 7 - Windows PowerShell* |

| | |
|---|---|
| 11. | Haga clic derecho, y seleccione “Ejecutar como administrador”:<br>  <br>*Ilustración 8 - Ejecución como administradorr*<br>**Nota:** Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada. |
| 12. | Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.<br>  <br>*Ilustración 9 - Copia de ruta* |
| 13. | Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.<br>  <br>*Ilustración 10 - Acceso a la ruta* |

| | |
|---|---|
| 14. | Ejecute el comando “dir” para verificar la ubicación y el contenido.<br>  <br>*Ilustración 11 - Contenido de la carpeta* |
| 15. | Ejecute el archivo “CCN-STIC-568_IncrementalServidorWSUS.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.<br>  <br>*Ilustración 12 - Ejecución del script* |
| 16. | A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:<br>  <br>*Ilustración 13 - Advertencia* |
| 17. | Escribir “S” y pulsar “Enter”.<br>  <br>*Ilustración 14 - Aceptación de advertencia* |
| 18. | Primero, se solicitará la URL completa del servidor. Esta dirección se aplicará en las directivas de grupo (GPO) de los equipos cliente, tanto en Windows Server 2025 como en Windows 11.<br>  <br>*Ilustración 15 – URL de Servidor WSUS.*<br>**Nota:** En el presente caso, se utiliza “WSUS-01” como el nombre del servidor de WSUS |

| | |
|---|---|
| 19. | Se crearán las directivas de grupo las cuales se vincularán a las OUs correspondientes. Se destacarán las siguientes GPOS:<br>- CCN-STIC-568 Incremental Servidores WSUS<br>- CCN-STIC-568 Incremental Windows 11 – Clientes WSUS<br>- CCN-STIC-568 Incremental Server2025 – Clientes WSUS |
| 20. | En el "Administrador del servidor", haga clic en "Herramientas" en la barra superior y seleccione "Administración de directivas de grupo". |

```
GpoId       : 76c8712f-7b9b-4507-befb-db82a7aff34a
DisplayName : CCN-STIC-568 Incremental Servidores WSUS
Enabled     : False
Enforced    : False
Target      : OU=Servidores WSUS,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local
Order       : 1

GPO vinculada a OU=Servidores WSUS,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local
```

*Ilustración 16 – GPO vinculada a Servidores WSUS.*

```
GpoId       : 343b0054-c211-477a-81fc-cc31eb994dd5
DisplayName : CCN-STIC-568 Incremental Windows 11 - Clientes WSUS
Enabled     : False
Enforced    : False
Target      : OU=Clientes,DC=dominio,DC=local
Order       : 1

GPO vinculada a OU=Clientes,DC=dominio,DC=local
```

*Ilustración 17 - GPO vinculada a Clientes*

```
GpoId       : 28e0eefd-682a-4bc8-bc8f-ef59a1e1bcec
DisplayName : CCN-STIC-568 Incremental Server2025 - Clientes WSUS
Enabled     : False
Enforced    : False
Target      : OU=Servidores,DC=dominio,DC=local
Order       : 1

GPO vinculada a OU=Servidores,DC=dominio,DC=local
```

*Ilustración 18 - GPO vinculada a Servidores*

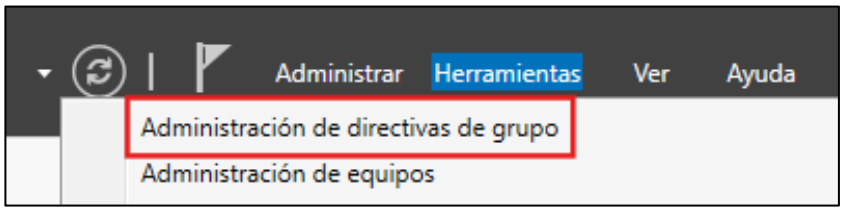
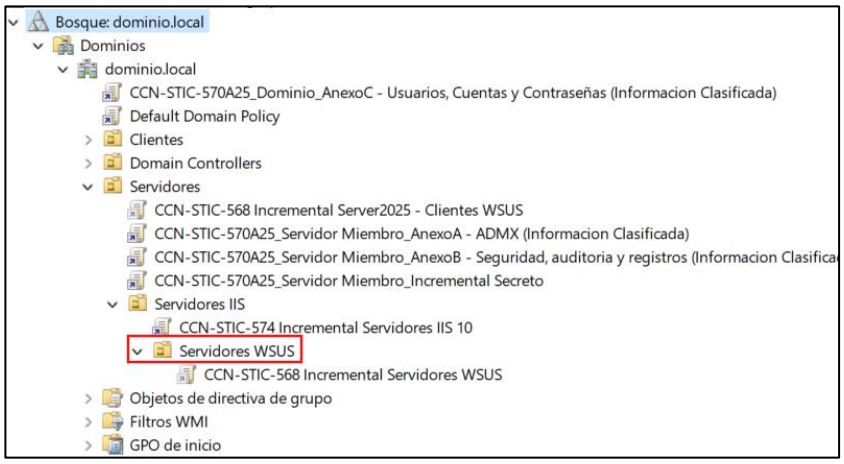
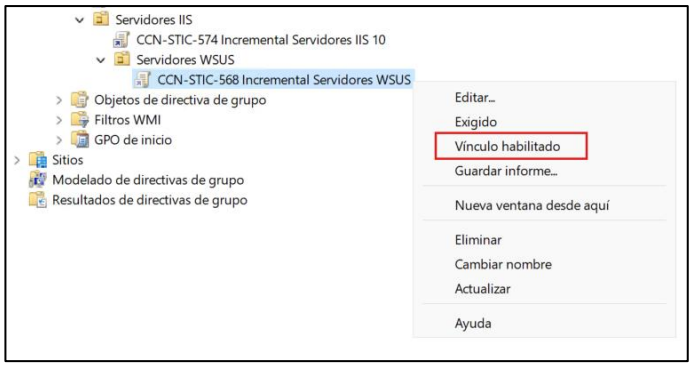
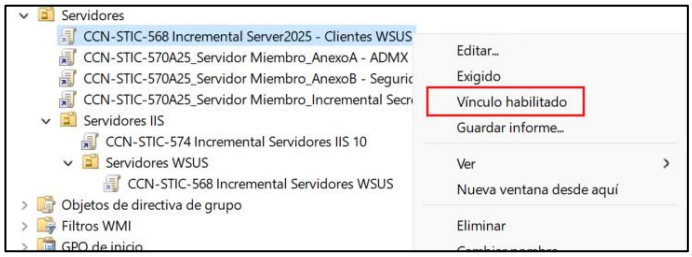
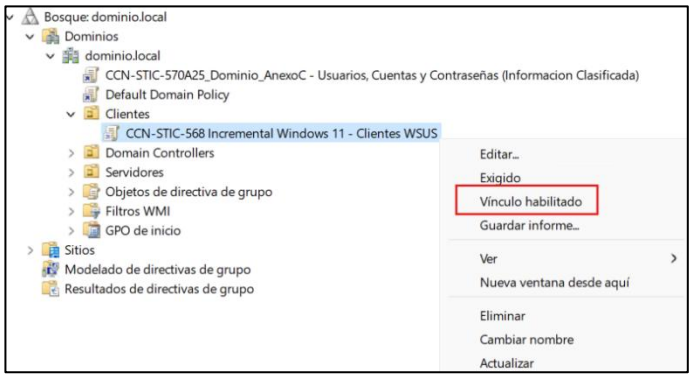
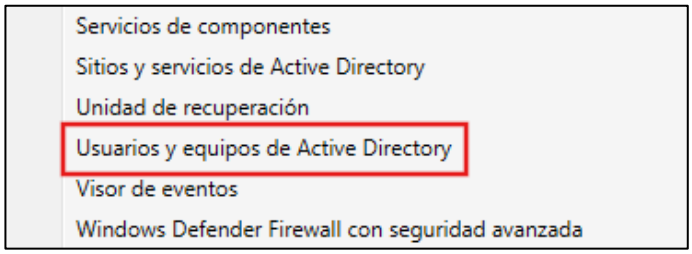
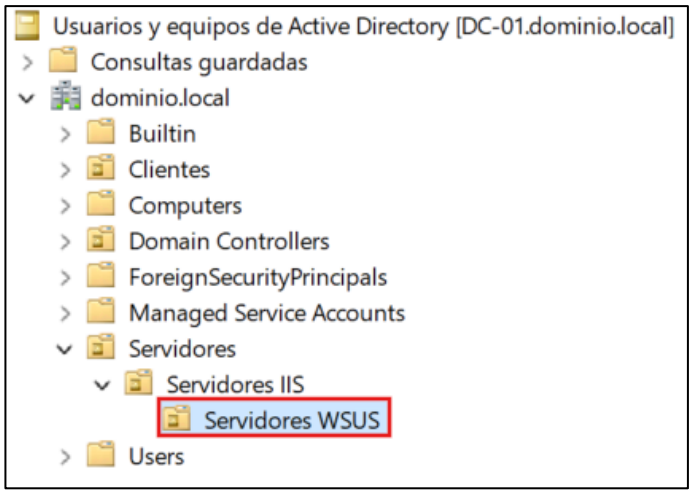
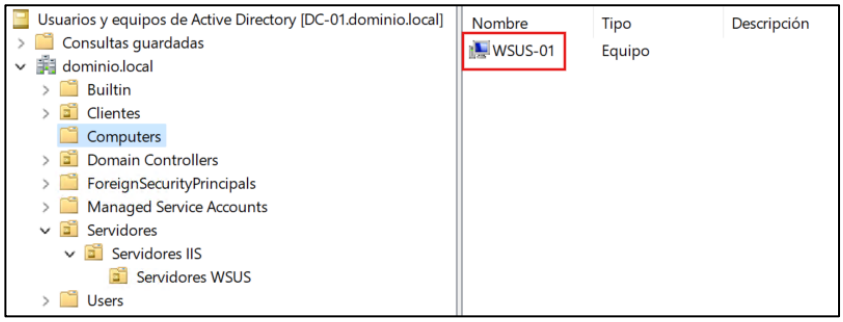
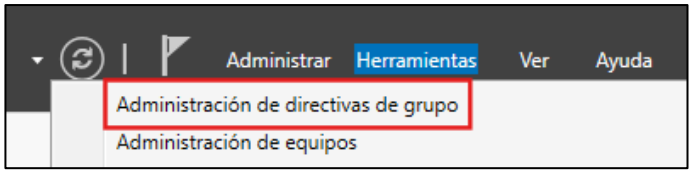
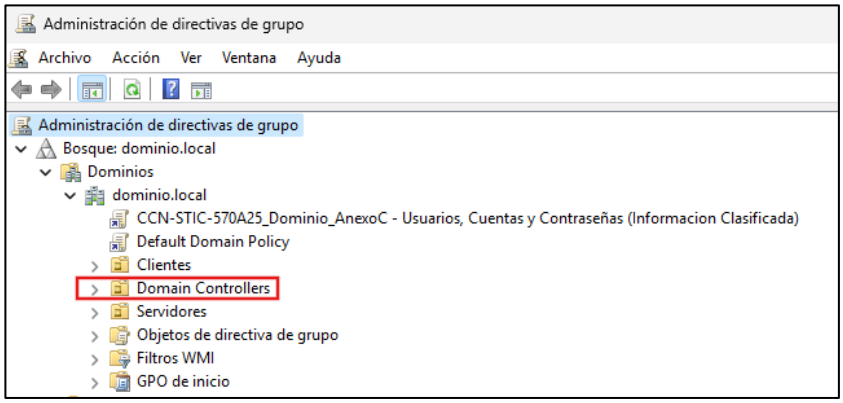



*Ilustración 19 - Administración de directivas de grupo*

| | |
|---|---|
| 21. | Despliegue la lista del menú izquierdo hasta localizar el dominio y, a continuación, acceda a la Unidad Organizativa de Servidores WSUS.<br>  <br>*Ilustración 20 - UO de Servidores WSUS* |
| 22. | Despliegue dicha OU y haga clic derecho sobre el GPO “CCN-STIC-568 Incremental Servidores WSUS”. Seleccione la opción “Vínculo habilitado”.<br>  <br>*Ilustración 21 - Vinculo habilitado GPO* |
| 23. | A continuación, habilite la GPO de equipos cliente para Windows Server 2025. Esta se encuentra por defecto en la OU de Servidores.<br>  <br>*Ilustración 22 - Vínculo habilitado GPO clientes* |

| | |
|---|---|
| 24. | Finalmente, habilite la GPO de equipos cliente para Windows 11. Esta se encuentra por defecto en la OU de Clientes.<br>  <br><br>*Ilustración 23 - Vínculo habilitado GPO clientes 2* |
| 25. | De nuevo en el "Administrador del servidor", haga clic en "Herramientas" en la barra superior, y seleccione "Usuarios y equipos de Active Directory".<br>  <br><br>*Ilustración 24 - Usuarios y equipos de Active Directory* |
| 26. | Despliegue la lista del panel izquierdo hasta visualizar la OU "Servidores WSUS".<br>  <br><br>*Ilustración 25 - OU Servidores WSUS* |

| | |
|---|---|
| 27. | Haga clic sobre la carpeta “Computers” y seleccione el servidor WSUS.<br>  <br>*Ilustración 26 - Selección del servidor.* |
| 28. | Arrástrelo a la OU “Servidores WSUS”. Aparecerá una advertencia. Haga clic en “Sí”. |
| 29. | A continuación, arrastre los distintos equipos cliente, tanto Windows Server 2025 como Windows 11, a las OUs correspondientes. |
| 30. | A continuación, reinicie uno a uno los controladores de dominio para que se les aplique el GPO de Dominio. Una vez hecho, reinicie tanto el servidor WSUS, como los equipos clientes que se correspondan para que se les apliquen los GPOs de Dominio de Servidor. |
| 31. | Finalmente, inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Controlador de Dominio. |
| 32. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.<br>  <br>*Ilustración 27 - Administración de direcitvas de grupo* |
| 33. | Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.<br>  <br>*Ilustración 28 - OU Domain Controllers* |

| | |
|---|---|
| 34. | Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”. |
| 35. | En el panel izquierdo, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para ver las políticas que aplica |
| 36. | Haga doble clic sobre la política “Activar la ejecución de scripts”. |
| 37. | En el desplegable de la política, seleccione “Permitir solo scripts firmados”, y haga clic en “Aplicar” y “Aceptar”. |
| 38. | Reinicie el controlador de dominio para que se aplique la configuración correctamente. |

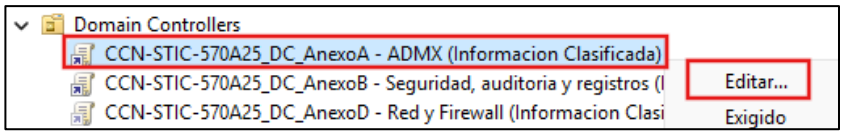



*Ilustración 29 - Edición ADMX 570A25*

| Configuración | Estado | Comentario |
|---|---|---|
| Activar registro de módulos | Habilitada | No |
| Activar el registro de bloque de script de PowerShell | Habilitada | No |
| Activar la ejecución de scripts | Habilitada | No |
| Activar la transcripción de PowerShell | Habilitada | No |
| Establecer la ruta de acceso de origen de Update-Help | No configurada | No |

*Ilustración 30 - Políticas de PowerShell*

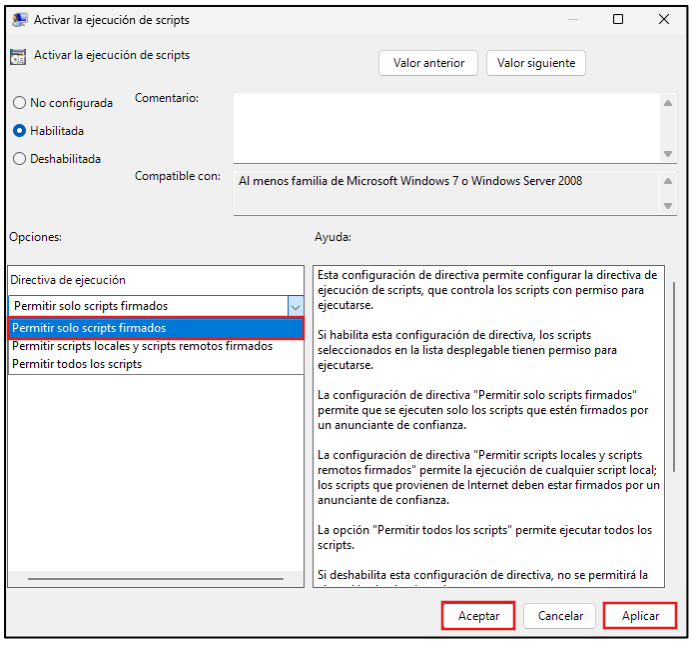
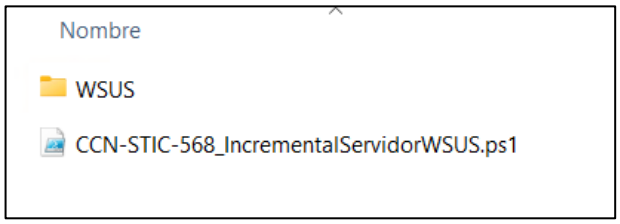
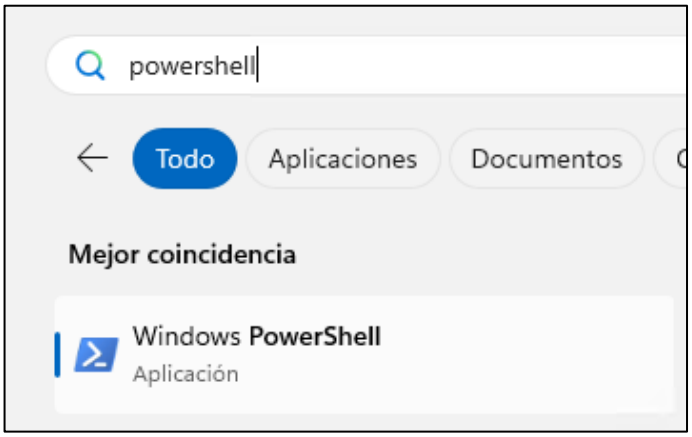
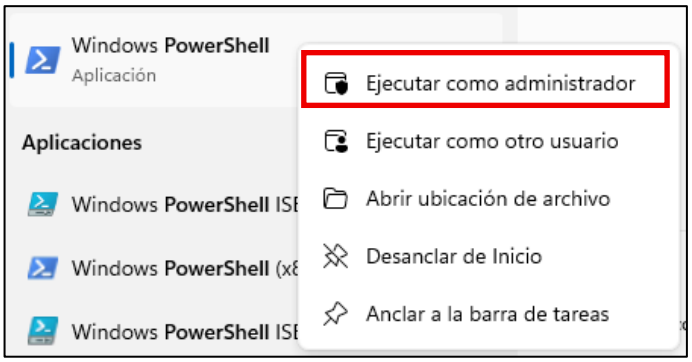
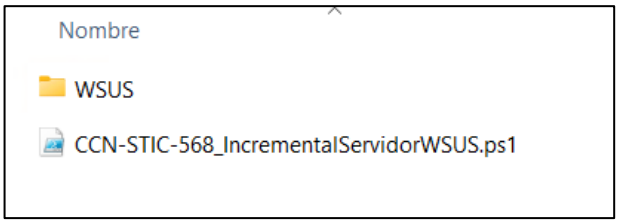
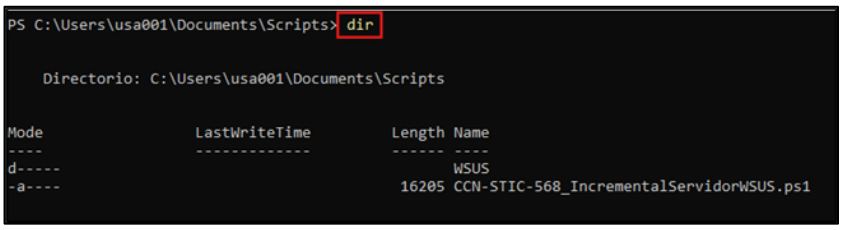
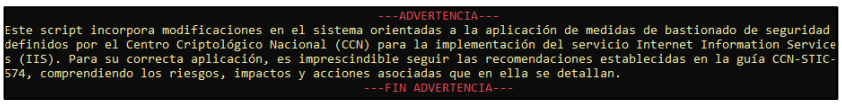
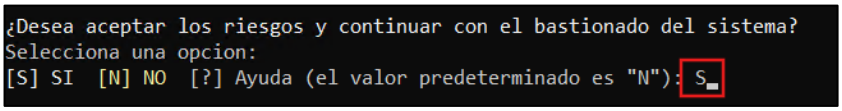
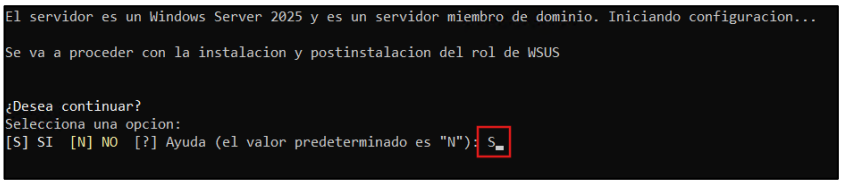



*Ilustración 31 - Selección de "Permitir solo scripts firmados"*

## ANEXO A.1.2. PASO A PASO DE CONFIGURACIÓN DE SEGURIDAD EN SERVIDOR WSUS

| Paso | Descripción |
|---|---|
| 1. | Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor WSUS. |
| 2. | Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta.<br>Verifique que en su interior se encuentran los siguientes archivos:<br>- Directorio: WSUS<br>- Fichero: CCN-STIC-568_IncrementalServidorWSUS.ps1<br>  <br>*Ilustración 32 - Archivos asociados a la guía* |
| 3. | Sobre la barra de búsqueda, escriba "PowerShell":<br>  <br>*Ilustración 33 - Windows PowerShell* |

| | |
|---|---|
| 4. | Haga clic derecho, y seleccione “Ejecutar como administrador”:<br>  <br>*Ilustración 34 - Ejecución como administrador*<br>**Nota:** Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada. |
| 5. | Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.<br>  <br>*Ilustración 35 - Copia de ruta* |
| 6. | Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.<br>  <br>*Ilustración 36 - Acceso a la ruta* |
| 7. | Ejecute el comando “dir” para verificar la ubicación y el contenido.<br>  <br>*Ilustración 37 - Contenido de la carpeta* |

| | |
|---|---|
| 8. | Ejecute el archivo “CCN-STIC-568_IncrementalServidorWSUS.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.<br>  <br>*Ilustración 38 - Ejecución del script* |
| 9. | A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:<br>  <br>*Ilustración 39 - Advertencia* |
| 10. | Escribir “S” y pulsar “Enter”.<br>  <br>*Ilustración 40 - Aceptación de advertencia* |
| 11. | A continuación, aparecerá un mensaje informativo comentando que se procederá con la instalación y postinstalación del rol de WSUS en el propio servidor miembro del dominio. Escribir “S” y pulsar “Enter”.<br>  <br>*Ilustración 41 - Mensaje de instalación WSUS*<br>**Nota:** El ejemplo de la guía se basa en un servidor miembro del dominio recién instalado. Si el servidor ya estaba configurado antes de aplicar la guía, la ubicación del contenido de los archivos de WSUS será la correspondiente a la configuración existente. |
| 12. | Espere a que finalice la instalación. Después, indique la ruta para almacenar el contenido de WSUS (en el presente caso, “C:\WSUS”) y se iniciará la postinstalación.<br>  <br>*Ilustración 42 - Ubicación archivos WSUS* |
| 13. | Una vez haya terminado la ejecución del script, cierre la consola de PowerShell. |

| | |
|---|---|
| 14. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Windows Server Update Services”. |

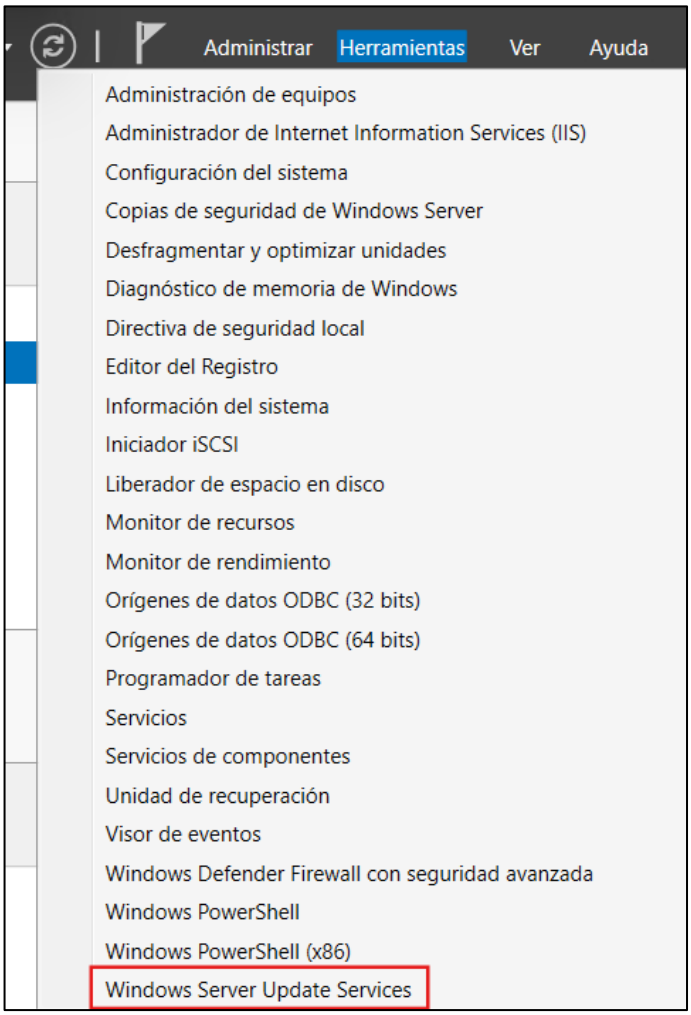



*Ilustración 43 - Windows Server Update Services*

| | |
|---|---|
| 15. | Se abrirá la consola de administración de Windows Server Update Services diríjase en el menú de la izquierda a “Opciones”. |

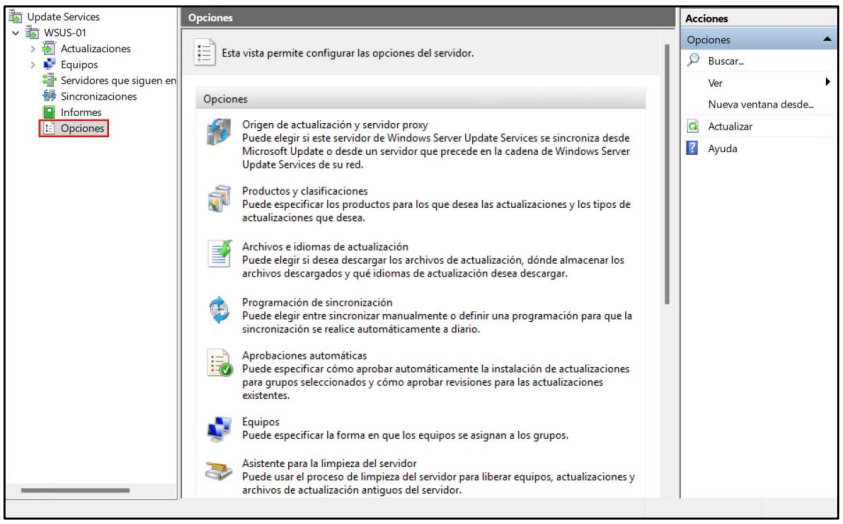



*Ilustración 44 - Opciones de WSUS*

| | |
|---|---|
| 16. | En la pestaña “Opciones”, pinche en “Equipos”. |

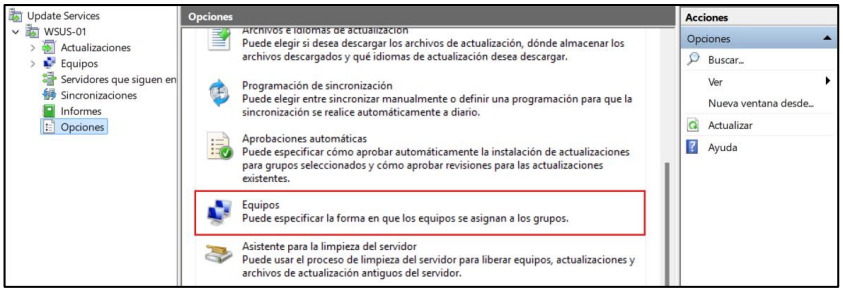
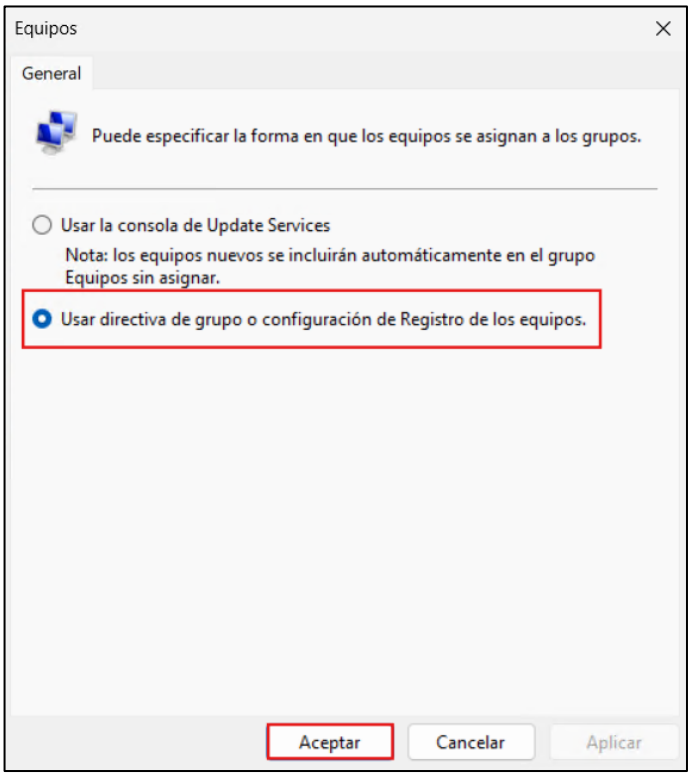
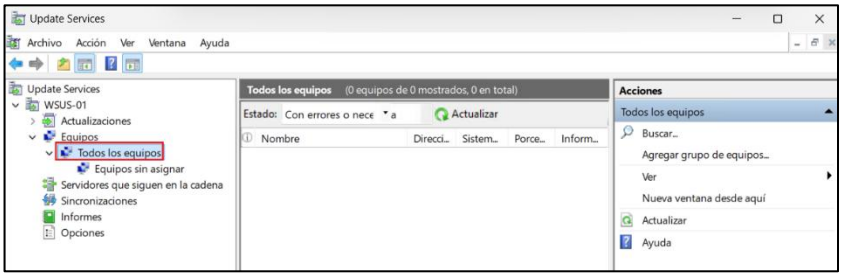
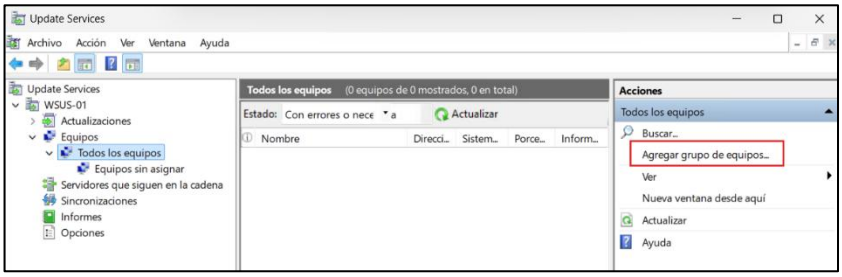
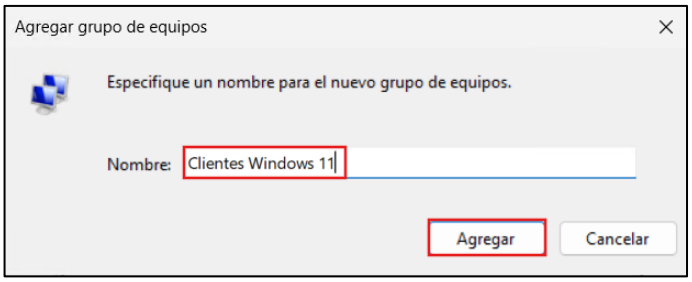
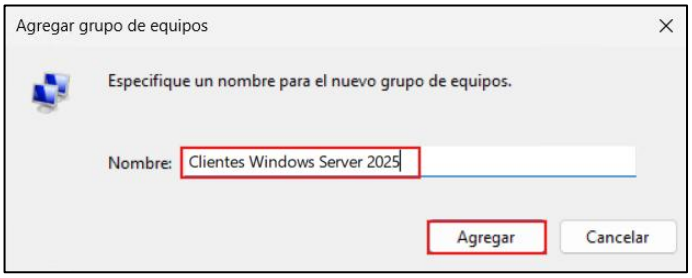
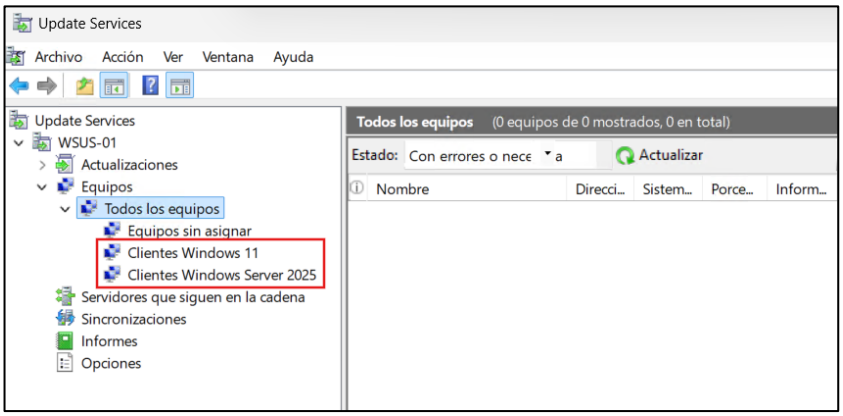



*Ilustración 45 - Opciones de equipos*

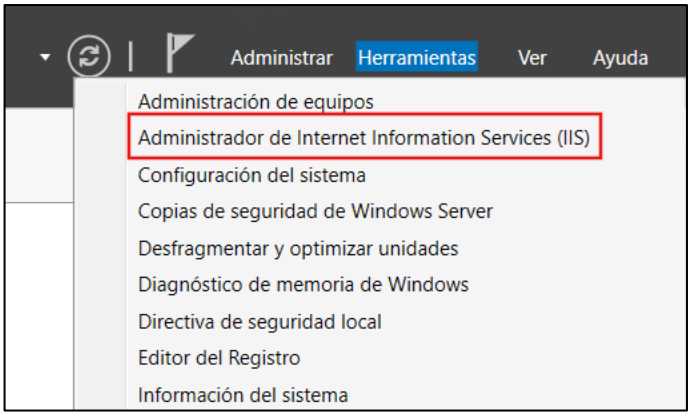
| | |
|---|---|
| 17. | Se abrirá una nueva ventana, deberá marcar la segunda opción: "Usar directiva de grupo o configuración de Registro de los equipos". Pulse en "Aceptar" para guardar los cambios.<br>  <br><br>*Ilustración 46 - Opción para los archivos de WSUS* |
| 18. | A continuación, se crearán los grupos de equipos correspondientes a Windows 11 y Windows Server 2025 desde la consola de WSUS. Para ello, sitúese en el menú en "Todos los equipos".<br>  <br><br>*Ilustración 47 - Grupos de equipos* |

| | |
|---|---|
| 19. | En la parte de la derecha, pinche en “Agregar grupo de equipos…”.<br>  <br>*Ilustración 48 - Agregar grupo* |
| 20. | Se abrirá una ventana, donde se deberá indicar el nombre del grupo que se va a crear, añada “Clientes Windows 11”. Pulse en “Agregar”.<br>  <br>*Ilustración 49 - Grupo Windows 11* |
| 21. | Seguidamente, agregue también el grupo de clientes Windows Server 2025 de la misma manera que se agregó el anterior.<br>  <br>*Ilustración 50 - Grupo Windows Server 2025* |

| | |
|---|---|
| 22. | Se habrán agregado los grupos en la pestaña de “Equipos > Todos los equipos”, tal y como se muestra en la imagen.<br>  <br>*Ilustración 51 - Grupos creados* |

## ANEXO A.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD

### ANEXO A.2.1. PROTEGER WSUS CON EL PROTOCOLO SSL

| Paso | Descripción |
|---|---|
| 1. | Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor WSUS. |
| 2. | Ejecute la consola de Administrador de Internet Information Services (IIS) desde el menú “Inicio > Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)”.<br>  <br>*Ilustración 52 - Administrador de IIS* |

| | |
|---|---|
| 3. | En la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, diríjase a "(Su servidor IIS) > Sitios > Administración de WSUS > SimpleAuthWebService" |

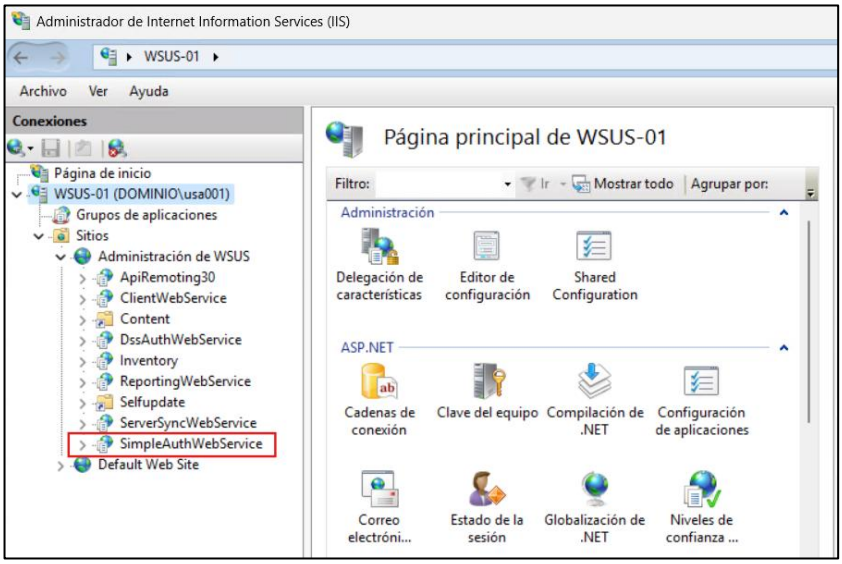



*Ilustración 53 - Sitio SimpleAuthWebService*

| | |
|---|---|
| 4. | En la página principal de "/SimpleAuthWebService", haga doble clic sobre la característica "Configuración SSL". |

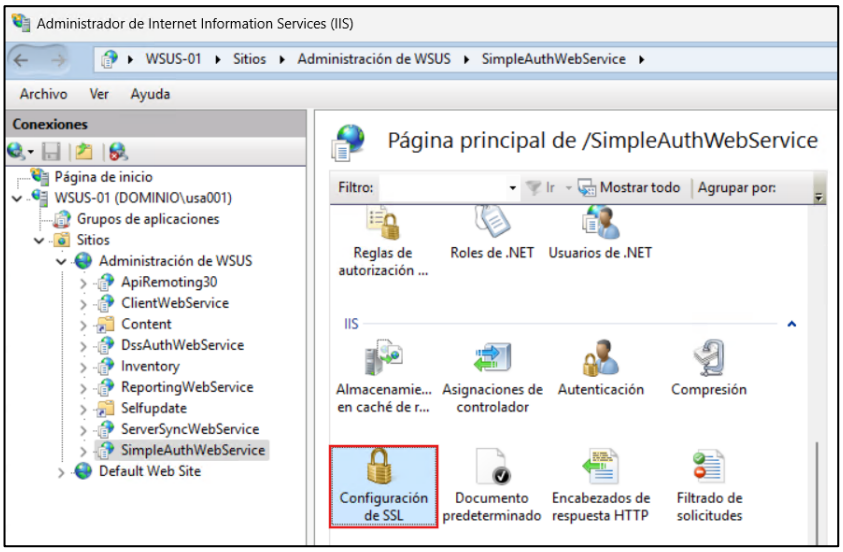
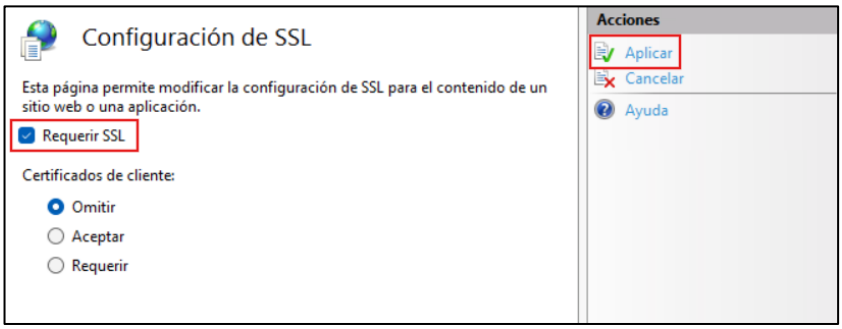
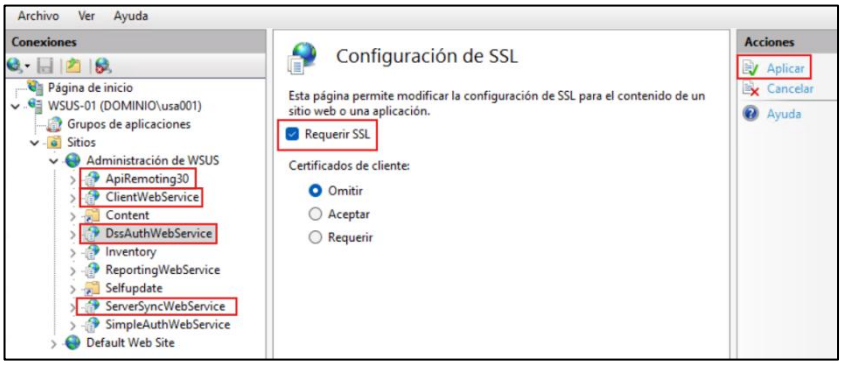
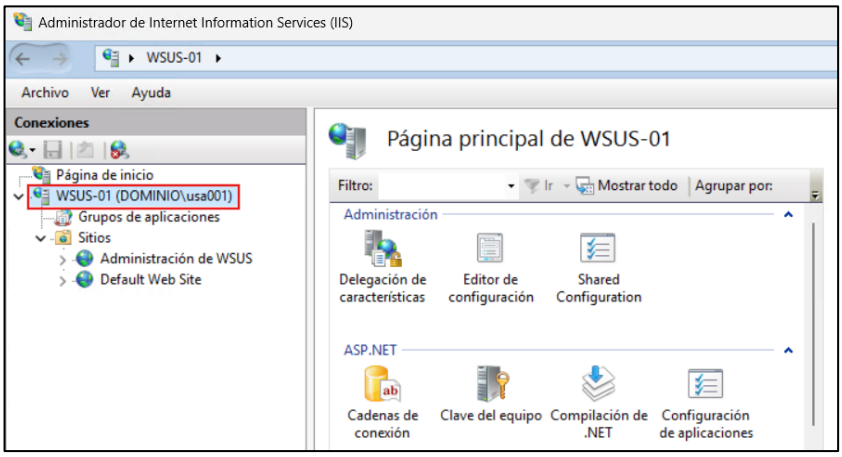
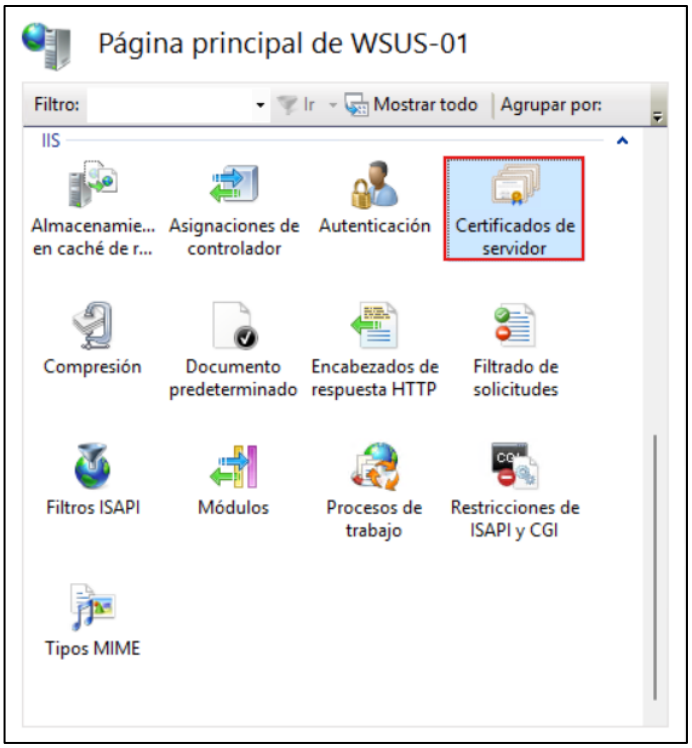
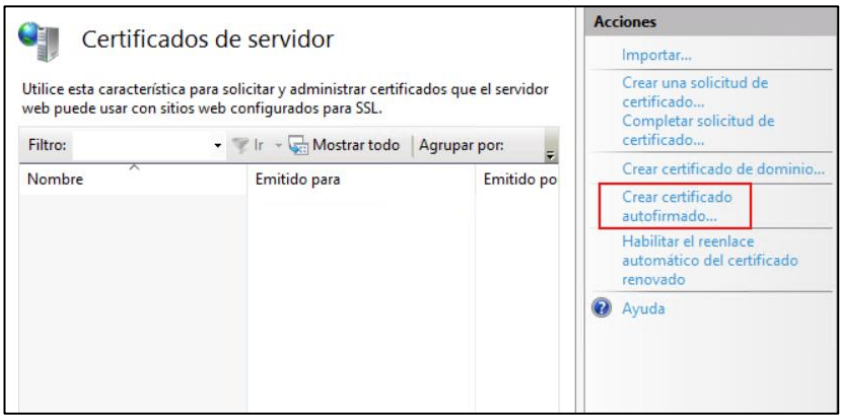
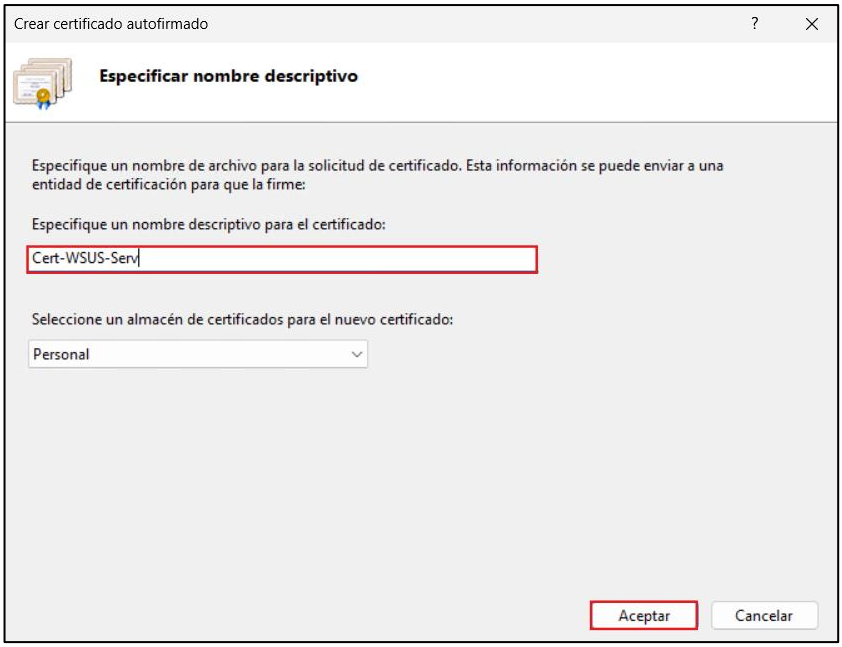
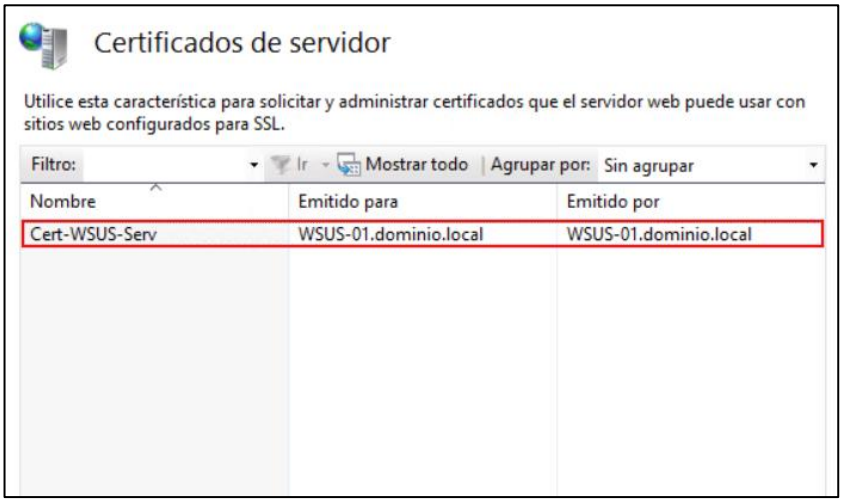
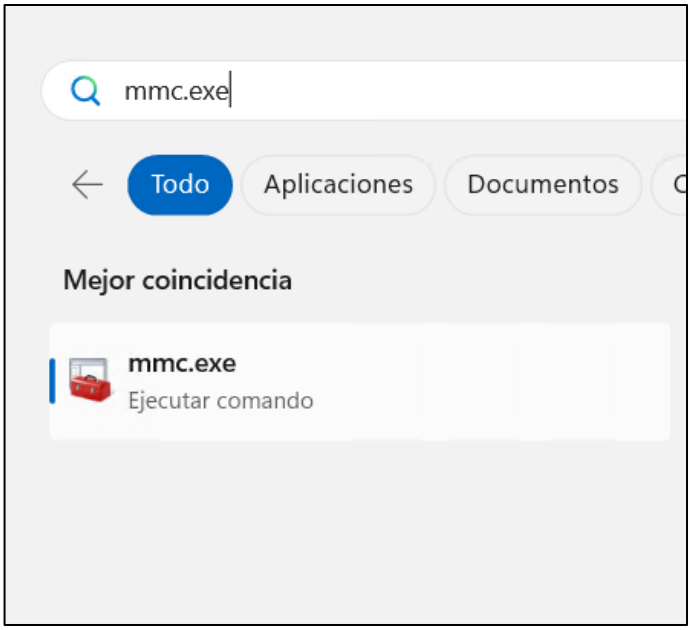



*Ilustración 54 - Configuración SSL de SimpleAuthWebService*

| | |
|---|---|
| 5. | Dentro de la característica "Configuración de SSL", debe habilitar la pestaña de "Requerir SSL". A continuación, pinche en "Aplicar" para guardar los cambios.<br>  <br>*Ilustración 55 - Aplicar requerimiento SSL* |
| 6. | De igual modo que se ha aplicado el requerimiento SSL en SimpleAuthWebService, se habilitará en las páginas siguientes:<br>- /DssAuthWebService<br>- /ServerSyncWebService<br>- /ApiRemoting30<br>- /ClientWebService<br>  <br>*Ilustración 56 - Configuración SSL de las páginas de WSUS* |

| | |
|---|---|
| 7. | A continuación, diríjase en la consola de Administrador de Internet Information Services (IIS), en la parte izquierda, a “Página de inicio > (Su servidor IIS)”.<br>  <br><br>*Ilustración 57 - Página principal IIS* |
| 8. | En la parte central de la consola, haga doble clic en “Certificados de servidor”.<br>  <br><br>*Ilustración 58 - Certificados de servidor* |

| | |
|---|---|
| 9. | Dentro de “Certificados de servidor”, en la columna de la derecha pulse sobre “Crear certificado autofirmado…”<br>  <br>*Ilustración 59 - Crear certificado autofirmado* |
| 10. | Se abrirá una ventana donde se indicará el nombre y el almacenamiento del certificado. Cuando haya proporcionado un nombre, pulse en “Aceptar” para continuar.<br>  <br>*Ilustración 60 - Especificar nombre de certificado*<br>**Nota:** En este ejemplo se utiliza el nombre descriptivo como Cert-WSUS-Server. |

| | |
|---|---|
| 11. | Se habrá creado el certificado en “Certificados del servidor”.<br>  <br><br>*Ilustración 61 - Certificado creado* |
| 12. | A continuación, se procederá a exportar el certificado. Para ello, ejecute sobre la barra de búsqueda “mmc.exe” y ejecútelo.<br>  <br><br>*Ilustración 62 - mmc.exe* |

| | |
|---|---|
| 13. | Se abrirá la consola MMC, seguidamente pinche en “Archivo > Agregar o quitar complemento...”. |

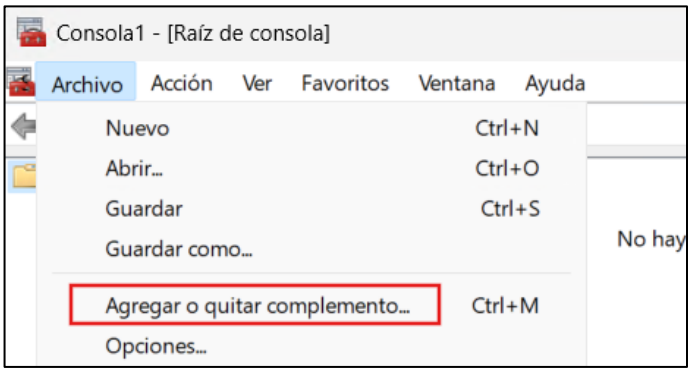



*Ilustración 63 - Agregar complemento*

| | |
|---|---|
| 14. | En “Agregar o quitar complemento” seleccione “Certificados” y pulse en “Agregar”. |

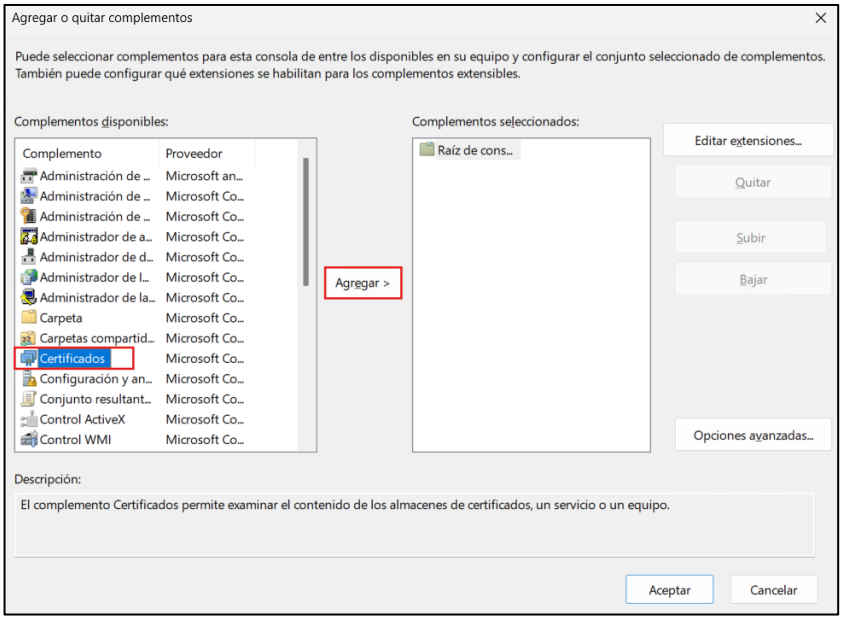
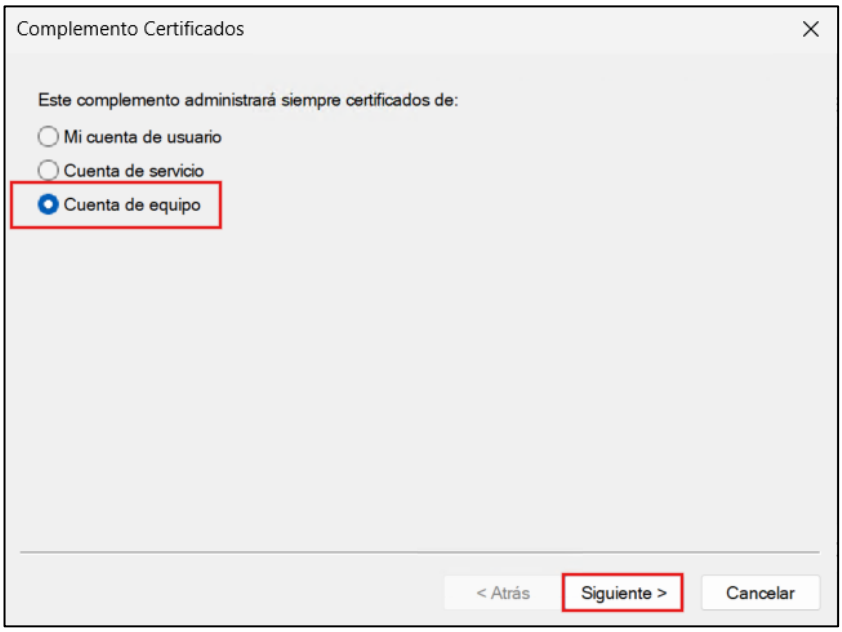
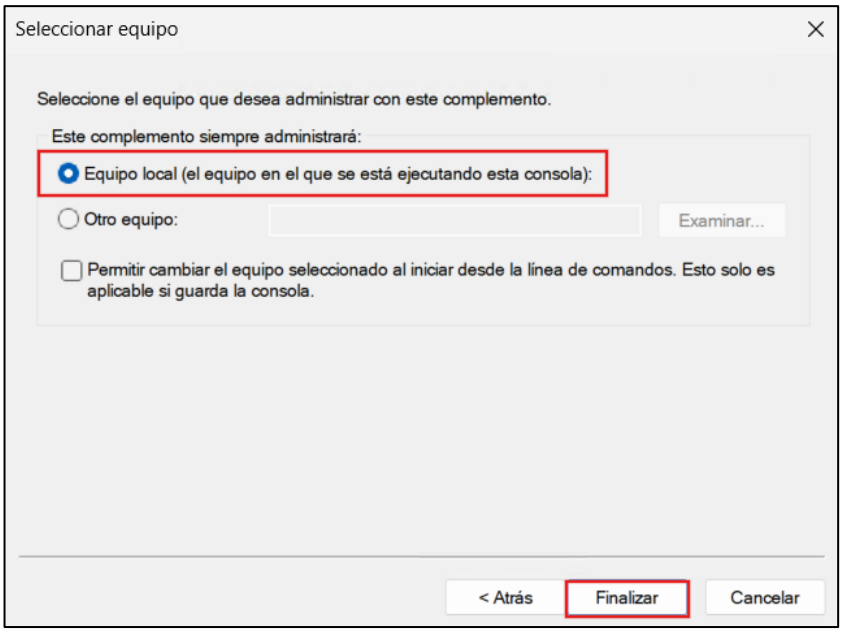
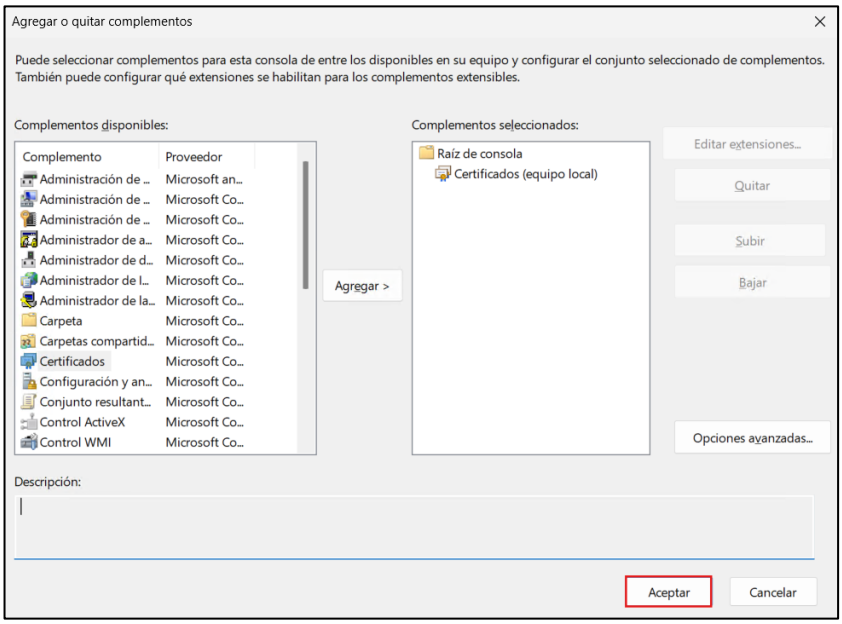
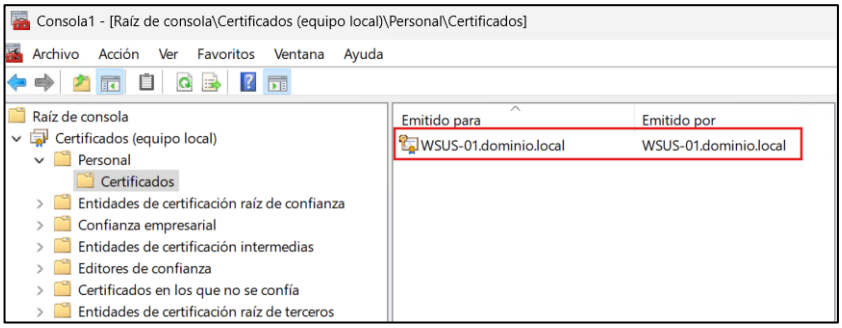



*Ilustración 64 - Agregar certificados*

| | |
|---|---|
| 15. | En la venta de “Complemento Certificados”, seleccione “Cuenta de equipo” y pulse en “Siguiente”.<br>  <br>*Ilustración 65 - Cuenta de equipos de certificados* |
| 16. | Seleccione “Equipo Local (el equipo en el que se está ejecutando esta consola)” en la ventana siguiente, seguidamente pulse “Finalizar”.<br>  <br>*Ilustración 66 - Certificado en equipo local* |

| | |
|---|---|
| 17. | Pulse en “Aceptar” en la ventana de “Agregar o quitar complementos” para guardar los cambios.<br>  <br>*Ilustración 67 - Aceptar complementos de certificados* |
| 18. | 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.<br>  <br>*Ilustración 68 - Certificado instalado* |

| | |
|---|---|
| 19. | 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 …” |
| 20. | Se abrirá el “Asistente para exportar certificados”, pulse “Siguiente” para continuar. |
| 21. | En “Exportar la clave privada”, seleccione “No exportar la clave privada” y pulse en “Siguiente”. |

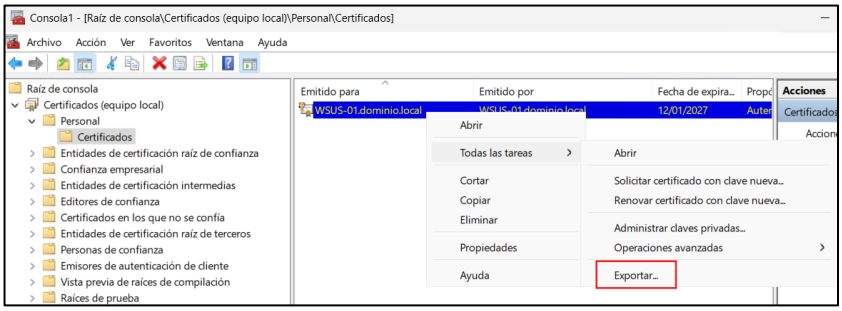



*Ilustración 69 - Exportar certificado*

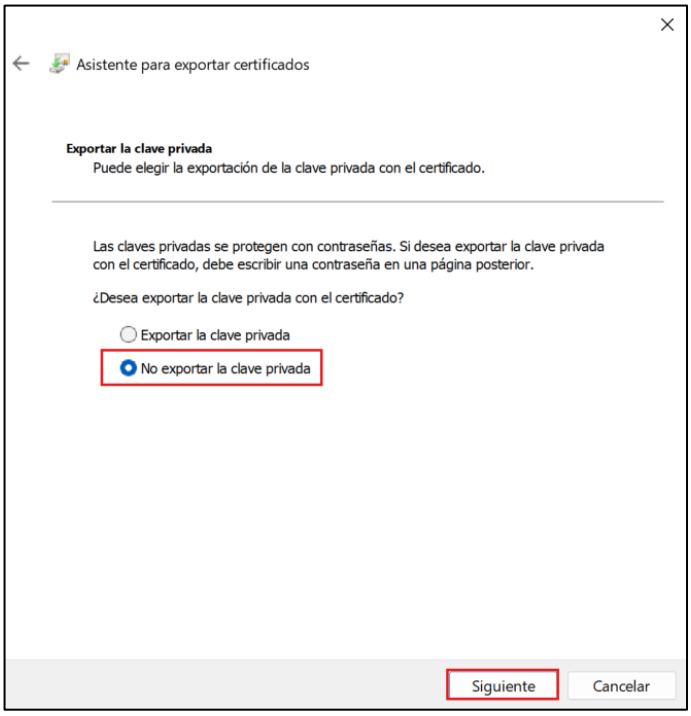
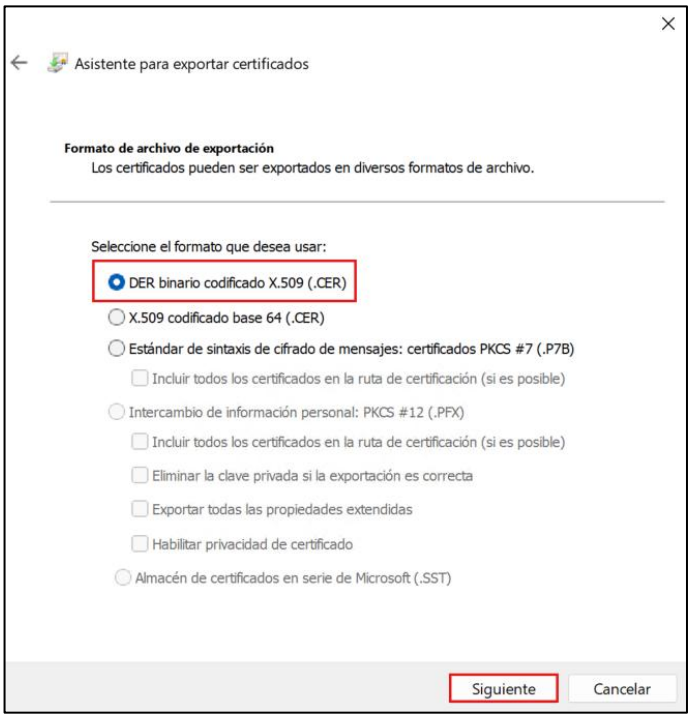



*Ilustración 70 - No exportar clave privada*

| | |
|---|---|
| 22. | Para el formato de archivo de exportación, deje seleccionado “DER binario codificado X.509 (.CER)”, seguidamente pulse “Siguiente”.  |

23. A continuación, pulse en “Examinar”, e indique la ubicación y el nombre del certificado exportado y pulse en “Guardar”.

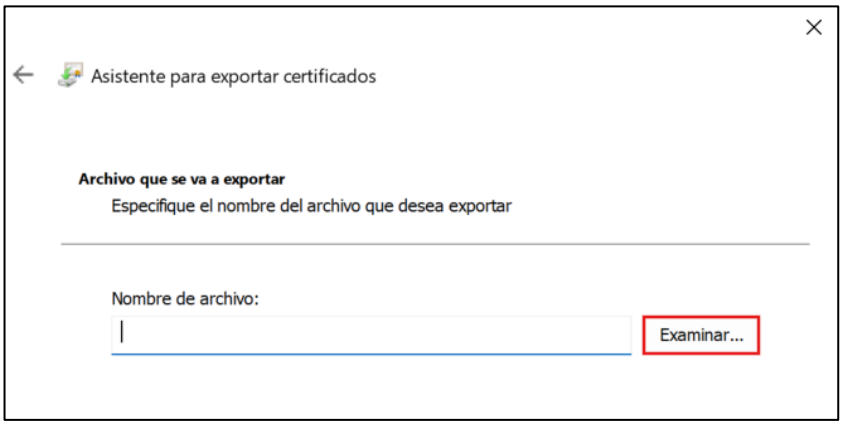



*Ilustración 71 - Examinar nombre*

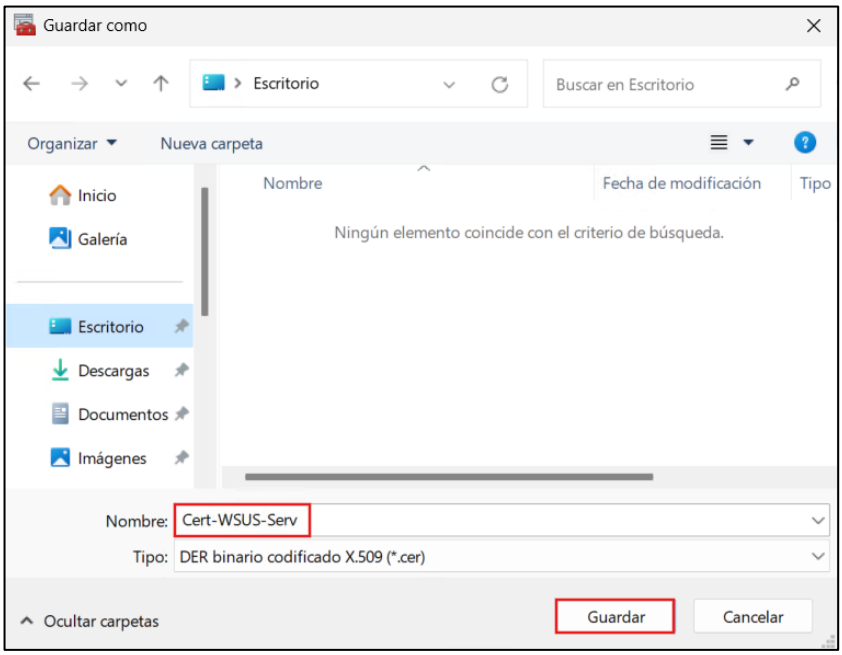
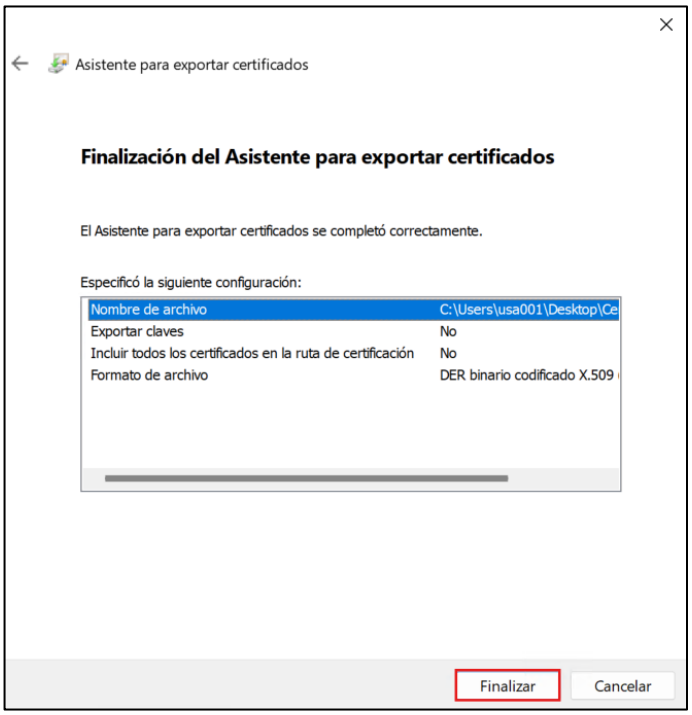
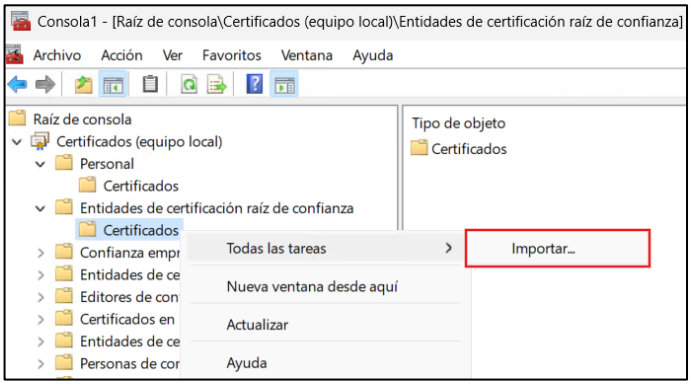
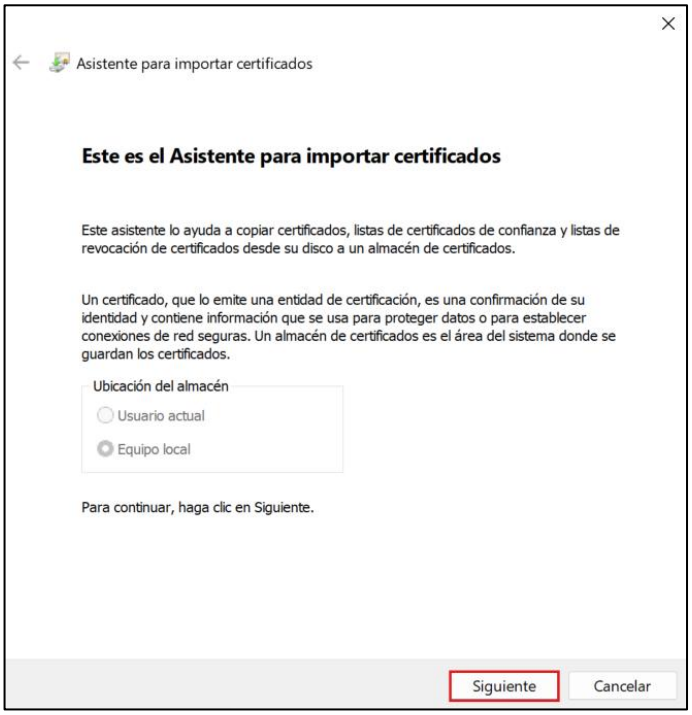
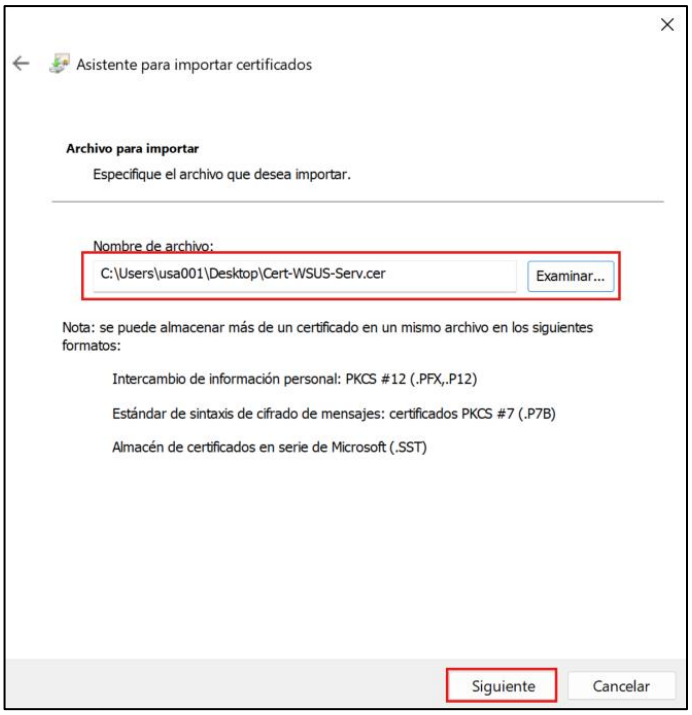
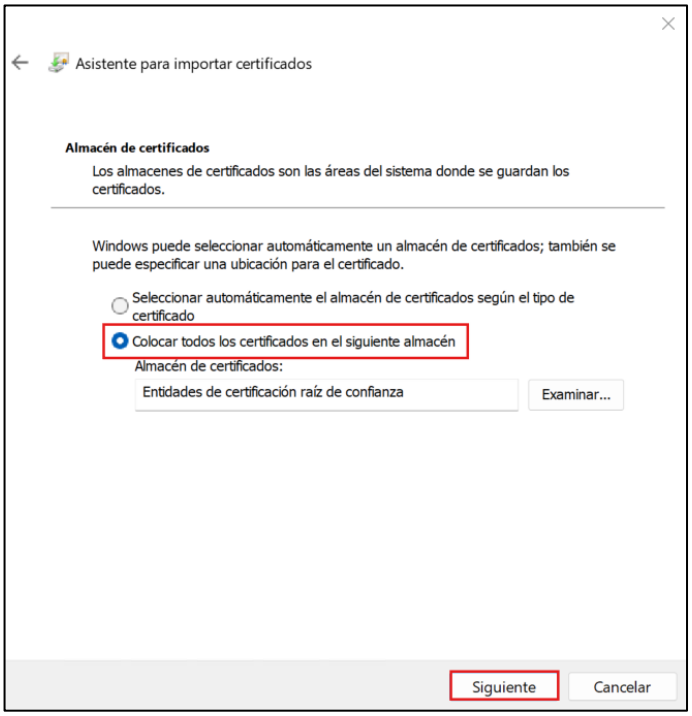
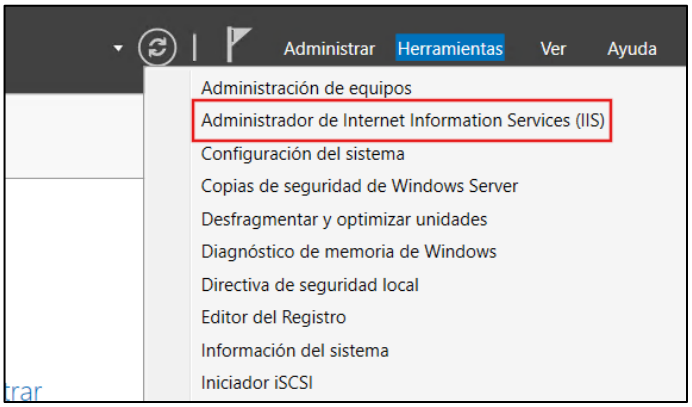


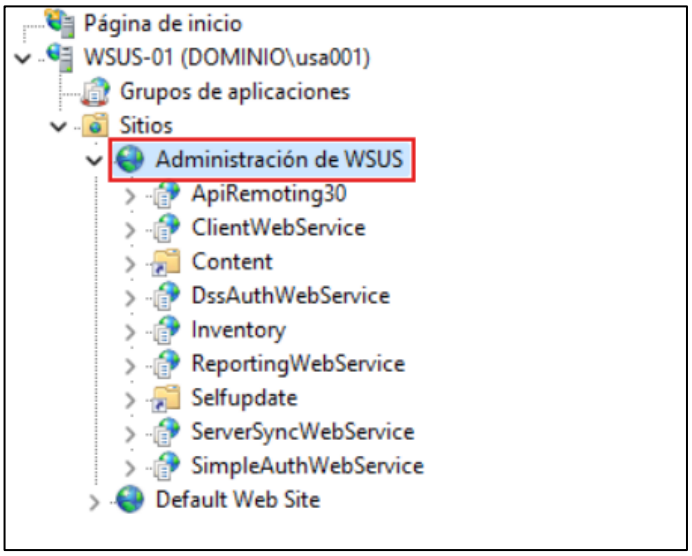
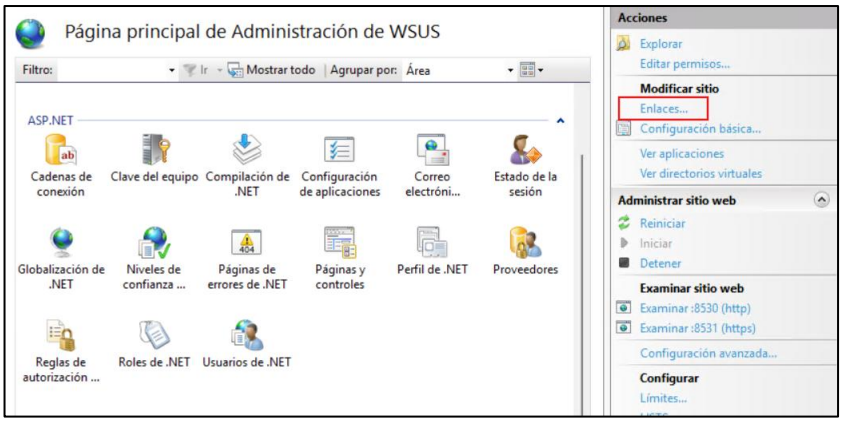

*Ilustración 72 - Nombre importado certificado*

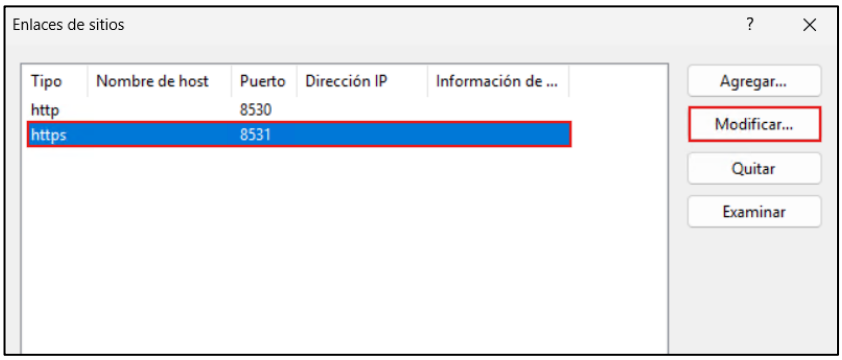
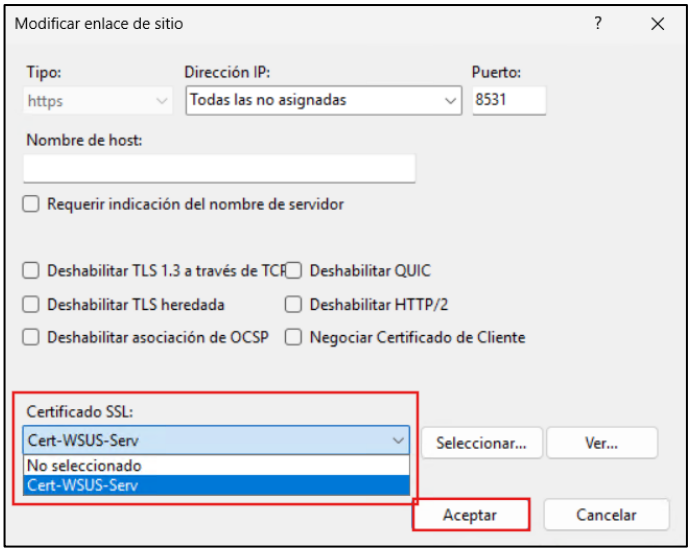
**Nota:** Deberá almacenar el certificado en un sitio seguro y que no olvide, ya que volverá a utilizar el certificado exportado para asignarlo a una GPO que aplique a todos los equipos clientes del servidor WSUS.

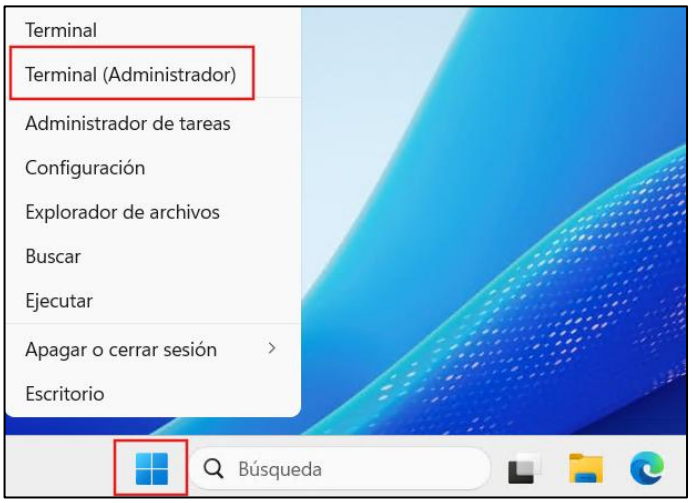
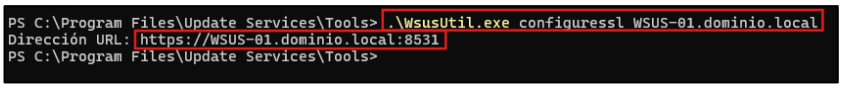
| | |
|---|---|
| 24. | El asistente para exportar certificados mostrará un resumen de la configuración que usted ha facilitado, indicándole que la exportación se ha realizado correctamente. Pulse en “Finalizar” para terminar con la exportación.<br>  <br>*Ilustración 73 - Resumen de certificado exportado* |
| 25. | 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”.<br>  <br>*Ilustración 74 - Importar certificado* |

| | |
|---|---|
| 26. | Se abrirá el asistente de importación de certificados, pulse “Siguiente” para continuar.<br>  <br>*Ilustración 75 - Información Asistente de certificados* |
| 27. | Importe el certificado que acaba de exportar, para ello, pulse en “Examinar” y selecciónelo. Pulse “Siguiente” para continuar.<br>  <br>*Ilustración 76 - Importar certificado* |

| | |
|---|---|
| 28. | Deje seleccionado “Colocar todos los certificados en el siguiente almacén” como almacén de certificados. Pulse “Siguiente” para continuar. Pulse “Siguiente” para continuar.<br>  <br>*Ilustración 77 - Almacén de certificados* |
| 29. | Pulse “Finalizar” para terminar con la importación. |
| 30. | Ejecute la consola de Administrador de Internet Information Services (IIS) desde el menú “Inicio > Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)”.<br>  <br>*Ilustración 78 - Herramienta IIS* |

| | |
|---|---|
| 31. | Dentro de la consola de IIS, sitúese en la parte izquierda en “Página de inicio > <<su servidor WSUS>> > Sitios > Administración de WSUS”.<br>  <br>*Ilustración 79 - Sitio de WSUS en IIS* |
| 32. | Pinche sobre “Enlaces” que se encuentra en la parte da la derecha.<br>  <br>*Ilustración 80 - Enlaces del sitio de WSUS* |

| | |
|---|---|
| 33. | En el asistente de “Enlaces de sitios”, seleccione HTTPS y seguidamente pulse en “Modificar…”.<br>  <br>*Ilustración 81 - Modificar https* |
| 34. | En la siguiente ventana debe seleccionar el certificado exportado anteriormente. Pulse “Aceptar” para continuar.<br>  <br>*Ilustración 82 - Selección de certificado* |

| | |
|---|---|
| 35. | A continuación, ejecute el "Terminal", para ello pinche con el botón derecho sobre el "Inicio" y seleccione "Terminal (administrador)".<br>  <br>*Ilustración 83 - Terminal en administrador* |
| 36. | Sitúese en "C:\Program Files\Update Services\Tools\", seguidamente ejecute: "wsusutil.exe configuressl <su servidor WSUS.dominio.local>" y pulse "Intro".<br>Si la configuración se realizó correctamente, el comando devuelve la dirección https.<br>  <br>*Ilustración 84 - Detección URL* |

## ANEXO A.2.2. CONFIGURACIÓN Y ADMINISTRACIÓN DE WSUS

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. | Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor WSUS. |

| | |
|---|---|
| 2. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Windows Server Update Services”. |

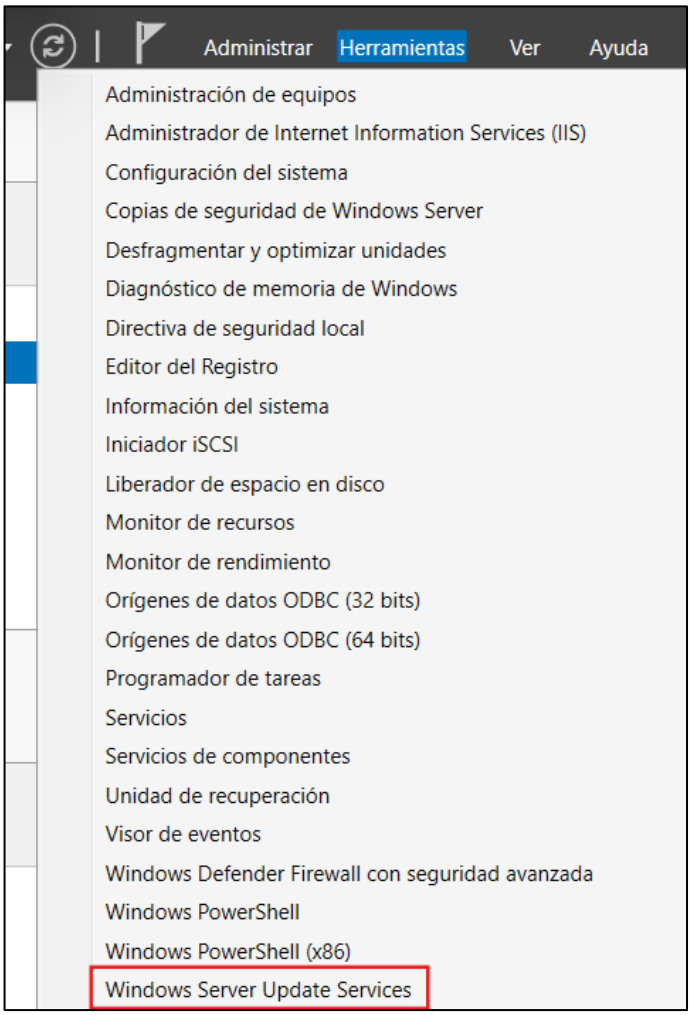



*Ilustración 85 - Herramienta WSUS*

| | |
|---|---|
| 3. | Dentro del menú de la izquierda, pinche en “Opciones”. |

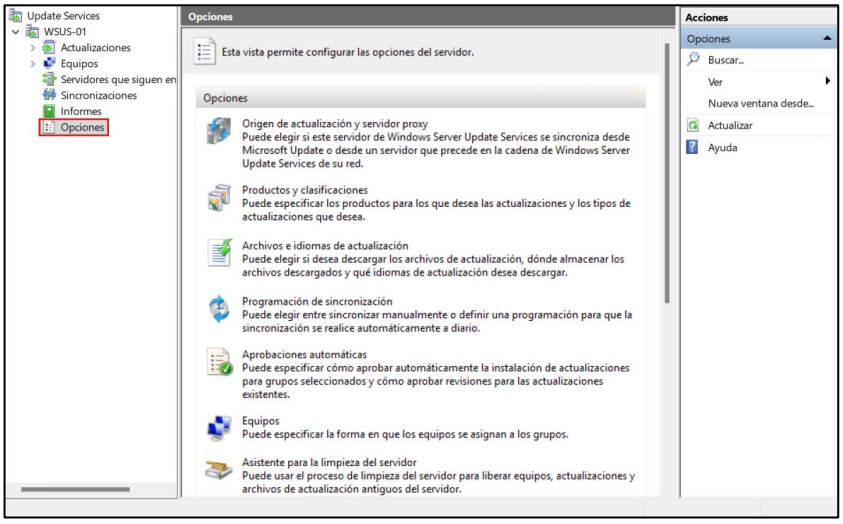



*Ilustración 86 - Menú WSUS*

| | |
|---|---|
| 4. | Seleccione “Productos y clasificaciones”. |

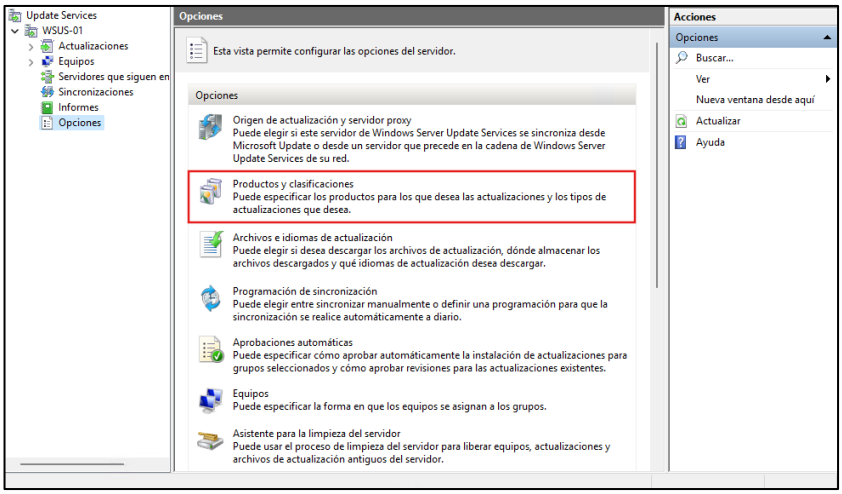
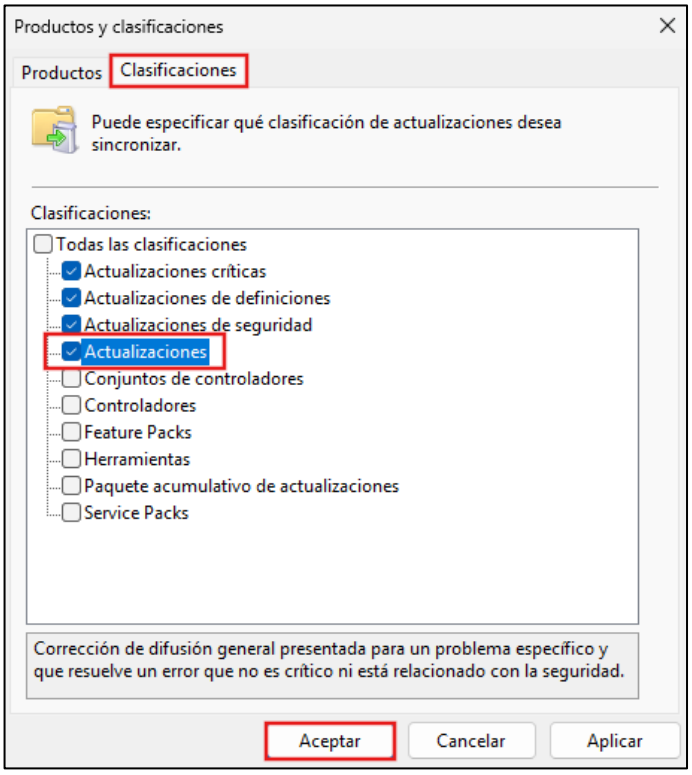
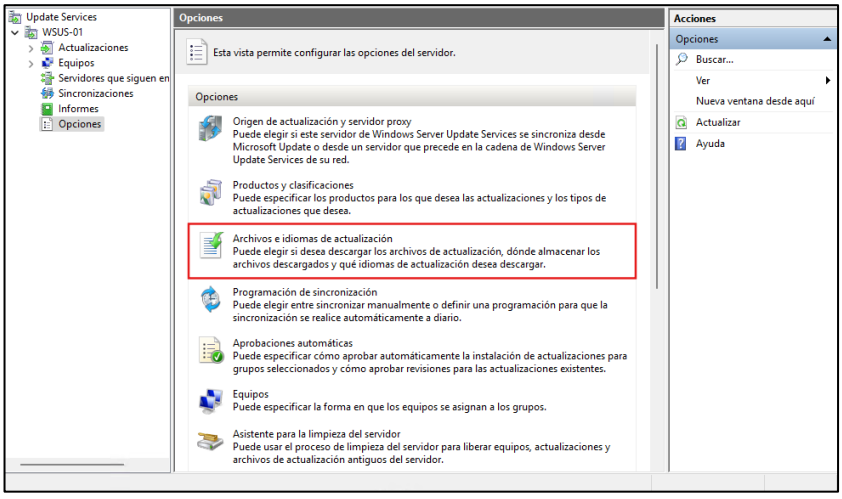



*Ilustración 87 - Productos y clasificaciones*

| | |
|---|---|
| 5. | Se abrirá una ventana donde dispondrá de dos pestañas una de “Productos” y otra de “Clasificaciones”, ubíquese en la pestaña “Clasificaciones”.<br>Marque la casilla “Actualizaciones”. Pulse “Aceptar” para guardar los cambios.<br>  <br>*Ilustración 88 - Clasificación de actualizaciones* |
| 6. | Manténgase en “Opciones”, y piche sobre “Archivos e idiomas de actualización”.<br>  <br>*Ilustración 89 - 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 solo cuando las actualizaciones estén aprobadas”. |

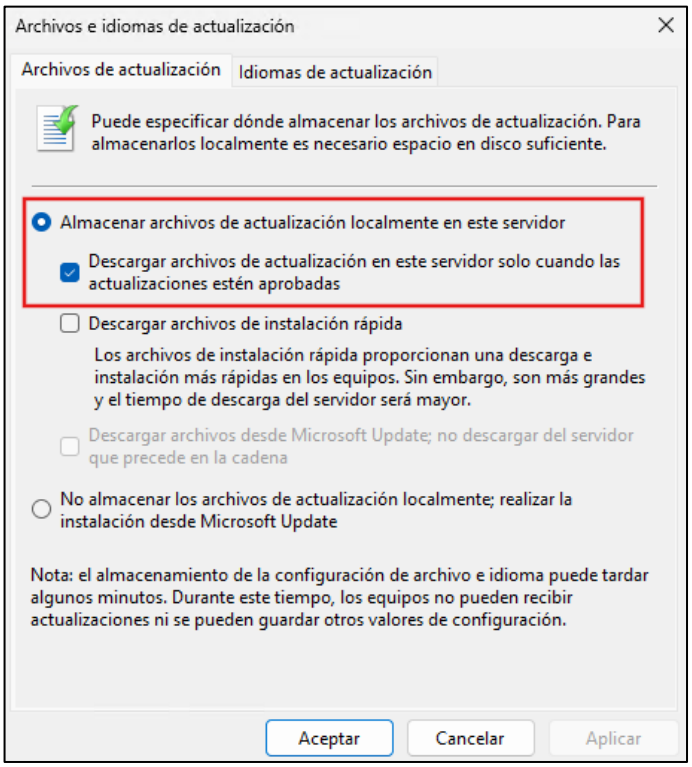



*Ilustración 90 - Configuración de actualizaciones*

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”.

Pulse “Aceptar” para guardar los cambios

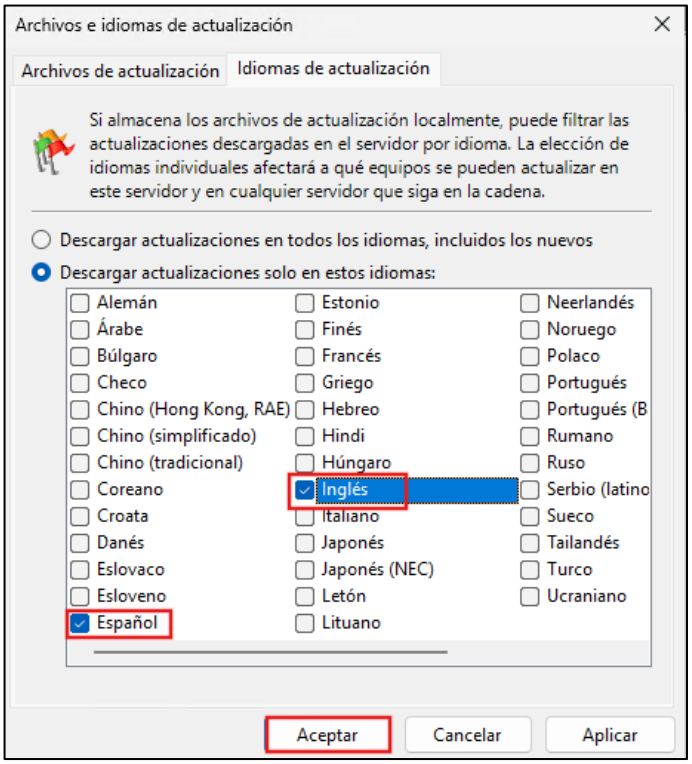



*Ilustración 91 - Idiomas de actualizaciones*

**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.

9. A continuación, entre en “Aprobaciones automáticas”.

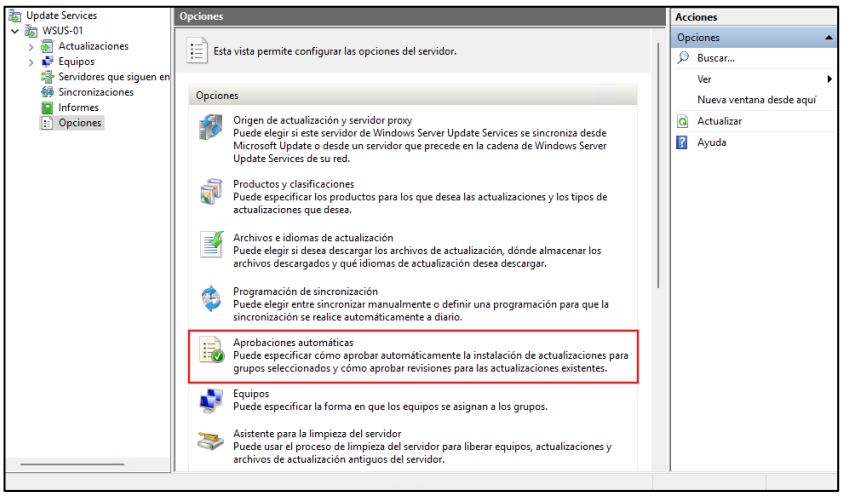
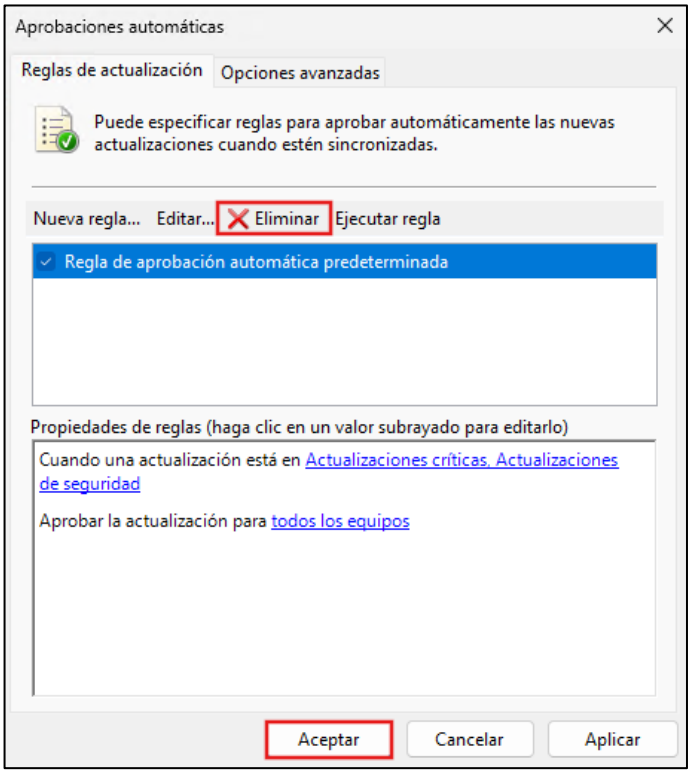



*Ilustración 92 - Aprobaciones automáticas*

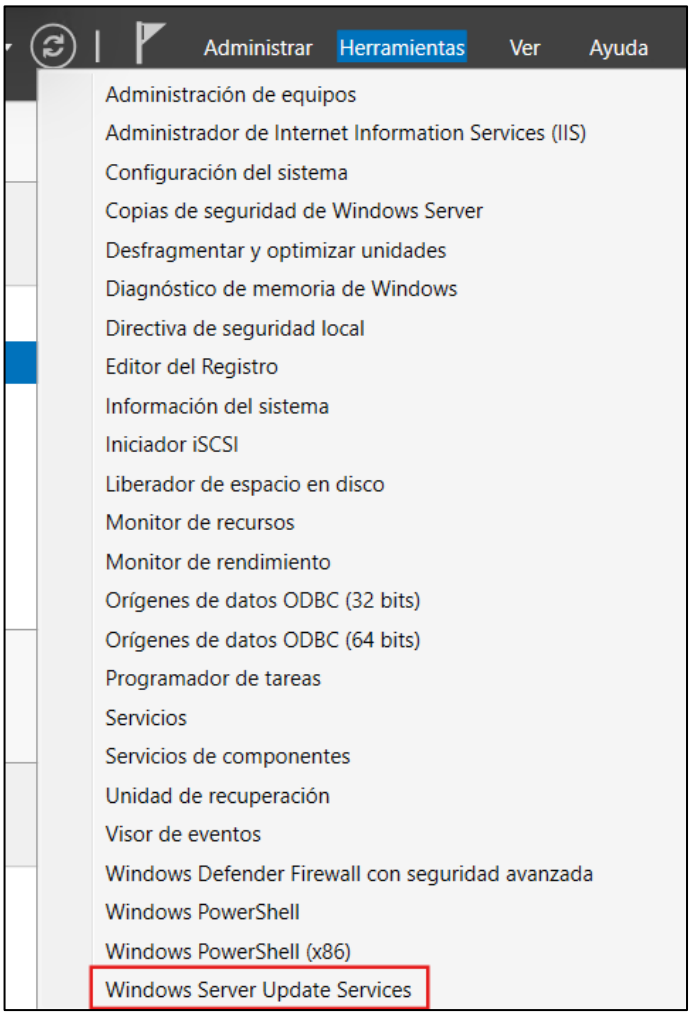
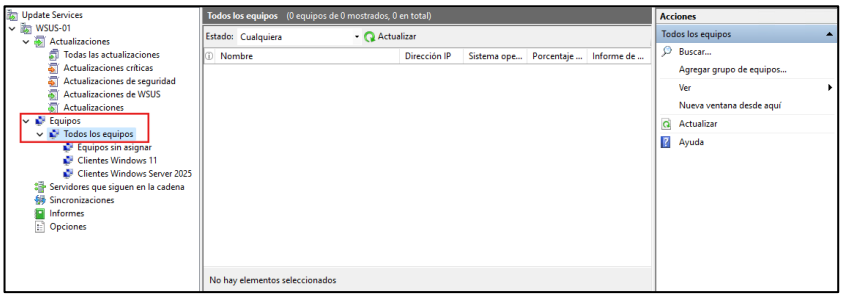
| | |
|---|---|
| 10. | En la pestaña “Regla de actualización”, seleccione la regla predeterminada que ya existe y pulse sobre “Eliminar”.<br>Pulse “Aceptar” para guardar los cambios.<br>  <br>*Ilustración 93 - Eliminar regla predeterminada* |

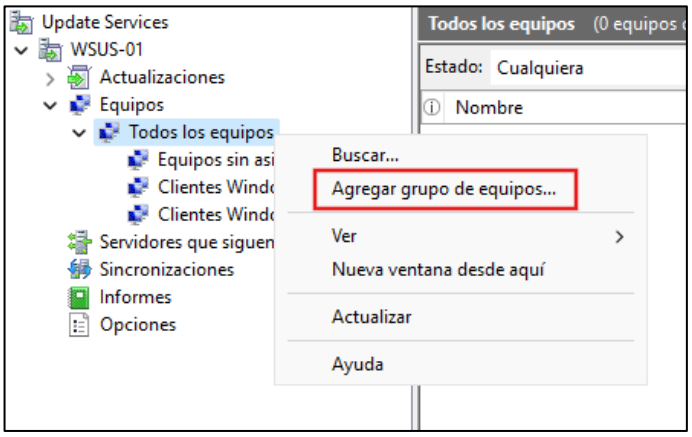
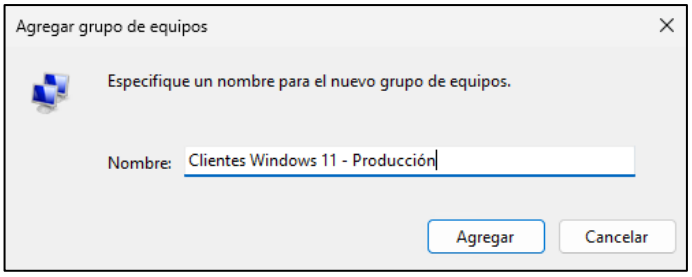
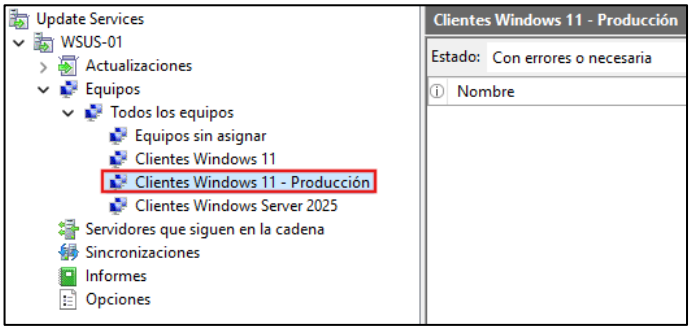
## ANEXO A.2.3. CREACIÓN Y ADMINISTRACIÓN DE GRUPOS DE EQUIPOS

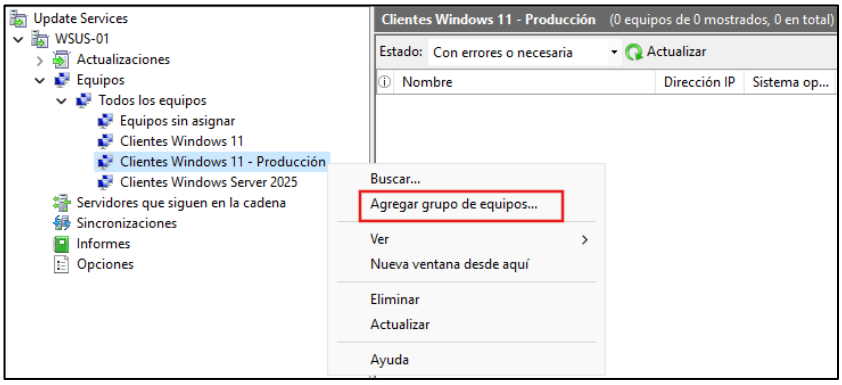
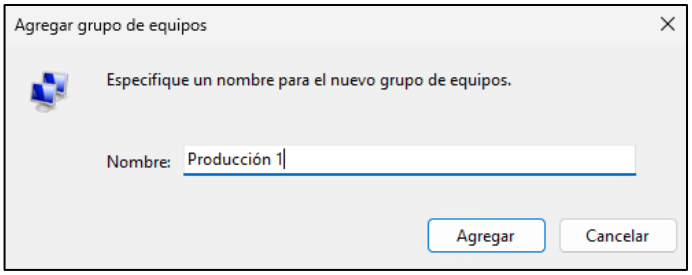
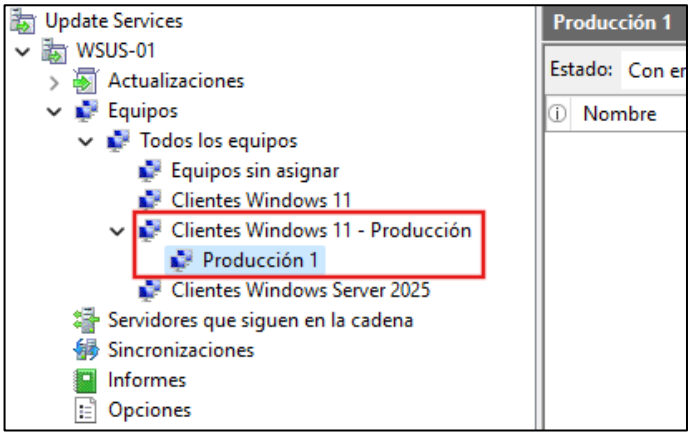
A continuación, se detalla cómo gestionar correctamente los grupos de equipos en el servidor Windows Server Update Services. Es conveniente tener una organización correcta de los equipos asociados al servidor, ya que esto ayudará a tener un control a la hora de aplicar las actualizaciones más organizadamente 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 |
|---|---|
| 1. | Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor WSUS. |

| | |
|---|---|
| 2. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Windows Server Update Services”.<br>  <br>*Ilustración 94 - Herramienta WSUS* |
| 3. | Dentro de la consola “Update Services”, despliegue la pestaña “Equipos > Todos los equipos” que se encuentra en la parte izquierda.<br>  <br>*Ilustración 95 - Grupo de equipos WSUS* |

| | |
|---|---|
| 4. | Para crear un grupo de equipos, pulse con el botón derecho sobre “Todos los equipos” y seleccione “Agregar grupo de equipos…”.<br>  <br>*Ilustración 96 - Agregar grupo de equipos* |
| 5. | Introduzca el nombre que quiera asignar al grupo que va a crear, a continuación “Agregar”.<br>  <br>*Ilustración 97 - Nombre de grupo*<br>**Nota:** Para este ejemplo, se nombra el grupo como “Clientes Windows 11 - Producción”. Usted deberá asignar el que más se adecue a sus necesidades |
| 6. | Observe que el grupo creado recientemente se agregó a la pestaña “Todos los equipos” en la consola “Update Services”.<br>  <br>*Ilustración 98 - Grupo creado* |

| | |
|---|---|
| 7. | Podrá crear grupos dentro de grupos ya creados, seleccione el grupo “Clientes Windows 11 - Producción” y pulse sobre él, con el botón derecho, seleccione “Agregar grupo de equipos…”<br>  <br>*Ilustración 99 - Agregar subgrupo* |
| 8. | Introduzca un nombre para el grupo.<br>  <br>*Ilustración 100 - Nombre de subgrupo*<br>**Nota:** Para este ejemplo, se nombra el grupo como “Producción 1”. Usted deberá asignar el que más se adecue a sus necesidades. |
| 9. | Observe que el grupo creado recientemente se agregó dentro del grupo “Clientes Windows 11 – Producción”.<br>  <br>*Ilustración 101 - Subgrupo creado* |

## ANEXO A.2.4. EXPORTACIÓN E IMPORTACIÓN DE ACTUALIZACIONES DE WSUS

En el presente punto se detalla cómo integrar las actualizaciones descargadas por un 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.

| Paso | Descripción |
|---|---|
| 1. | En primer lugar, inicie sesión en el servidor de Windows Server Update Services que no se encuentra dentro de la red de dominio. |

| | |
|---|---|
| 2. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Windows Server Update Services”. |

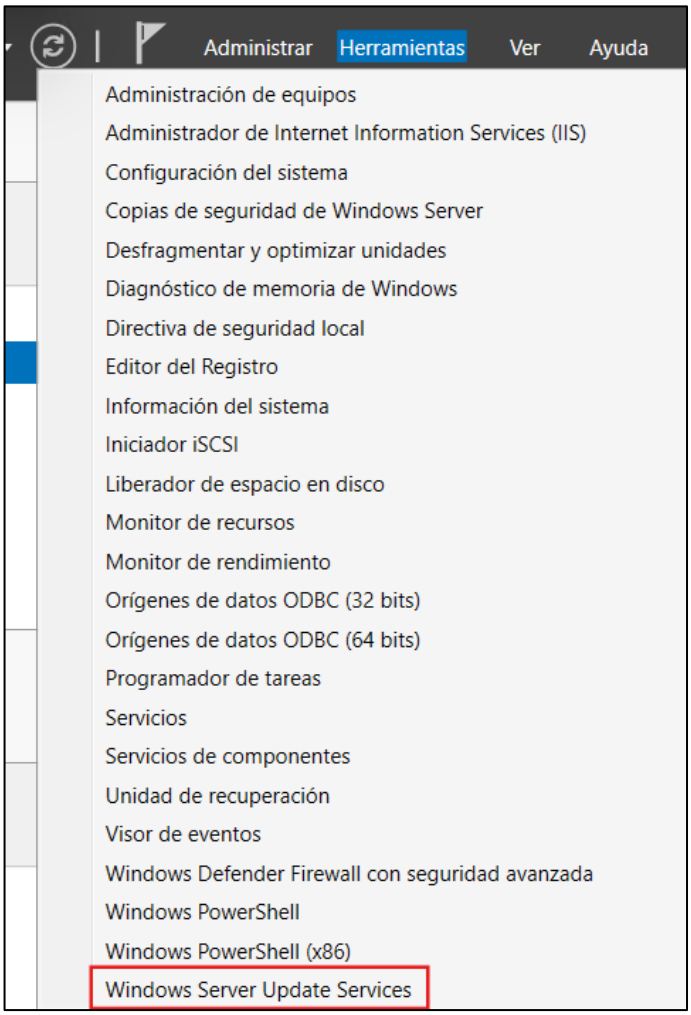



*Ilustración 102 - Windows Server Update Services*

3. 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 Online]> 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:

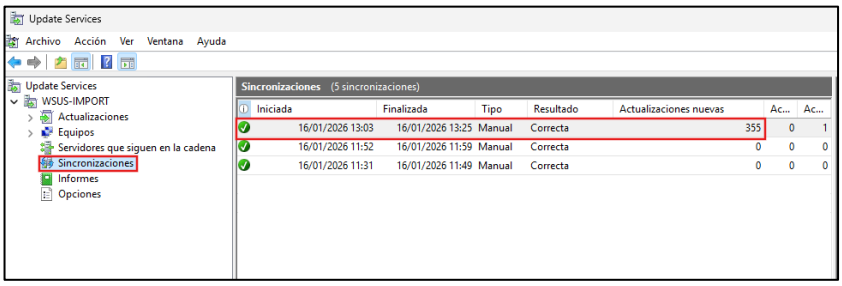



*Ilustración 103 - Sincronización*

**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".

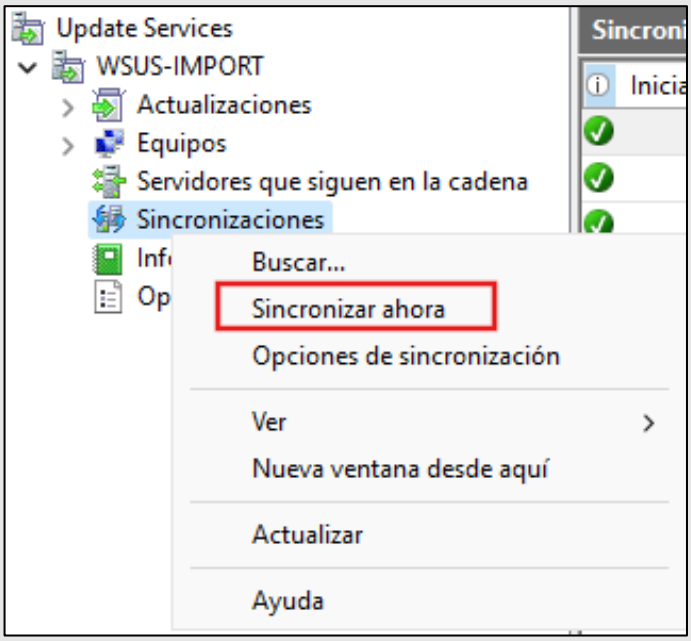
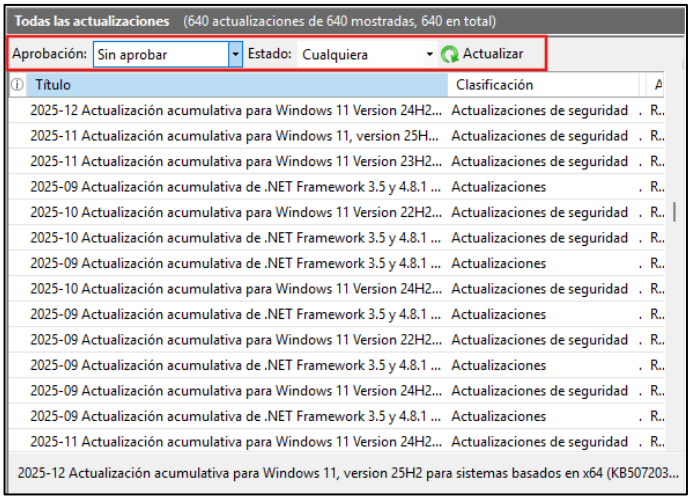
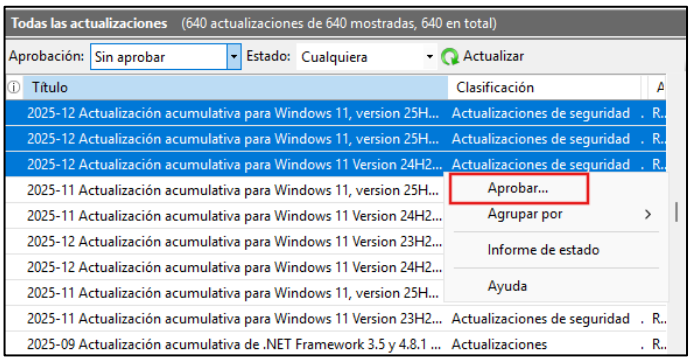
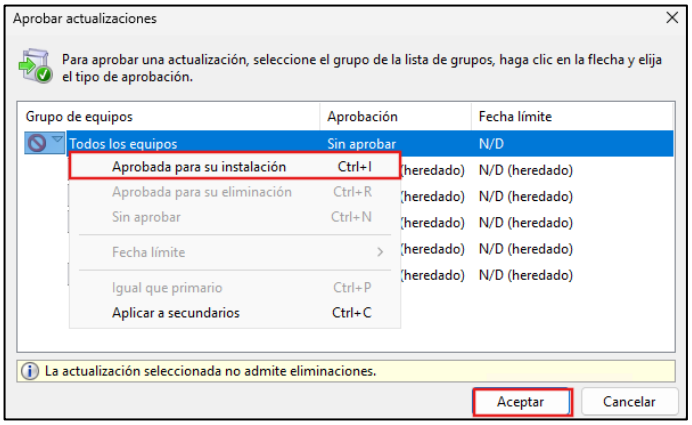
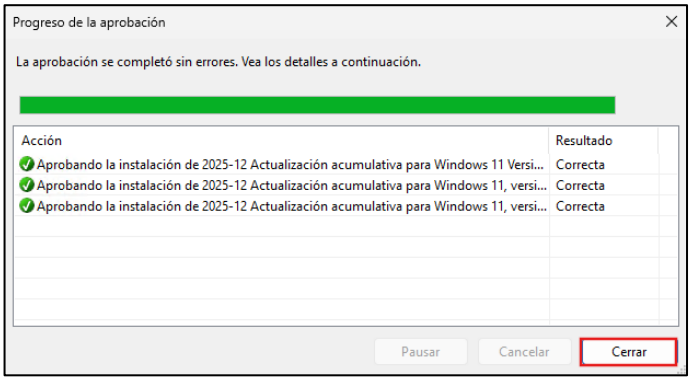
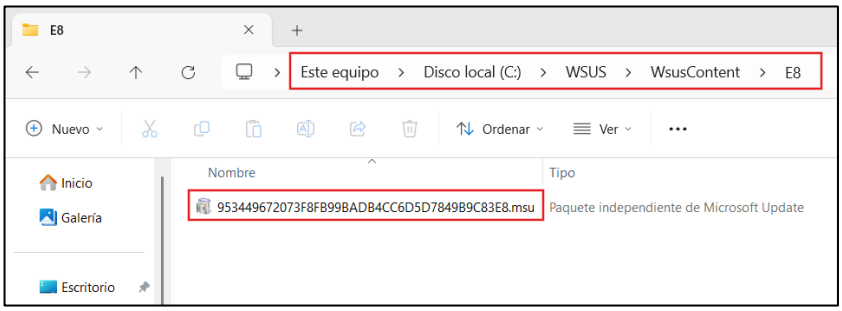
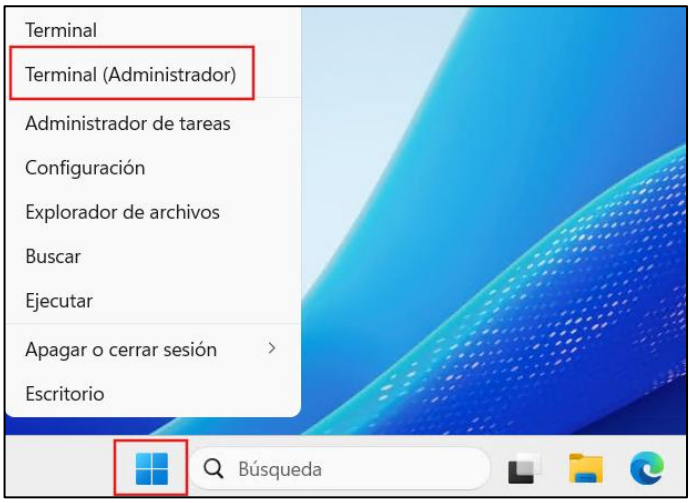
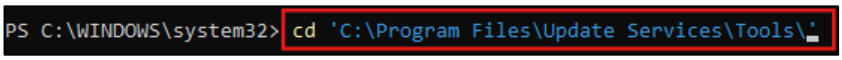
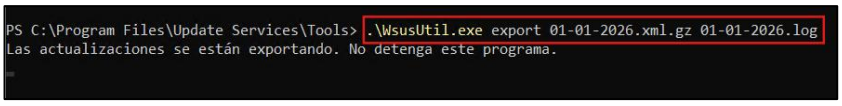
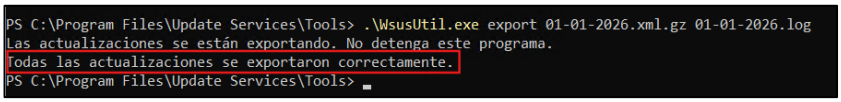


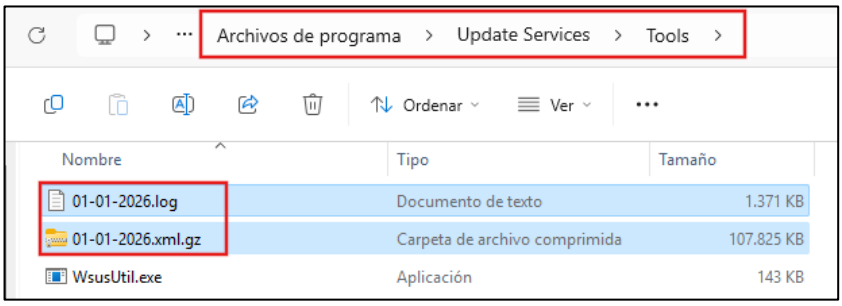
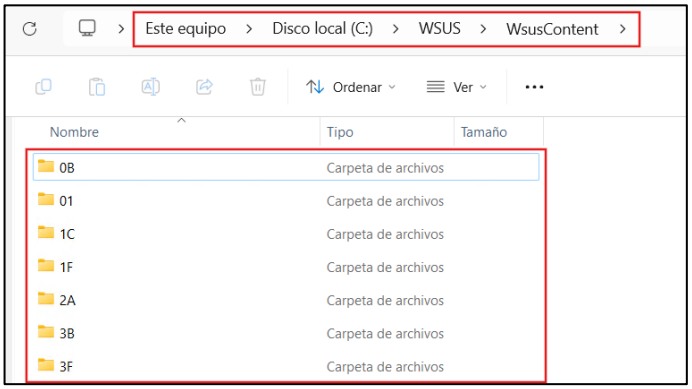

*Ilustración 104 - Sincronizar ahora*

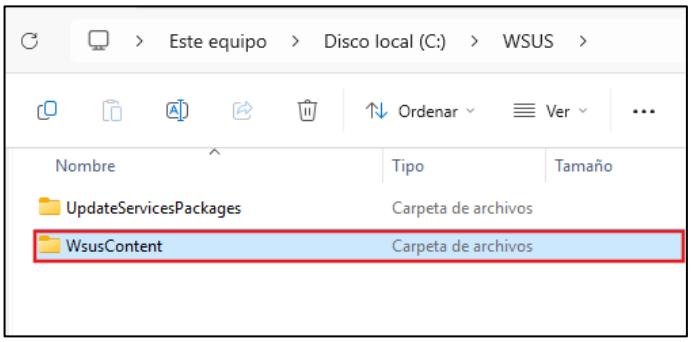
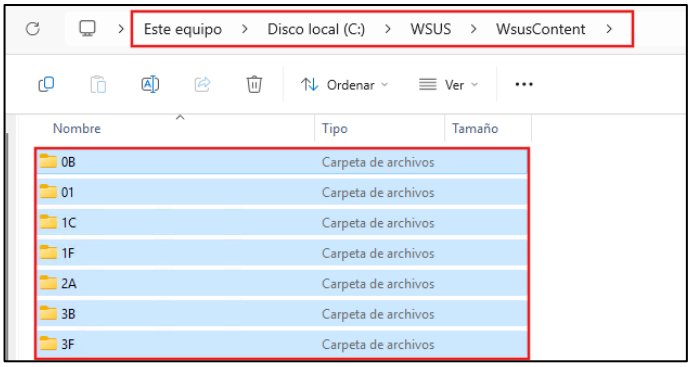
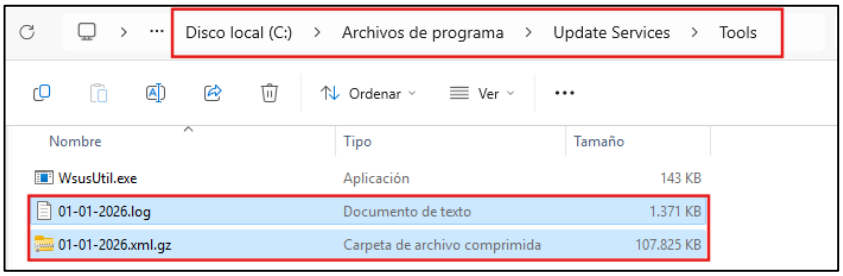
| | |
|---|---|
| 4. | A continuación, sitúese en Update Services>[Su servidor WSUS]>Todas las actualizaciones, y en el panel central, configure las pestañas "Aprobación" y "Estado" de la siguiente manera:<br>- Aprobación: Sin aprobar.<br>- Estado: Cualquiera.<br>Una vez hecho esto, pulse sobre "Actualizar". Seguidamente podrá observar todas las actualizaciones disponibles de Microsoft Update.<br>  <br><br>*Ilustración 105 - Clasificación de actualizaciones* |
| 5. | 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".<br>  <br><br>*Ilustración 106 - Aprobar actualizaciones*<br>**Nota:** En este caso, solo se muestran cuatro actualizaciones el sistema operativo Windows 11. |

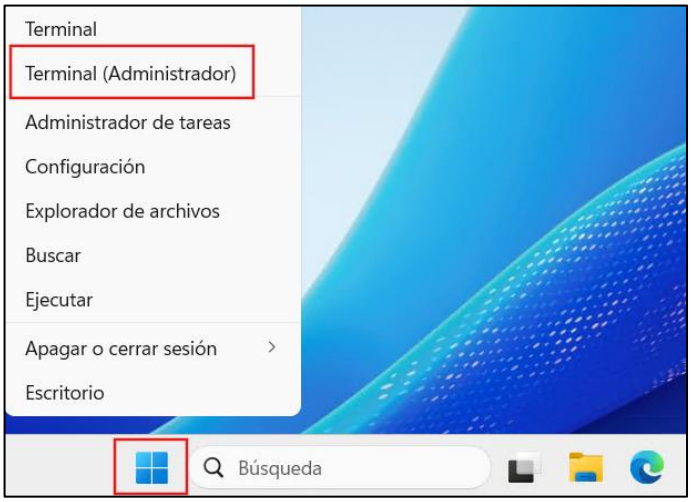
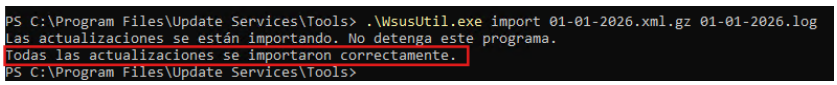
| | |
|---|---|
| 6. | Seguidamente, aparecerá un asistente donde indicará el grupo de equipos para los que quiere aprobar estas actualizaciones.<br>Seleccione la pestaña “Todos los equipos” y a continuación pulse sobre “Aprobada para su instalación” y “Aceptar”.<br>  <br>*Ilustración 107 - Aprobar actualizaciones* |
| 7. | Comenzará el proceso de aprobación, cuando haya terminado pulse sobre “Cerrar” para finalizar el asistente.<br>  <br>*Ilustración 108 - Progreso de la aprobación* |
| 8. | 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.<br>  <br>*Ilustración 109 - Icono de descarga* |

| | |
|---|---|
| 9. | 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.<br>  <br>*Ilustración 110 - Icono de actualización descargada* |
| 10. | Por último, para dar por finalizado el proceso de descarga, deberá comprobar que las actualizaciones se han almacenado en la ubicación correcta.<br>**Nota:** En este caso se ha configurado en la ruta C:\WSUS\WsusContent. |
| 11. | 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.<br>  <br>*Ilustración 111 - Archivo .cab* |
| 12. | A continuación, se procederá con el proceso de exportación. Para ello, desde el servidor de Windows Server Update Services, ejecute un símbolo de sistema con derechos de administrador.<br>Pinche con el botón derecho sobre el “Inicio” y seleccione “Terminal (administrador)”.<br>  <br>*Ilustración 112 - Terminal (Administrador)* |

| | |
|---|---|
| 13. | Se abrirá un símbolo de sistema con privilegios de administrador. Después sitúese en "C:\Program Files\Update Services\Tools\".<br>  <br>*Ilustración 113 - Ruta de wsusutil* |
| 14. | 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 [FECHA].xml.gz [FECHA].log", seguidamente se pulsará "Intro", para que se ejecute el comando introducido.<br>  <br>*Ilustración 114 - Comando exportación archivos*<br>**Nota:** El formato GZIP es el más habitual para exportar metadatos porque soporta grandes volúmenes sin limitaciones de tamaño, generando un archivo .xml.gz. No obstante, cuando el conjunto de datos es pequeño, también se puede usar el formato CAB con extensión .cab, adecuado para exportaciones reducidas. Si el tamaño supera el límite del CAB (aprox. 2 GB), será obligatorio utilizar GZIP. |
| 15. | Espere a que termine, cuando el proceso acabe se emitirá un mensaje notificando que la exportación se ha realizado correctamente.<br>  <br>*Ilustración 115 - Actualizaciones exportadas correctamente* |

| | |
|---|---|
| 16. | Compruebe que se han generado un archivo .xml.gzip 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.<br>  <br><br>*Ilustración 116 - Archivos a copiar*<br>**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). |
| 17. | Finalmente, 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 "C:\WSUS\WsusContent\". Deberá copiar todos los directorios que se encuentran dentro de la carpeta WsusContent.<br>  <br><br>*Ilustración 117 - Copiar archivos de actualización* |
| 18. | A continuación, se procederá con el proceso de almacenamiento e importación de las actualizaciones, todos los pasos se realizarán desde el servidor WSUS Offline.<br>Inicie sesión en el servidor Windows Server Update Services miembro del dominio con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. |

| | |
|---|---|
| 19. | Diríjase a ruta “C:\WSUS” que tenga en su servidor Windows Server Update Services, dentro de la carpeta “WsusContent”.<br>  <br>*Ilustración 118 - Carpeta WsusContent* |
| 20. | Dentro de la carpeta “WsusContent”, deben estar ubicados los paquetes de actualizaciones copiados anteriormente desde el servidor WSUS Online.<br>  <br>*Ilustración 119 - Copiar archivos de actualización* |
| 21. | Deberá copiar también los archivos .xml.gzip y .log generados en el proceso de exportación de estás actualizaciones. Deberá ubicarlos en “C:\Archivos de programa\Update Service\Tools”.<br>  |

| | |
|---|---|
| 22. | Una vez que tenga almacenados los archivos en la ubicación correcta, deberá importar las actualizaciones, para ello, ejecute un símbolo de sistema con derechos de administrador.<br>Pinche con el botón derecho sobre el "Inicio" y seleccione "Terminal (administrador)".<br>  <br>*Ilustración 120 - Terminal (Administrador)* |
| 23. | Ubíquese en "C:\Archivos de programa\Update Services\Tools\", ejecute el siguiente comando: ".\WsusUtil.exe import [FECHA].xml.gz [FECHA].log".<br>  <br>*Ilustración 121 - Importar actualizaciones*<br>**Nota:** Para este ejemplo los archivos .xml.gz y .log se han nombrado 01-01-2026.xml.gz y 01-01-2026.log respectivamente. |
| 24. | Cuando termine de importar, mostrará un mensaje en pantalla para confirmar la importación. Cierre el terminal del sistema.<br>  <br>*Ilustración 122 - Actualizaciones importadas* |

| | |
|---|---|
| 25. | 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. |

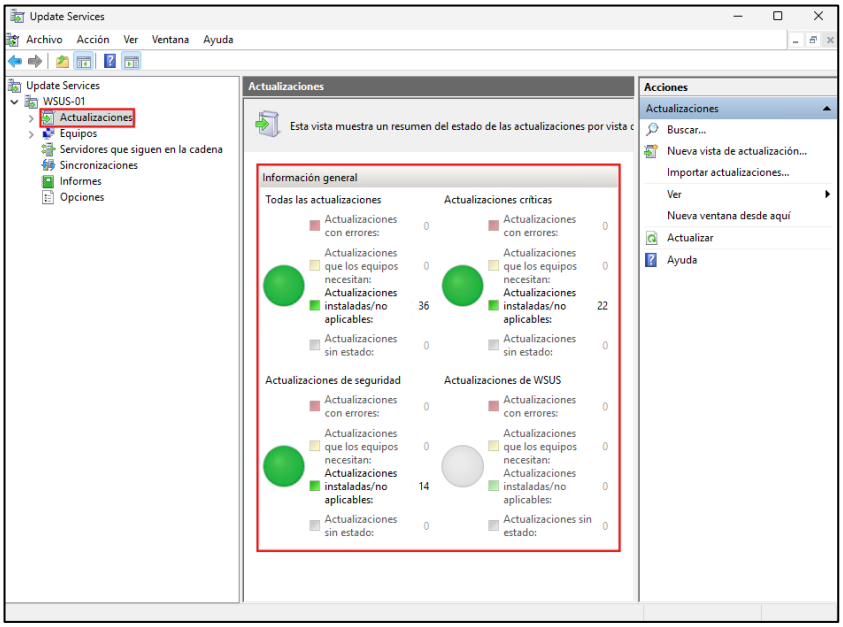



*Ilustración 123 - Resumen actualizaciones importadas*

## ANEXO A.2.5. ADMINISTRACIÓN ADECUADA DE ACTUALIZACIONES IMPORTADAS

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 |
|---|---|
| 1. | Inicie sesión en el servidor Windows Server Update Services con una cuenta con privilegios de Administrador local de la máquina o administrador del dominio. |

| | |
|---|---|
| 2. | En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Windows Server Update Services”. |

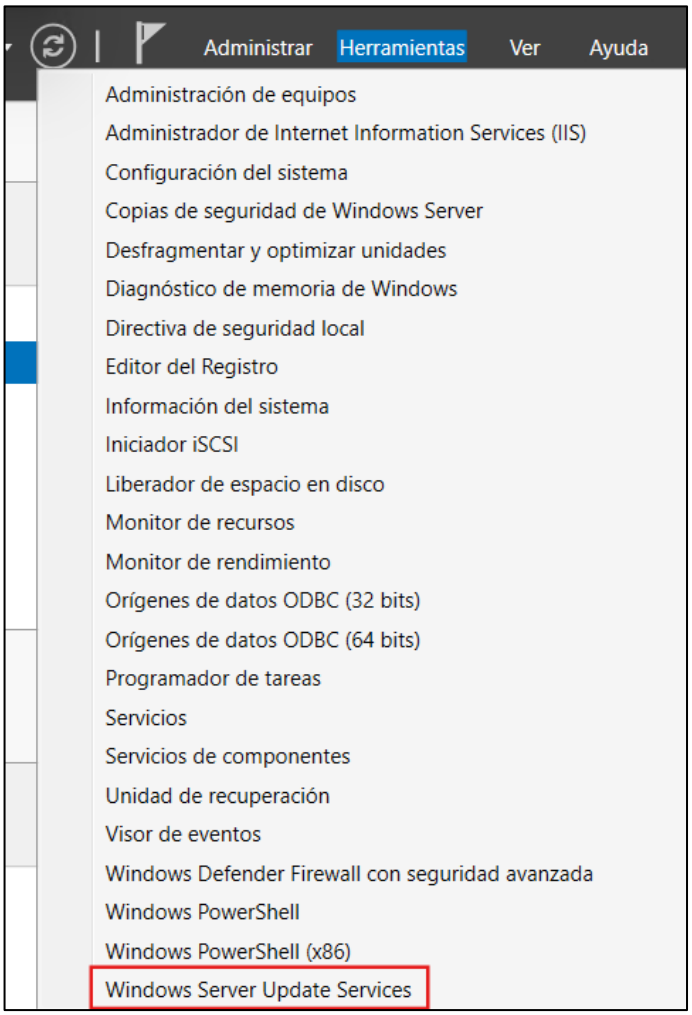
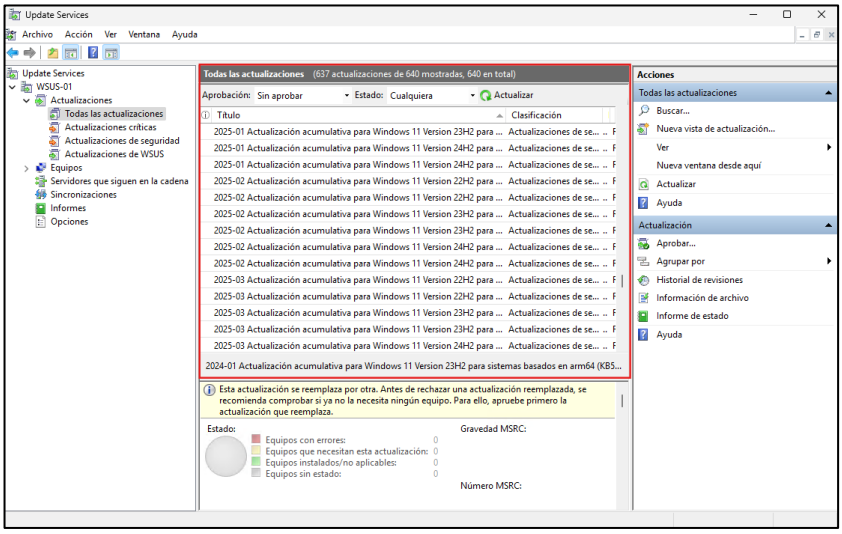
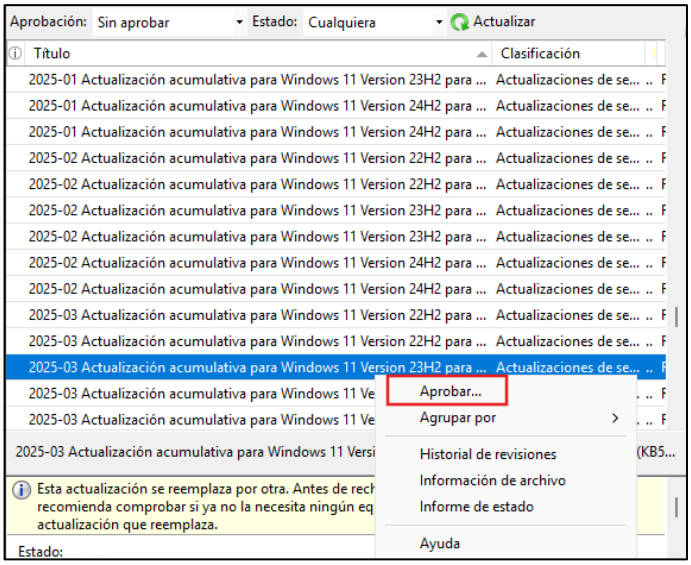
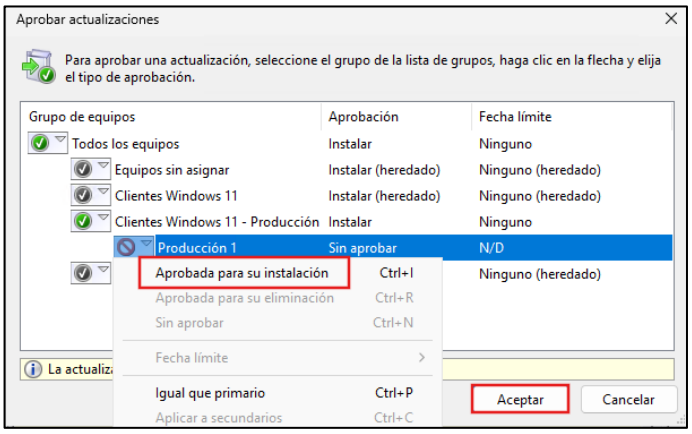
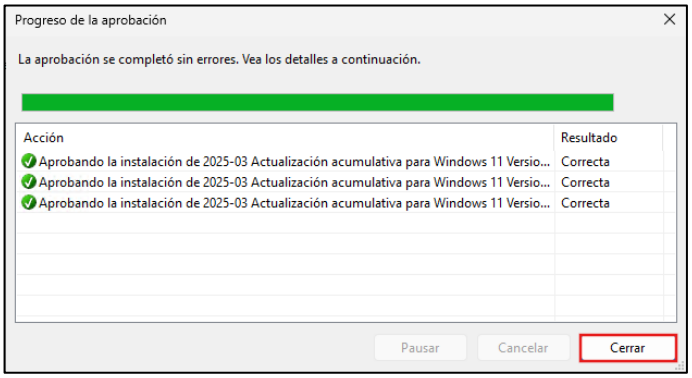
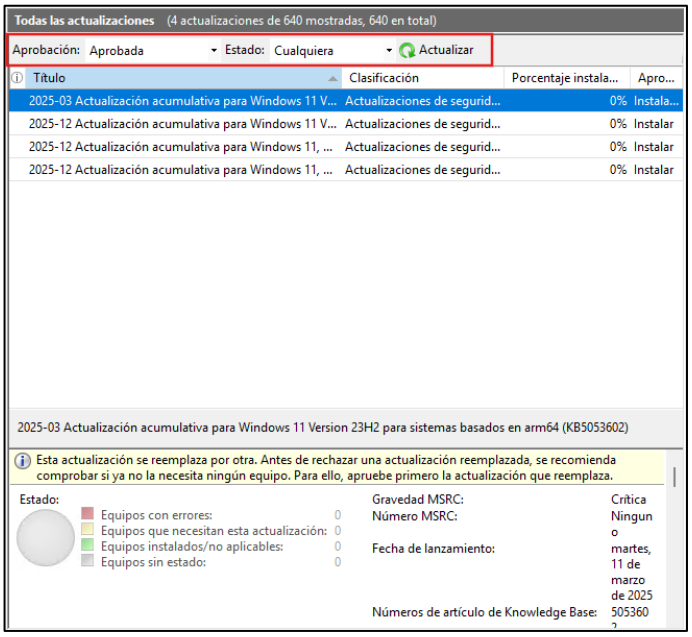
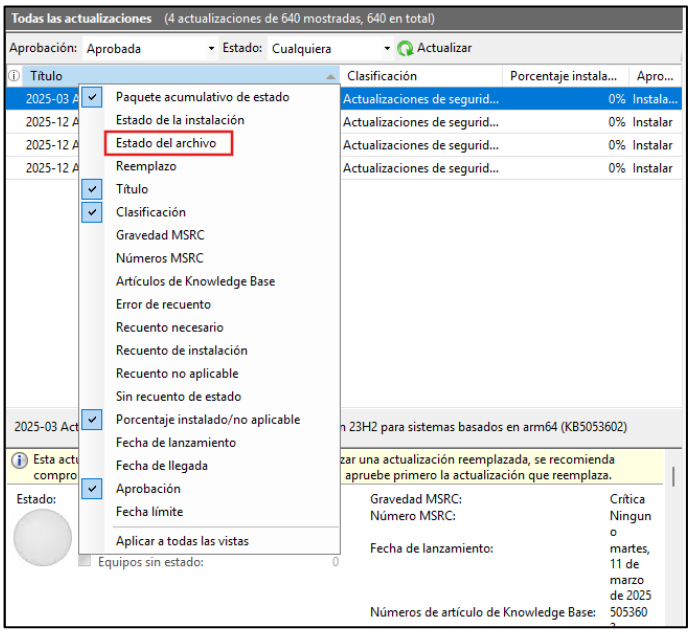
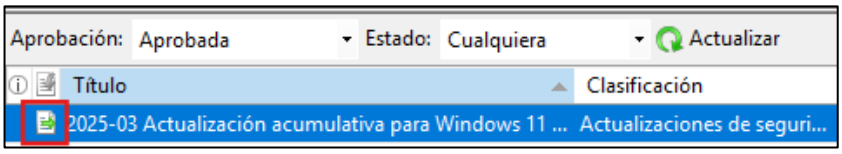



*Ilustración 124 - Windows Server Update Services*

| | |
|---|---|
| 3. | En la consola “Update Services”, despliegue la pestaña “Actualizaciones > Todas las actualizaciones”. Podrá observar, que se encuentran todas las actualizaciones que se han importado.<br>  <br>*Ilustración 125 - Actualizaciones importadas* |
| 4. | Para realizar una aprobación, pinche sobre una actualización y con el botón derecho seleccione “Aprobar…”.<br>  <br>*Ilustración 126 - Aprobar actualización* |

| | |
|---|---|
| 5. | 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”.<br>  <br><br>*Ilustración 127 - Aprobar instalación*<br>**Nota:** Para este ejemplo, se ha seleccionado la aprobación para los equipos cliente Windows 11 (Producción 1), ya que el paquete de actualizaciones que se ha aprobado va dirigido a los sistemas Windows 11. |
| 6. | Una vez que se haya completado la aprobación, pulse “Cerrar”.<br>  <br><br>*Ilustración 128 - Progreso de la aprobación* |

| | |
|---|---|
| 7. | Para visualizar las actualizaciones aprobadas, deberá establecer las pestañas “Aprobación” y “Estado” de la siguiente manera.<br>- Aprobación: Aprobada.<br>- Estado: Cualquiera.<br>Pulse en “Actualizar” para visualizar las actualizaciones aprobadas.<br>  <br><br>*Ilustración 129 - Aplicaciones instaladas* |
| 8. | Sobre la barra de “Título”, piche con el botón derecho y seleccione “Estado de archivo”. Esto comprobará si la actualización está lista para instalarse.<br>  <br><br>*Ilustración 130 - Estado del archivo* |

| | |
|---|---|
| 9. | Se generará un icono nuevo que indicará si la actualización se está descargando o si ya está lista para su instalación.<br>  <br><br>*Ilustración 131 - Actualización descargada*<br>**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. |
| 10. | 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. |