

Guía de Seguridad de las TIC CCN-STIC 598A25

APLICACIÓN DE SEGURIDAD SOBRE ENTIDAD DE CERTIFICACIÓN



SEPTIEMBRE 2026

Edita:



Pº de la Castellana 109, 28046 Madrid
© Autor y editor, 2026
(edición en línea)



Firmado digitalmente por CCN
Nombre de reconocimiento (DN): c=ES,
l=MADRID, o=CCN, ou=SELLO
ELECTRONICO, 2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J, cn=CCN
Fecha: 2026.09.07 13:57:27 +02'00'

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.



[Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Centro Criptológico Nacional.» No se puede modificar. No se puede utilizar con fines comerciales.](#)

INDICE

1.	INTRODUCCIÓN	5
2.	OBJETO.....	5
3.	ALCANCE	7
4.	DESCRIPCIÓN DE USO DE ESTA GUÍA	8
4.1.	REQUISITOS PREVIOS PARA LA ENTIDAD DE CERTIFICACIÓN	8
5.	PERFILADO DE CUMPLIMIENTO TÉCNICO	8
6.	APLICACIÓN DE SEGURIDAD SOBRE ENTIDAD DE CERTIFICACIÓN	9
6.1.	OPCION A. CONFIGURACIÓN DE SEGURIDAD PARA ENTIDAD DE CERTIFICACIÓN ENTERPRISE ÚNICA.....	10
6.1.1.	PASO A PASO DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE EL DOMINIO.....	10
6.1.2.	PASO A PASO DE INSTALACIÓN DE ENTIDAD DE ENTIDAD DE CERTIFICACIÓN ENTERPRISE.....	23
6.1.3.	CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN ENTERPRISE.....	35
6.2.	OPCIÓN B. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA CON ENTIDAD RAÍZ EN DOMINIO	51
6.2.1.	PASO A PASO DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE EL DOMINIO.....	51
6.2.2.	PASO A PASO DE INSTALACIÓN EN ENTIDAD DE CERTIFICACIÓN RAÍZ EN DOMINIO.....	65
6.2.3.	CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA.....	73
6.2.4.	PASO A PASO DE INSTALACIÓN EN ENTIDAD DE CERTIFICACIÓN SUBORDINADA EN DOMINIO.....	93
6.2.5.	CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA.....	103
6.2.6.	PASO A PASO DE FUNCIONAMIENTO	131
6.3.	OPCIÓN C. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA CON ENTIDAD RAÍZ INDEPENDIENTE	136
6.3.1.	PASO A PASO DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE EL DOMINIO.....	136
6.3.2.	PASO A PASO DE INSTALACIÓN Y CONFIGURACIÓN DE SEGURIDAD EN ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE	149
6.3.3.	CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE A UN DOMINIO	160
6.3.4.	PASO A PASO DE INSTALACIÓN DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA EN DOMINIO.....	182

6.3.5.	PASO A PASO DE INTERCAMBIO DE CERTIFICADOS ENTRE LA ENTIDAD SUBORDINADA Y LA ENTIDAD RAIZ INDEPENDIENTE DEL DOMINIO	191
6.3.6.	PASO A PASO DE FUNCIONAMIENTO	222
7.	CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN.....	227
7.1.	SEGREGACIÓN DE ROLES.....	227
7.2.	CONFIGURACIÓN DE AUDITORÍA	236
7.3.	RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA.....	240
7.4.	COPIA DE SEGURIDAD Y RESTAURACIÓN DE UNA ENTIDAD DE CERTIFICACIÓN	242
7.4.1.	COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN	242
7.4.2.	RESTAURACIÓN DE COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN	248

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 Exchange Subscription Edition, el cual requiere la instalación del rol **Internet Information 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-576A25 sobre Microsoft Exchange, aplicable a los servidores que alojarán el servicio de Exchange.

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 **Entidad de Certificación**, instalado en un servidor miembro Windows Server 2025 perteneciente a un dominio Windows Server de Directorio Activo.

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 Entidad de Certificación, 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 basa, principalmente, en las disposiciones establecidas por el CCN en la Instrucción Técnica de Seguridad de las TIC (CCN-STIC-301) y otras normativas nacionales de aplicación.

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, 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 Entidad de Certificación en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración.

El escenario en el cual está basada la guía CCN-STIC-598A25 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) Dos servidores miembros del dominio 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 Entidad de Certificación de Microsoft. Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en este servicio.
- d) Guía paso a paso. Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor con Entidad de Certificación de Microsoft.
 - a. Se incluye el paso a paso de configuración de seguridad de entidad de certificación subordinada única.
 - b. Se incluye el paso a paso de configuración de seguridad de entidad de certificación subordinada con entidad raíz, ambos en dominio.
 - c. Se incluye el paso a paso de configuración de seguridad de entidad de certificación subordinada con entidad raíz independiente.

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 Entidad de Certificación:** Las configuraciones de seguridad del servicio y de los componentes necesarios del sistema se modifican por medio de objetos de política de grupo (GPO), junto a configuraciones en los servidores de Entidad de Certificación. Dicha configuración está desarrollada en el apartado 6. *APLICACIÓN DE SEGURIDAD SOBRE ENTIDAD DE CERTIFICACIÓN*.
- **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 apartado 7. *CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN*.

4.1. REQUISITOS PREVIOS PARA LA ENTIDAD DE CERTIFICACIÓN

Antes de aplicar las medidas descritas en esta guía, es necesario que el servidor disponga de un sistema operativo compatible. El servicio de Entidad de Certificación 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 **Entidad de Certificación de Microsoft**, 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)** y los requisitos de seguridad

de la guía **CCN-STIC-574A25 Aplicación de seguridad sobre Microsoft Internet Information Services**. Del mismo modo, en los servidores con rol de Entidad de Certificación Raíz, configurados de manera independiente al dominio, se deberán aplicar los requisitos de seguridad recogidos en guías publicadas para servidores independientes. En este caso, **CCN-STIC-570B** para redes clasificadas.

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

En los apartados siguientes se desarrollarán los controles específicos aplicables a un sistema, 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 Internet Information 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>

6. APLICACIÓN DE SEGURIDAD SOBRE ENTIDAD DE CERTIFICACIÓN

El presente anexo detalla el procedimiento técnico para la configuración de las medidas de seguridad exigidas en entornos de producción basados en Microsoft Windows Server 2025 con Entidad de Certificación.

Este despliegue tiene como objetivo principal establecer una gestión automática, centralizada y robusta de la seguridad, garantizando que la infraestructura tecnológica que da soporte a la organización opere bajo condiciones controladas de integridad, confidencialidad y disponibilidad.

Para la correcta aplicación de estas medidas, la metodología se basa en el aprovechamiento de los elementos técnicos nativos del ecosistema Microsoft, articulándose en torno a los siguientes pilares:

- **Uso de Objetos de Directiva de Grupo (GPO):** Se emplearán GPOs como mecanismo principal para el despliegue masivo y homogéneo de configuraciones de seguridad.
- **Gestión de identidad y acceso:** Configuración de políticas en Directorio Activo para garantizar la segregación de roles y funciones, asegurando que los permisos administrativos se asignen bajo el principio de menor privilegio.
- **Alineación normativa base:** Los servidores miembros del dominio deberán haber sido implementados previamente siguiendo las directrices de la guía CCN-STIC-570A25 Perfilado de seguridad para Windows Server (DC o MS).

A continuación, se describe el flujo de trabajo paso a paso para la aplicación de seguridad sobre Entidad de Certificación de manera centralizada.

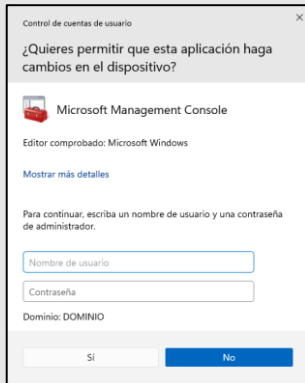
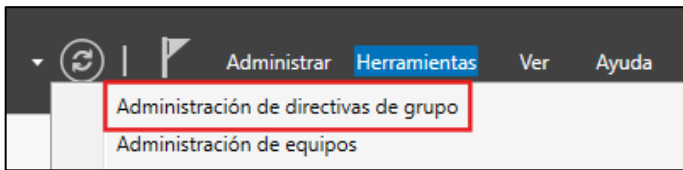
6.1. OPCION A. CONFIGURACIÓN DE SEGURIDAD PARA ENTIDAD DE CERTIFICACIÓN ENTERPRISE ÚNICA

Este apartado presenta el procedimiento de configuración de seguridad, descrito de manera ordenada y detallada, en un entorno formado por un Controlador de Dominio y un Servidor Miembro de Dominio que asumirá el rol de Entidad de Certificación única.

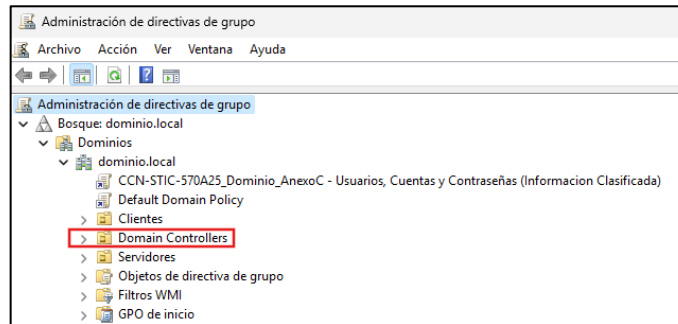
Antes de iniciar con el proceso de configuración, es necesario disponer de los siguientes elementos:

- Un servidor controlador de dominio Windows Server 2025 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A25.
- Un servidor miembro de dominio Windows Server 2025 que ejercerá como Entidad de Certificación única siguiendo la guía de seguridad CCN-STIC-570A25. Este contendrá el servicio de Internet Information Services instalado y asegurado mediante la guía CCN-STIC-574A25.

6.1.1. PASO A PASO DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE EL DOMINIO

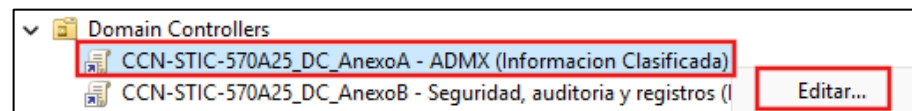
Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo “Admins. de Dominio” en un Controlador de Dominio e inicie la consola de “Administrador del servidor”. Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 1 - Introducir credenciales de administrador</i>
2.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  <i>Ilustración 2 - Administración de directivas de grupo</i>

3. Despliegue en el panel izquierdo hasta llegar a la OU “Domain Controllers”.



Ilustraci3n 3 - OU Domain Controllers

4. Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificaci3n)”, y seleccione “Editar”.



Ilustraci3n 4 - Edici3n de ADMX 570A25

5. En el panel “Editor de administraci3n de directivas de grupo”, despliegue la lista y dirijase a la siguiente ruta: “**Configuraci3n del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell**”. Haga clic sobre “Windows PowerShell” para consultar las pol3ticas que aplica.

Configuraci3n	Estado	Comentario
 Activar registro de m3dulos	Habilitada	No
 Activar el registro de bloque de script de PowerShell	Habilitada	No
 Activar la ejecuci3n de scripts	Habilitada	No
 Activar la transcripci3n de PowerShell	Habilitada	No
 Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Ilustraci3n 5 - Pol3ticas de PowerShell

6. Haga doble clic sobre la pol3tica “Activar la ejecuci3n de scripts”.

7. En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”.

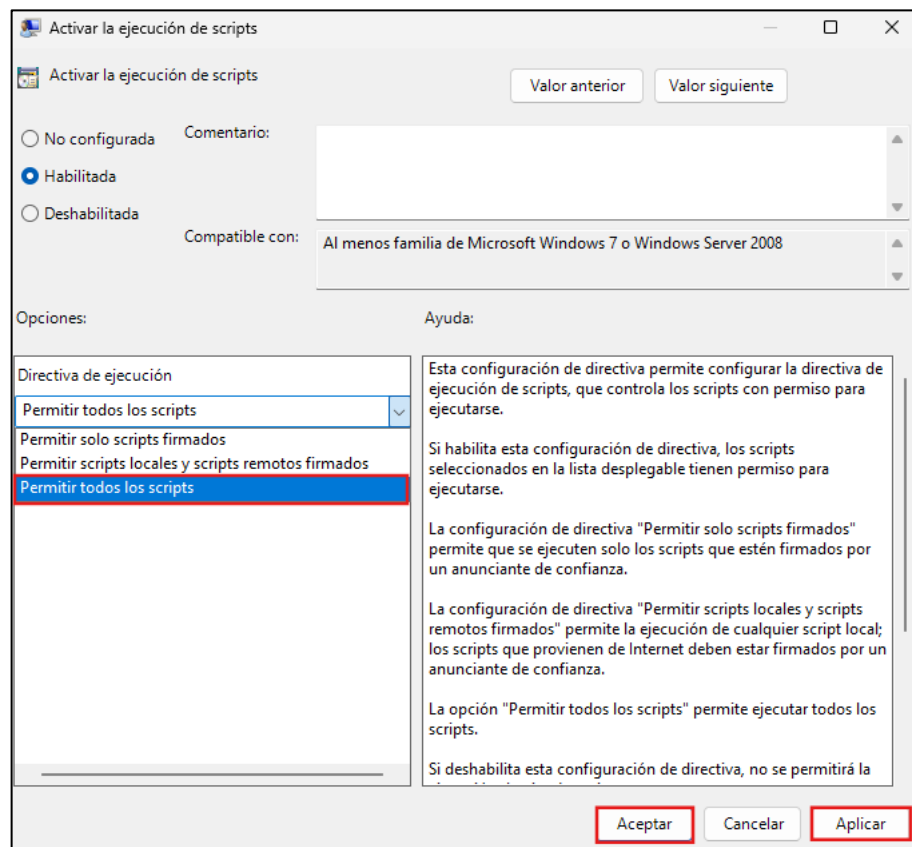


Ilustración 6 - Selección de "Permitir todos los scripts"

8. Reinicie el controlador de dominio para que se aplique la configuración correctamente. Tras ello, inicie sesión de nuevo con un usuario con privilegios de administración del dominio.

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.

Verifique que en su interior se encuentran los siguientes archivos:

- Directorio: CA INCREMENTAL DOMINIO
- Directorio: CA SERVIDORES
- Directorio: CA SERVIDORES – SHELL REMOTO
- Directorio: IIS
- Fichero: CCN-STIC-598A25_IncrementalServidorCA.ps1

	CA INCREMENTAL DOMINIO	24/07/2026 13:40	Carpeta de archivos
	CA SERVIDORES	24/07/2026 13:48	Carpeta de archivos
	CA SERVIDORES - SHELL REMOTO	24/07/2026 14:15	Carpeta de archivos
	IIS	24/07/2026 13:40	Carpeta de archivos
	CCN-STIC-598A25_EntidadCertificacion	24/07/2026 14:05	Script de Window...

Ilustración 7 - Copia de ficheros necesarios

10. Asegúrese de que el script está desbloqueado antes de comenzar con su ejecución. Para ello, haga clic derecho sobre el mismo y seleccione “Propiedades”.

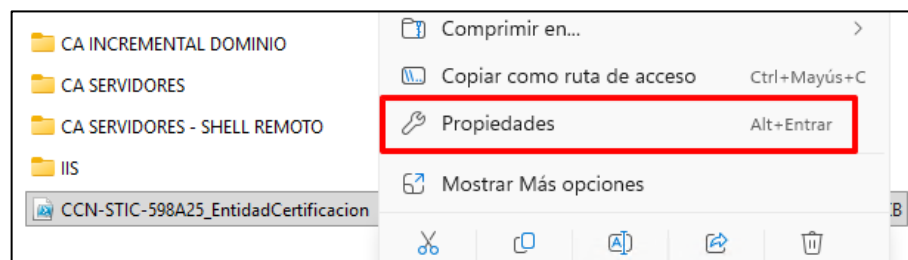


Ilustración 8 - Propiedades del script

11. En la parte inferior de la ventana emergente, marque la casilla “Desbloquear” si ésta aparece, y haga clic en “Aceptar”.

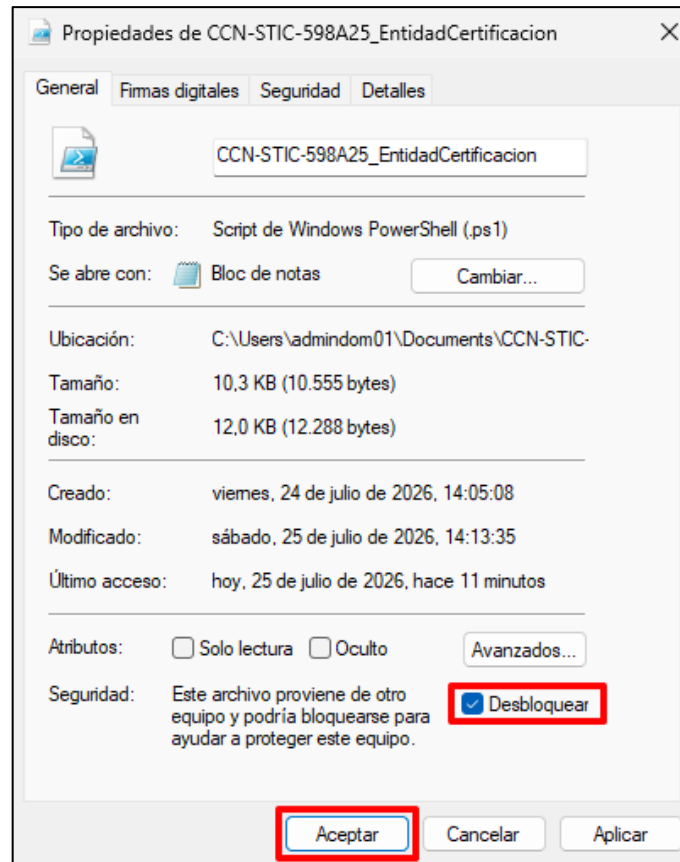


Ilustración 9 - Desbloqueo del script

12. Repita la misma operación con los archivos “.ps1” que se encuentran dentro de las cuatro subcarpetas de scripts.

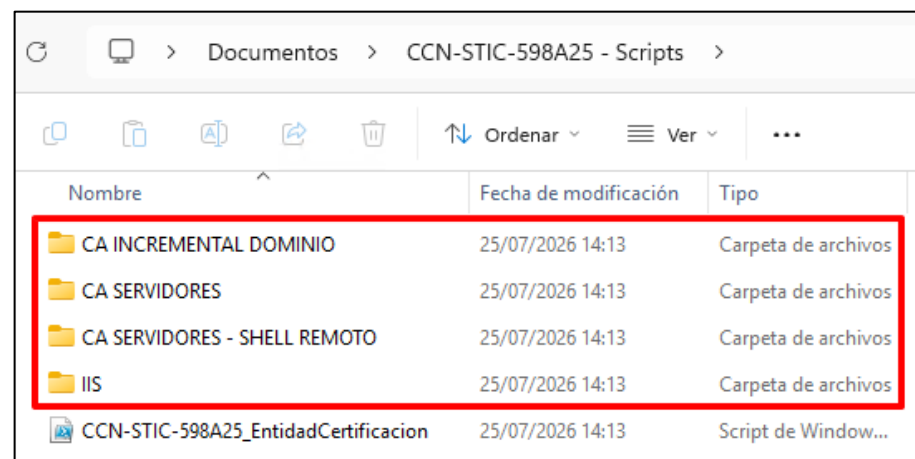


Ilustración 10 - Desbloqueo del resto de scripts

13. Sobre la barra de búsqueda, escriba “PowerShell”:

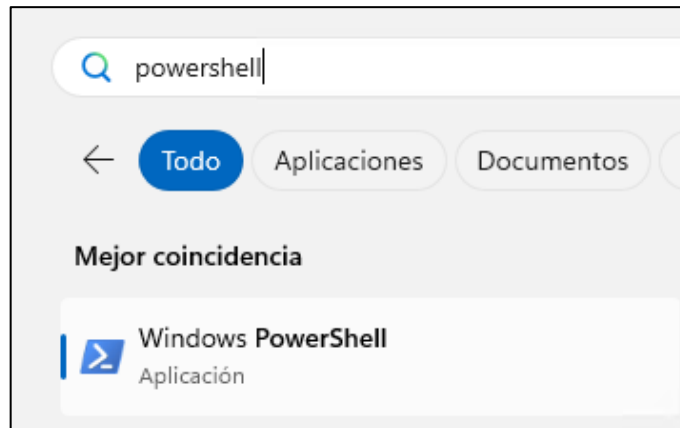


Ilustración 11 - Windows PowerShell

14. Haga clic derecho, y seleccione “Ejecutar como administrador”:

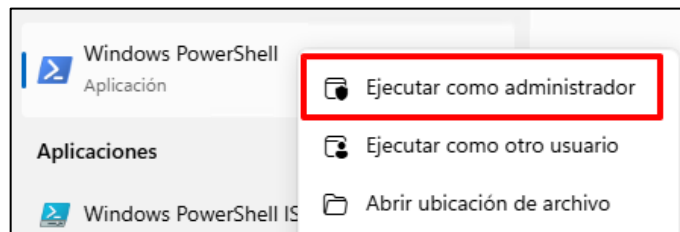


Ilustración 12 - Ejecución como administrador

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. Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

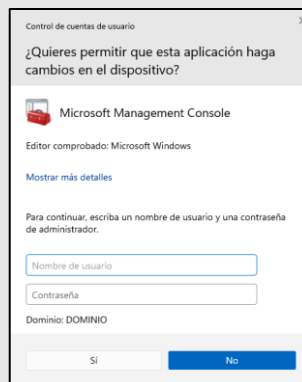


Ilustración 13 - Introduzca credenciales de administrador

15. 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”.

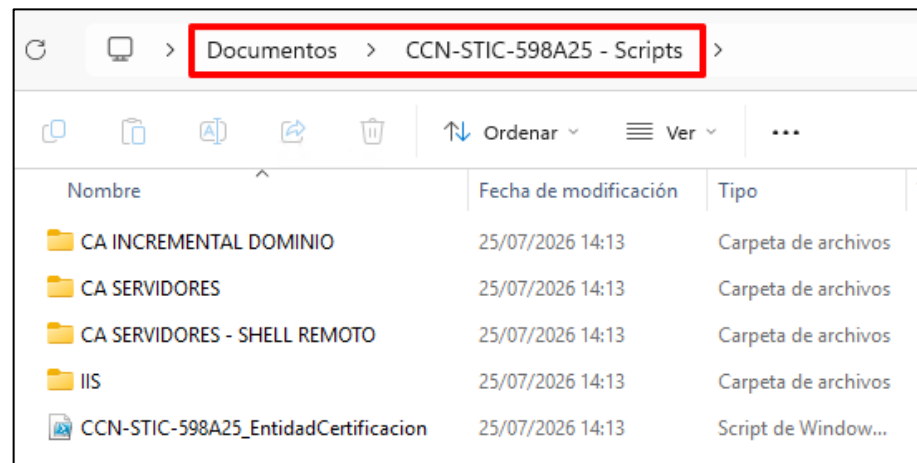


Ilustración 14 - Copia de ruta

16. Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.

```
PS C:\WINDOWS\system32> cd "C:\Users\admindom01\Documents\CCN-STIC-598A25 - Scripts"
```

Ilustración 15 - Acceso a la ruta

17. Ejecute el comando “dir” para verificar la ubicación y el contenido.

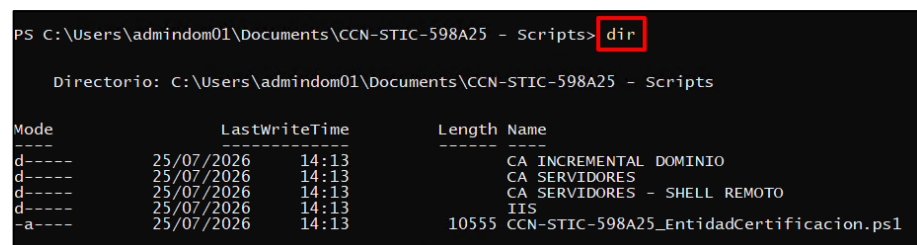


Ilustración 16 - Contenido de la carpeta

18. Ejecute el archivo “CCN-STIC-598A25_EntidadCertificacion.ps1” escribiendo “.” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.

```
PS C:\Users\admindom01\Documents\CCN-STIC-598A25 - Scripts> .\CCN-STIC-598A25_EntidadCertificacion.ps1
```

Ilustración 17 - Ejecución del script

19.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje. <pre> ---ADVERTENCIA--- Este script incorpora modificaciones en Active Directory orientadas a la aplicación de medidas de bastionado para servidores de Autoridad de Certificación, conforme a la guía CCN-STIC-598A25. Antes de continuar, revise el impacto de las GPO que se van a crear, importar y vincular. ---FIN ADVERTENCIA--- </pre> <i>Ilustración 18 - Advertencia</i>
20.	Escriba “S” y pulse “Enter”. <pre> ¿Desea aceptar los riesgos y continuar con el bastionado del sistema? Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S </pre> <i>Ilustración 19 - Aceptación de advertencia</i>
21.	En primer lugar, el script verificará que si se encuentra aplicada la GPO de IIS a la Unidad Organizativa de “Servidores IIS”. Como el Controlador de Dominio sólo tiene aplicada la guía 570A25, escriba “S” y pulse “Enter”. <pre> Comprobando Unidad Organizativa: OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores' ya existe. Comprobando Unidad Organizativa: OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores IIS' ya existe. Comprobando Unidad Organizativa: OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores Entidad de Certificación' ya existe. Jerarquía de OUs preparada correctamente: - OU=Servidores,DC=dominio,DC=local - OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local - OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local Comprobando si existe la GPO 'CCN-STIC-574 Incremental Servidores IIS'... ADVERTENCIA: No se ha encontrado la GPO 'CCN-STIC-574 Incremental Servidores IIS'. Se procederá a importar y vincular la GPO 'CCN-STIC-574 Incremental Servidores IIS'. ¿Desea continuar? Confirmacion Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S </pre> <i>Ilustración 20 – Verificación UO IIS</i> Nota: Si se ha implementado previamente la guía CCN-STIC-574A25 para IIS, el presente paso se omitirá.
22.	A continuación, se importará la GPO Incremental en dominio. Escriba “S” y pulse “Enter”. <pre> Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental Dominio'. ¿Desea continuar? Confirmacion Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S </pre> <i>Ilustración 21 - Implementación Incremental Dominio</i>

23. Después, se importará la GPO Incremental de Servidores Entidad de Certificación a la Unidad Organizativa correspondiente. Escriba “S” y pulse “Enter”.

```
Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental Servidor Entidad de Certificacion'. ¿Desea continuar?

Confirmacion
Seleccione una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S_
```

Ilustración 22 - Implementación Incremental Servidores CA

24. Por último, se importará la GPO Incremental shell remoto a la Unidad Organizativa correspondiente. Escriba “S” y pulse “Enter”.

```
Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental shell remoto' en la UO 'Servidores Entidad de Certificacion'. ¿Desea continuar? Esta se eliminará más adelante

Confirmacion
Seleccione una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S_
```

Ilustración 23 - Implementación Incremental shell remoto

Nota: La GPO Incremental shell remoto sólo será necesaria durante la configuración de Active Directory Certificate Services. Una vez se finalice la implementación de la guía, se darán las indicaciones para desvincularla. Si su entidad de certificación se encuentra instalada y configurada, puede omitir este paso.

25. Espere a que finalice la ejecución; al terminar, se mostrará un mensaje indicando las GPO que se han vinculado correctamente a las Unidades Organizativas correspondientes. Cierre el terminal de Powershell.

```
===== RESUMEN DE APLICACION =====
Se han aplicado satisfactoriamente las siguientes GPOs:
- CCN-STIC-574 Incremental Servidores IIS
- CCN-STIC-598A25 Incremental Dominio
- CCN-STIC-598A25 Incremental Servidor Entidad de Certificacion
- CCN-STIC-598A25 Incremental shell remoto
=====
```

Ilustración 24 - GPOs aplicadas correctamente

26. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

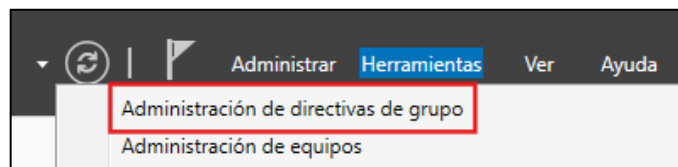
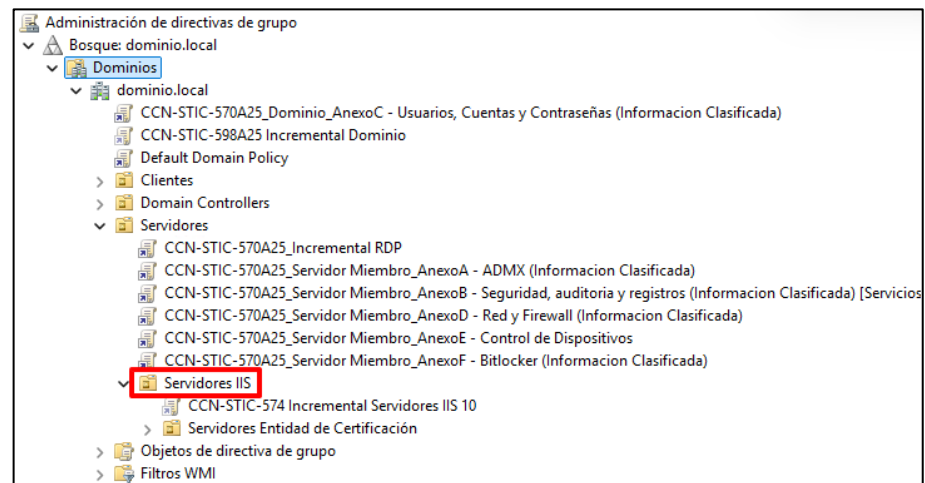


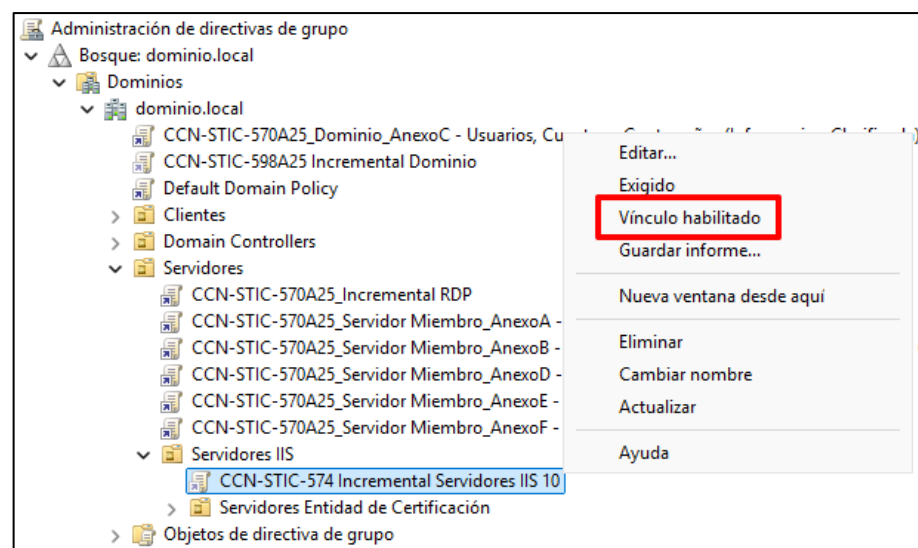
Ilustración 25 - Administración de directivas de grupo

27. Despliegue la lista del menú izquierdo hasta localizar el dominio y, a continuación, acceda a la Unidad Organizativa de “Servidores IIS”.



Ilustraci3n 26 - OU Servidores IIS

28. Despliegue dicha OU y haga clic derecho sobre el GPO “CCN-STIC-574 Incremental Servidores IIS 10”. Seleccione la opci3n “V3nculo habilitado”.



Ilustraci3n 27 - Habilitar GPO.

29. Despliegue la OU de “Servidores Entidad de Certificación” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Servidores Entidad de Certificación”. Seleccione la opción “Vínculo habilitado”. Haga lo mismo con el GPO “CCN-STIC-598A25 Incremental shell remoto”.

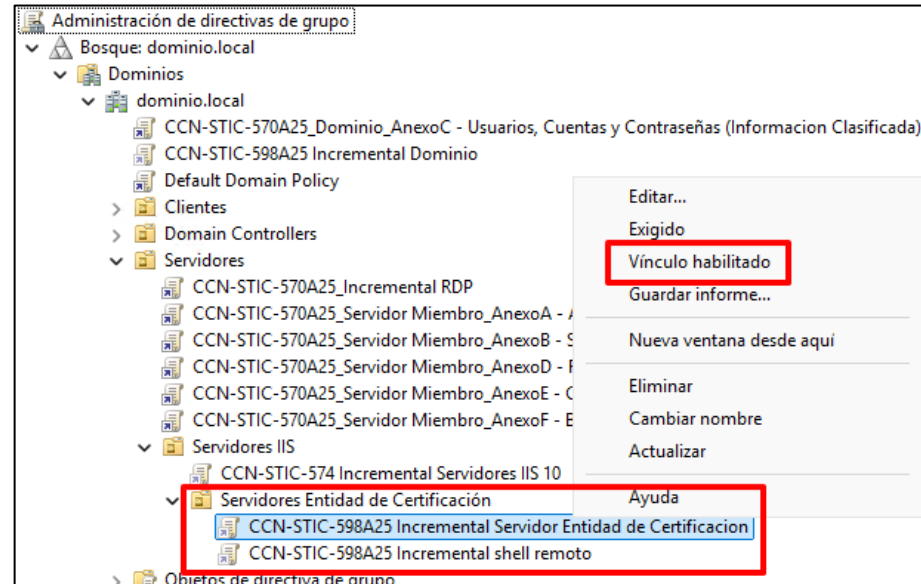


Ilustración 28 - Habilitar GPO CA

30. Diríjase a “dominio.local” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Dominio”. Seleccione la opción “Vínculo habilitado”.

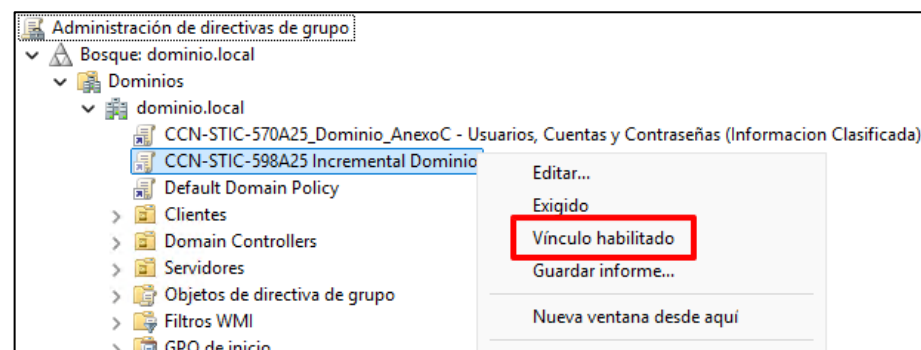


Ilustración 29 - Habilitar GPO Dominio

31. Haga clic sobre “dominio.local” y, en la parte derecha del Administrador de directivas de grupo, asegúrese de que la GPO “CCN-STIC-598A25 Incremental Dominio” se encuentra en primer lugar.

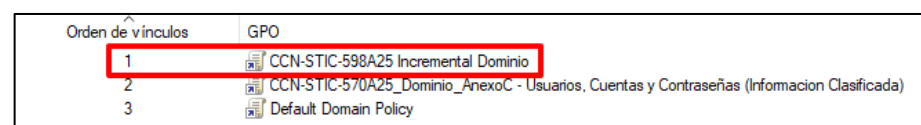


Ilustración 30 - Orden de las GPOs

32. De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior, y seleccione “Usuarios y equipos de Active Directory”.

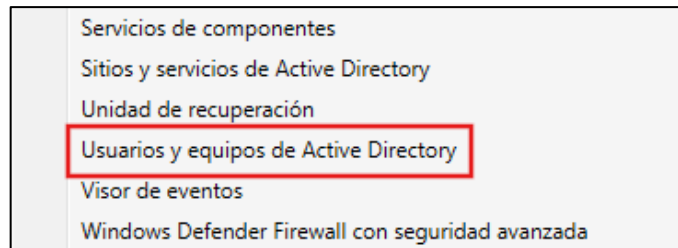


Ilustración 31 - Usuarios y equipos de Active Directory

33. Despliegue la lista del panel izquierdo hasta visualizar la OU “Servidores Entidad de Certificación”.

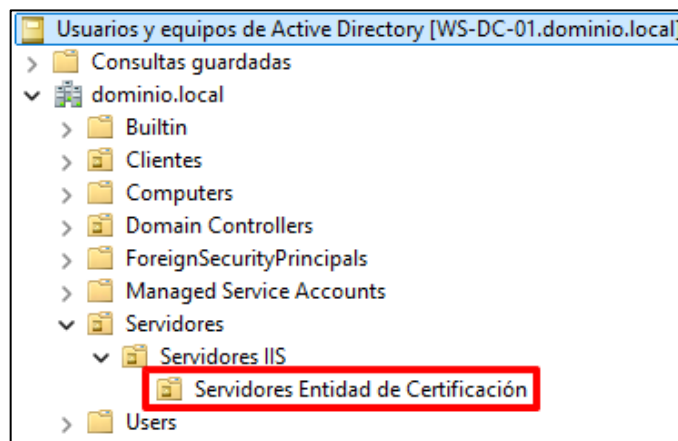


Ilustración 32 - OU Servidores Entidad de Certificación

34. Haga clic sobre la carpeta “Computers” y seleccione el servidor de Entidad de Certificación (en este caso, CAENT01).

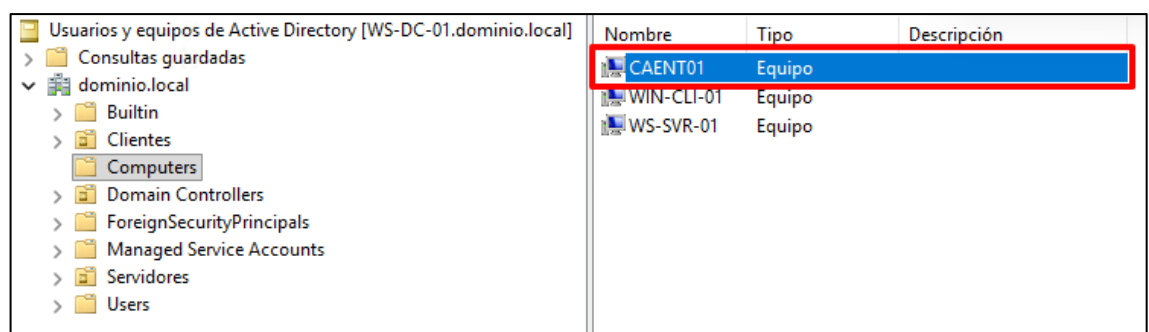


Ilustración 33 - Selección del servidor.

35. Arrástrelo a la OU “Servidores Entidad de Certificación”. Aparecerá una advertencia. Haga clic en “Sí”.
Puede cerrar la ventana de “Usuarios y equipos de Active Directory”.

36. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

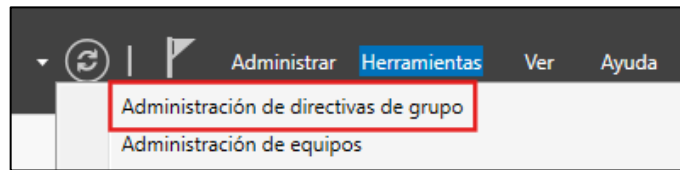


Ilustración 34 - Administración de directivas de grupo

37. Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.

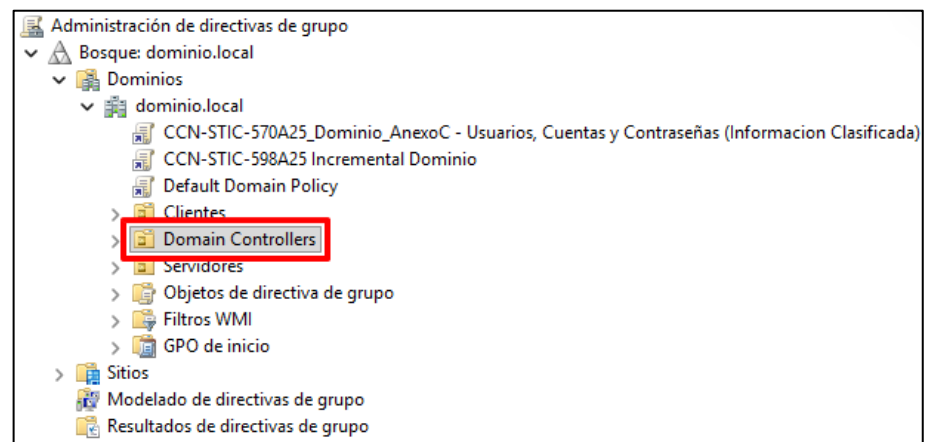


Ilustración 35 - OU Domain Controllers

38. Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

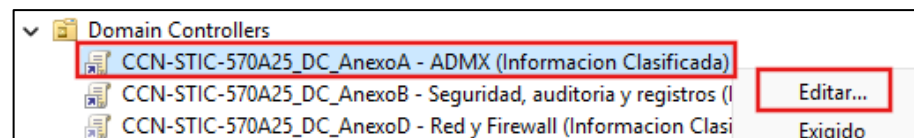


Ilustración 36 - Edición ADMX 570A25

39. 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.

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 37 - Políticas de PowerShell

40. Haga doble clic sobre la política “Activar la ejecución de scripts”.

41. En el desplegable de la política, seleccione “Permitir solo scripts firmados”, y haga clic en “Aplicar” y “Aceptar”.

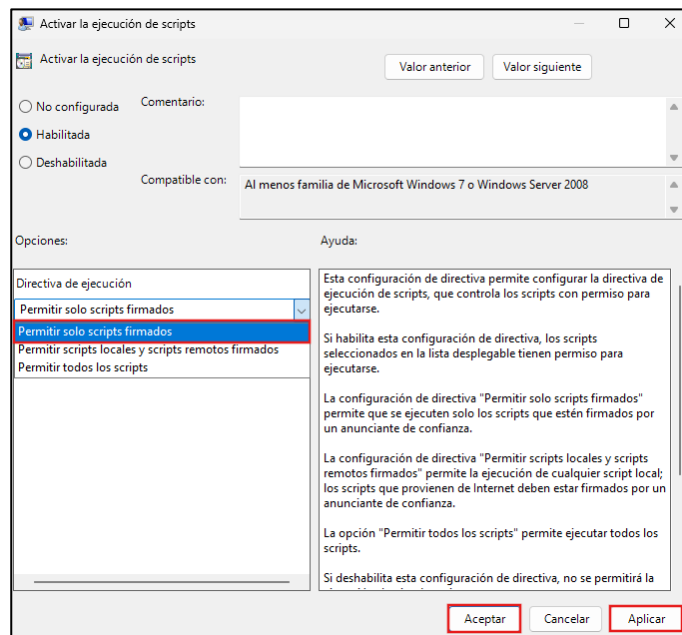


Ilustración 38 - Selección de "Permitir solo scripts firmados"

42. Reinicie el controlador de dominio para que se aplique la configuración correctamente.

6.1.2. PASO A PASO DE INSTALACIÓN DE ENTIDAD DE ENTIDAD DE CERTIFICACIÓN ENTERPRISE

Los pasos descritos a continuación corresponden a la configuración inicial de la Entidad de Certificación partiendo de un entorno sin configuración previa.

Nota: Si su entidad de certificación ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
43.	Inicie sesión en el equipo donde se va a instalar el servidor Entidad de Certificación del dominio.

44. A continuación, se ejecutará el Administrador del servidor para configurar el servidor de Entidad de Certificación.

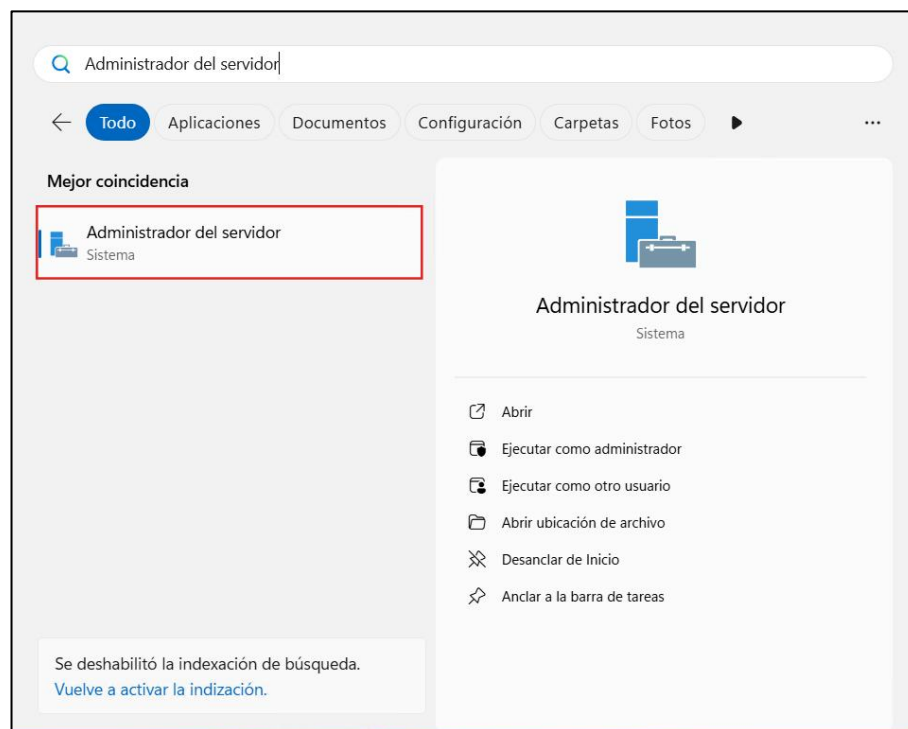


Ilustración 39 - Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

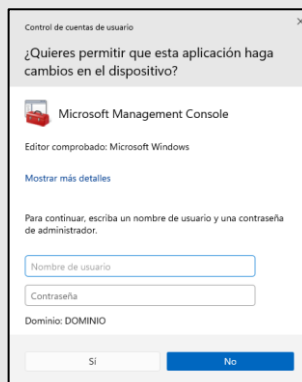


Ilustración 40 - Introducir credenciales de administrador

45. Le aparecerá una ventana para proceder con la configuración, pulse en “Configurar Servicios de certificados de Active Directory”.



Ilustración 41 - Configurar Servicios de certificados de Active Directory

Nota: Si el rol de “Servicios de certificados de Active Directory no ha sido implementado en el equipo esta advertencia no se mostrará. Se ha de instalar manualmente antes de comenzar con la configuración de este procedimiento.

46. Especifique las credenciales para configurar servicios de rol. Pulse en “Siguiente”.

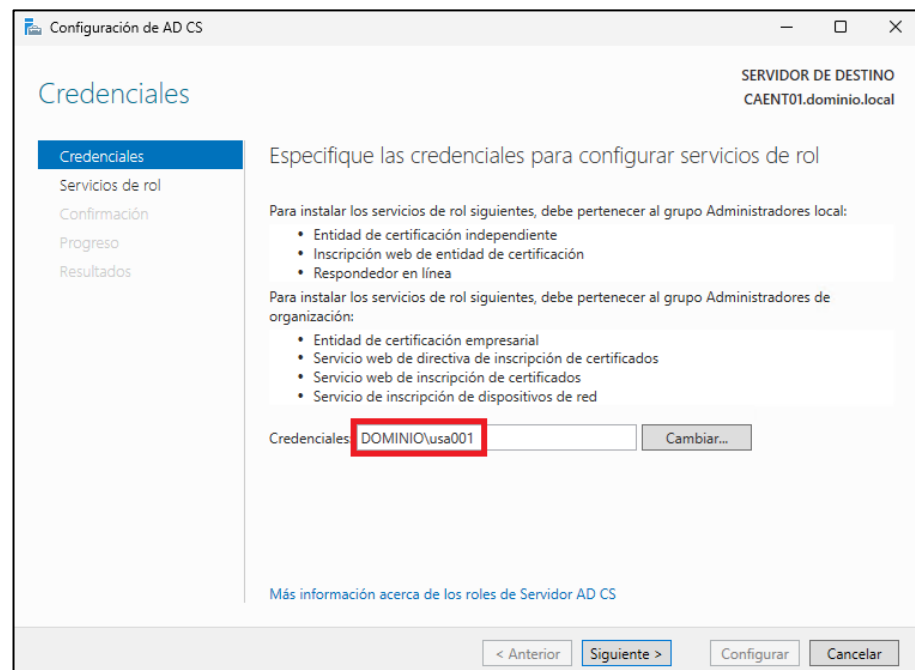


Ilustración 42 – Especificación de credenciales

Nota: El usuario administrador que se utilizará en todo el escenario será **usa001**.

47. Seleccione los servicios de rol que dispondrá el servidor de Entidad de Certificación. En el presente caso serán “Entidad de certificación” e “Inscripción web de entidad de certificación”. Pulse en “Siguiente”.

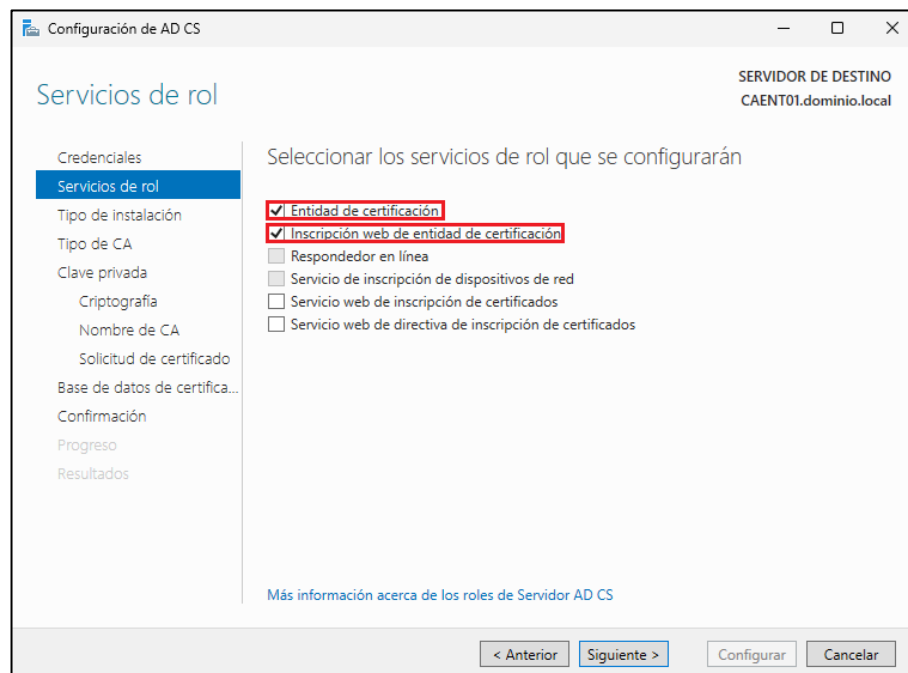


Ilustración 43 - Servicios de rol

48. Especifique el tipo de instalación de la CA, seleccione “CA empresarial”. Pulse en “Siguiente”.

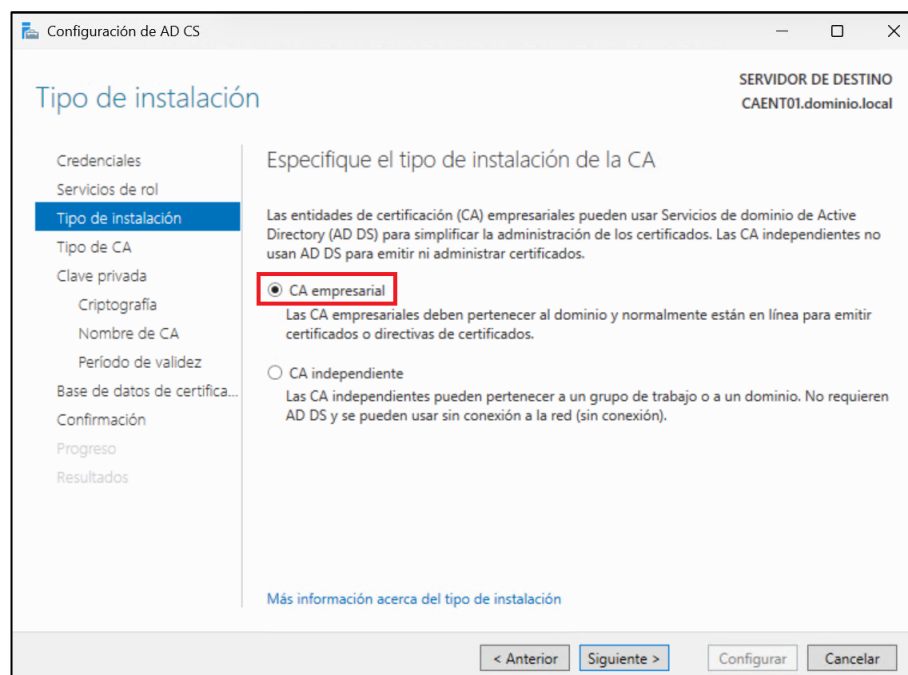


Ilustración 44 – Especificación del tipo de instalación de CA

49. Seleccione “CA raíz”. Pulse en “Siguiente”.

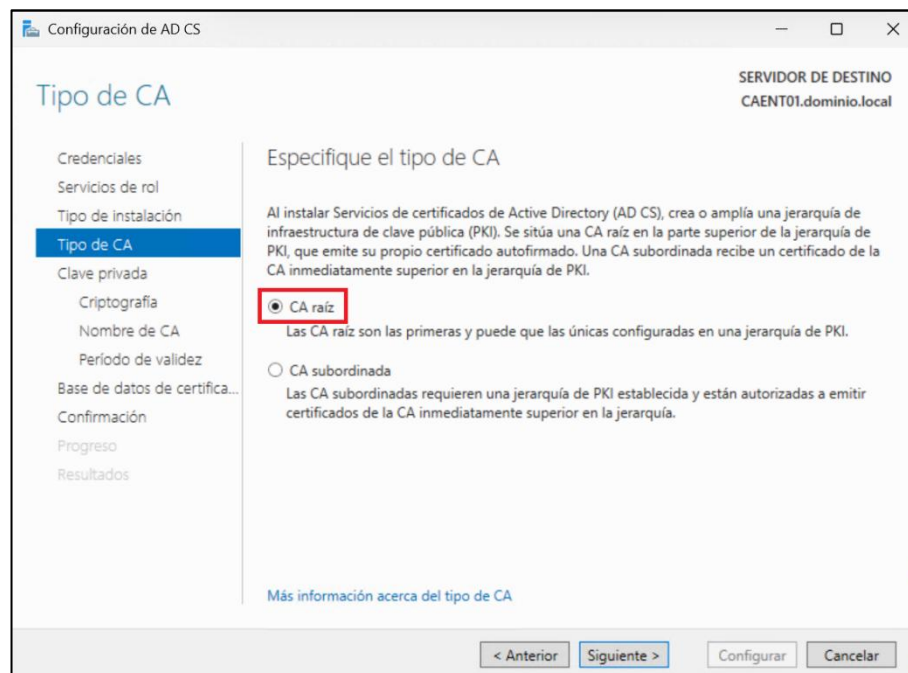


Ilustración 45 – Especificación de CA

50. A continuación, seleccione la opción de “Crear una clave privada nueva”. Pulse en “Siguiente”.

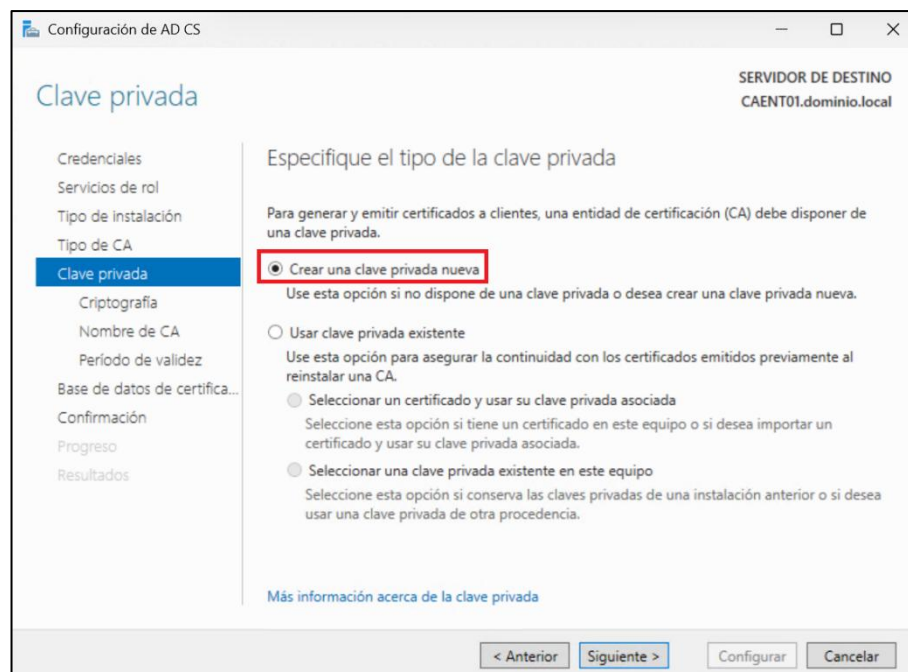


Ilustración 46 – Creación de una clave privada

51. Las opciones criptográficas que se seleccionarán serán.

- Longitud: 2048
- Tipo de algoritmo hash: SHA256

Posteriormente, pulse en “Siguiente”.

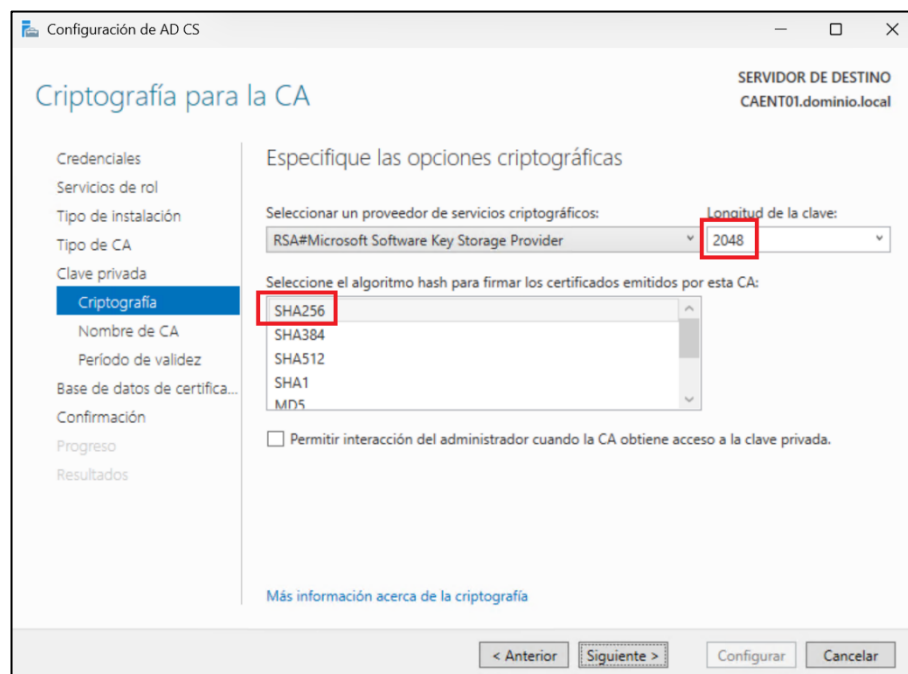


Ilustración 47 – Especificar las opciones criptográficas

52. A continuación, se especificará el nombre para la entidad de certificación. En el presente caso, será “dominio-CAENT01-CA”. Posteriormente, pulse en “Siguiente”.

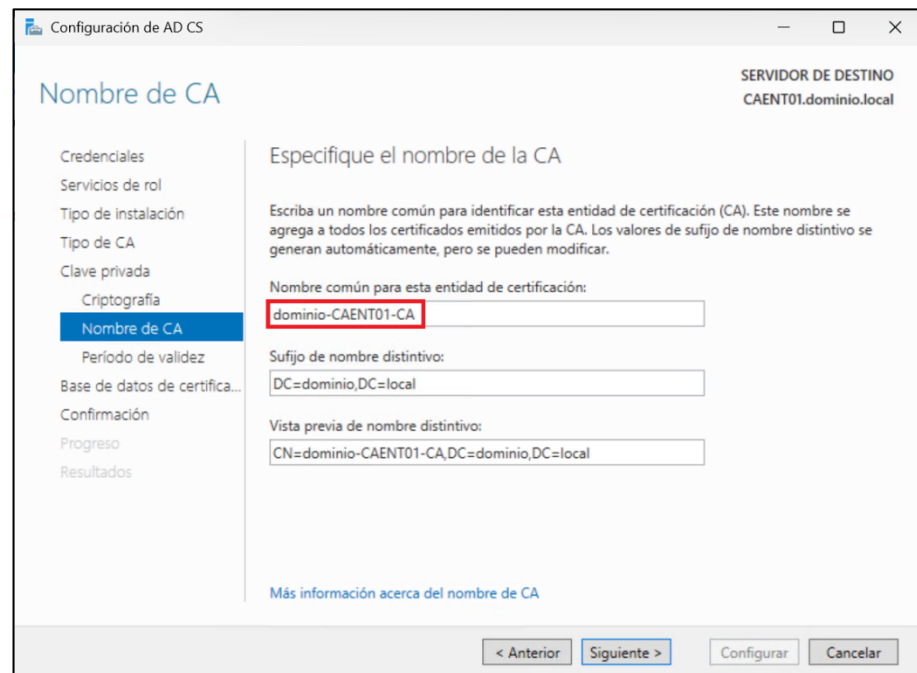


Ilustración 48 – Especificar el nombre de la CA empresarial

53. Especifique el período de validez para el certificado para esta entidad de certificación. Se establecerá en 5 años. Pulse en “Siguiente”.

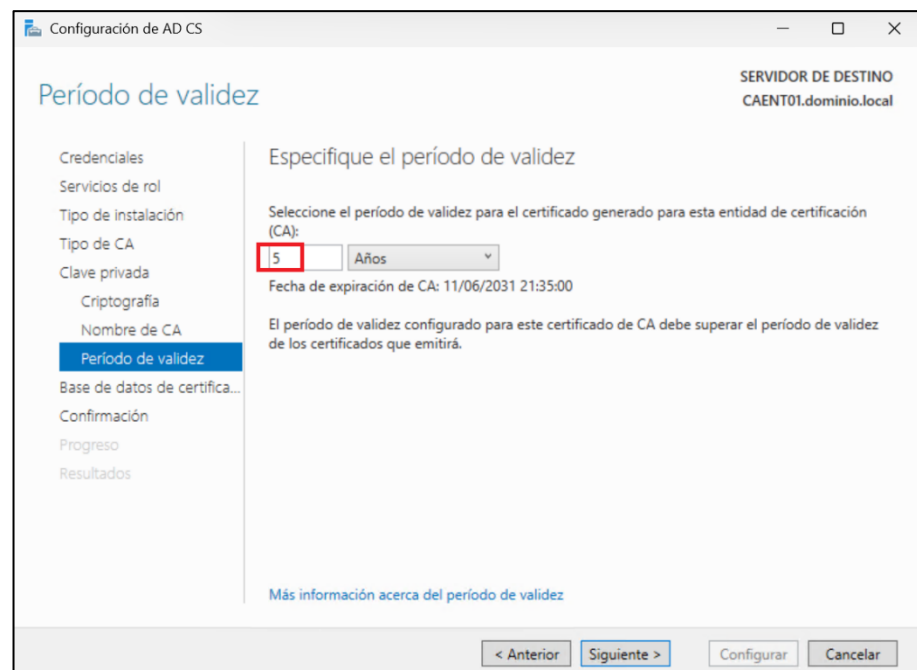


Ilustración 49 – Especificación de período de validez

54. En la siguiente página se especificarán las ubicaciones donde se almacenarán los certificados. Se establecerán las carpetas por defecto. Pulse en “Siguiente”.

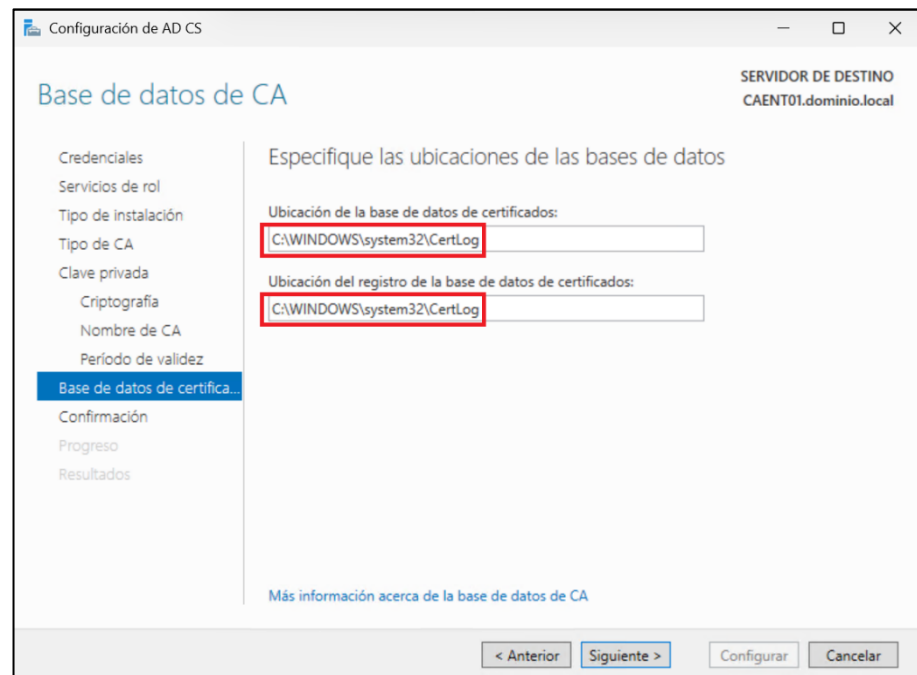


Ilustración 50 – Ubicación de bases de datos

Nota: Si su entorno dispone de un sitio específico, deberá indicarlo en este apartado.

55. Finalmente, se visualiza un resumen de toda la configuración. Pulse en “Configurar”.

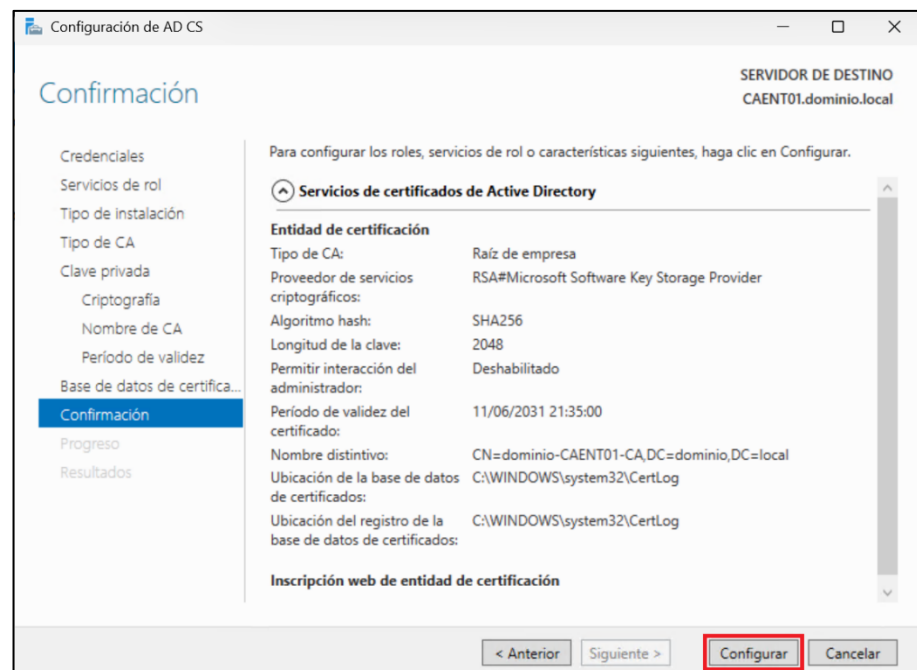


Ilustración 51 – Resumen de la configuración

56. Una vez haya terminado el proceso, aparecerá una ventana que le preguntará si desea configurar servicios de rol adicionales. Pulse “Sí”.

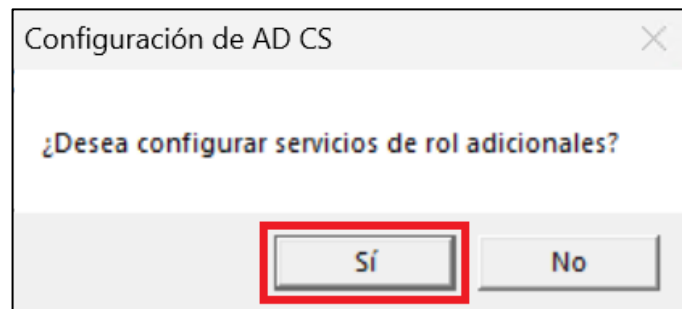


Ilustración 52 – Ventana de aviso

57. Los roles adicionales que se seleccionarán serán “Servicio web de inscripción de certificados” y “Servicio web de directiva de inscripción de certificados”. Posteriormente, pulse en “Siguiente”.

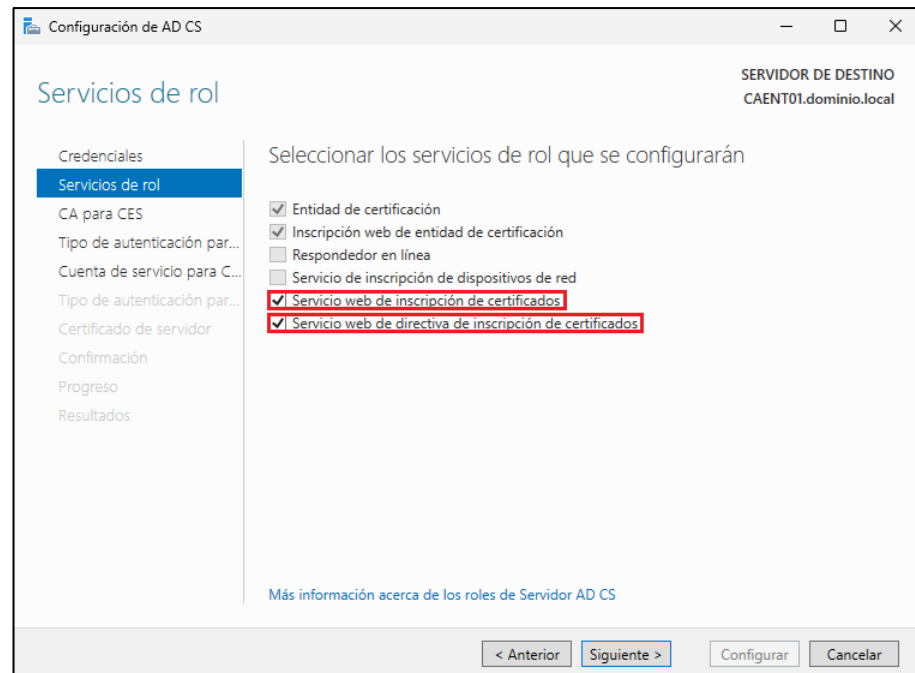


Ilustración 53 – Servicios de rol que se configurarán

Nota: Si su entorno no necesita estos roles, no es necesario su aplicación. Puede continuar con siguientes apéndices.

58. Se especificará la CA para los Servicios web de inscripción de certificados. Seleccione la opción de “Nombre de CA”. Posteriormente, pulse en “Siguiente”.

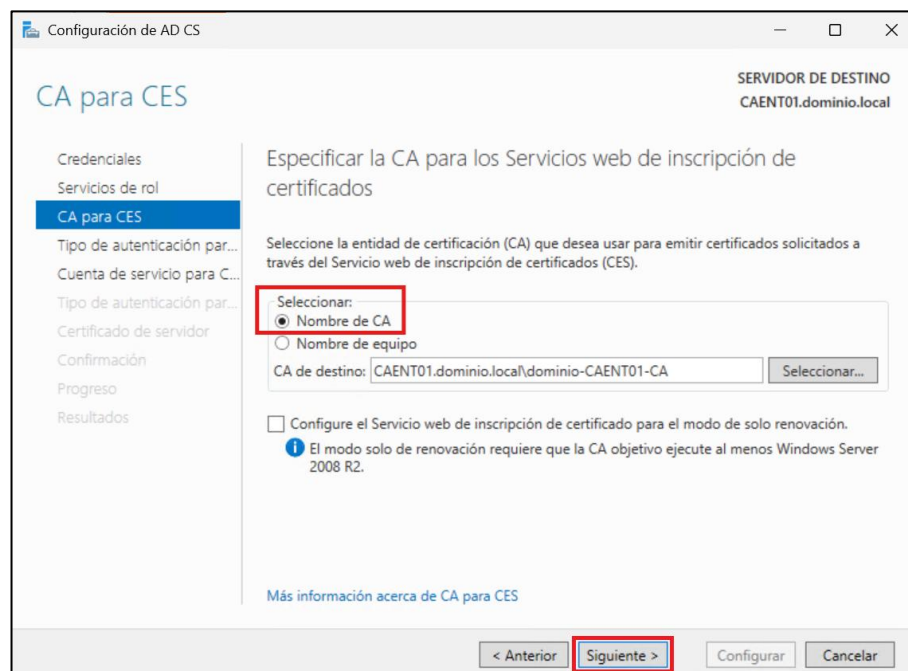


Ilustración 54 – Especificar el nombre de la CA

59. El tipo de autenticación será “Autenticación integrada de Windows”. Pulse en “Siguiente”.

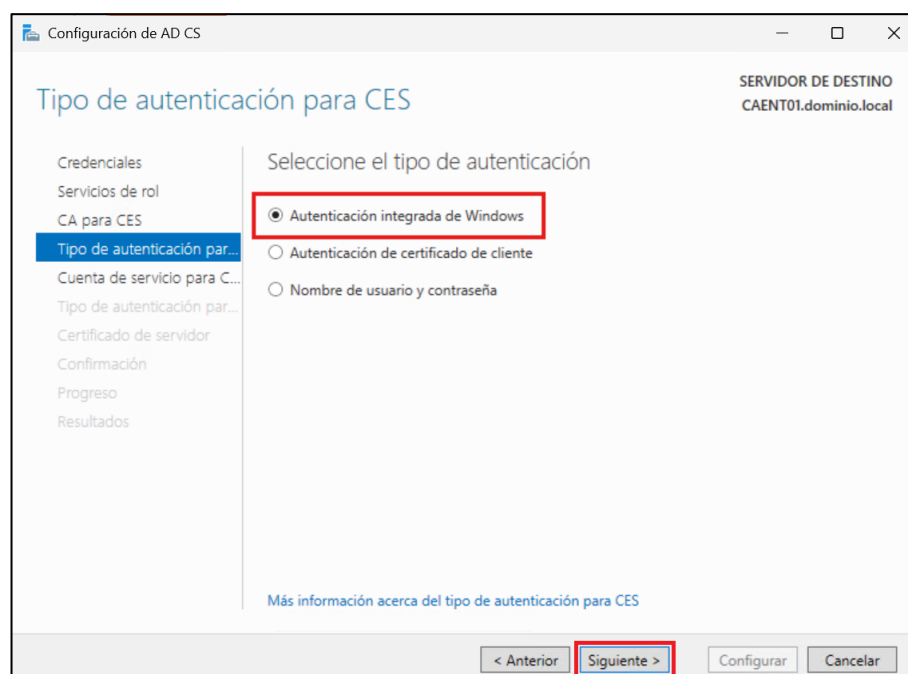


Ilustración 55 – Selección del tipo de autenticación

60. Mantenga seleccionada la opción de “Usar la identidad del grupo de aplicaciones integrada”. Pulse en “Siguiente”.

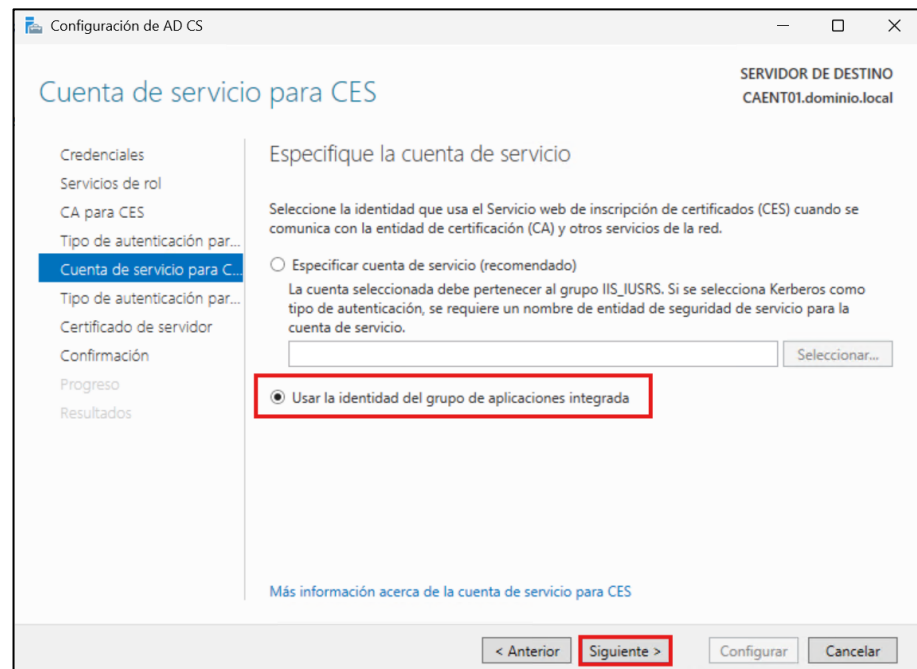


Ilustración 56 – Usar la identidad del grupo de aplicaciones integrada

61. Seleccione de nuevo “Autenticación integrada de Windows” en la selección del tipo de autenticación y a continuación, pulse en “Siguiente”.

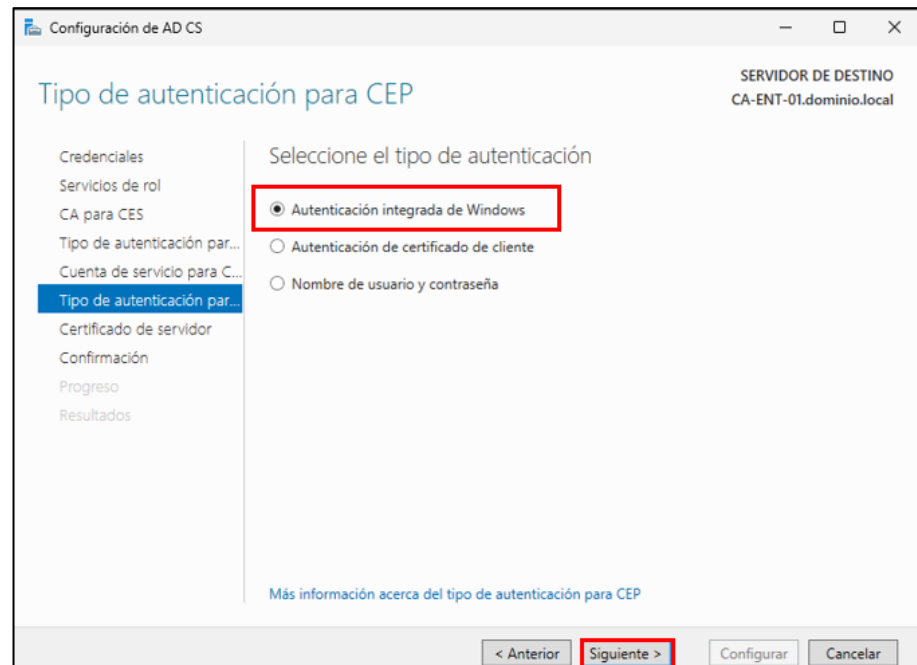


Ilustración 57 - Selección del tipo de autenticación

62. A continuación, seleccione el certificado del equipo de Entidad de Certificación para el cifrado SSL. Posteriormente, pulse en “Siguiente”.

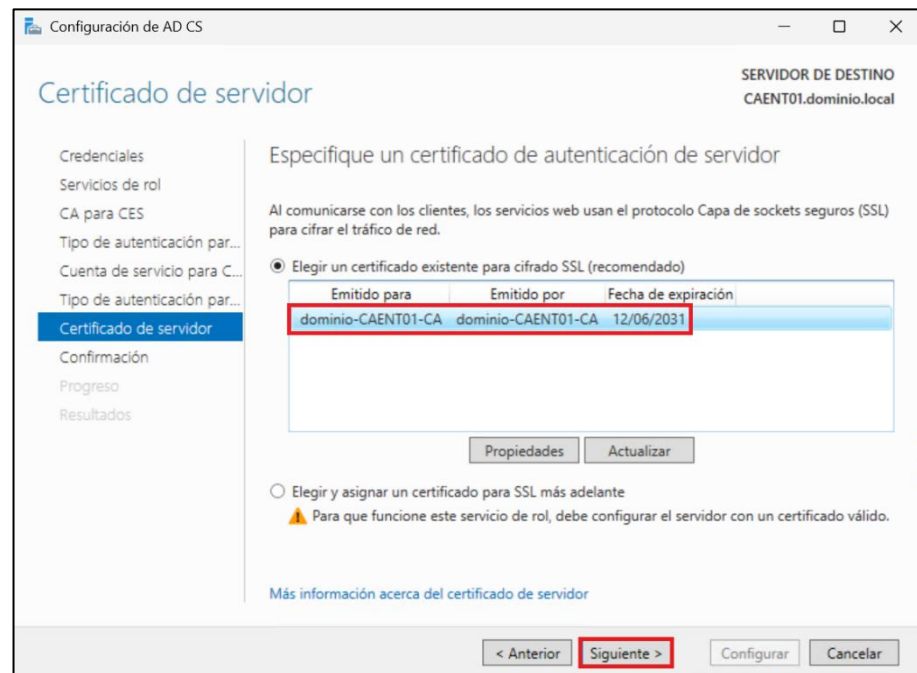


Ilustración 58 – Selección del certificado de autenticación

63. Finalmente, se visualiza un resumen de todo el progreso. Una vez revisado, pulse en “Configurar”.

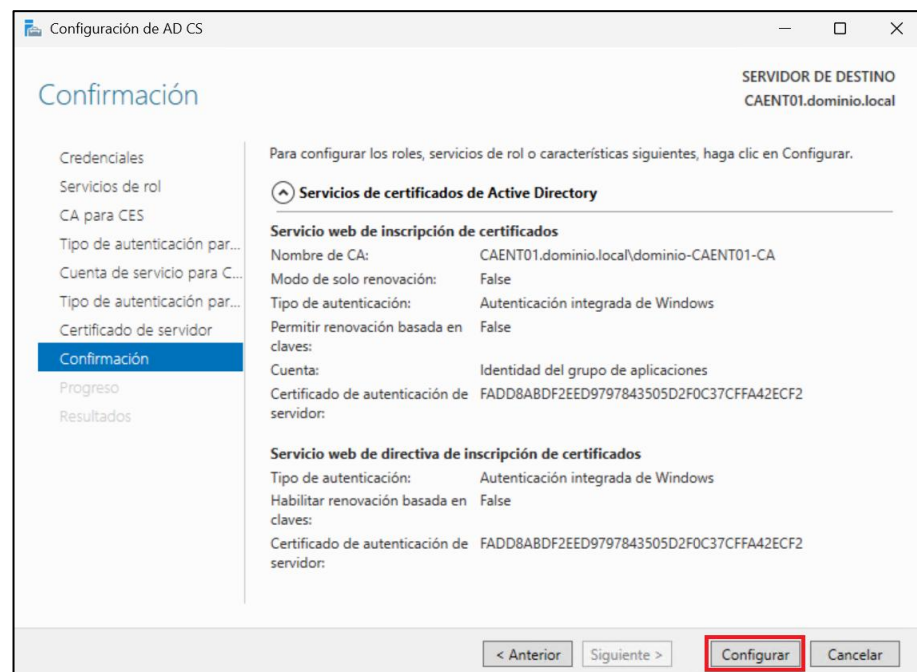
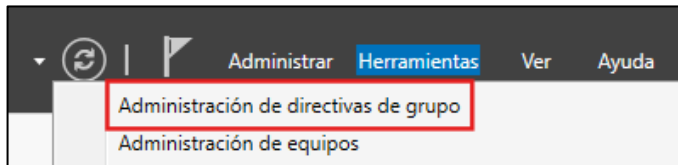
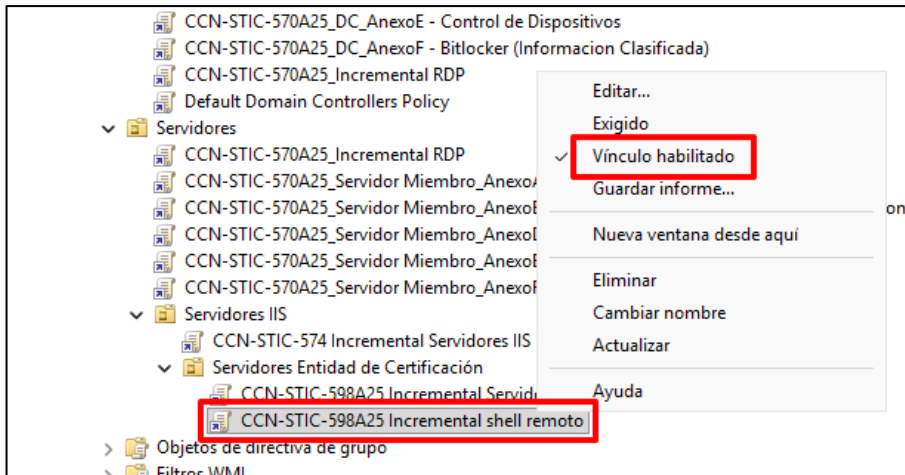


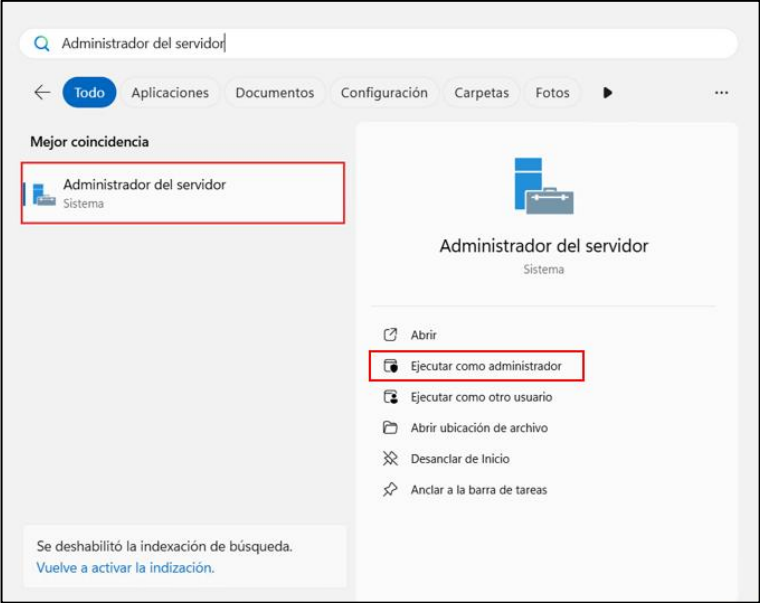
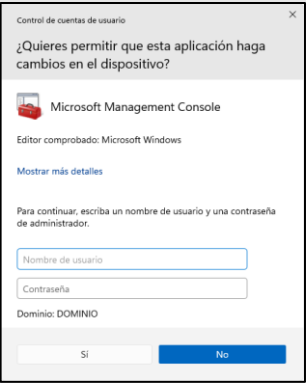
Ilustración 59 – Resumen de configuración de certificados

64.	El servidor se encuentra actualmente configurado y listo para emitir certificados en el dominio.
65.	Por último, se deberá desvincular o deshabilitar la GPO “CCN-STIC-598A25 Incremental shell remoto”. Para ello, inicie sesión en un controlador de dominio con un usuario perteneciente al grupo “Admins. del dominio”.
66.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  <i>Ilustración 60 - Administración de directivas de grupo</i>
67.	Diríjase a la OU “Servidores Entidad de Certificación”, haga clic derecho sobre la GPO “CCN-STIC-598A25 Incremental shell remoto” y haga clic sobre “Vínculo habilitado” para deshabilitar el vínculo”.  <i>Ilustración 61 - Desvinculación de GPO incremental shell remoto</i>
68.	Habrá finalizado la configuración y los usuarios podrán solicitar nuevos certificados a la entidad.

6.1.3. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN ENTERPRISE.

En este apartado, se establecerá la configuración que permite que un sitio web mantenga las CRLs de modo que sean accesibles por todos los clientes de la Entidad de Certificación.

Nota: Si su entidad de certificación ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
69.	Inicie sesión con un usuario administrador en el controlador de dominio del entorno donde se ha implementado la entidad de certificación raíz.
70.	Inicie la consola “Administrador del servidor” con privilegios de administración.  <i>Ilustración 62 - Administrador del servidor</i> Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 63 - Introducir credenciales de administrador</i>

71. En el panel de administración del servidor, haga clic en “Herramientas” y posteriormente en “DNS” para iniciar la consola de administración del servicio de nombres.

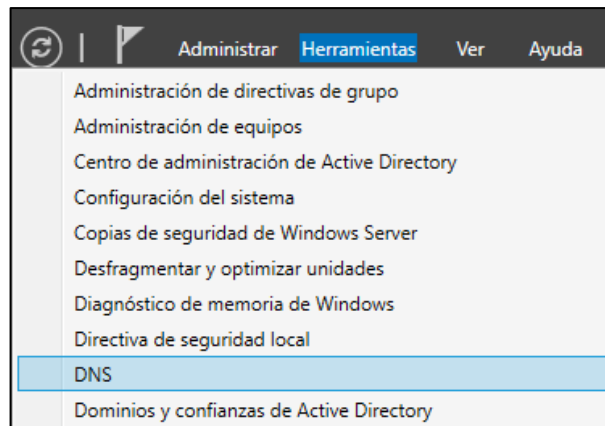


Ilustración 64 - Acceso a la consola DNS

72. Despliegue las zonas de búsqueda directa del árbol de dominio y pulse con el botón derecho sobre “dominio.local”. A continuación, haga clic sobre “Alias nuevo (CNAME)”.

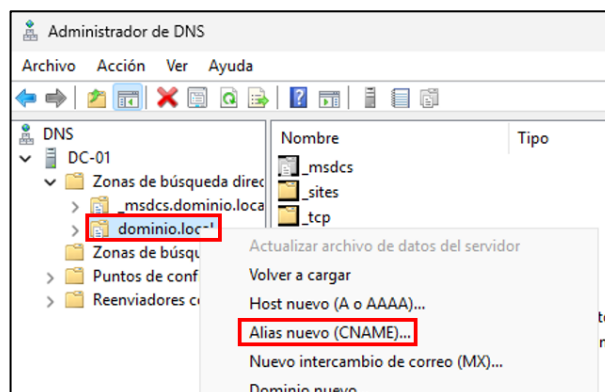


Ilustración 65 - Creación de CNAME

73. En el campo “Nombre de alias”, introduzca el nombre alternativo que se desea configurar como, por ejemplo, “crl”.

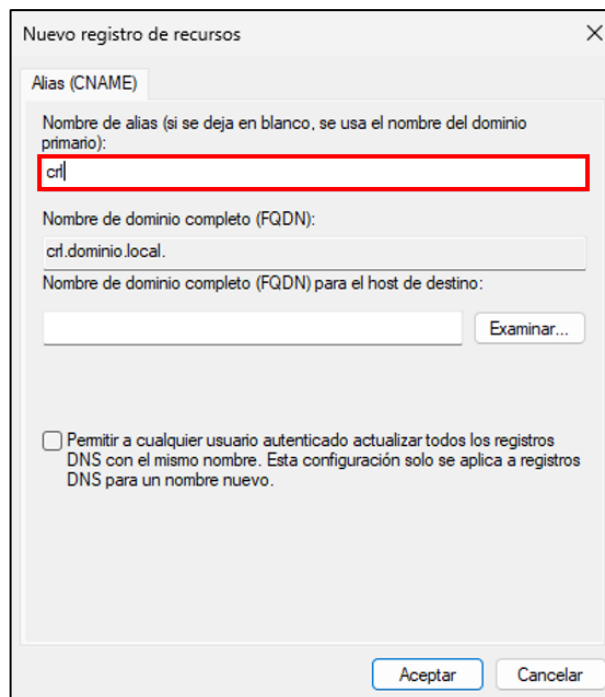


Ilustración 66 - Creación de CNAME

74. Haga clic en “Examinar” y navegue hasta el nombre de la entidad de certificación enterprise que se utilizará para publicar la CLR. A continuación, pulse en “Aceptar”.

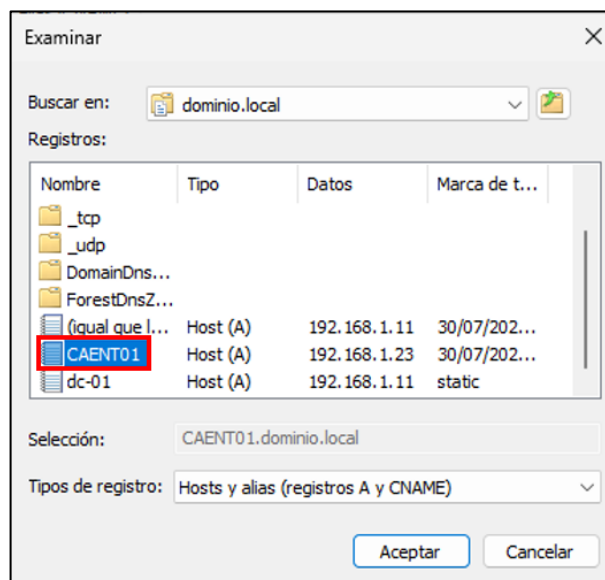


Ilustración 67 - Selección de objeto para el alias

75. De nuevo, pulse en “Aceptar” para registrar la creación del CNAME.

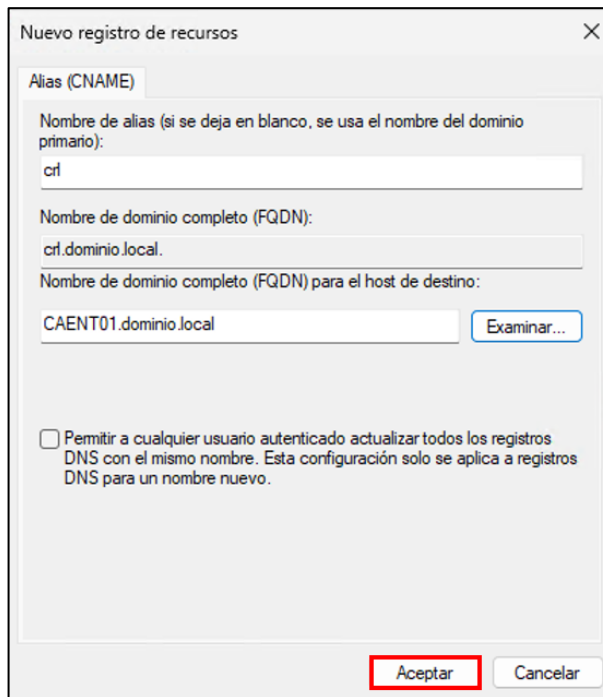


Ilustración 68 - Creación de CNAME

76. Cierre la consola de administración DNS y cierre la sesión en el controlador de dominio. Del mismo modo, inicie sesión en el servidor de entidad de certificación recién configurado con un usuario con privilegios administrativos.

77. En el panel de administración del servidor, pulse en “Herramientas”, y a continuación “Entidad de certificación”.

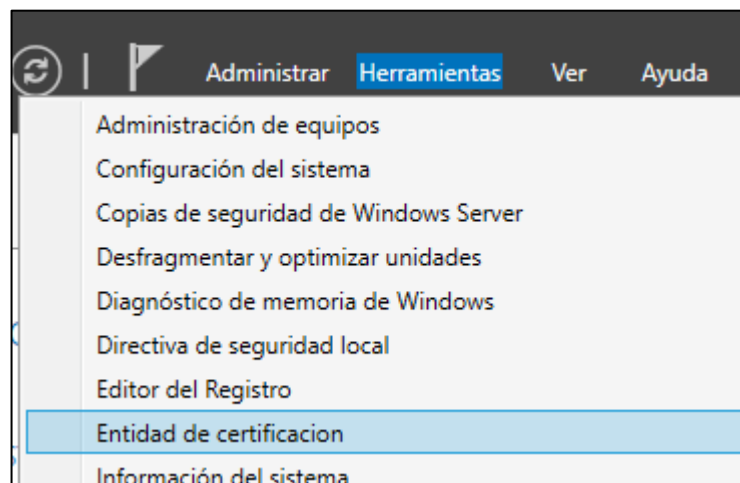


Ilustración 69 - Administración de Entidad de Certificación

78. Haga clic sobre el nombre de la entidad de certificación, y posteriormente en propiedades.

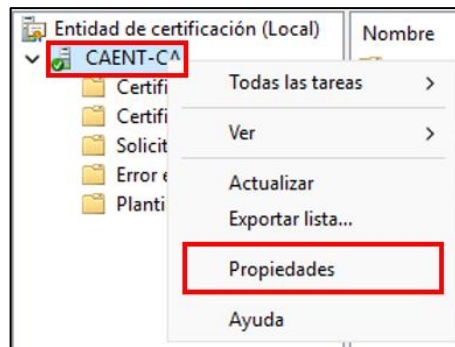


Ilustración 70 - Propiedades de la configuración de la CA

79. En la ventana de "Propiedades" diríjase a la pestaña "Extensiones" y, manteniendo seleccionada la extensión "Puntos de distribución de lista de revocación de certificados (CDP)", revise la publicación de CRLs mediante la ruta local seleccionando "C:\Windows\System32\CertSrv\CertEnroll\

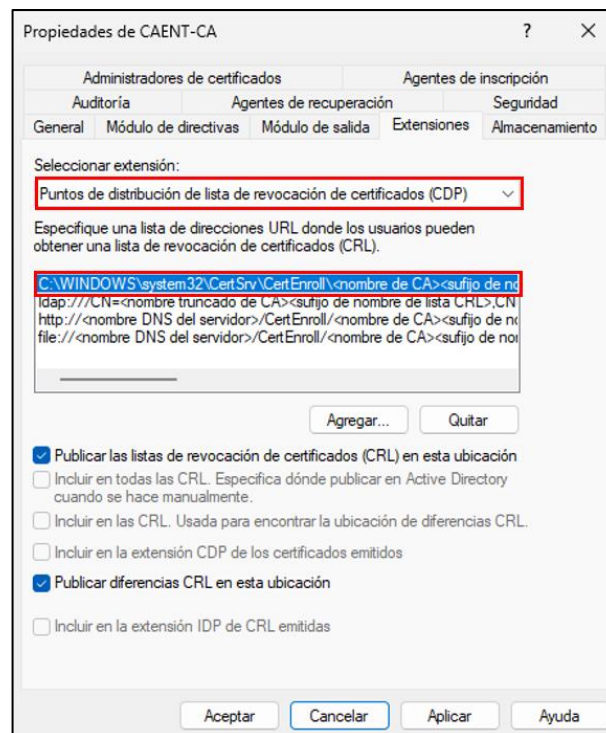


Ilustración 71 - Confirmación de configuración de extensión

80. A continuación, deshabilite la publicación de CRLs mediante LDAP seleccionando “ldap://CN=<nombre truncado de CA>< sufijo de nombre de lista CRL>,CN=nombre corto del servidor>,CN=CDP,CN=Public Key Services,<contenedor de configuración><clase de objeto CDP>”. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.

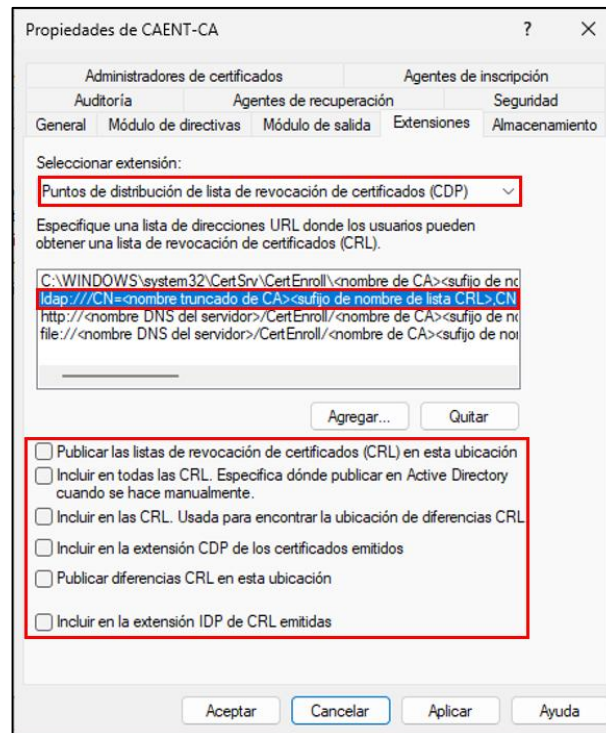


Ilustración 72 - Configuración de extensión LDAP

81. Para continuar, seleccione “file://<nombre DNS del servidor>/CertEnroll/<nombre de CA>/sufijo de nombre de lista CRL<diferencias entre listas CRL permitidas>.crl” y desmarque todas las opciones como muestra la siguiente figura.

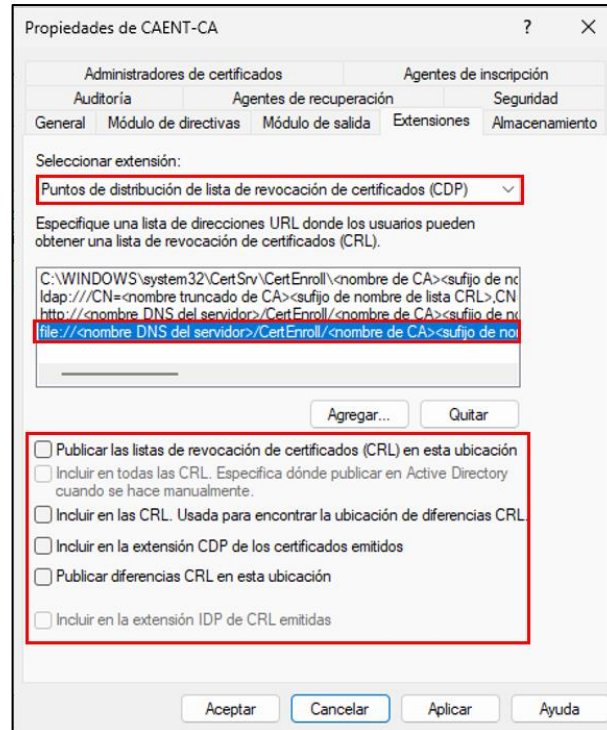


Ilustración 73 - Configuración de extensión "file"

82. Una vez realizada dicha configuración, seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre de CA><sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y pulse “Control + C”, para copiar el objeto.

83. Pulse en “Agregar”.

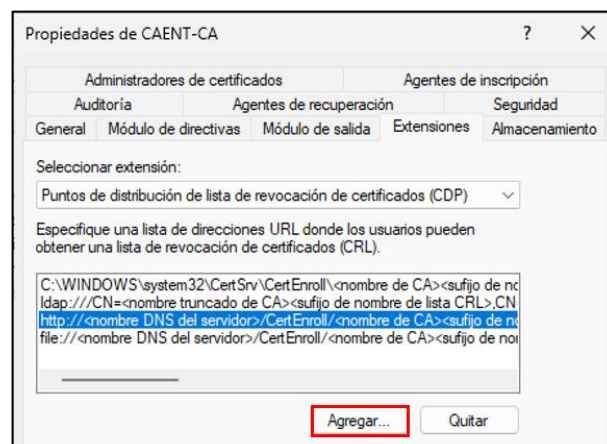
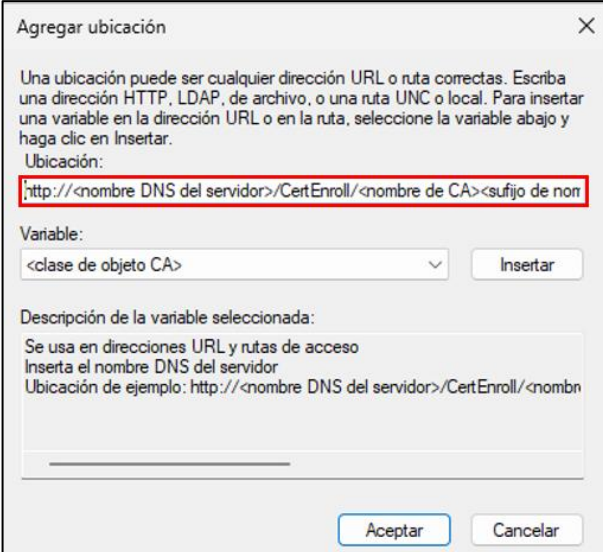


Ilustración 74 - Adición de extensión HTTP

84. En el campo “Ubicación”, pegue la ruta copiada en el paso anterior.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de non

Variable:

<clase de objeto CA>

Insertar

Descripción de la variable seleccionada:

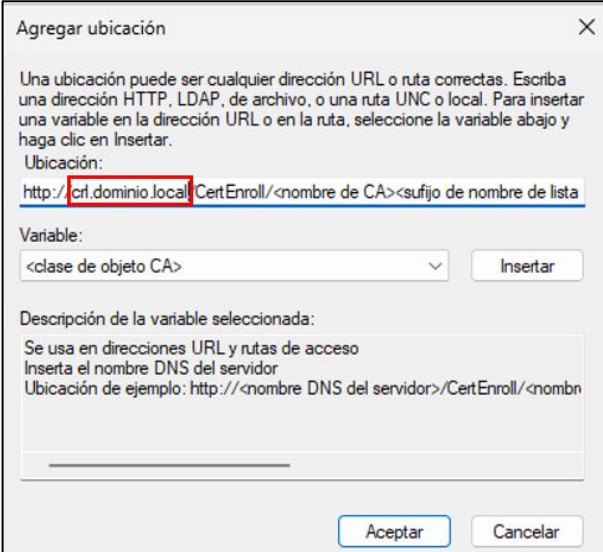
Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 75 - Pegar mediante CTRL+V

Nota: No pulse el botón “Aceptar”.

85. Localice “<nombre DNS del servidor>” al inicio de la ruta, y sustitúyalo por el CNAME generado al inicio de este procedimiento.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://crl.dominio.local/CertEnroll/<nombre de CA>< sufijo de nombre de lista

Variable:

<clase de objeto CA>

Insertar

Descripción de la variable seleccionada:

Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 76 - Sustitución de Nombre DNS por alias CNAME

86. Pulse sobre el botón “Aceptar” y a continuación, seleccionando la nueva entrada, marque los siguientes componentes.

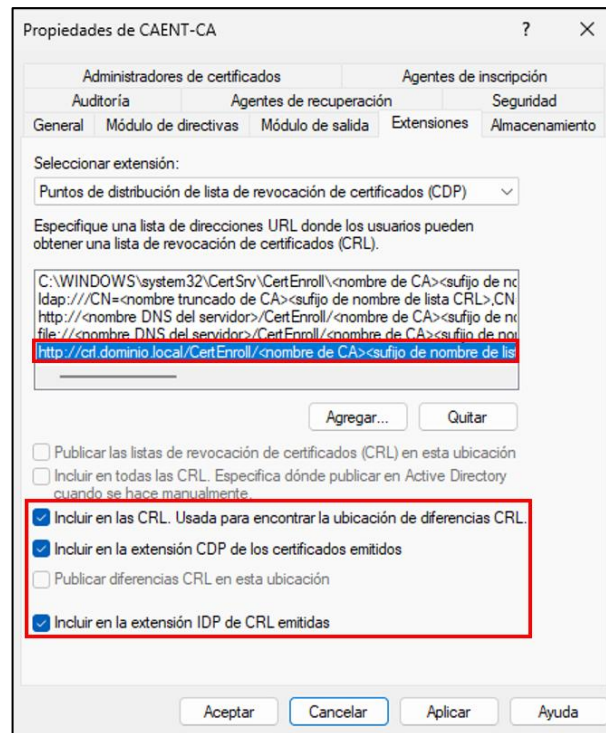


Ilustración 77 - Configurar opciones de extensión

87. Para continuar, en el desplegable “Seleccionar extensión”, elija “Acceso a la información de entidad (AIA)”.

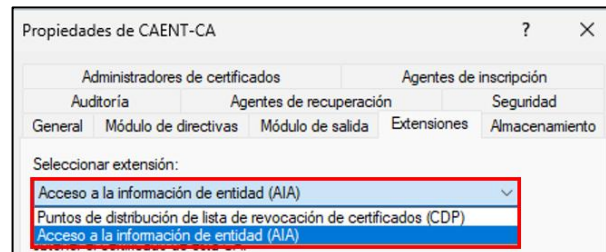


Ilustración 78 - Selección de "Acceso a la información de entidad AIA"

88. Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\

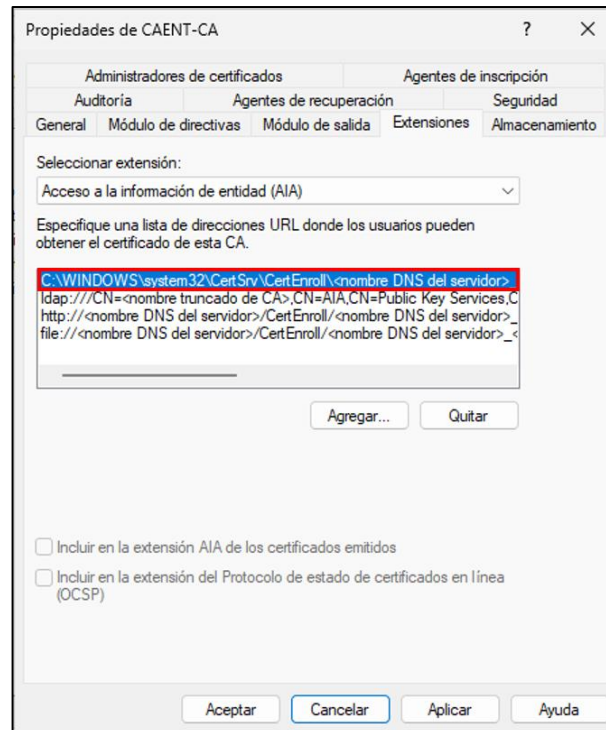


Ilustración 79 - Comprobación de extensión

89. Seleccione el objeto “ldap://CN=<nombre truncado de CA>,CN=AIA,CN=Public Key Services,CN=Services,<contenedor de configuración><clase de objeto CA>” y desmarque todas las casillas tal y como se muestra en la siguiente figura.

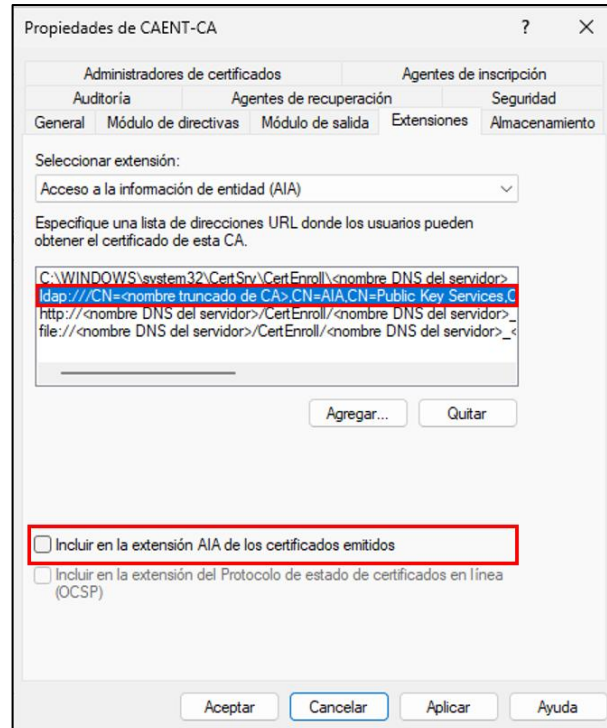


Ilustración 80 - Configuración de extensión LDAP

90. Seleccione ahora “file://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y confirme que la opción “Incluir en la extensión AIA de los certificados emitidos” se encuentra deshabilitada.

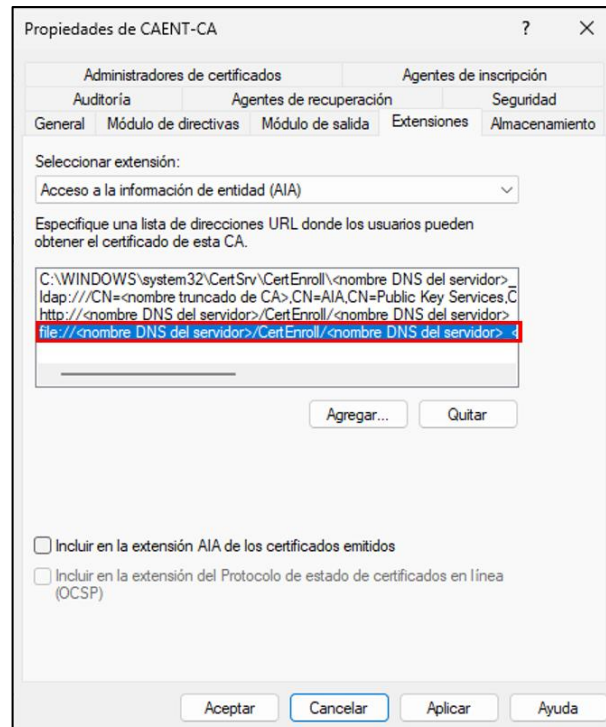


Ilustración 81 - Confirmar configuración de extensión

91. Seleccione ahora “http://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y copie el elemento mediante la combinación de teclas “Control + C”. A continuación, pulse en “Agregar”.

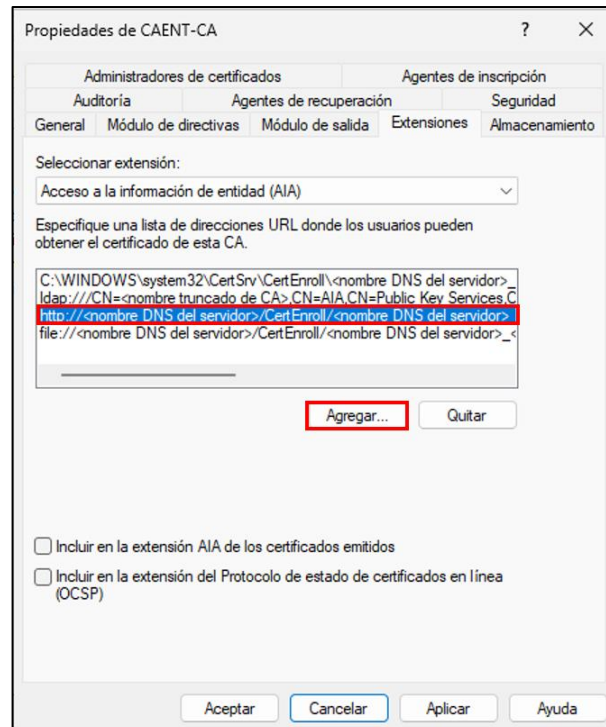


Ilustración 82 - Copiar extensión HTTP y agregar nueva entrada

92. En el campo “Ubicación” pegue el contenido copiado.

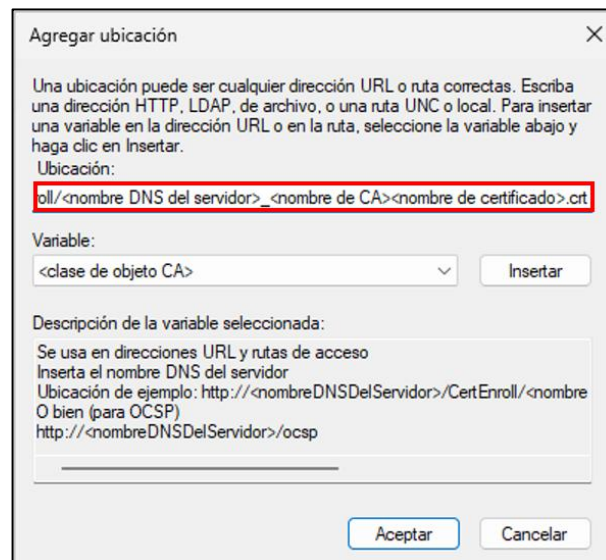


Ilustración 83 - Pegar nueva entrada

Nota: Aún no pulse sobre el botón “Aceptar”.

93. Localice y sustituya el valor “<nombre DNS del servidor>” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y su alias CNAME.

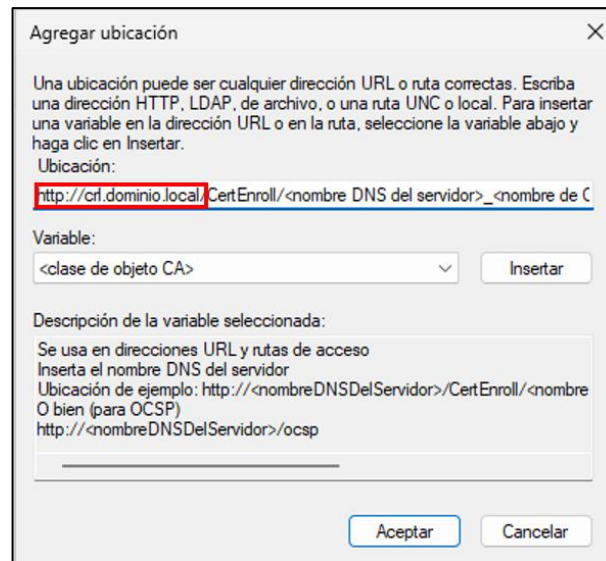


Ilustración 84 - Modificar el valor de la entrada

94. Pulse “Aceptar” y a continuación, marque la casilla “Incluir en la extensión AIA de los certificados emitidos”. A continuación, pulse en “Aplicar” y “Aceptar”.

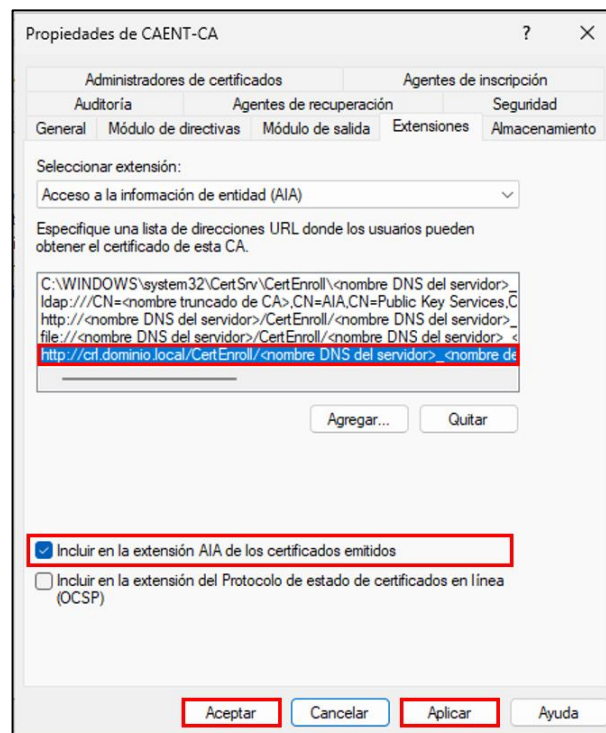
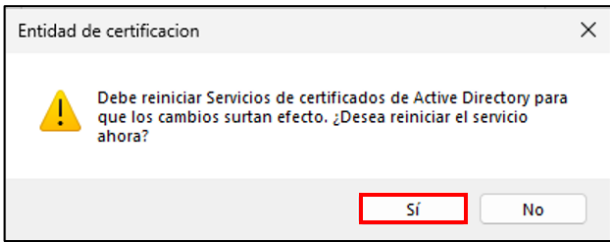


Ilustración 85 - Incluir en la extensión AIA de los certificados

95.	El sistema solicitará reiniciar los servicios de certificados. Pulse en “Sí”.  <i>Ilustración 86 - Reiniciar el servicio de certificados de Active Directory</i>
96.	Una vez finalice el proceso, la entidad de certificación empresarial estará disponible para emitir certificados.

Nota: En caso de que su configuración corresponda a una única entidad de certificación empresarial, puede continuar con la revisión del “Anexo 7. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN”

6.2. OPCIÓN B. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA CON ENTIDAD RAÍZ EN DOMINIO

Este apartado presenta el procedimiento de configuración de seguridad, descrito de manera ordenada y detallada, en un entorno formado por un Controlador de Dominio, un Servidor Miembro de Dominio que asumirá el rol de Entidad de Certificación Subordinada y un Servidor Miembro de Dominio que asumirá el rol de Entidad de Certificación Raíz.

Antes de iniciar con el proceso de configuración, es necesario disponer de los siguientes elementos:

- a) Un servidor **controlador de dominio** Windows Server 2025 (DC01) que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A25.
- b) Un servidor miembro de dominio Windows Server 2025 que ejercerá como **Entidad de Certificación subordinada** (CASUB01) siguiendo la guía de seguridad CCN-STIC-570A25. Este contendrá el servicio Web Internet Information Services instalado y preparado, este seguirá la guía CCN-STIC-574A25.
- c) Un servidor miembro de dominio Windows Server 2025 que ejercerá como **Entidad de Certificación raíz** (CARAIZ01) siguiendo la guía de seguridad CCN-STIC-570A25.

6.2.1. 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. Inicie la consola “Administrador del servidor” con privilegios de administración.

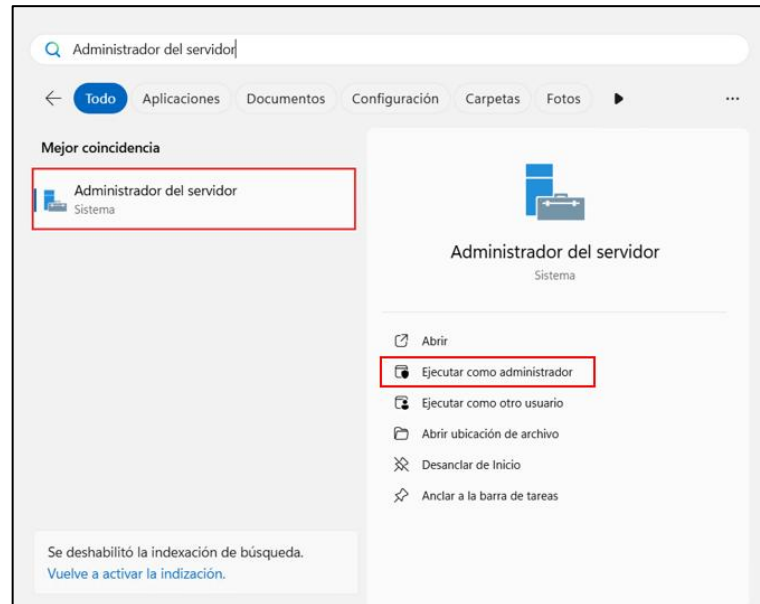


Ilustración 87 - Iniciar consola de Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

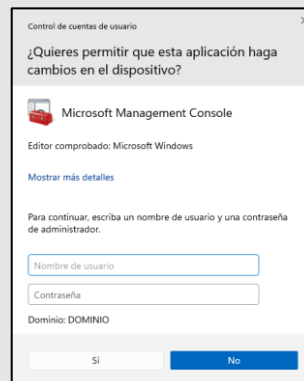


Ilustración 88 - Introducir credenciales de administrador

3. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

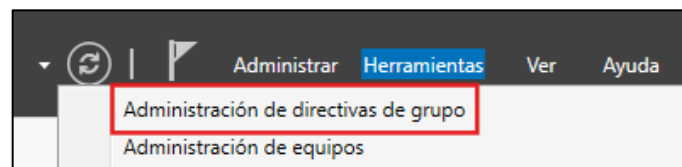


Ilustración 89 - Administración de directivas de grupo

4. Despliegue en el panel izquierdo hasta llegar a la OU “Domain Controllers”.

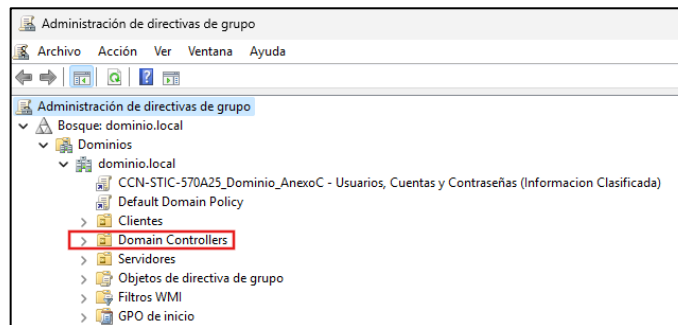


Ilustración 90 - OU Domain Controllers

5. Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

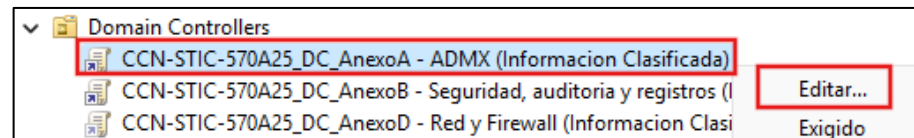


Ilustración 91 - Edición de ADMX 570A25

6. 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.

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 92 - Políticas de PowerShell

7. Haga doble clic sobre la política “Activar la ejecución de scripts”.

8. En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”.

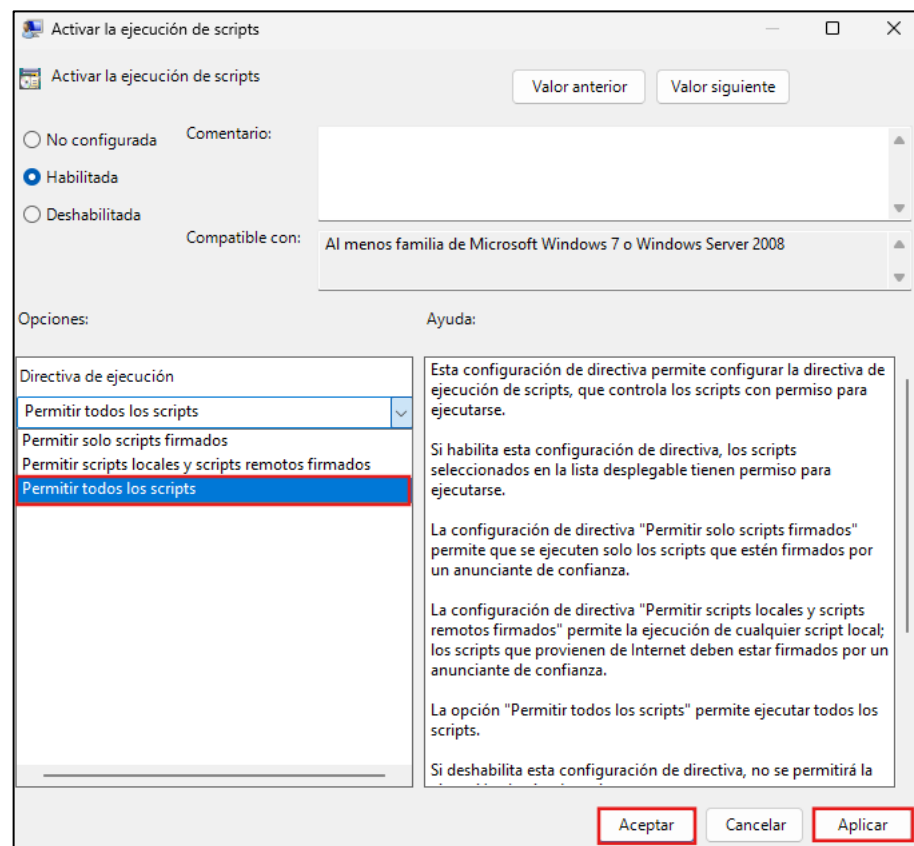


Ilustración 93 - Selección de "Permitir todos los scripts"

9. Reinicie el controlador de dominio para que se aplique la configuración correctamente. Tras ello, inicie sesión de nuevo con un usuario administrador del dominio.

10. Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta.

Verifique que en su interior se encuentran los siguientes archivos:

- Directorio: CA INCREMENTAL DOMINIO
- Directorio: CA SERVIDORES
- Directorio: CA SERVIDORES – SHELL REMOTO
- Directorio: IIS
- Fichero: CCN-STIC-598A25_IncrementalServidorCA.ps1

	CA INCREMENTAL DOMINIO	24/07/2026 13:40	Carpeta de archivos
	CA SERVIDORES	24/07/2026 13:48	Carpeta de archivos
	CA SERVIDORES - SHELL REMOTO	24/07/2026 14:15	Carpeta de archivos
	IIS	24/07/2026 13:40	Carpeta de archivos
	CCN-STIC-598A25_EntidadCertificacion	24/07/2026 14:05	Script de Window...

Ilustración 94 - Copia de ficheros necesarios

11. Asegúrese de que el script está desbloqueado antes de comenzar con su ejecución. Para ello, haga clic derecho sobre el mismo y seleccione “Propiedades”.

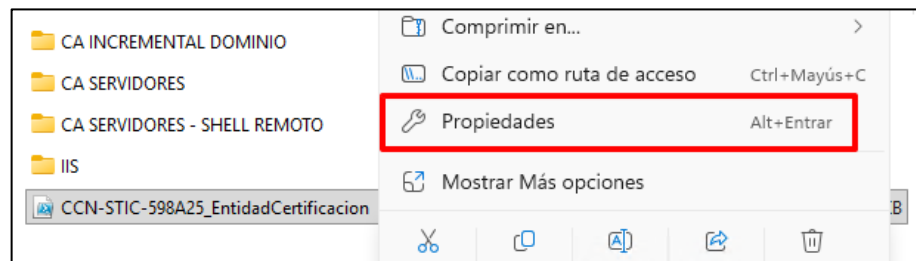


Ilustración 95 - Propiedades del script

12. En la parte inferior de la ventana emergente, marque la casilla “Desbloquear” si ésta aparece, y haga clic en “Aceptar”.

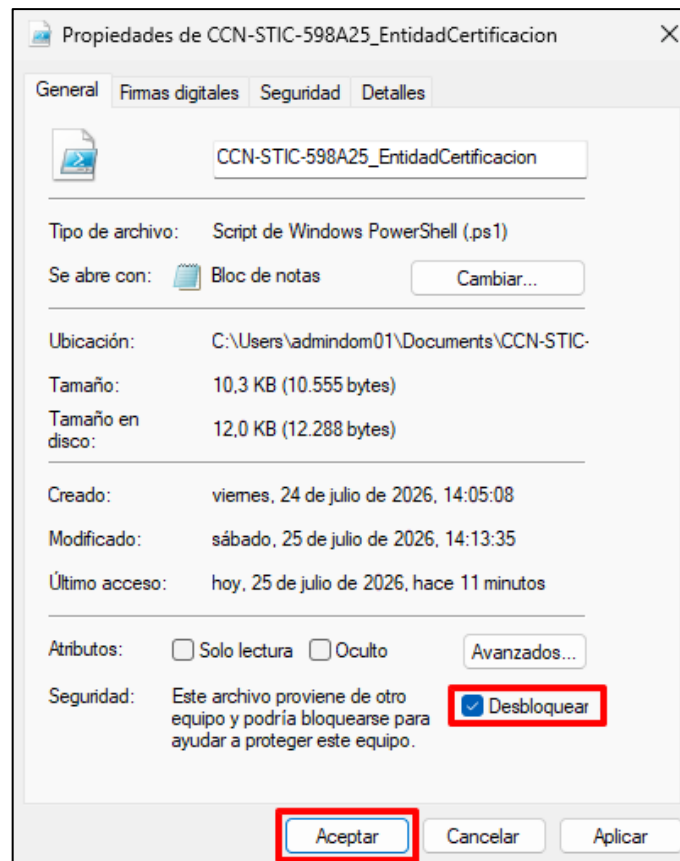


Ilustración 96 - Desbloqueo del script

13. Repita la misma operación con los archivos “.ps1” que se encuentran dentro de las cuatro subcarpetas de scripts.

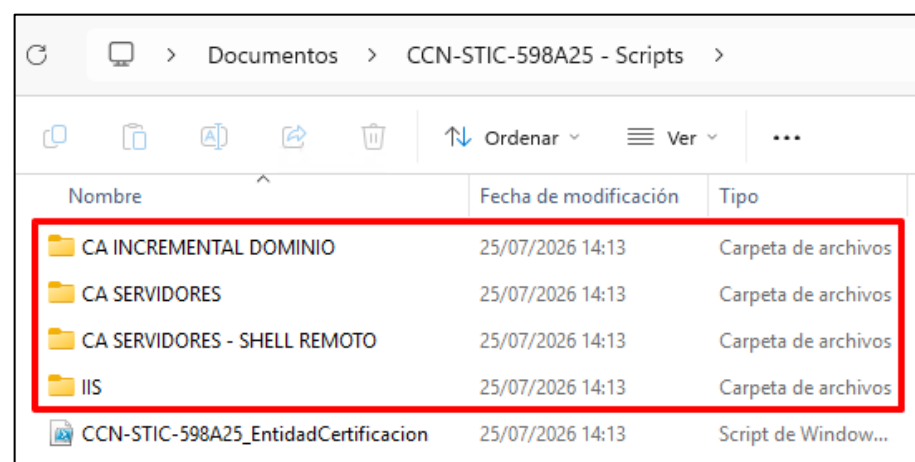


Ilustración 97 - Desbloqueo del resto de scripts

14. Sobre la barra de búsqueda, escriba “PowerShell”:

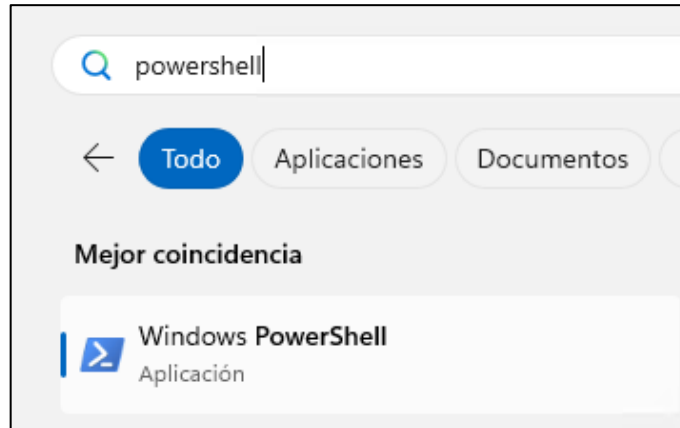


Ilustración 98 - Windows PowerShell

15. Haga clic derecho, y seleccione “Ejecutar como administrador”:

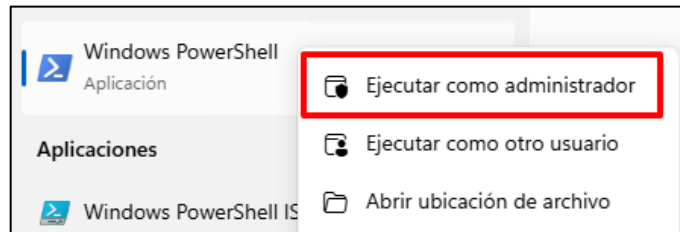


Ilustración 99 - Ejecución como administrador

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. Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

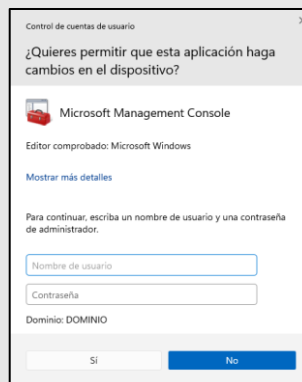


Ilustración 100 - Introducir credenciales de administrador

16. 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”.

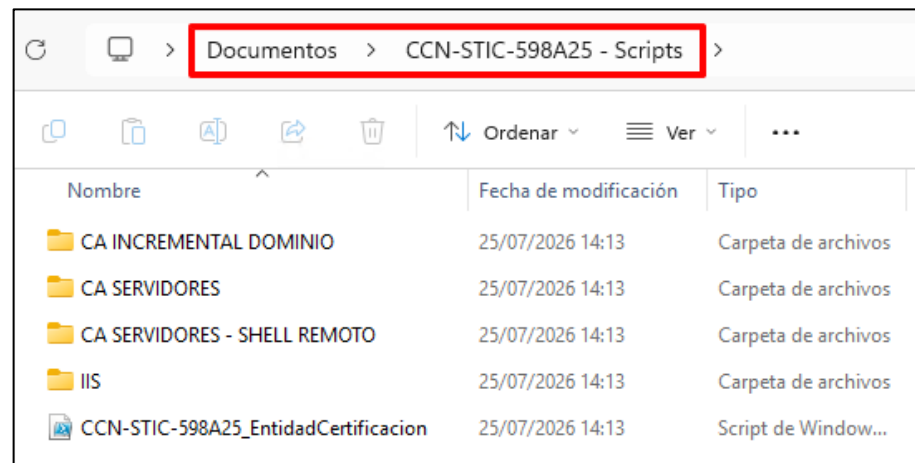


Ilustración 101 - Copia de ruta

17. Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.

```
PS C:\WINDOWS\system32> cd "C:\Users\admindom01\Documents\CCN-STIC-598A25 - Scripts"
```

Ilustración 102 - Acceso a la ruta

18. Ejecute el comando “dir” para verificar la ubicación y el contenido.

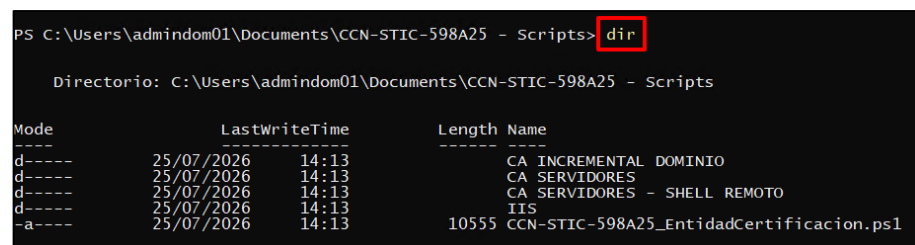


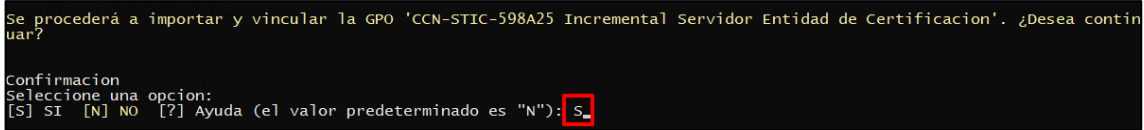
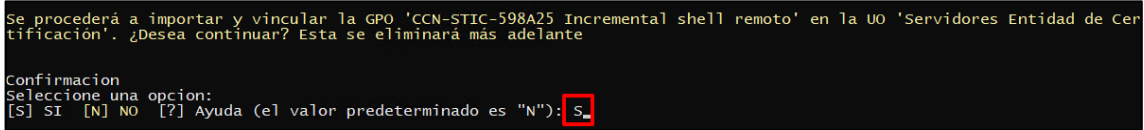
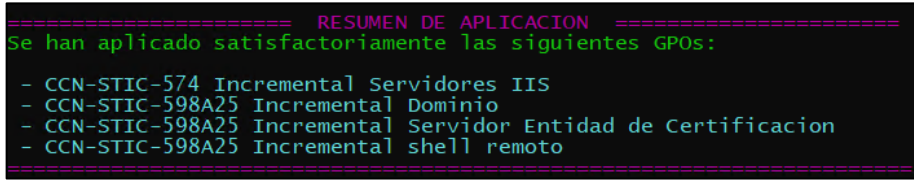
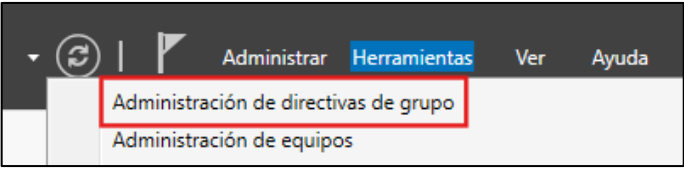
Ilustración 103 - Contenido de la carpeta

19. Ejecute el archivo “CCN-STIC-598A25_EntidadCertificacion.ps1” escribiendo “.” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.

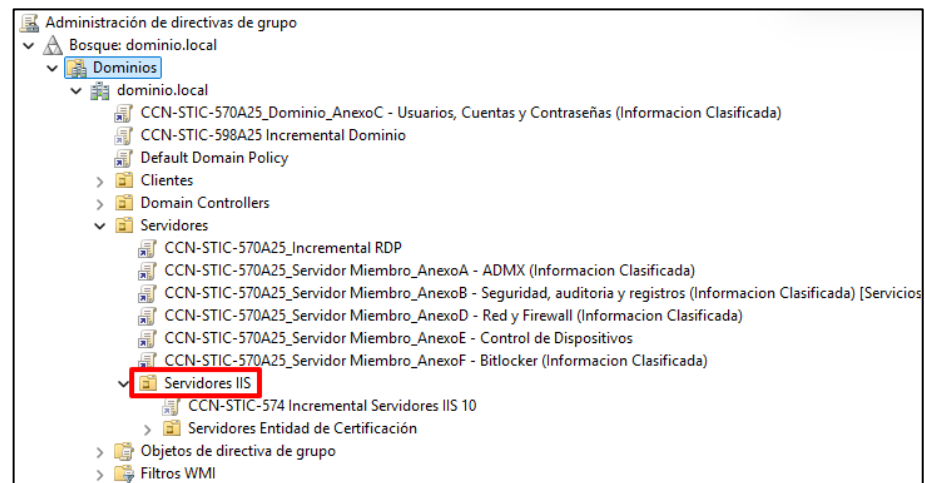
```
PS C:\Users\admindom01\Documents\CCN-STIC-598A25 - Scripts> .\CCN-STIC-598A25_EntidadCertificacion.ps1
```

Ilustración 104 - Ejecución del script

20.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje: <pre> ---ADVERTENCIA--- Este script incorpora modificaciones en Active Directory orientadas a la aplicación de medidas de bastionado para servidores de Autoridad de Certificación, conforme a la guía CCN-STIC-598A25. Antes de continuar, revise el impacto de las GPO que se van a crear, importar y vincular. ---FIN ADVERTENCIA---</pre> <i>Ilustración 105 - Advertencia</i>
21.	Escribir “S” y pulsar “Enter”. <pre> ¿Desea aceptar los riesgos y continuar con el bastionado del sistema? Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S</pre> <i>Ilustración 106 - Aceptación de advertencia</i>
22.	En primer lugar, el script verificará que si se encuentra aplicada la GPO de IIS a la Unidad Organizativa de “Servidores IIS”. Como el Controlador de Dominio sólo tiene aplicada la guía 570A25, escriba “S” y pulse “Enter”. <pre> Comprobando Unidad Organizativa: OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores' ya existe. Comprobando Unidad Organizativa: OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores IIS' ya existe. Comprobando Unidad Organizativa: OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local La Unidad Organizativa 'Servidores Entidad de Certificación' ya existe. Jerarquía de OUs preparada correctamente: - OU=Servidores,DC=dominio,DC=local - OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local - OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local Comprobando si existe la GPO 'CCN-STIC-574 Incremental Servidores IIS'... ADVERTENCIA: No se ha encontrado la GPO 'CCN-STIC-574 Incremental Servidores IIS'. Se procederá a importar y vincular la GPO 'CCN-STIC-574 Incremental Servidores IIS'. ¿Desea continuar? Confirmacion Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S</pre> <i>Ilustración 107 – Verificación UO IIS</i> Nota: Si se ha implementado previamente la guía CCN-STIC-574A25 para IIS, el presente paso se omitirá.
23.	A continuación, se importará la GPO Incremental en dominio. Escriba “S” y pulse “Enter”. <pre> Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental Dominio'. ¿Desea continuar? Confirmacion Seleccione una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S</pre> <i>Ilustración 108 - Implementación Incremental Dominio</i>

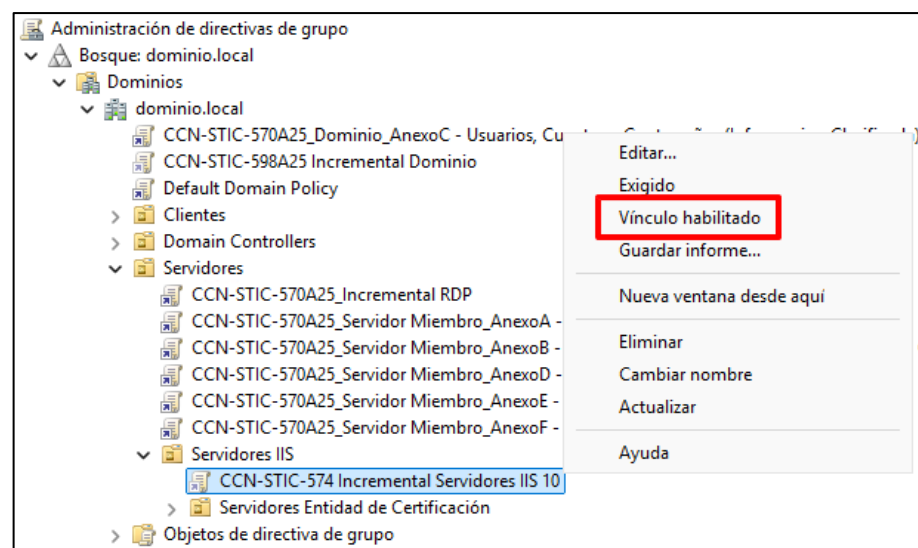
24.	Posteriormente, se importará la GPO Incremental de Servidores Entidad de Certificación a la Unidad Organizativa correspondiente. Escriba “S” y pulse “Enter”.  <i>Ilustración 109 - Implementación Incremental Servidores CA</i>
25.	Por último, se importará la GPO Incremental shell remoto a la Unidad Organizativa correspondiente. Escriba “S” y pulse “Enter”.  <i>Ilustración 110 - Implementación Incremental shell remoto</i> Nota: La GPO Incremental shell remoto sólo será necesaria durante la configuración de Active Directory Certificate Services. Una vez se finalice la implementación de la guía, se darán las indicaciones para desvincularla.
26.	Espere a que finalice la ejecución; al terminar, se mostrará un mensaje indicando las GPO que se han vinculado correctamente a las Unidades Organizativas correspondientes. Cierre el terminal de Powershell.  <i>Ilustración 111 - GPOs aplicadas correctamente</i>
27.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  <i>Ilustración 112 - Administración de directivas de grupo</i>

28. Despliegue la lista del menú izquierdo hasta localizar el dominio y, a continuación, acceda a la Unidad Organizativa de “Servidores IIS”.



Ilustraci3n 113 - OU Servidores IIS

29. Despliegue la OU y haga clic derecho sobre el GPO “CCN-STIC-574 Incremental Servidores IIS 10”. Seleccione la opci3n “V3nculo habilitado”.



Ilustraci3n 114 - Habilitar GPO.

30. Despliegue la OU de “Servidores Entidad de Certificación” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Servidores Entidad de Certificación”. Seleccione la opción “Vínculo habilitado”. Repita esta acción para la directiva “CCN-STIC-598A25 Incremental Shell remoto”.

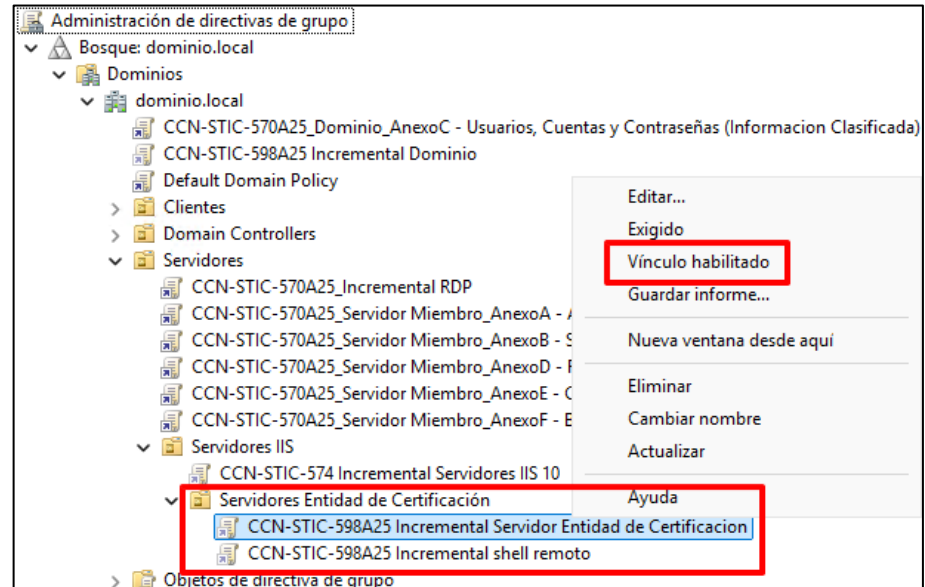


Ilustración 115 - Habilitar GPO CA

31. Diríjase a “dominio.local” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Dominio”. Seleccione la opción “Vínculo habilitado”.

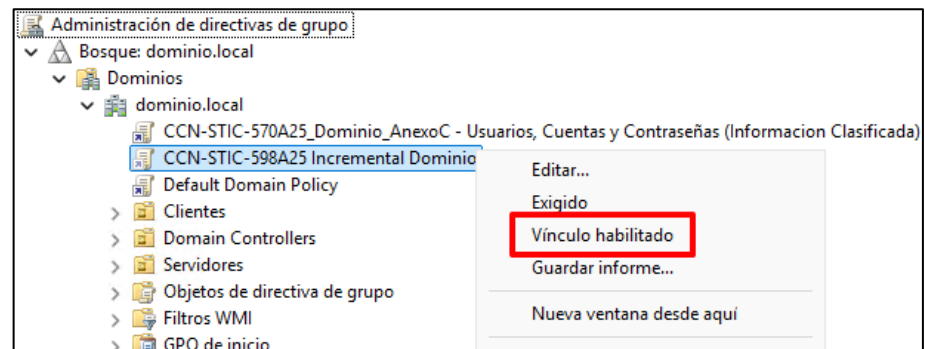


Ilustración 116 - Habilitar GPO Dominio

32. En la parte derecha del Administrador de directivas de grupo asegúrese de que la GPO “CCN-STIC-598A25 Incremental Dominio” se encuentra en primer lugar.

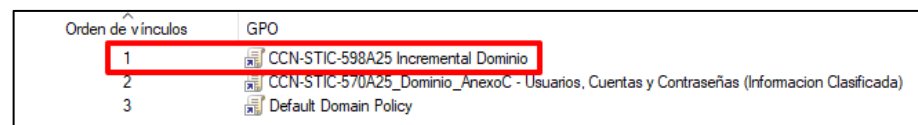


Ilustración 117 - Orden de las GPOs

33. De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior, y seleccione “Usuarios y equipos de Active Directory”.

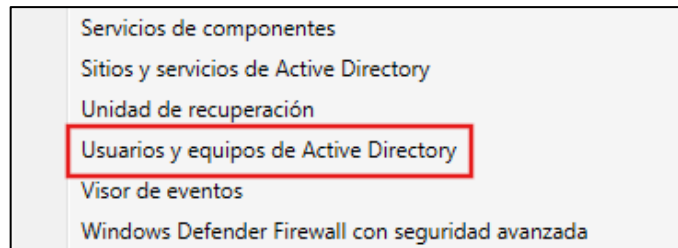


Ilustración 118 - Usuarios y equipos de Active Directory

34. Despliegue la lista del panel izquierdo hasta visualizar la OU “Servidores Entidad de Certificación”.

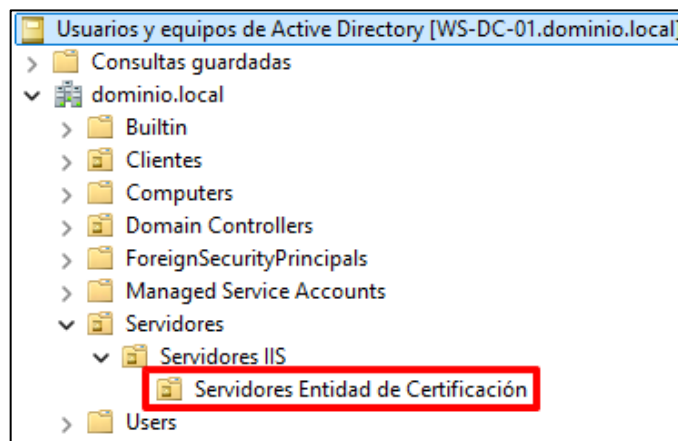


Ilustración 119 - OU Servidores Entidad de Certificación

35. Haga clic sobre la carpeta “Computers” y seleccione los servidores de Entidad de Certificación (en este caso, CARAIZ01 y CASUB01).

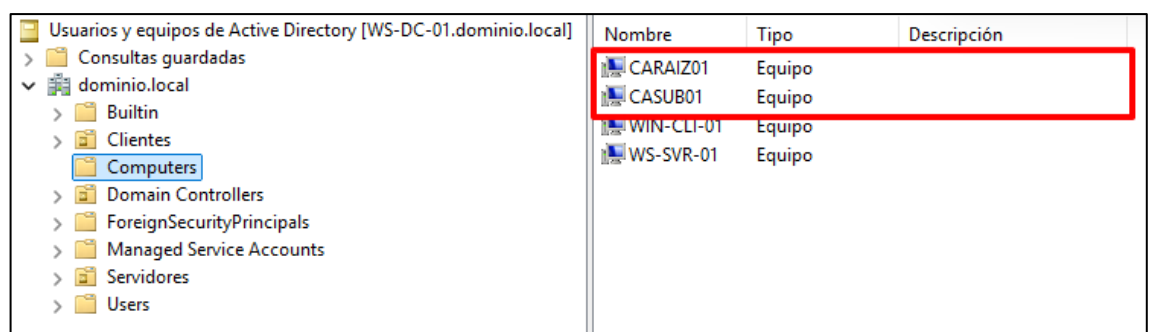


Ilustración 120 - Selección del servidor.

36. Arrástrelos a la OU “Servidores Entidad de Certificación”. Aparecerá una advertencia. Haga clic en “Sí”.
Puede cerrar la ventana de “Usuarios y equipos de Active Directory”.

37. De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

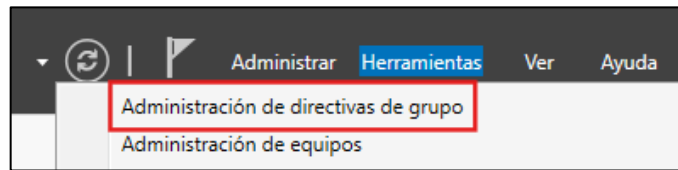


Ilustración 121 - Administración de directivas de grupo

38. Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.

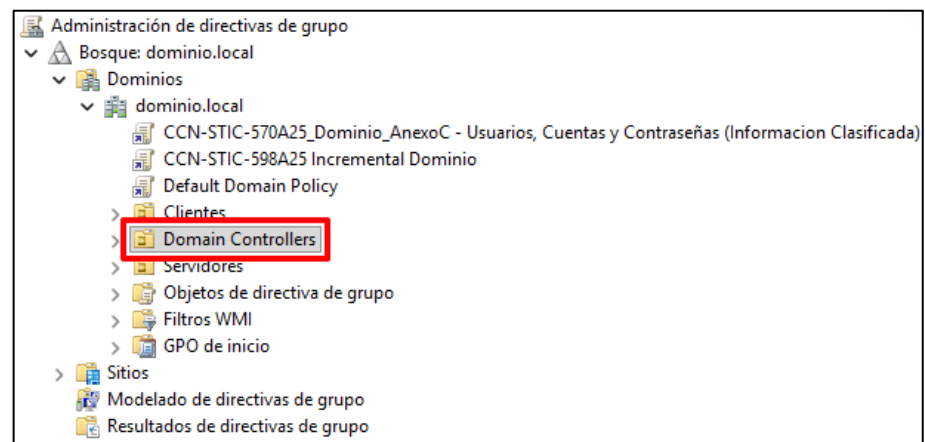


Ilustración 122 - OU Domain Controllers

39. Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

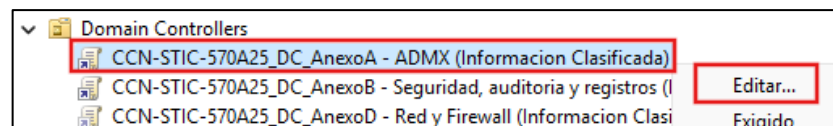


Ilustración 123 - Edición ADMX 570A25

40. 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

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 124 - Políticas de PowerShell

41. Haga doble clic sobre la política “Activar la ejecución de scripts”.

42. En el desplegable de la política, seleccione “Permitir solo scripts firmados”, y haga clic en “Aplicar” y “Aceptar”.

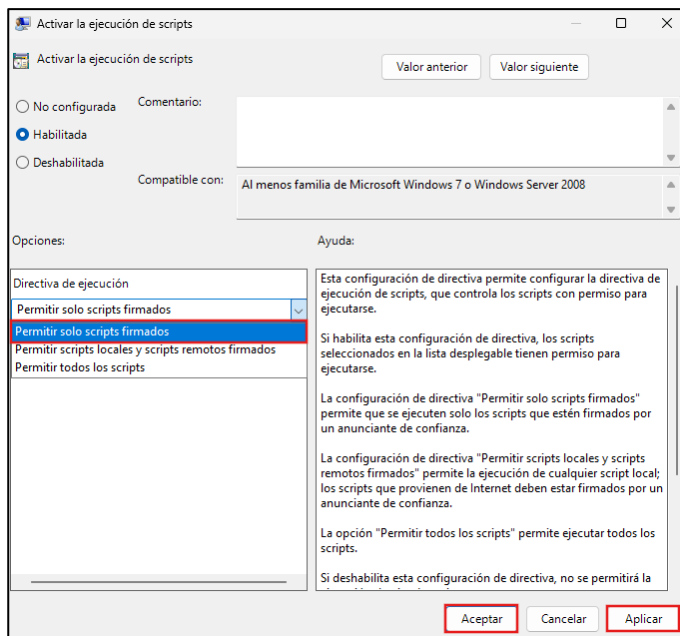


Ilustración 125 - Selección de "Permitir solo scripts firmados"

43. Reinicie el controlador de dominio para que se aplique la configuración correctamente.

6.2.2. PASO A PASO DE INSTALACIÓN EN ENTIDAD DE CERTIFICACIÓN RAÍZ EN DOMINIO

Los pasos que se describen a continuación se realizarán en el servidor Entidad de Certificación Raíz en el dominio.

Nota: Si su entidad de certificación raíz ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
44.	Inicie sesión en el equipo donde se va a instalar el servidor Entidad de Certificación raíz del dominio.

45. A continuación, se ejecutará como administrador el “Administrador del servidor” para configurar el servidor de Entidad de Certificación.

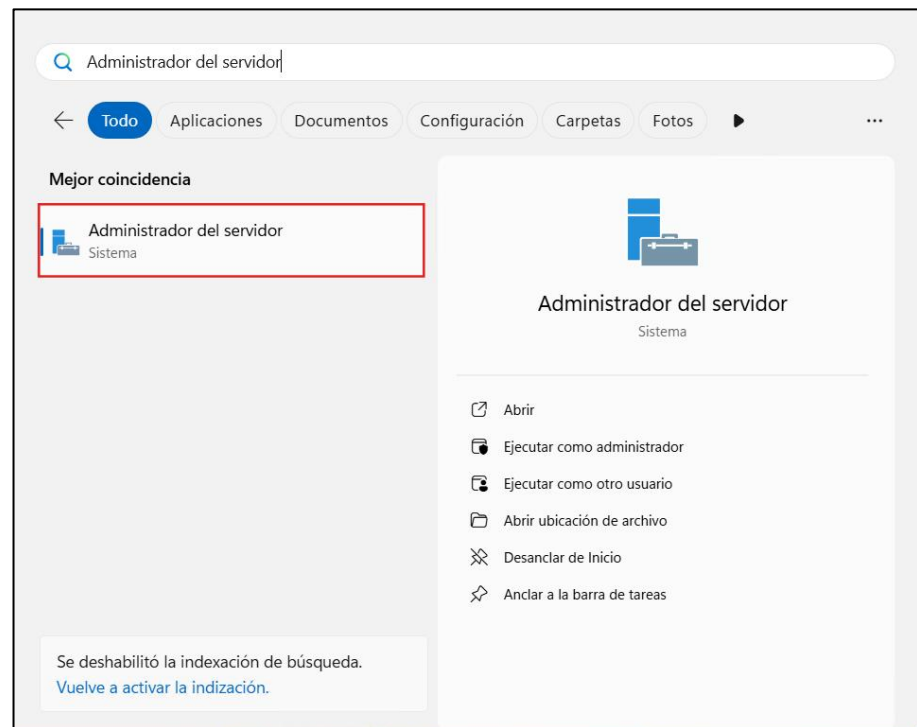


Ilustración 126 – Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

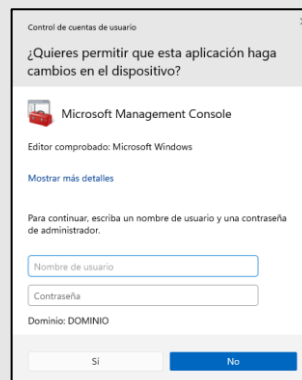


Ilustración 127 - Introducir credenciales de administración

46. Le aparecerá una ventana para proceder con la configuración, pulse en “Configurar Servicios de certificados de Active Directory”.



Ilustración 128 – Configurar Servicios de certificados

Nota: Si el rol de Entidad de certificación no se encuentra instalado, esta advertencia no se apreciará en el administrador del servidor. Añadir la funcionalidad desde “Administrar > Agregar roles y características”.

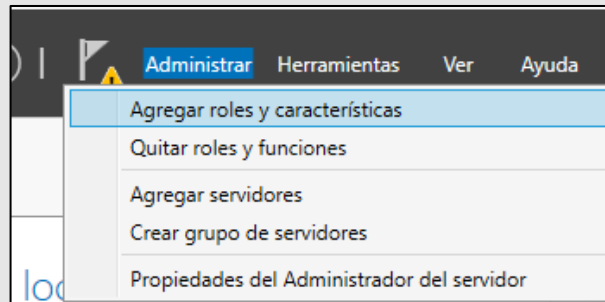


Ilustración 129 - Agregar rol de Entidad de certificación

47. Especifique las credenciales para configurar servicios de rol. Pulse en “Siguiente”.

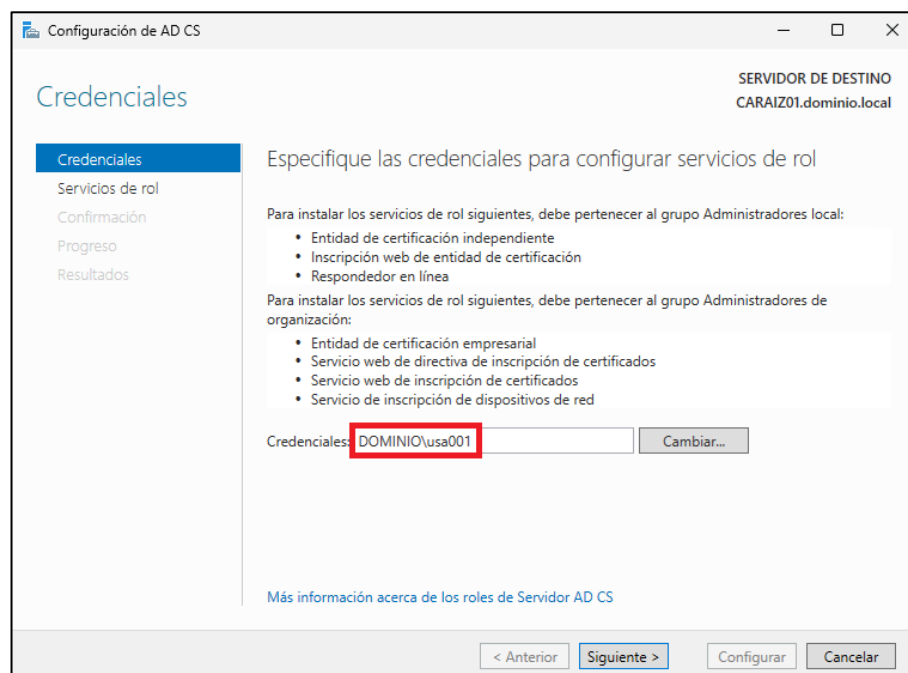


Ilustración 130 – Especificación de credenciales

Nota: El usuario administrador que se utilizará en todo el escenario será **usa001**.

48. Seleccione los servicios de rol que dispondrá el servidor de Entidad de Certificación. En el presente caso serán “Entidad de certificación”. Pulse en “Siguiente”.

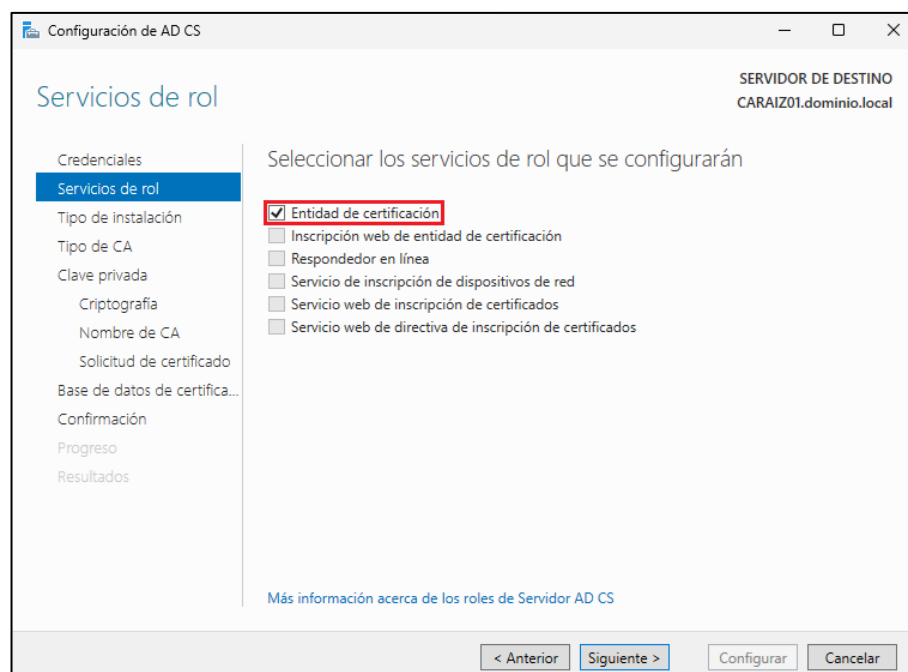


Ilustración 131 – Seleccionar servicios de rol

49. Especifique el tipo de instalación de la CA, seleccione “CA empresarial”. Pulse en “Siguiente”.

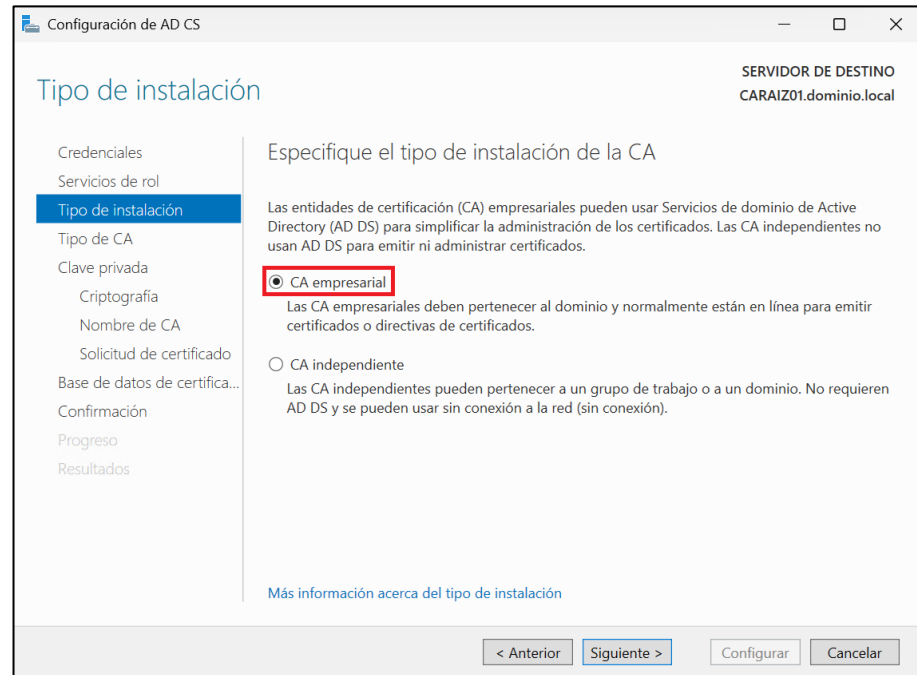


Ilustración 132 – Especificación de tipo de instalación

50. Seleccione “CA raíz”. Pulse en “Siguiente”.

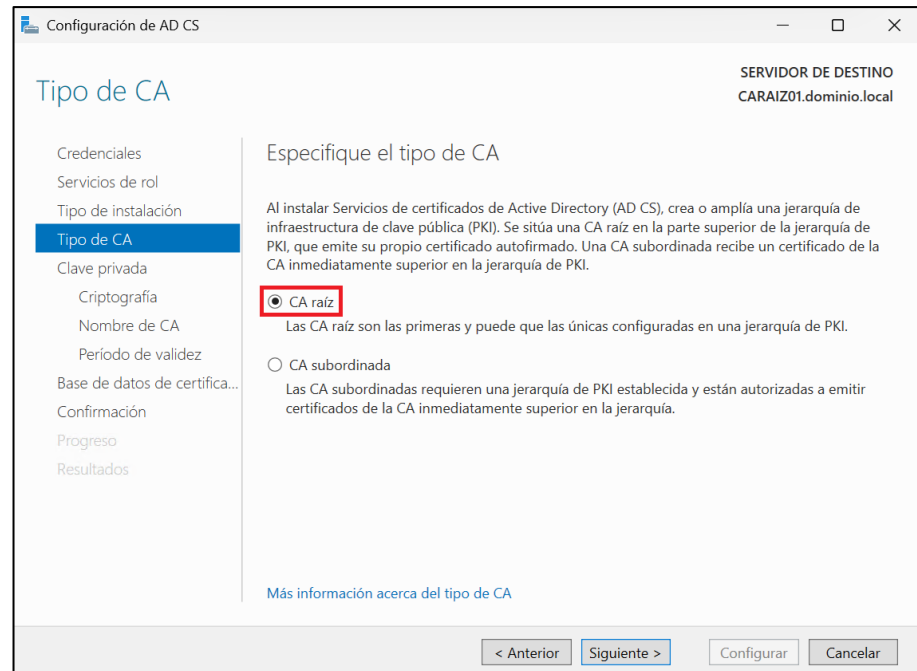


Ilustración 133 – Especificación de tipo de CA

51. A continuación, seleccione la opción de “Crear una clave privada nueva”. Pulse en “Siguiente”.

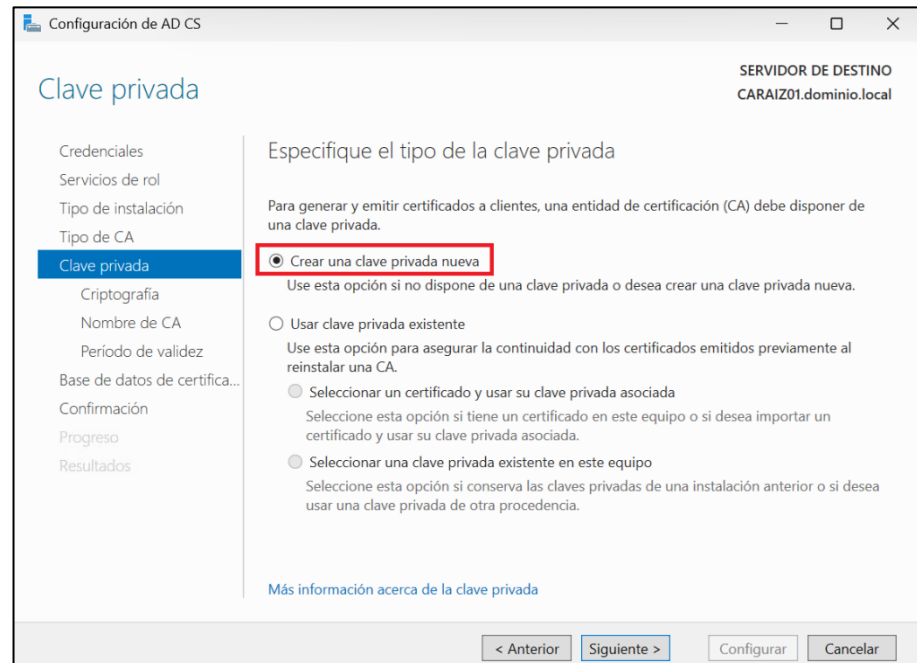


Ilustración 134 – Creación de clave privada

52. Las opciones criptográficas que se seleccionarán serán.
- Longitud: 2048
 - Tipo de algoritmo hash: SHA256
- Posteriormente, pulse en “Siguiente”.

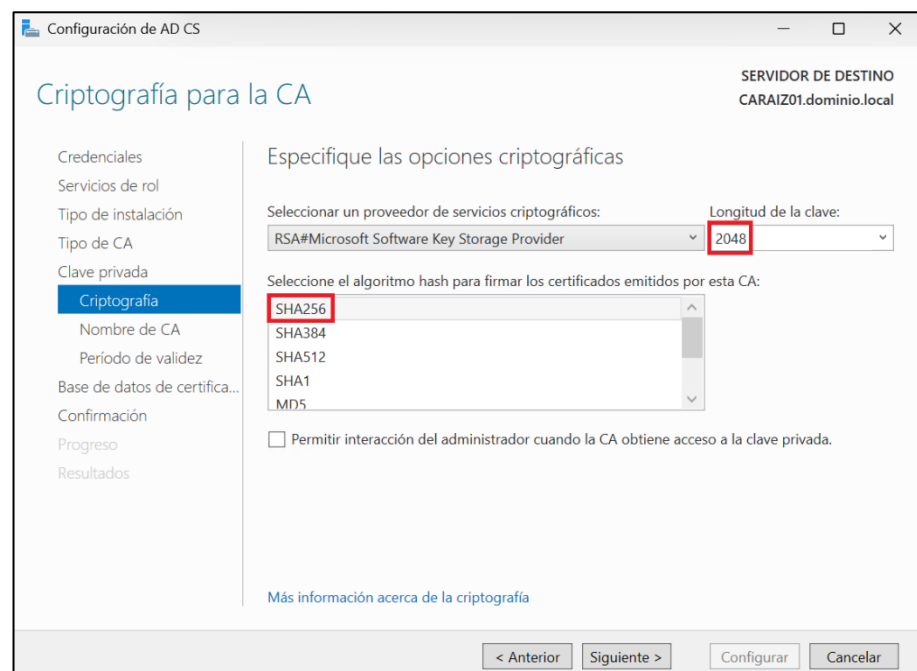
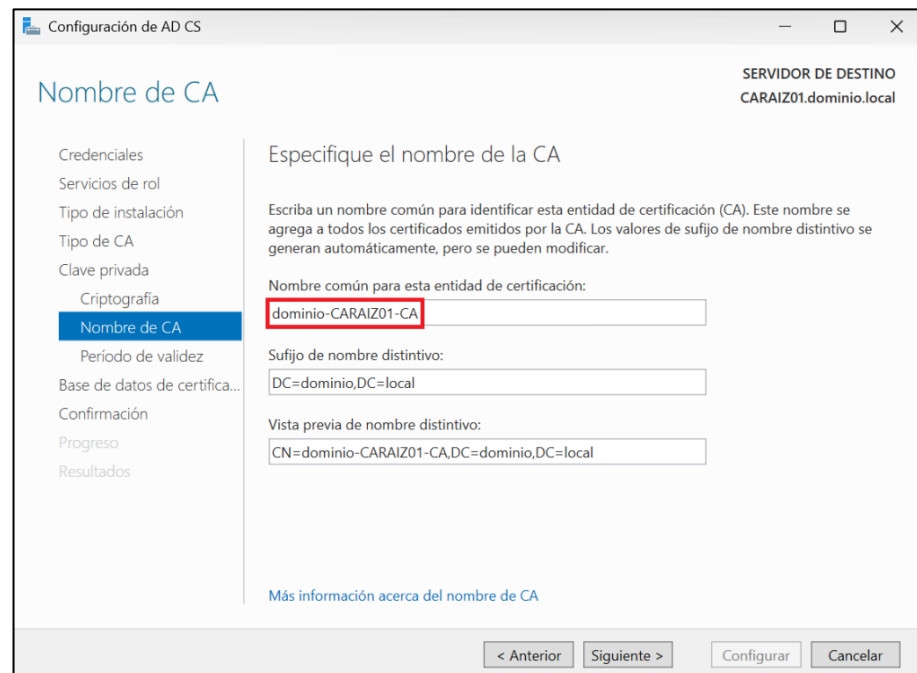


Ilustración 135 – Especificación de opciones criptográficas

53. A continuación, se especificará el nombre para la entidad de certificación. En el presente caso, será “dominio-CARAIZ01-CA”. Posteriormente, pulse en “Siguiente”.



Configuración de AD CS

SERVIDOR DE DESTINO
CARAIZ01.dominio.local

Nombre de CA

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Especifique el nombre de la CA

Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.

Nombre común para esta entidad de certificación:
dominio-CARAIZ01-CA

Sufijo de nombre distintivo:
DC=dominio,DC=local

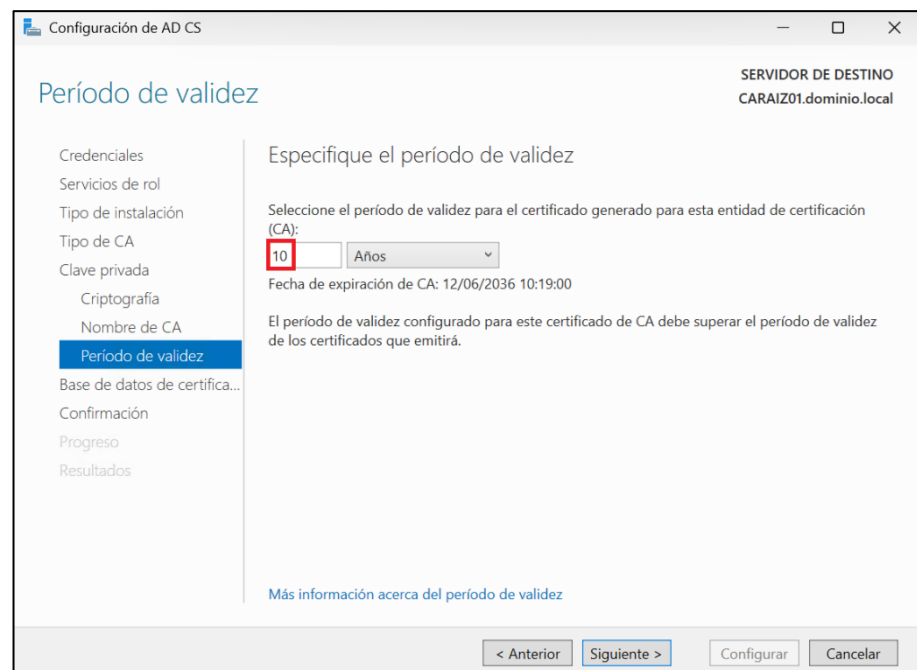
Vista previa de nombre distintivo:
CN=dominio-CARAIZ01-CA,DC=dominio,DC=local

[Más información acerca del nombre de CA](#)

< Anterior Siguiente > Configurar Cancelar

Ilustración 136 – Especificación de nombre de la CA

54. Especifique el período de validez para el certificado para esta entidad de certificación. Se establecerá en 10 años. Pulse en “Siguiente”.



Configuración de AD CS

SERVIDOR DE DESTINO
CARAIZ01.dominio.local

Período de validez

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Especifique el período de validez

Seleccione el período de validez para el certificado generado para esta entidad de certificación (CA):
10 Años

Fecha de expiración de CA: 12/06/2036 10:19:00

El período de validez configurado para este certificado de CA debe superar el período de validez de los certificados que emitirá.

[Más información acerca del período de validez](#)

< Anterior Siguiente > Configurar Cancelar

Ilustración 137 – Período de validez

55. En la siguiente página se especificará las ubicaciones donde se almacenarán los certificados. Se establecerán las carpetas por defecto. Finalmente, pulse en “Siguiente”.

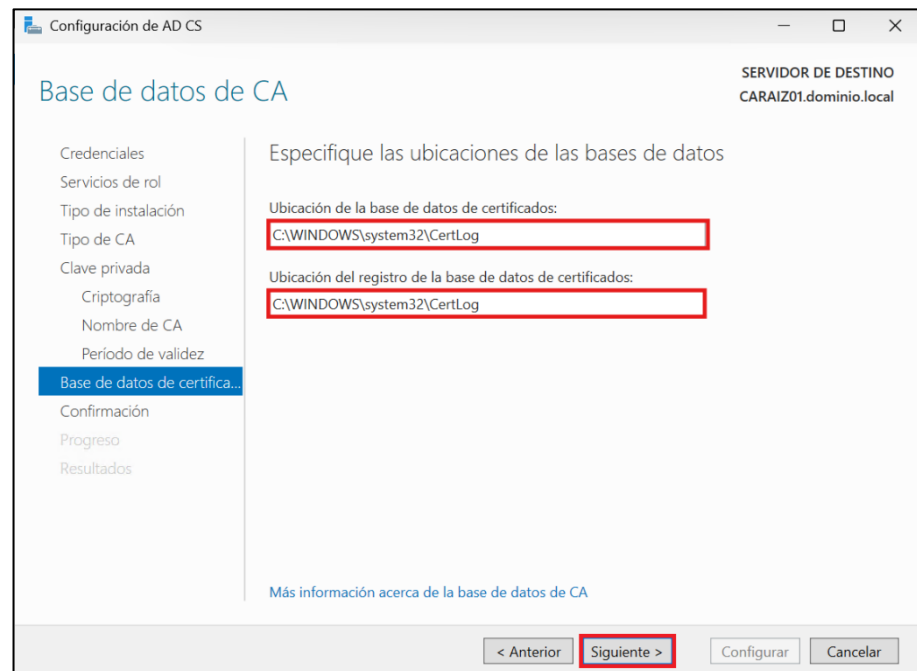


Ilustración 138 – Ubicaciones de bases de datos

Nota: Si su entorno dispone de un sitio específico, deberá indicarlo en este apartado.

56. Finalmente, se visualiza un resumen de toda la configuración. Pulse en “Configurar” y posteriormente, “Cerrar”.

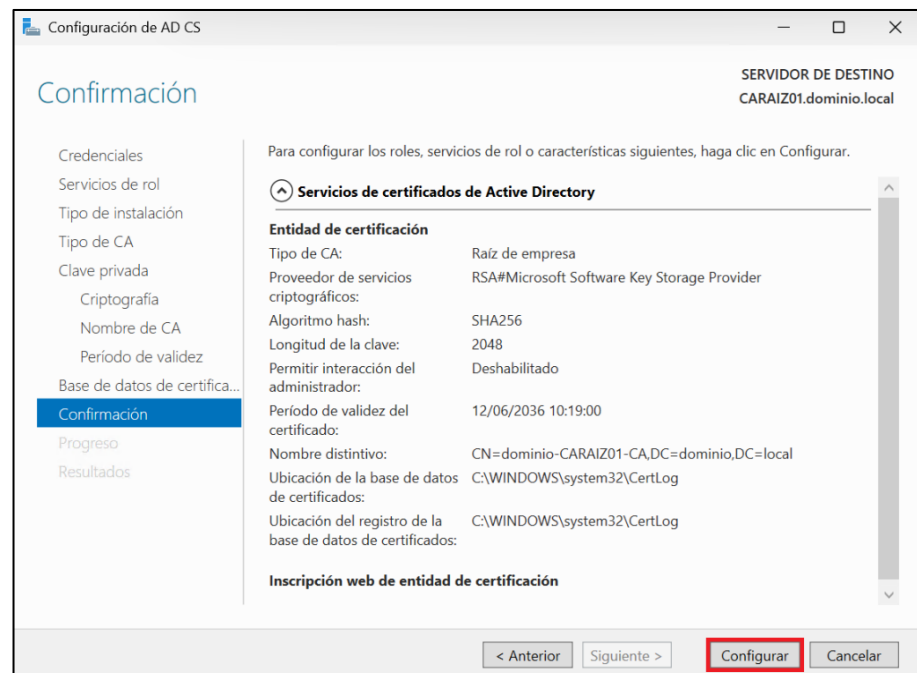
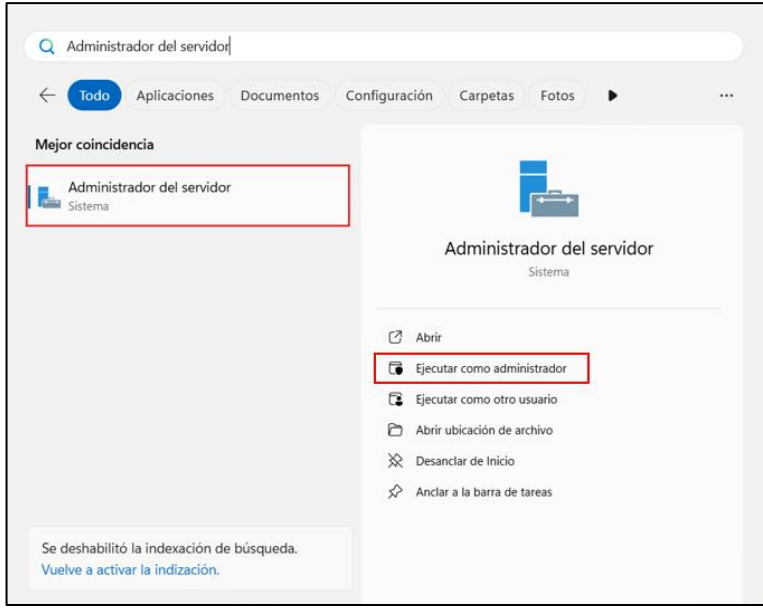
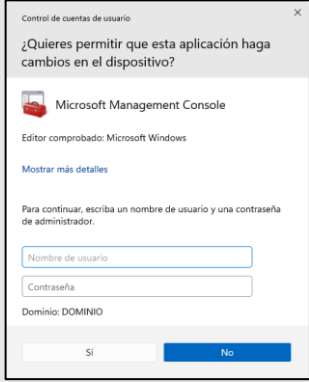


Ilustración 139 – Resumen de inscripción de servicio de certificados

6.2.3. CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA

Paso	Descripción
57.	Inicie sesión con un usuario administrador en el controlador de dominio del entorno donde se ha implementado la entidad de certificación raíz.
58.	Inicie la consola “Administrador del servidor” con privilegios de administración.  <i>Ilustración 140 - Iniciar Administrador del servidor</i> Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 141 - Introducir credenciales de administrador</i>

59. En el panel de administración del servidor, haga clic en “Herramientas” y posteriormente en “DNS” para iniciar la consola de administración del servicio de nombres.

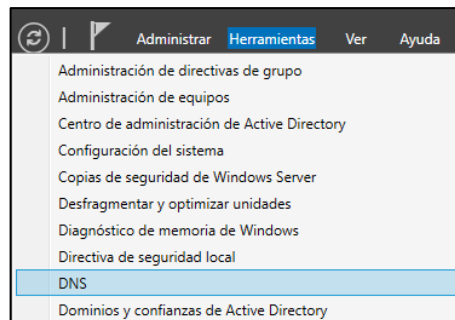


Ilustración 142 - Consola de administración DNS

60. Despliegue el árbol de dominio y pulse con el botón derecho sobre “dominio.local”. A continuación, haga clic sobre “Alias nuevo (CNAME)”.

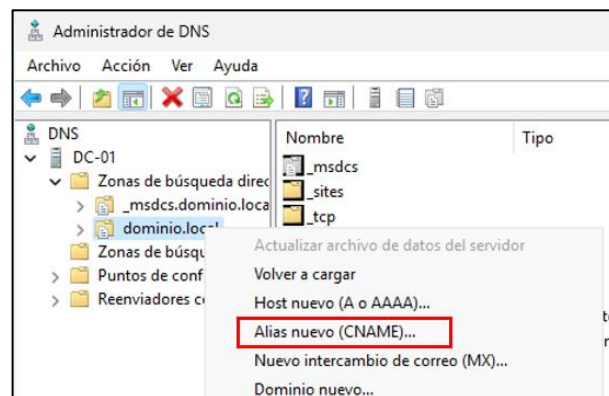


Ilustración 143 - Nuevo CNAME

61. En el campo “Nombre de alias”, introduzca el nombre alternativo que se desea configurar como, por ejemplo, “crl”.

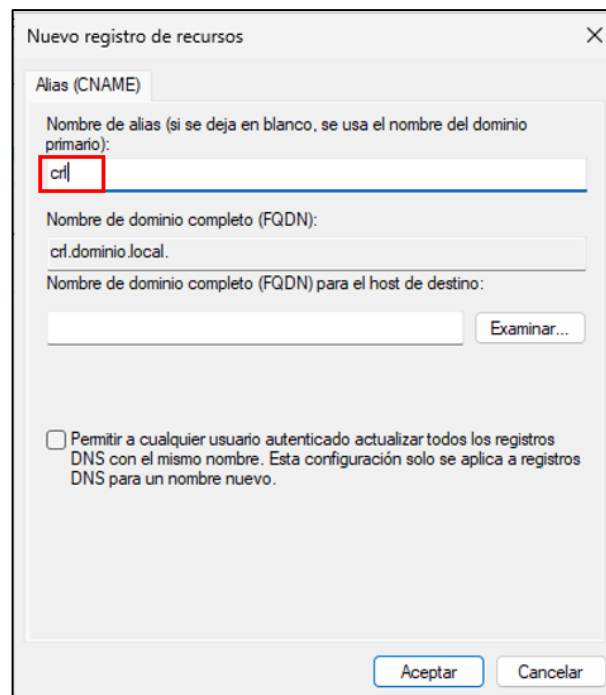


Ilustración 144 - Introducción de CRL como valor para el alias

62. Haga clic en “Examinar” y navegue hasta el nombre de la entidad de certificación subordinada que se utilizará para publicar la CLR. A continuación, pulse en “Aceptar”.

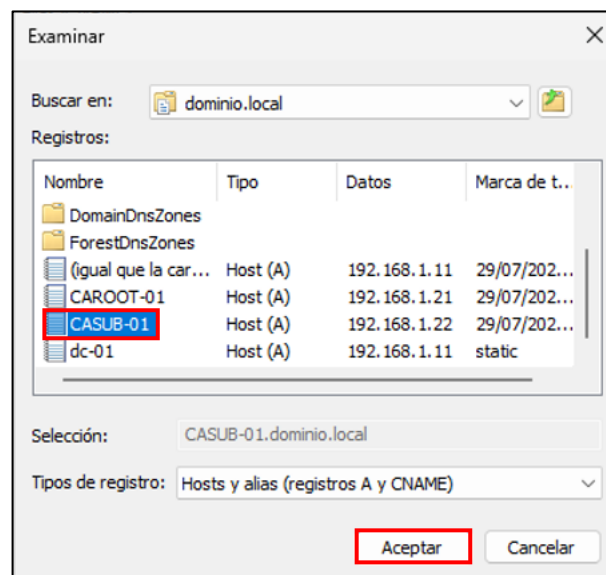


Ilustración 145 - Selección de objeto

63. De nuevo, pulse en “Aceptar” para registrar la creación del CNAME.

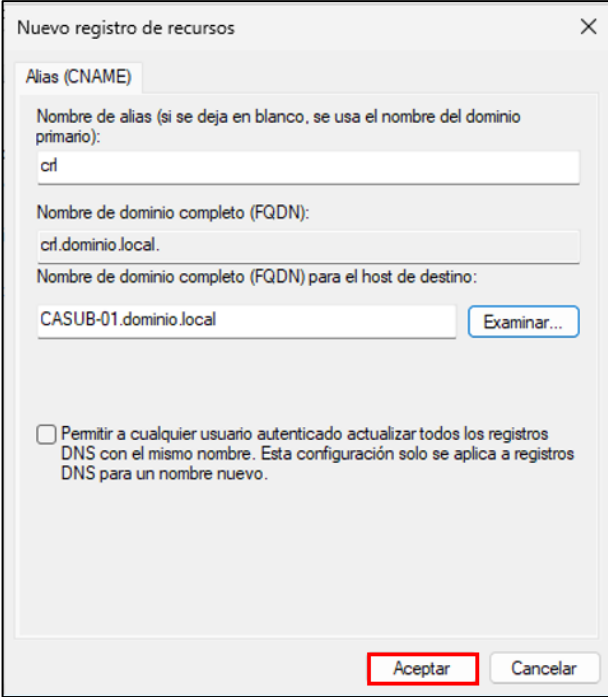


Ilustración 146 - Creación de CNAME

64. Cierre la consola de administración DNS e inicie sesión en el servidor de entidad de certificación recién configurado con un usuario con privilegios administrativos.

65. En el menú de inicio, busque “Powershell” para iniciar una consola y ejecútelo como administrador.

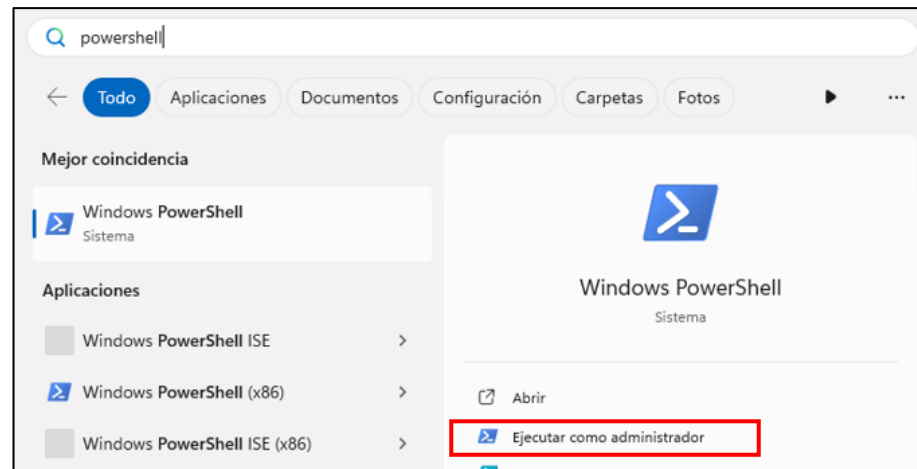


Ilustración 147 - Iniciar PowerShell como administrador

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

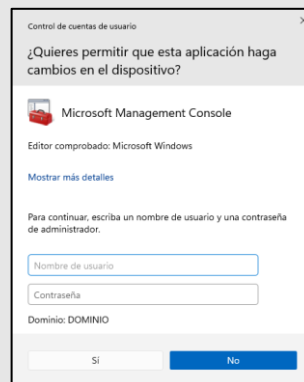


Ilustración 148 - Introducir credenciales de administrador

66. Introduzca “regedit” para abrir la consola de edición del registro y pulse “enter”.

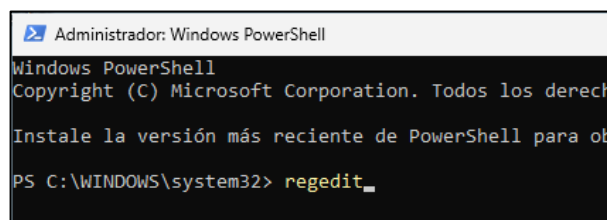


Ilustración 149 - Abrir editor del registro

67. Diríjase a la clave de registro “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration y acceda a clave de su ROOT CA.

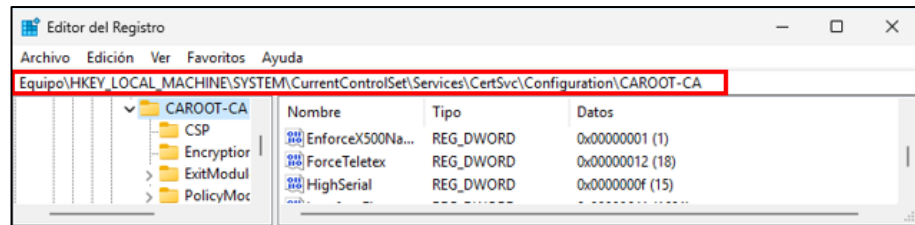


Ilustración 150 - Configuración del registro de CA RAIZ

68. Localice el valor “ValidityPeriodUnits” y edítelo pulsando con el botón derecho y “Modificar”.

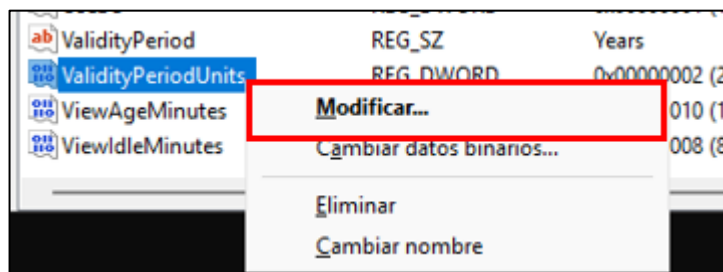


Ilustración 151 - Modificar valor de clave de registro

69. Introduzca el valor “5” y a continuación, pulse en “Aceptar”:

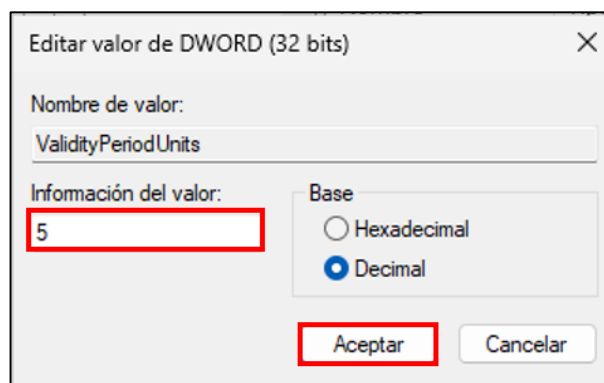


Ilustración 152 - Modificar valor de clave de registro

70. Cierre el editor del registro y la consola de Powershell.

71. En el panel de administración del servidor, pulse en “Herramientas”, y a continuación “Entidad de certificación”.

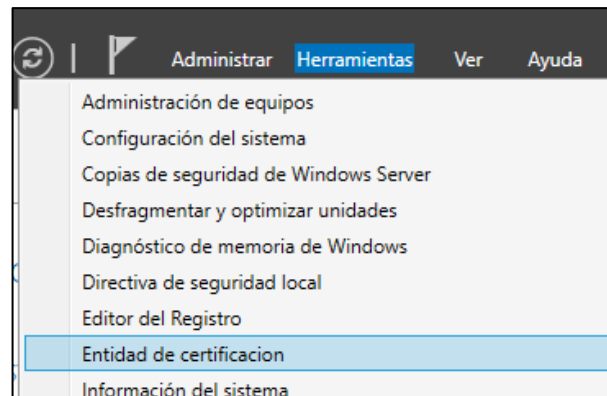


Ilustración 153 - Acceso a la consola de Entidad de certificación

72. Haga clic sobre el nombre de la entidad de certificación, y posteriormente en “Propiedades”.

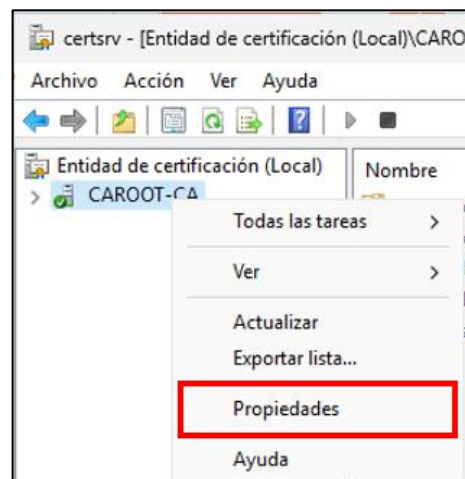


Ilustración 154 - Propiedades de CA

73. En la ventana de “Propiedades” diríjase a la pestaña “Extensiones” y, manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, revise la publicación de CRLs mediante la ruta local seleccionando “C:\Windows\System32\CertSrv\CertEnroll\<nombre de CA>< sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.

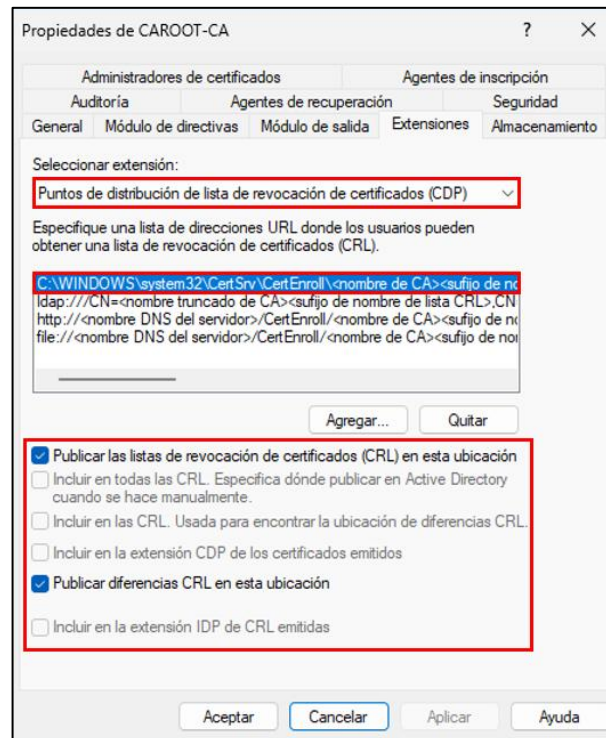


Ilustración 155 - Configuración de extensiones

74. A continuación, deshabilite la publicación de CRLs mediante LDAP seleccionando “ldap://CN=<nombre truncado de CA>< sufijo de nombre de lista CRL>,CN=nombre corto del servidor>,CN=CDP,CN=Public Key Services,<contenedor de configuración><clase de objeto CDP>” y desmarque todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.

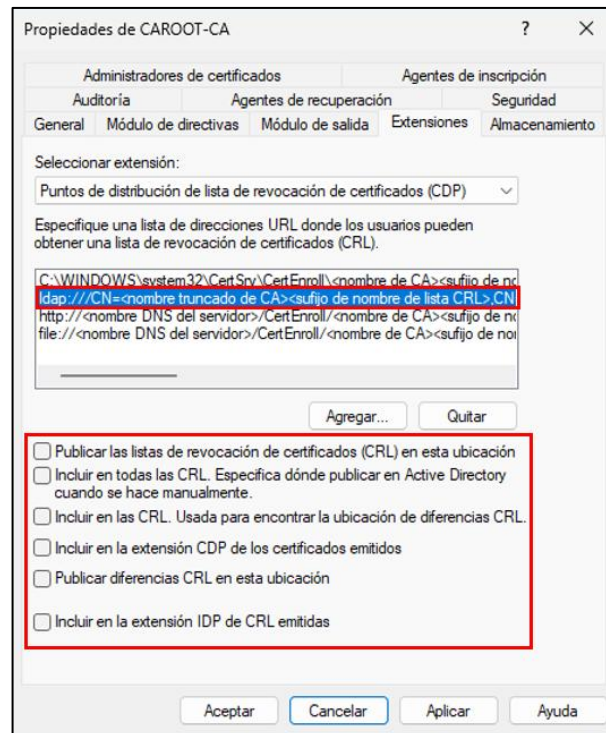


Ilustración 156 - Configuración de extensión LDAP

75. Para continuar, seleccione “file://<nombre DNS del servidor>/CertEnroll/<nombre de CA>/sufijo de nombre de lista CRL<diferencias entre listas CRL permitidas>.crl” y desmarque todas las opciones como muestra la siguiente figura.

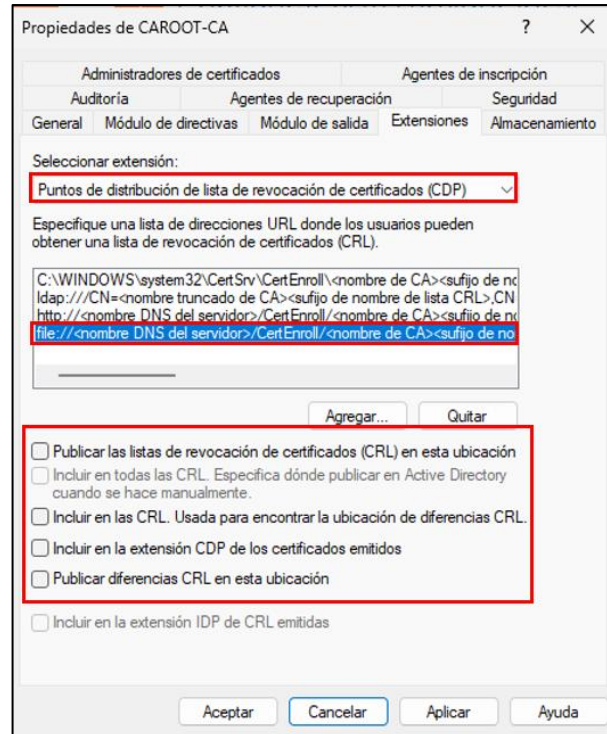


Ilustración 157 - Configuración de "file"

76. Una vez realizada dicha configuración, seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre de CA><sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y pulse “Control + C”, para copiar el objeto.

77. Pulse en Agregar.

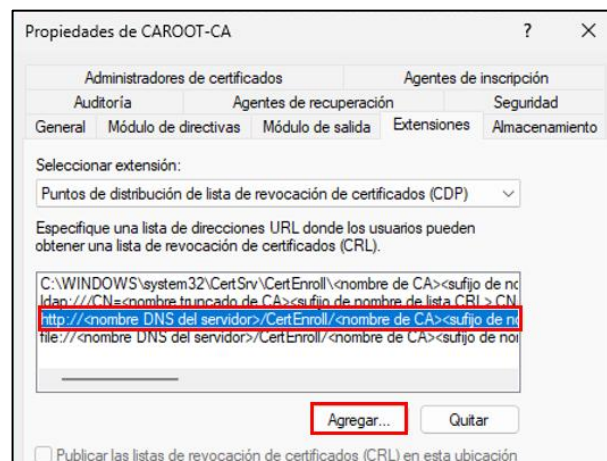
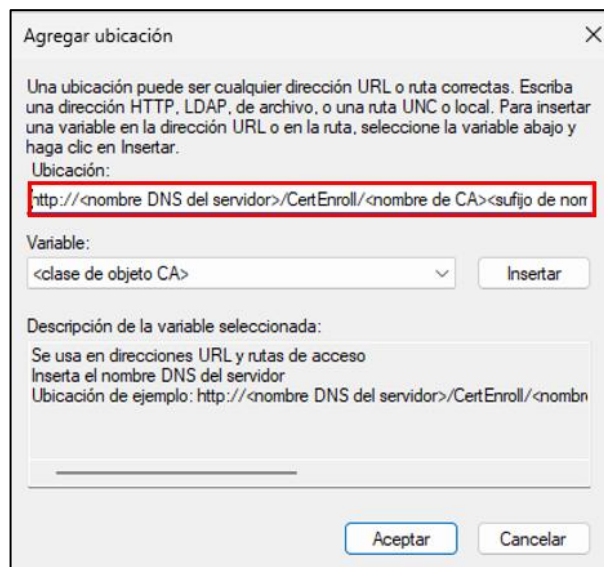


Ilustración 158 - Agregar extensión http

78. En el campo “Ubicación”, pegue la ruta copiada en el paso anterior.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:
 http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de non

Variable:
 <clase de objeto CA> Insertar

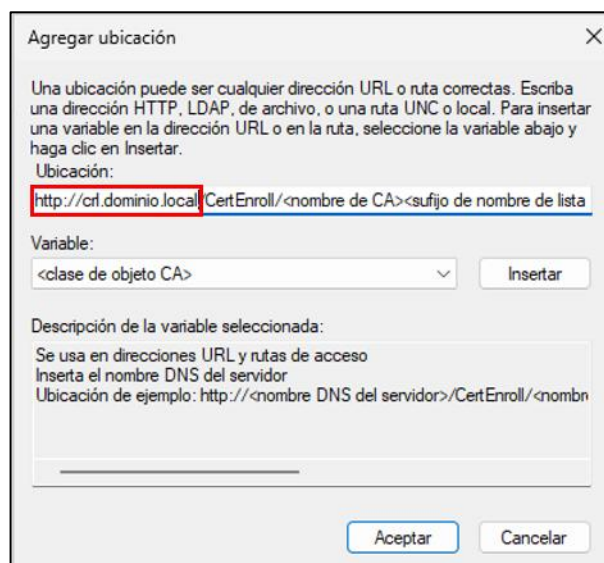
Descripción de la variable seleccionada:
 Se usa en direcciones URL y rutas de acceso
 Inserta el nombre DNS del servidor
 Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 159 - Pegar la ruta en el campo ubicación

Nota: No pulse el botón “Aceptar”.

79. Localice “<nombre DNS del servidor>” al inicio de la ruta, y sustitúyalo por el CNAME generado al inicio de este procedimiento.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:
 http://crl.dominio.local/CertEnroll/<nombre de CA>< sufijo de nombre de lista

Variable:
 <clase de objeto CA> Insertar

Descripción de la variable seleccionada:
 Se usa en direcciones URL y rutas de acceso
 Inserta el nombre DNS del servidor
 Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 160 - Modificación de ruta http

80. Pulse sobre el botón “Aceptar” y a continuación, seleccionando la nueva entrada, marque los siguientes componentes.

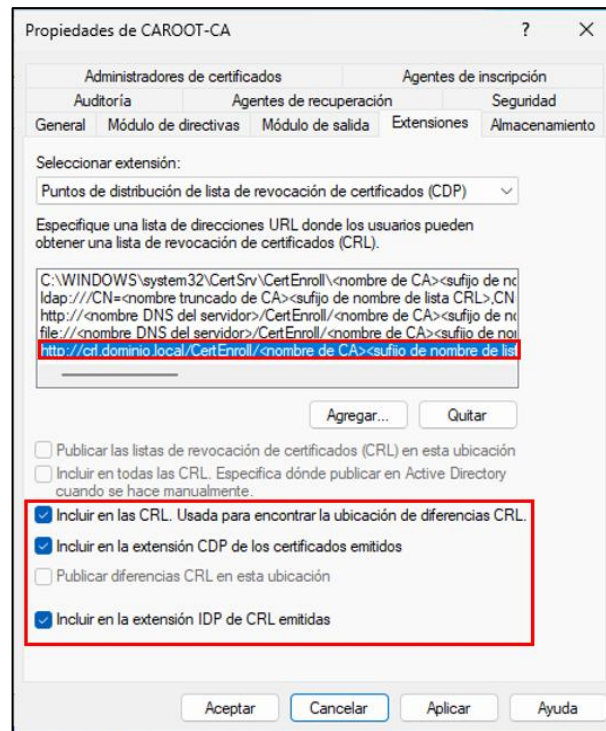


Ilustración 161 - Configuración de entrada http

81. Para continuar, en el desplegable “Seleccionar extensión”, elija “Acceso a la información de entidad (AIA)”.

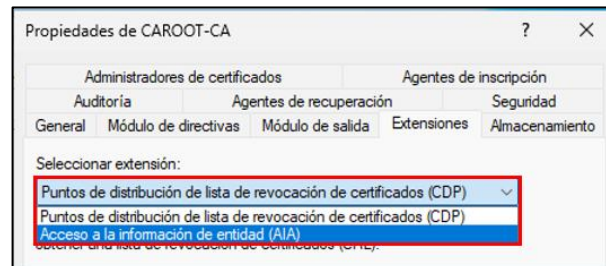


Ilustración 162 - Acceso a configuración AIA

82. Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\<nombre DNS del servidor>_<nombre de CA><Nombre de certificado>.crt” todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.

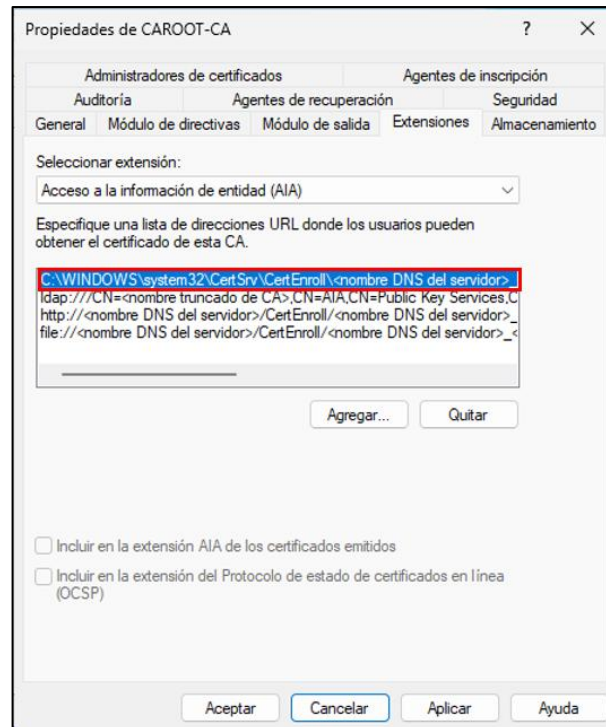


Ilustración 163 - Comprobación de entrada

83. Seleccione el objeto “ldap://CN=<nombre truncado de CA>,CN=AIA,CN=Public Key Services,CN=Services,<contenedor de configuración><clase de objeto CA>” y desmarque todas las casillas tal y como se muestra en la siguiente figura.

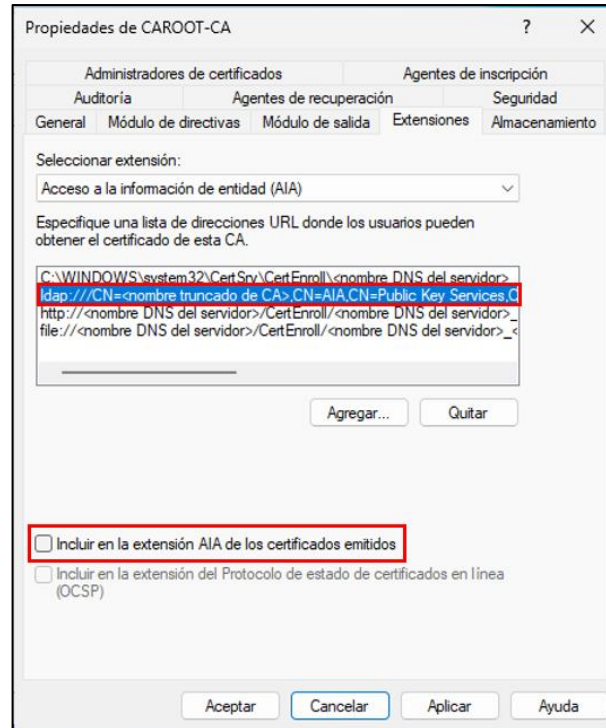


Ilustración 164 - Configuración de extensión LDAP

84. Seleccione ahora “file://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y confirme que la opción “Incluir en la extensión AIA de los certificados emitidos” se encuentra deshabilitada.

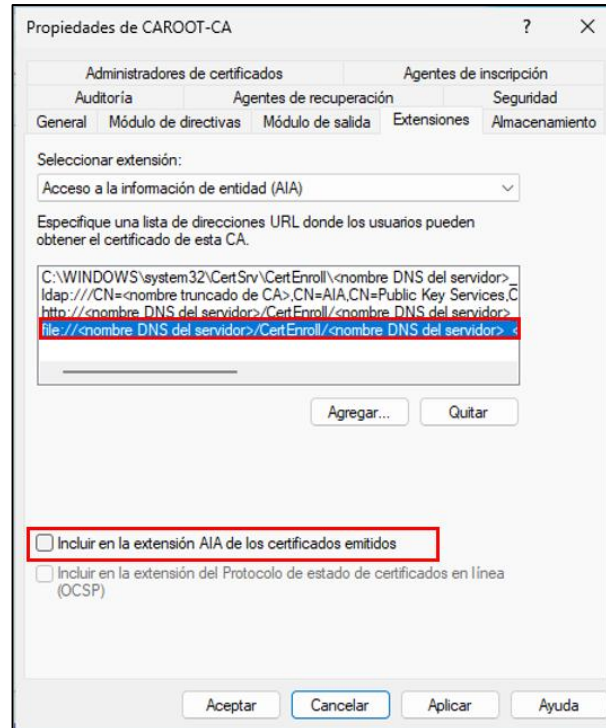


Ilustración 165 - Configuración de extensión file

85. Seleccione ahora “http://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y copie el elemento mediante la combinación de teclas “Control + C”. A continuación, pulse en “Agregar”.

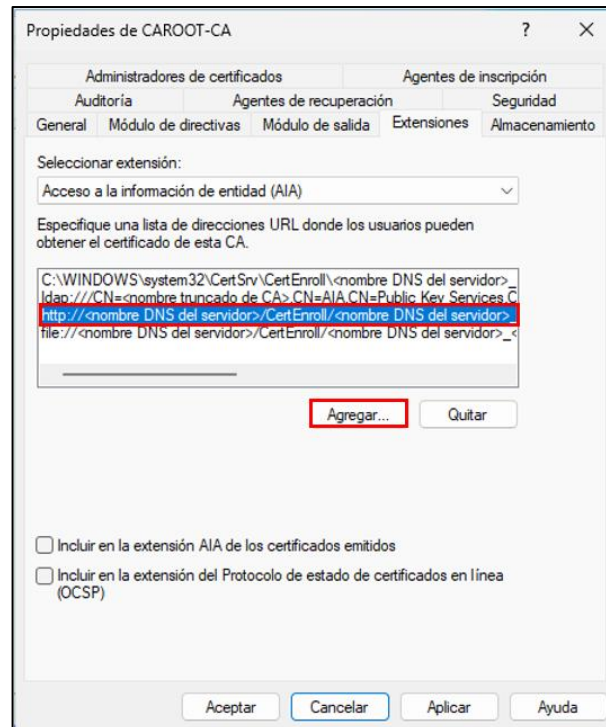


Ilustración 166 - Agregar nueva extensión http

86. En el campo “Ubicación” pegue el contenido copiado.

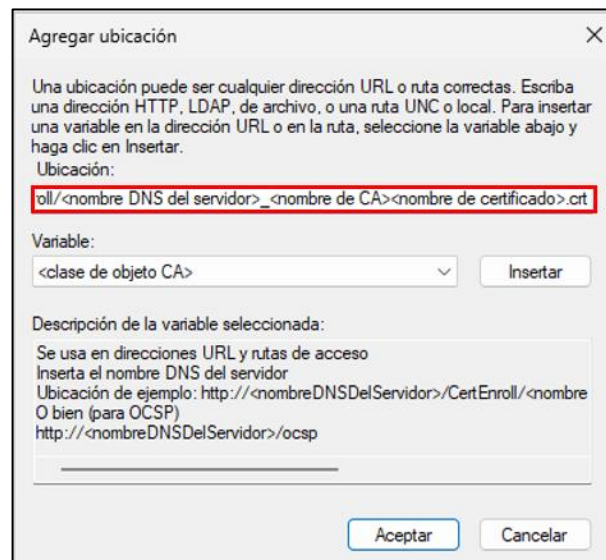


Ilustración 167 - Pegar nueva ruta para extensión http

Nota: Aún no pulse sobre el botón “Aceptar”.

87. Localice y sustituya el valor “<nombre DNS del servidor>” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y su alias CNAME.

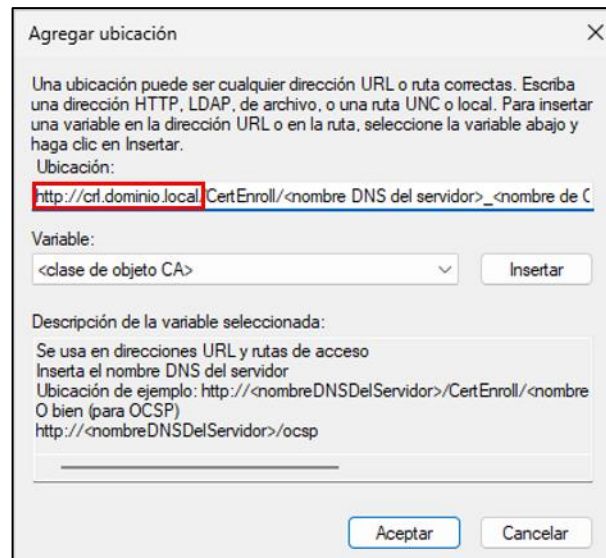


Ilustración 168 - Modificar valor DNS

88. Pulse “Aceptar” y a continuación, marque la casilla “Incluir en la extensión AIA de los certificados emitidos”. A continuación, pulse en “Aplicar” y “Aceptar”.

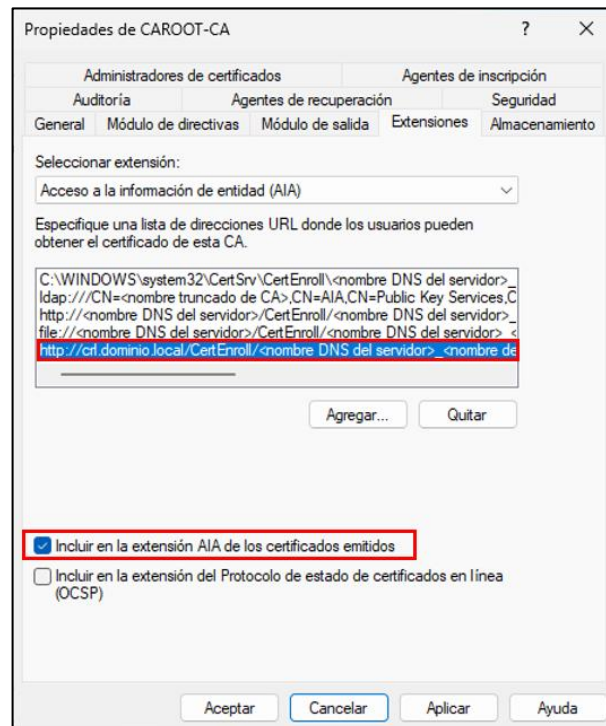


Ilustración 169 - Incluir en la extensión AIA de los certificados emitidos

89. El sistema solicitará reiniciar los servicios de certificados. Pulse en “Sí”.

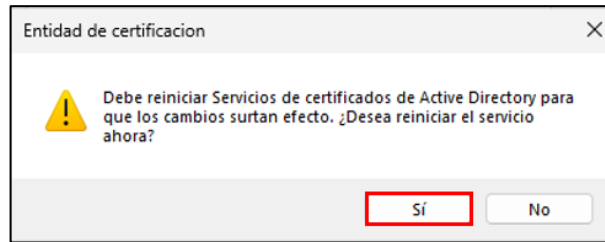


Ilustración 170 - Reiniciar servicios de certificados de Active Directory

90. A continuación, se establecerá un período de caducidad para la lista de revocación de certificados (CRL). Para ello, pulse con el botón derecho sobre “Certificados revocados”, y a continuación, seleccione “Propiedades”.

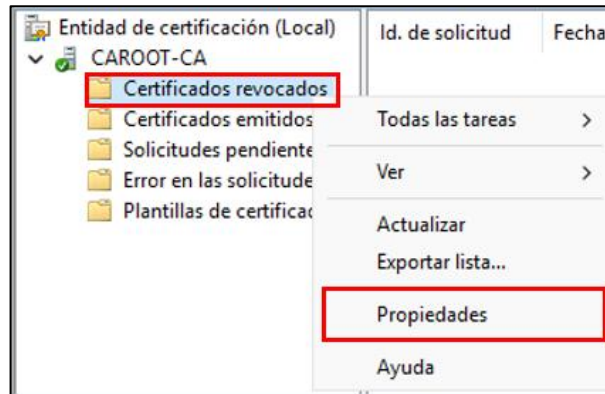


Ilustración 171 - Propiedades de certificados revocados

91. Seleccione el intervalo de publicación CRL con la validez del certificado de la entidad de certificación raíz (10), y a su vez, desmarque la posibilidad de “Publicar diferencias CLR”.

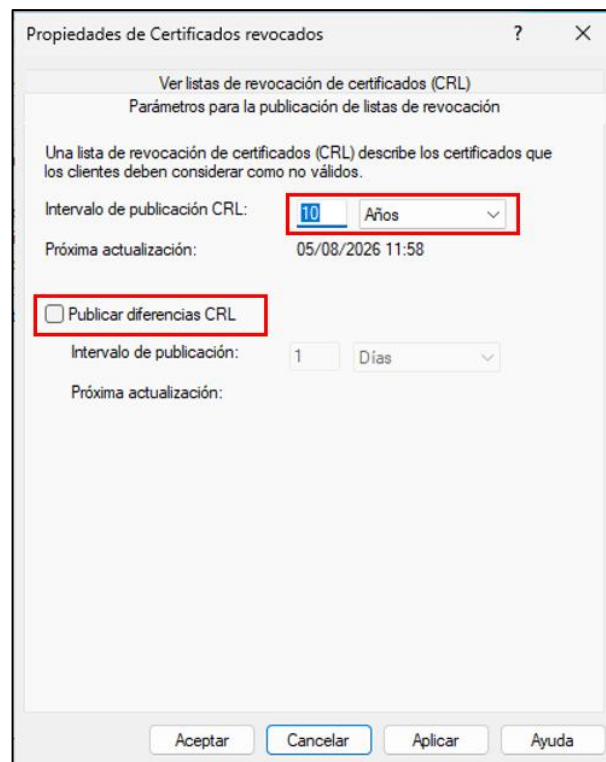


Ilustración 172 - Configuración de CRL

A continuación, pulse sobre el botón “Aplicar” y “Aceptar”.

92. Una vez realizados los cambios, pulse de nuevo con el botón derecho sobre “Certificados revocados”, y seleccione “Todas las tareas > Publicar”.

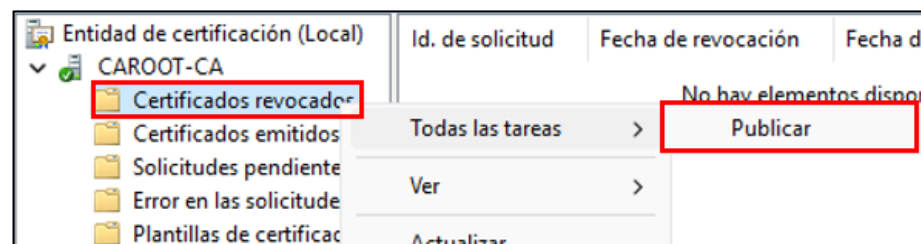


Ilustración 173 - Publicar nueva CRL

93. En el asistente de publicación de lista de revocación de certificados, pulse en “Aceptar”.



Ilustración 174 - Publicar nueva CRL

94. Una vez cambiados estos parámetros será necesario emitir un certificado de la entidad raíz actualizado. Para ello, sobre el objeto con el nombre de la Entidad de Certificación, pulse con el botón derecho y seleccione “Todas las tareas → Renovar certificado de CA...”.

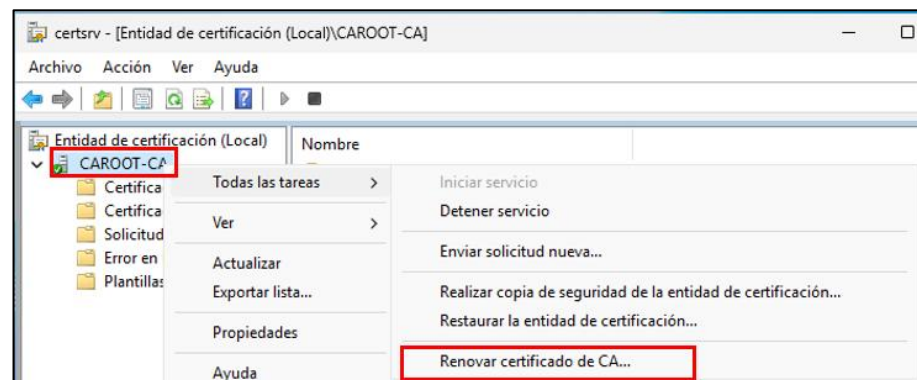


Ilustración 175 - Renovar certificados de CA

95. Pulse en “Sí” para confirmar la creación del nuevo certificado.

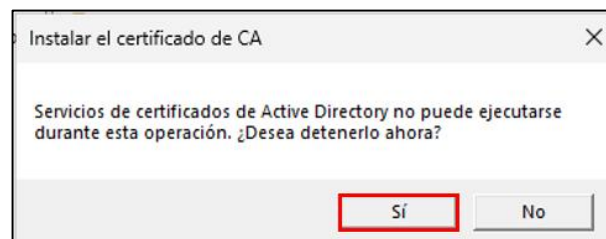


Ilustración 176 - Renovación de certificado de CA

96. En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.

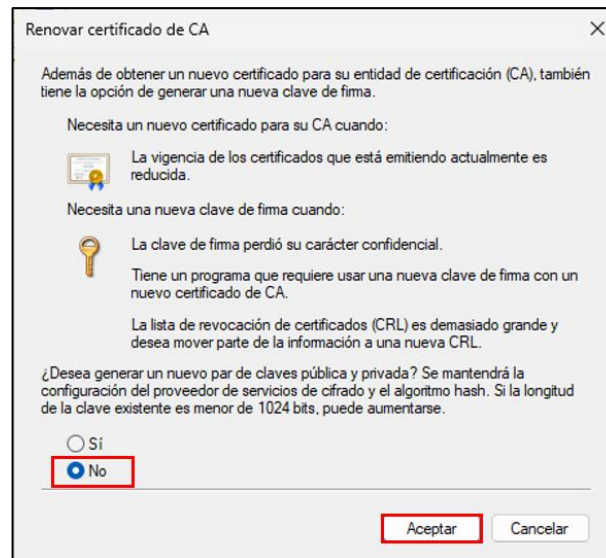


Ilustración 177 - Renovar certificado de CA

97. Una vez finalice el proceso, la entidad de certificación raíz estará disponible para generar el certificado de la entidad subordinada y establecer la jerarquía de certificación.

6.2.4. PASO A PASO DE INSTALACIÓN EN ENTIDAD DE CERTIFICACIÓN SUBORDINADA EN DOMINIO

Los pasos que se describen a continuación se realizarán en el servidor Entidad de Certificación Subordinada en el dominio.

Nota: Si su entidad de certificación subordinada ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
98.	Inicie sesión en el equipo donde se va a instalar el servidor Entidad de Certificación subordinada del dominio con un usuario con privilegios de administración.

99. A continuación, se ejecutará el Administrador del servidor para configurar el servidor de Entidad de Certificación.

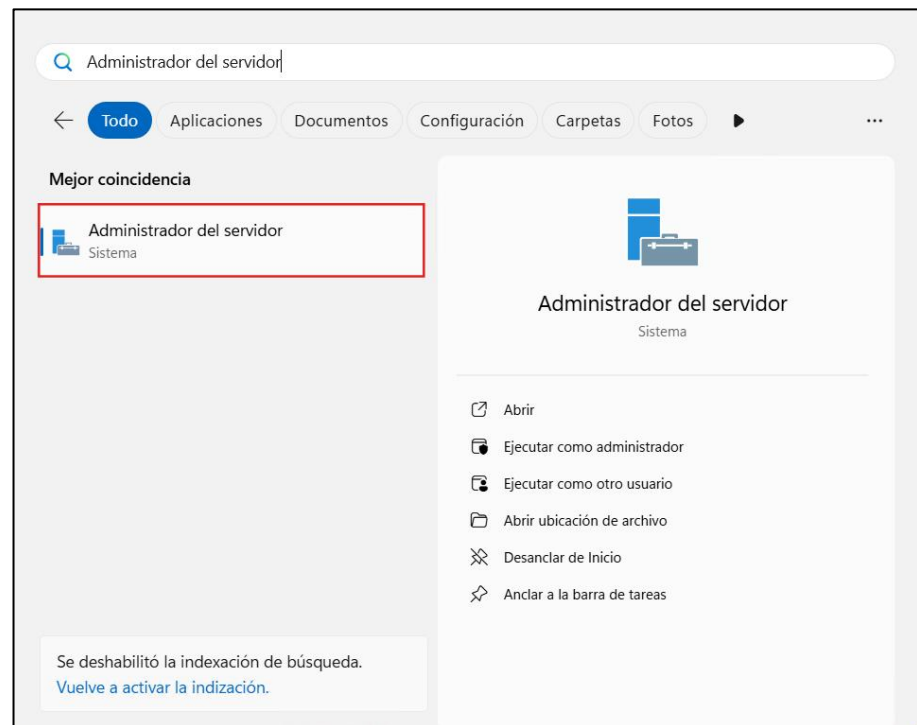


Ilustración 178 – Administración del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

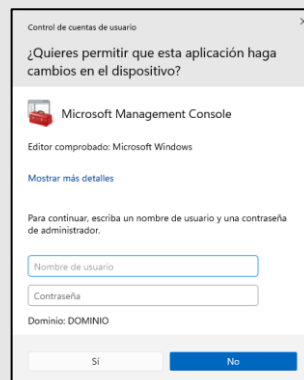


Ilustración 179 - Introducir credenciales de administrador

100. Le aparecerá una ventana para proceder con la configuración, pulse en “Configurar Servicios de certificados de Active Directory”.

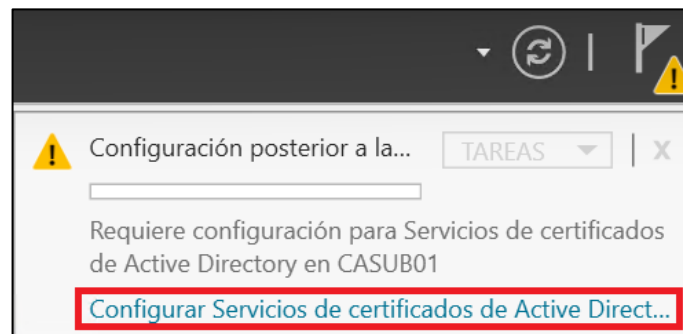


Ilustración 180 – Configurar Servicios de certificados

Nota: Si el rol de Entidad de certificación no se encuentra instalado, esta advertencia no se apreciará en el administrador del servidor. Añadir la funcionalidad desde “Administrar > Agregar roles y características”.

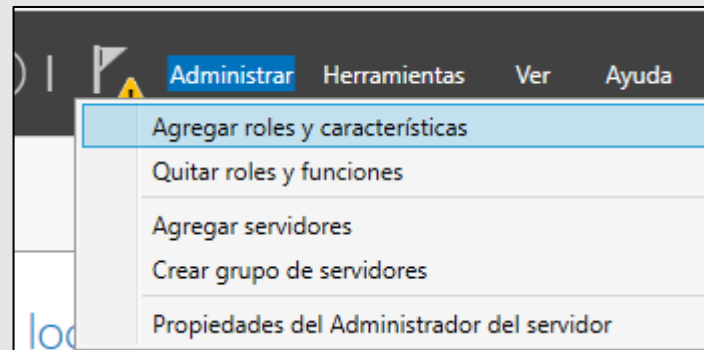


Ilustración 181 - Agregar roles y características

101. Especifique las credenciales para configurar servicios de rol. Pulse en “Siguiente”.

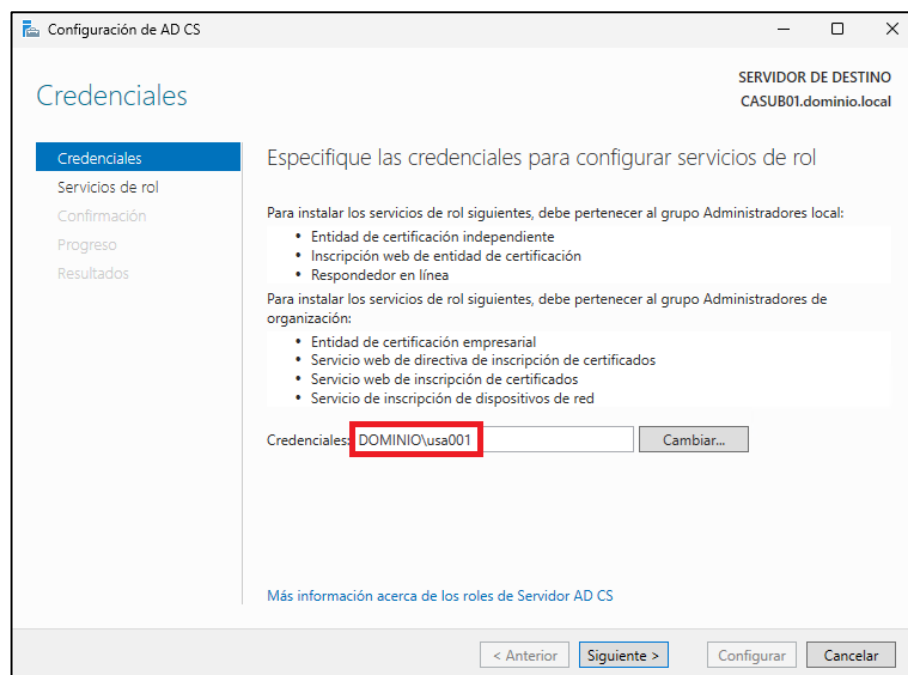


Ilustración 182 – Especificación de credenciales

Nota: El usuario administrador que se utilizará en todo el escenario será **usa001**.

102. Seleccione los servicios de rol que dispondrá el servidor de Entidad de Certificación. En el presente caso serán “Entidad de certificación”. Pulse en “Siguiente”.

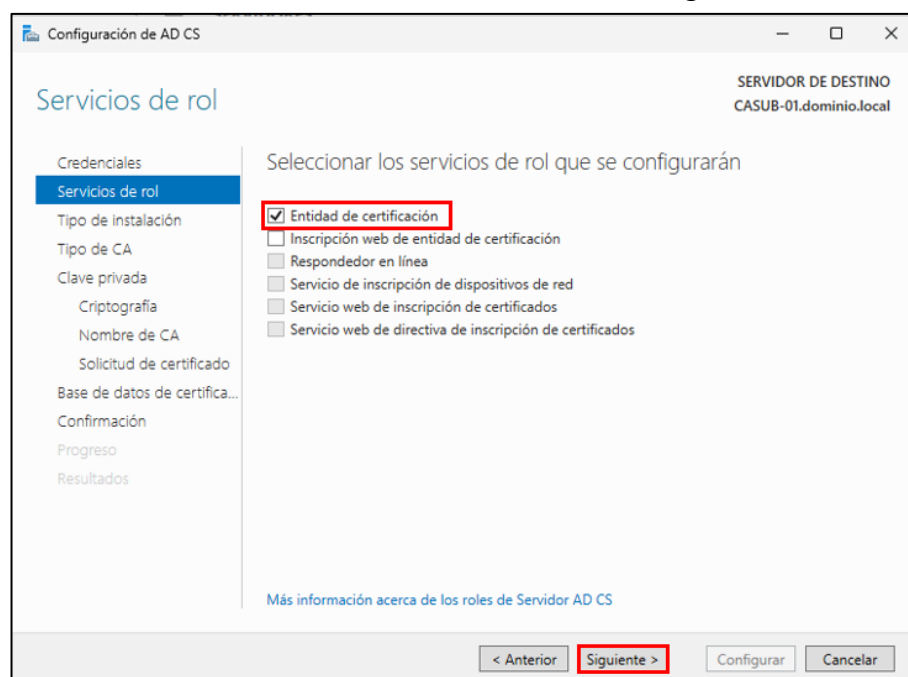


Ilustración 183 - Configuración de rol de Entidad de certificación

103. Especifique el tipo de instalación de la CA, seleccione “CA empresarial”. Pulse en “Siguiente”.

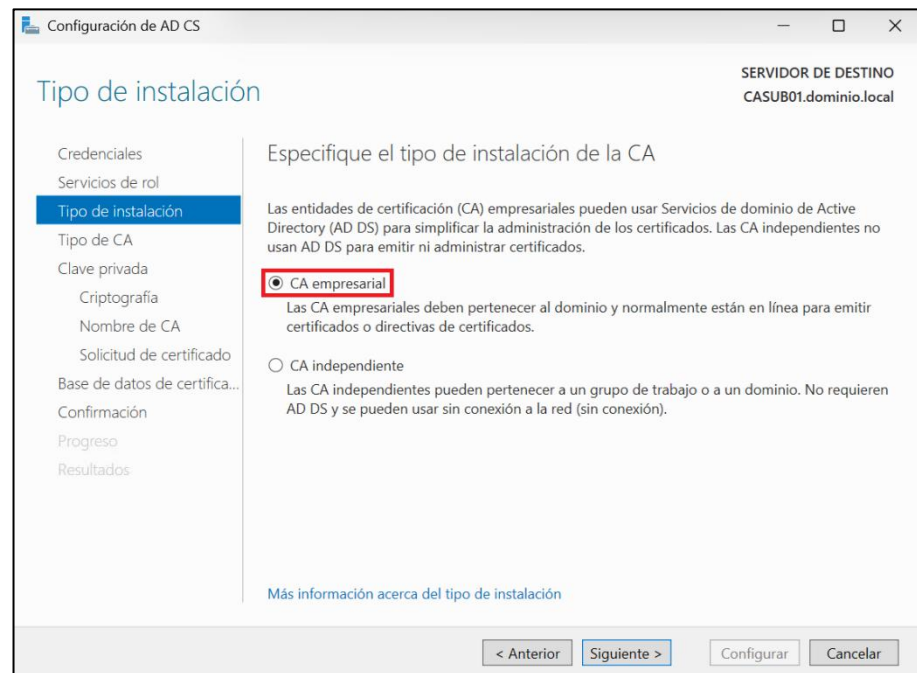


Ilustración 184 – Especificación del tipo de instalación de la CA

104. Seleccione “CA subordinada”. Pulse en “Siguiente”.

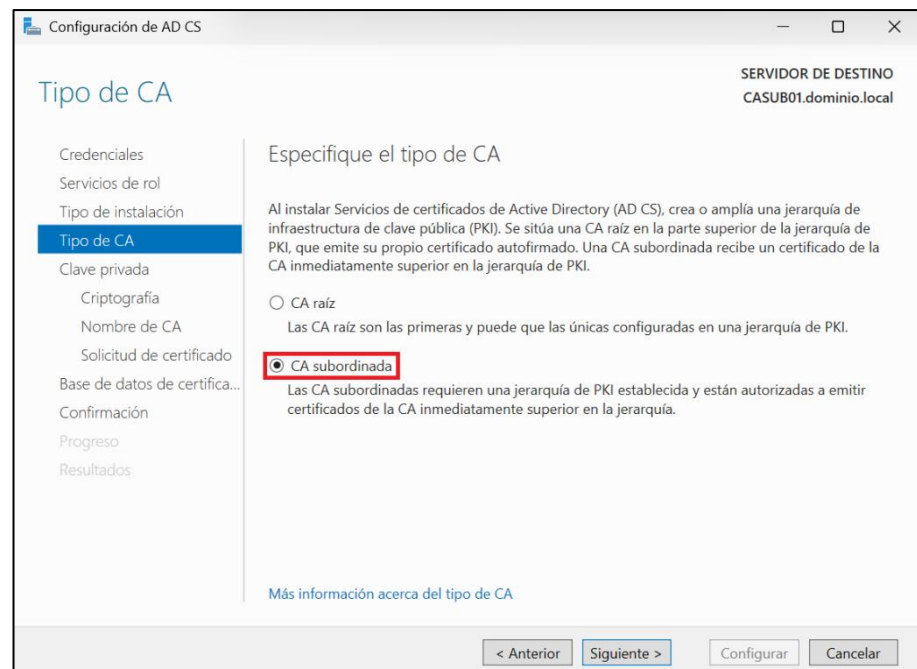


Ilustración 185 – Especificación del tipo de CA

105. A continuación, seleccione la opción de “Crear una clave privada nueva”. Pulse en “Siguiente”.

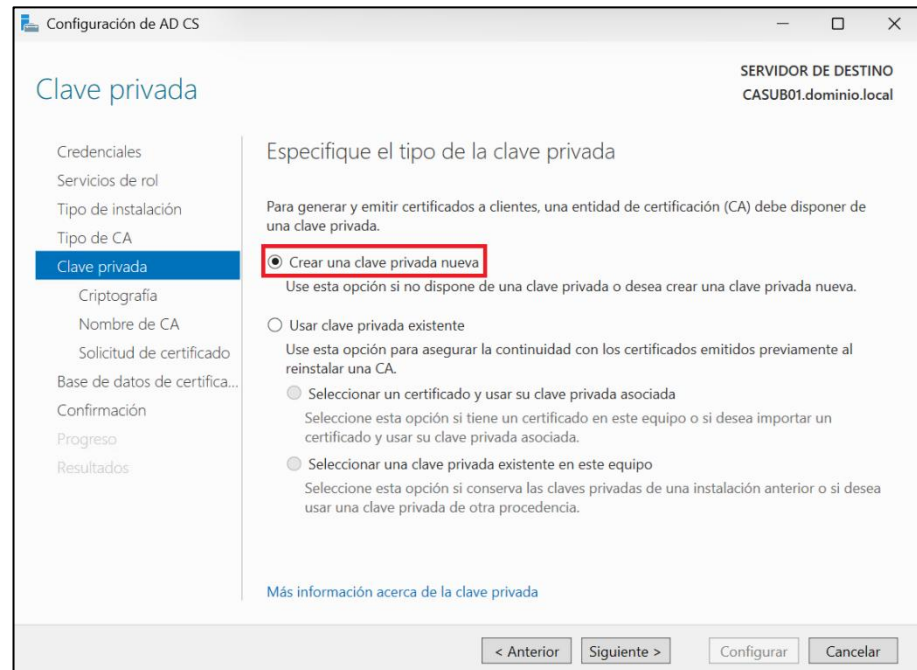


Ilustración 186 – Especificación del tipo de clave privada

106. Las opciones criptográficas que se seleccionarán serán.

- Longitud: 2048
- Tipo de algoritmo hash: SHA256

Posteriormente, pulse en “Siguiente”.

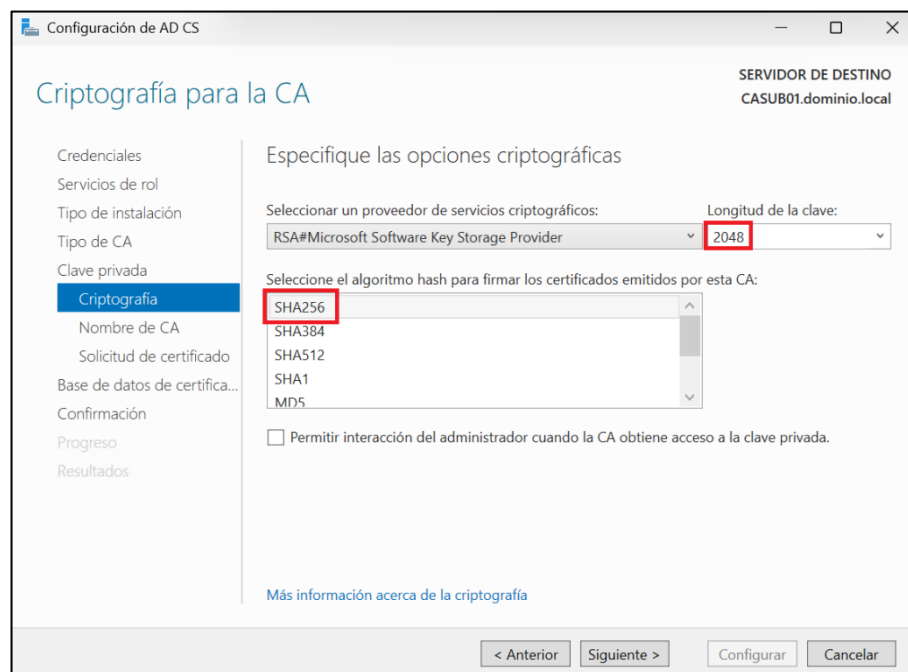


Ilustración 187 – Especificación de opciones criptográficas

107. A continuación, se especificará el nombre para la entidad de certificación. En el presente caso, será “dominio-CASUB01-CA”. Posteriormente, pulse en “Siguiente”.

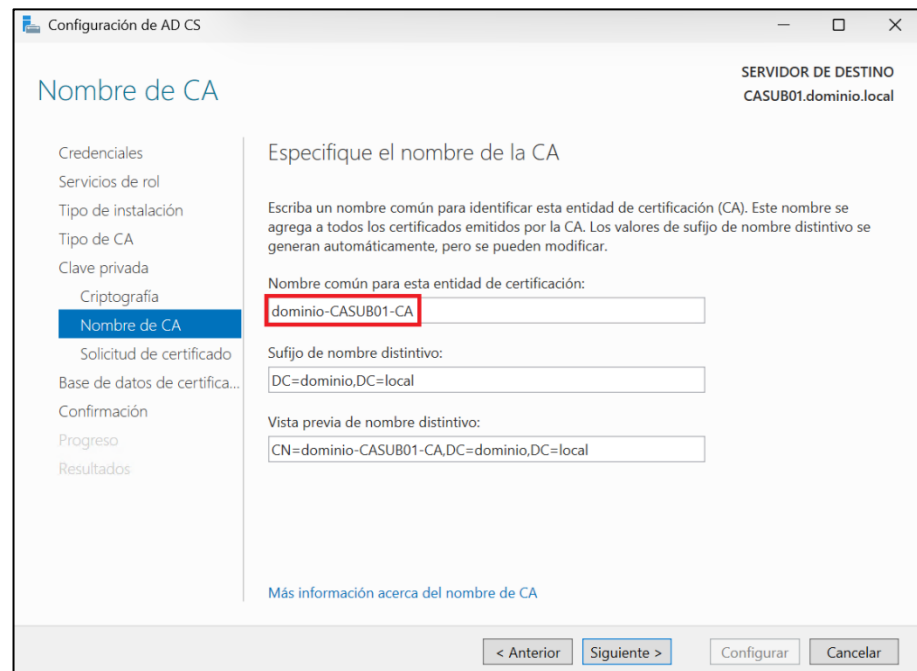


Ilustración 188 – Nombre de la CA

108. Seleccione la opción de “Guardar una solicitud de certificado en un archivo del equipo de destino” y establezca la ruta y el nombre del archivo de solicitud. Pulse en “Siguiente”.

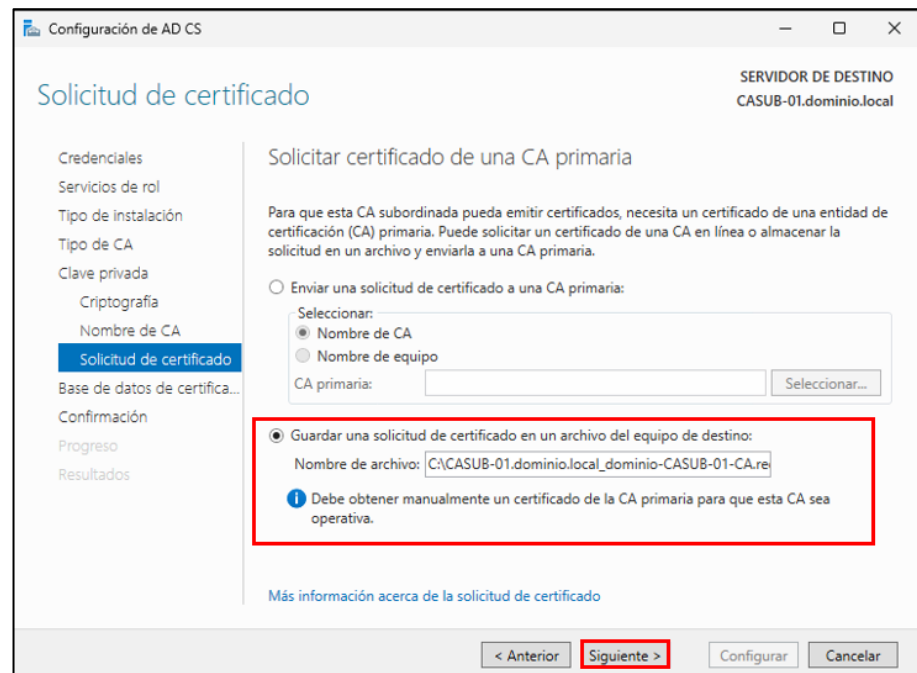


Ilustración 189 - Exportar solicitud de certificado

109. En la siguiente página se especificará las ubicaciones donde se almacenarán los certificados. Se establecerán las carpetas por defecto. Finalmente, pulse en “Siguiente”.

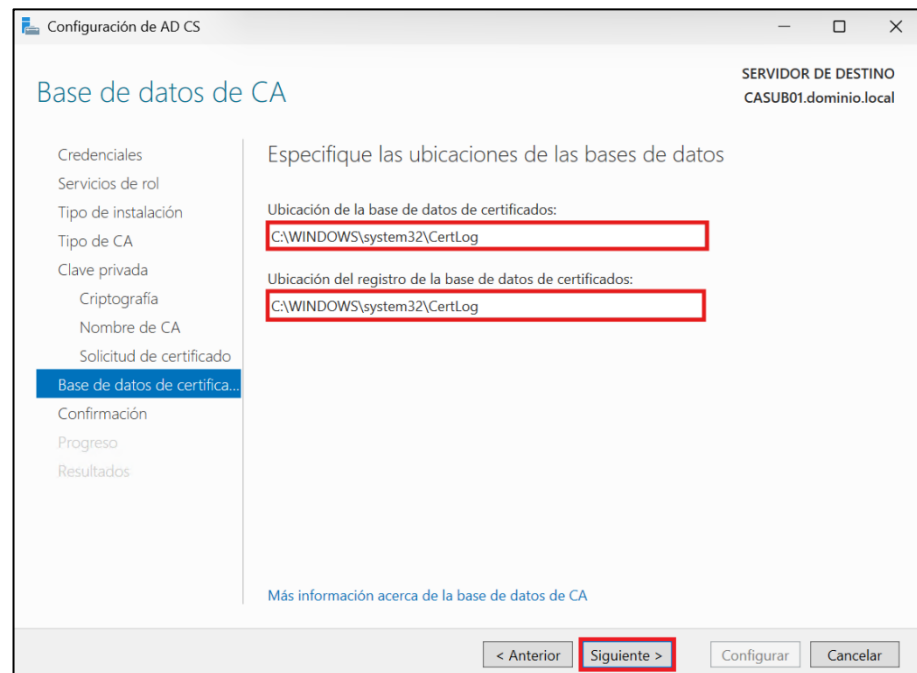


Ilustración 190 – Selección de la ubicación de base de datos

Nota: Si su entorno dispone de un sitio específico, deberá indicarlo en este apartado.

110. Finalmente, se visualiza un resumen de toda la configuración. Pulse en “Configurar”.

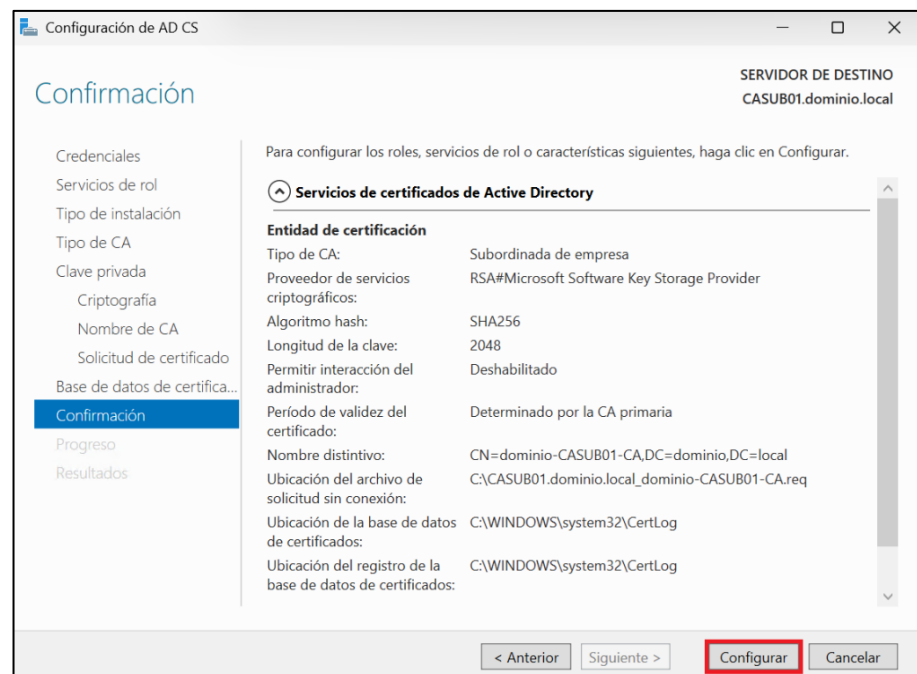


Ilustración 191 – Resumen de configuración

111. El proceso de instalación finalizará y para completar la configuración, será necesario generar el certificado en la entidad de certificación raíz. Puede pulsar en “Cerrar”.

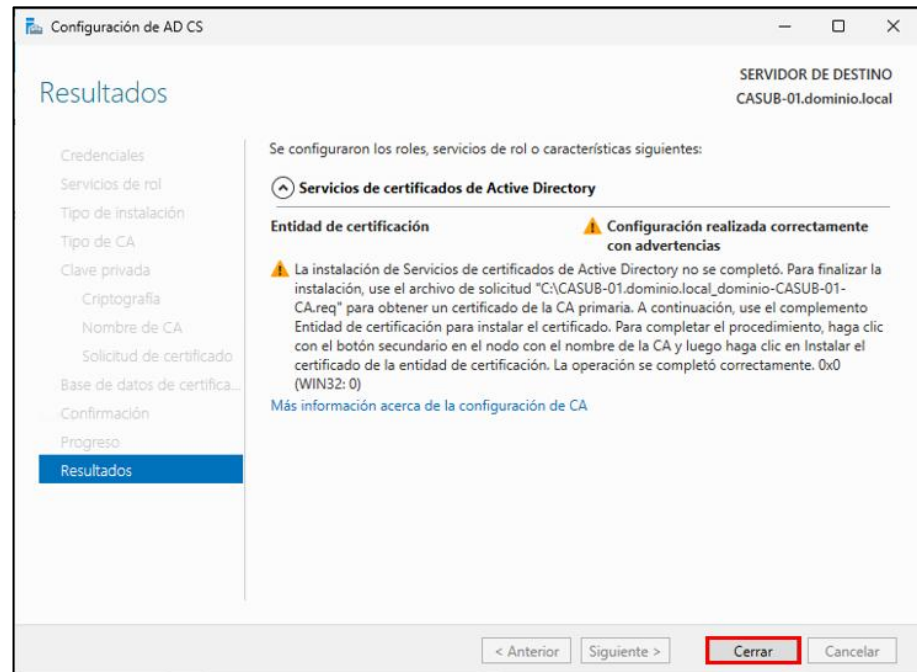


Ilustración 192 - Finalizar asistente

112. En caso de que la consola de “Administración del servidor” muestre la posibilidad de configurar servicios de rol adicionales, pulse “No” ya que la configuración de IIS se realizará posteriormente.

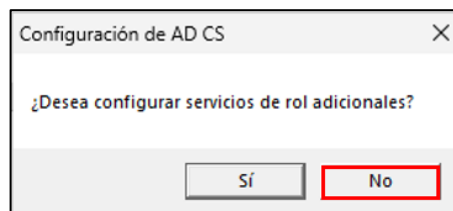


Ilustración 193 - No continuar con configuraciones adicionales

113.

A continuación, siguiendo el procedimiento de seguridad adecuado, copie el fichero generado durante la ejecución del asistente anterior a la entidad de certificación raíz y continúe con el siguiente anexo de configuración del rol de entidad de certificación subordinada.

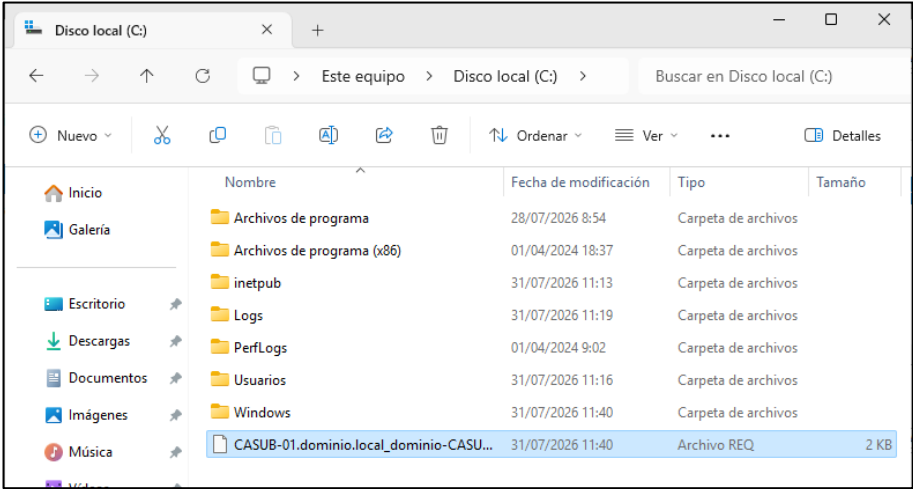


Ilustración 194 - Fichero de petición de emisión de certificado

6.2.5. CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA

Los pasos que se describen a continuación se realizarán en los servidores Entidad de Certificación Raíz y Subordinada del dominio.

Nota: Si su entidad de certificación subordinada ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
114.	Inicie sesión en la entidad de certificación raíz con un usuario con privilegios de administración.

115. A continuación, se ejecutará como administrador el “Administrador del servidor” para configurar el servidor de Entidad de Certificación.

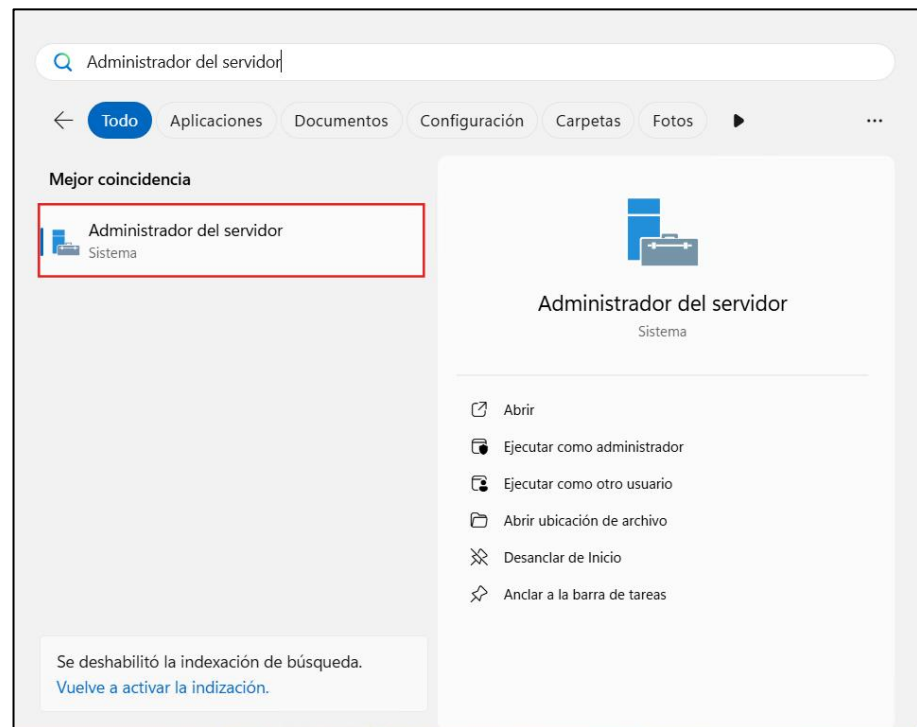


Ilustración 195 - Iniciar consola de Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

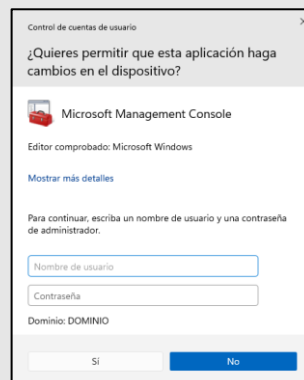


Ilustración 196 - Introducir credenciales de administrador

116. Desde el panel de “Administración del servidor”, haga clic en “Herramientas > Entidad de certificación”.

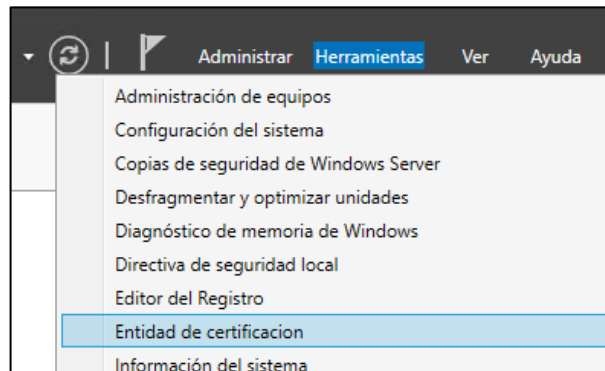


Ilustración 197 - Iniciar consola de administración de CA

117. Haga clic derecho sobre el nombre de la entidad raíz y a continuación, pulse en “Todas las tareas > Enviar solicitud nueva...”.

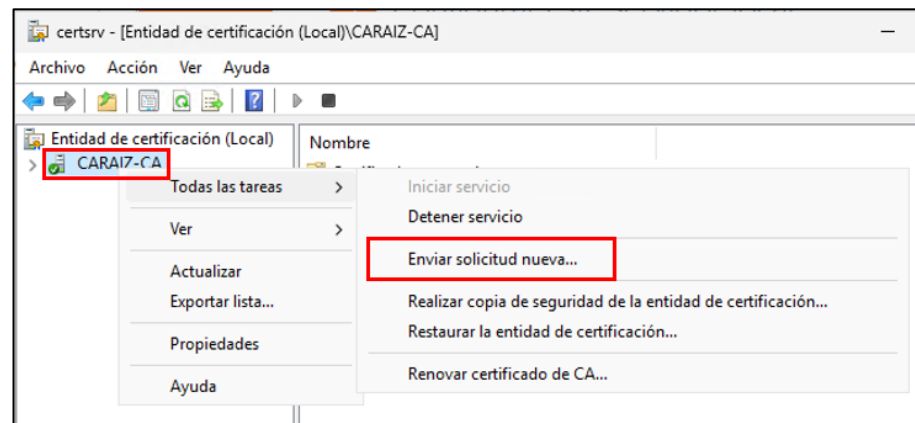


Ilustración 198 - Enviar solicitud nueva

118. Seleccione el fichero “*.req” generado y copiado en pasos anteriores. Posteriormente, pulse en “Abrir”.

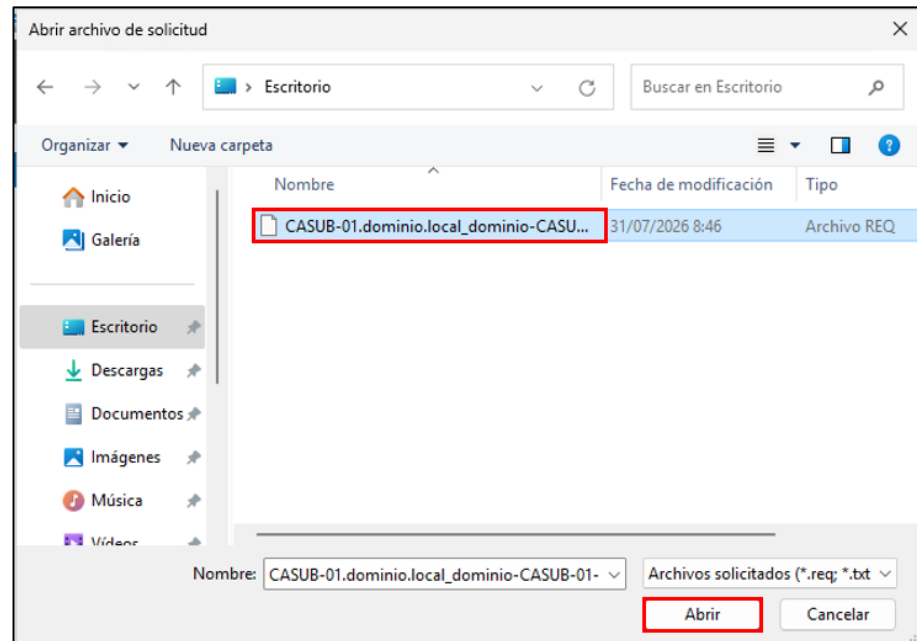


Ilustración 199 - Selección de petición de emisión

119. A continuación, aparecerá una nueva ventana para guardar el certificado que se generará. Introduzca un nombre descriptivo y pulse sobre el botón guardar.

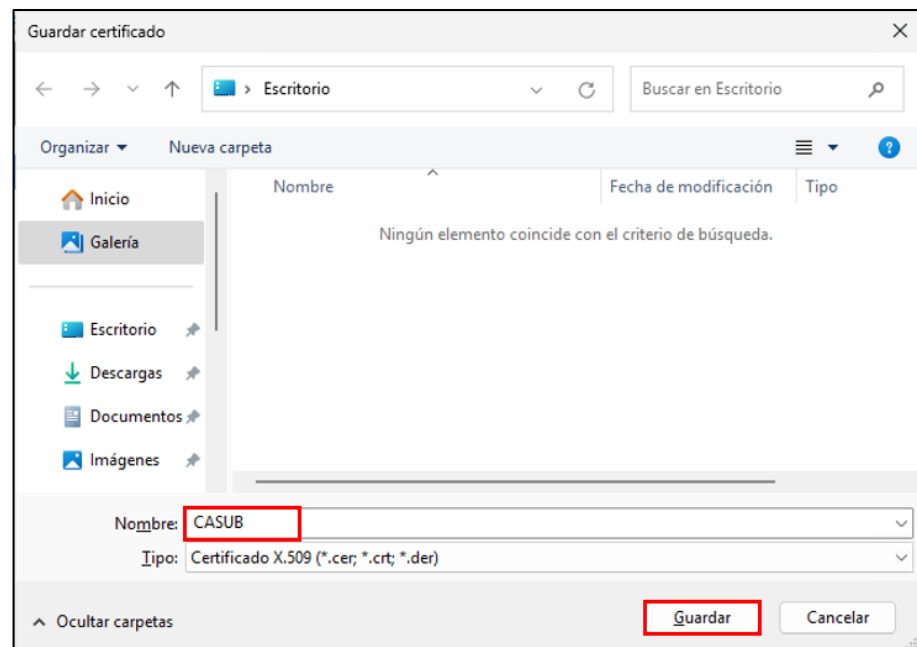


Ilustración 200 - Almacenar certificado de CA

120. Para continuar, copie el certificado generado a la entidad de certificación subordinada siguiendo los procedimientos operativos de seguridad definidos.

121. A su vez, diríjase a la ruta “C:\Windows\System32\CertSrv\CertEnroll” y copie todos los ficheros del directorio a la entidad de certificación subordinada.

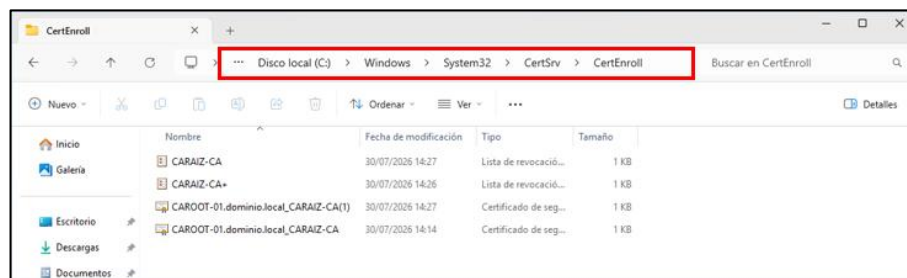


Ilustración 201 - Acceso a ruta de CertEnroll

122. Inicie sesión en el servidor de entidad de certificación subordinada con un usuario con privilegios de administración.

123. Inicie la consola “Administrador del servidor” con privilegios de administración.

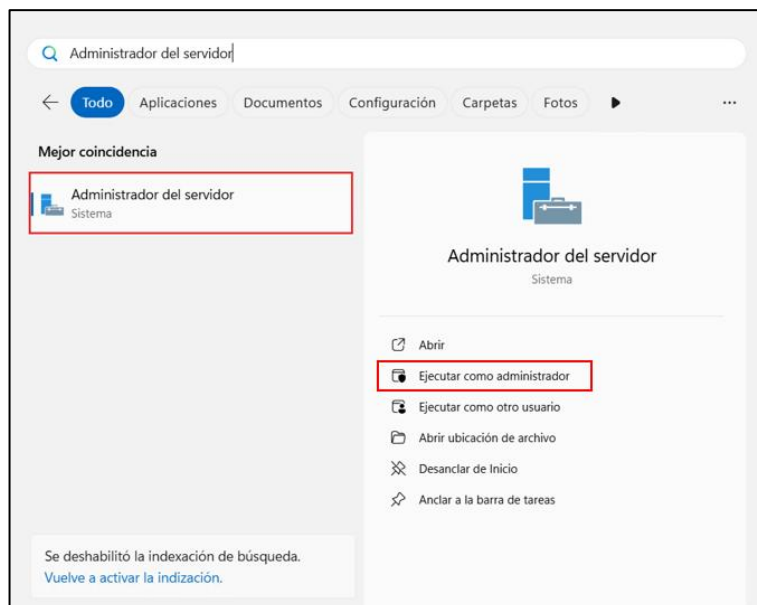


Ilustración 202 - Iniciar consola Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

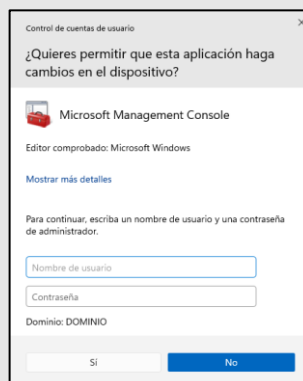


Ilustración 203 - Introducir credenciales de administrador

124. A continuación, en el administrador del servidor, haga clic sobre la advertencia de seguridad y pulse en “Configurar Servicios de certificados de Active Directory”.

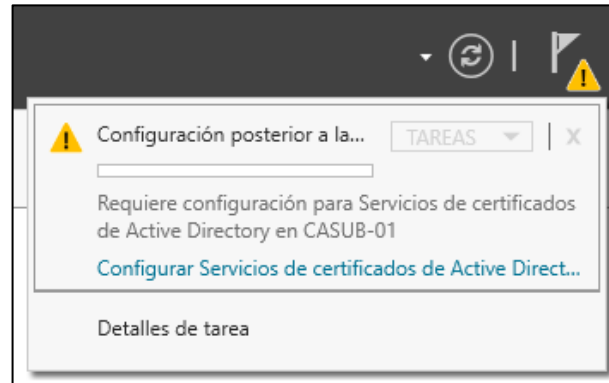


Ilustración 204 - Continuar con la configuración de CA

Nota: Si únicamente se ha instalado la característica de “Entidad de certificación”, esta advertencia no aparecerá en el panel de administración del servidor. Será necesario entonces instalar el servidor IIS de manera manual, y continuar con la configuración del servicio web descrita en siguientes pasos.

125. En el asistente, pulse “Siguiente” para continuar con las credenciales del usuario administrador.

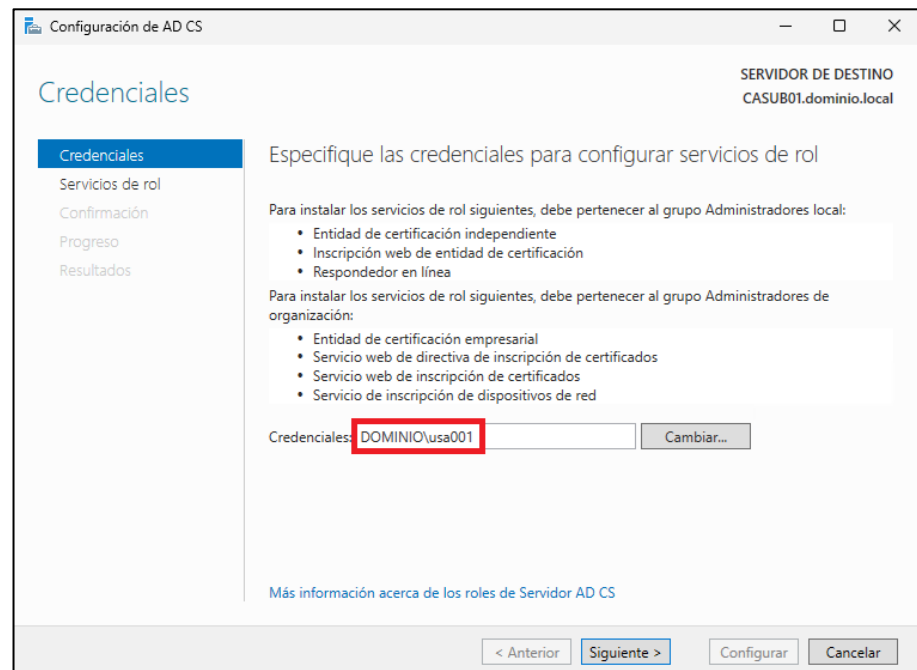


Ilustración 205 - Especificación de credenciales

126. Seleccione “Inscripción web de entidad de certificación” para habilitar el rol de IIS. Pulse “Siguiente”.

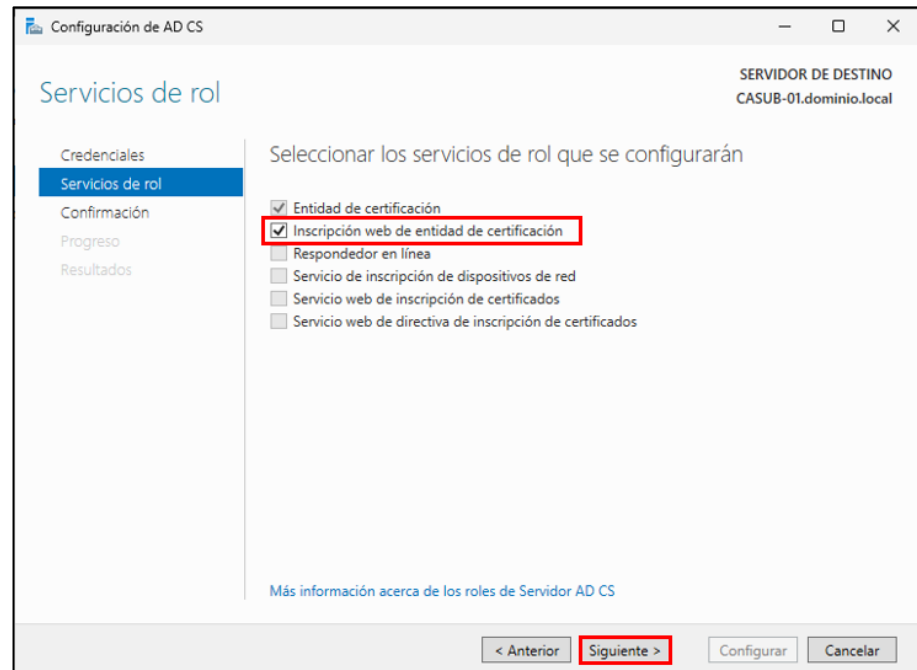


Ilustración 206 - Configuración de servicio Web en la Entidad de Certificación

127. Para confirmar la implementación, pulse en “Configurar”.

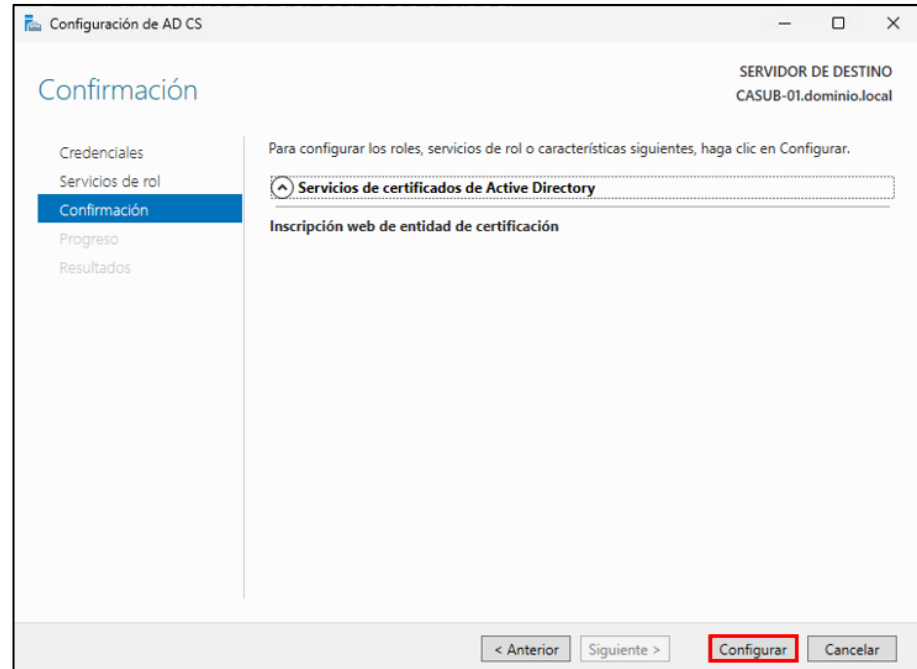


Ilustración 207 - Configuración del asistente

128. Tras la finalización del asistente, se mostrará la confirmación de que la configuración se ha realizado correctamente. Pulse “Cerrar”.

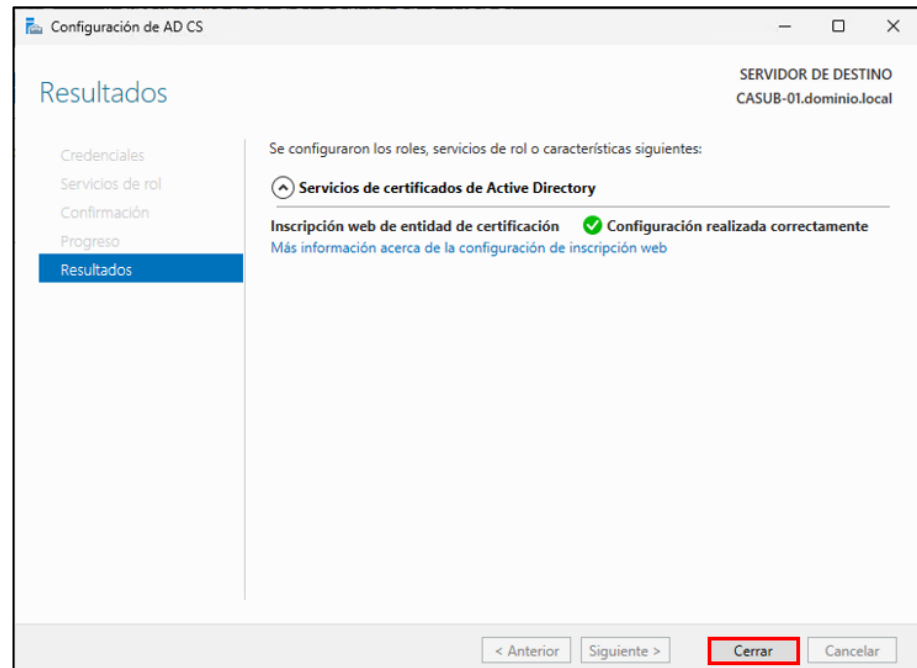


Ilustración 208 - Finalización del asistente

129. A continuación, inicie la consola de administración de IIS desde “Administrador del servidor > Herramientas > Administrador de Internet Information Services (IIS)”.

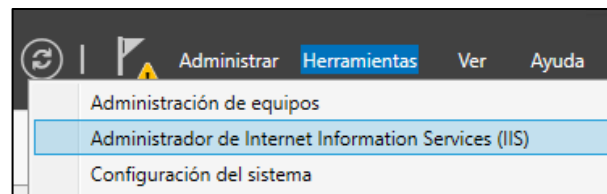


Ilustración 209 - Iniciar consola de Administración IIS

130. Despliegue el árbol del servidor web y diríjase al directorio virtual “CertEnroll”. A continuación, haga doble clic en “Autenticación”.

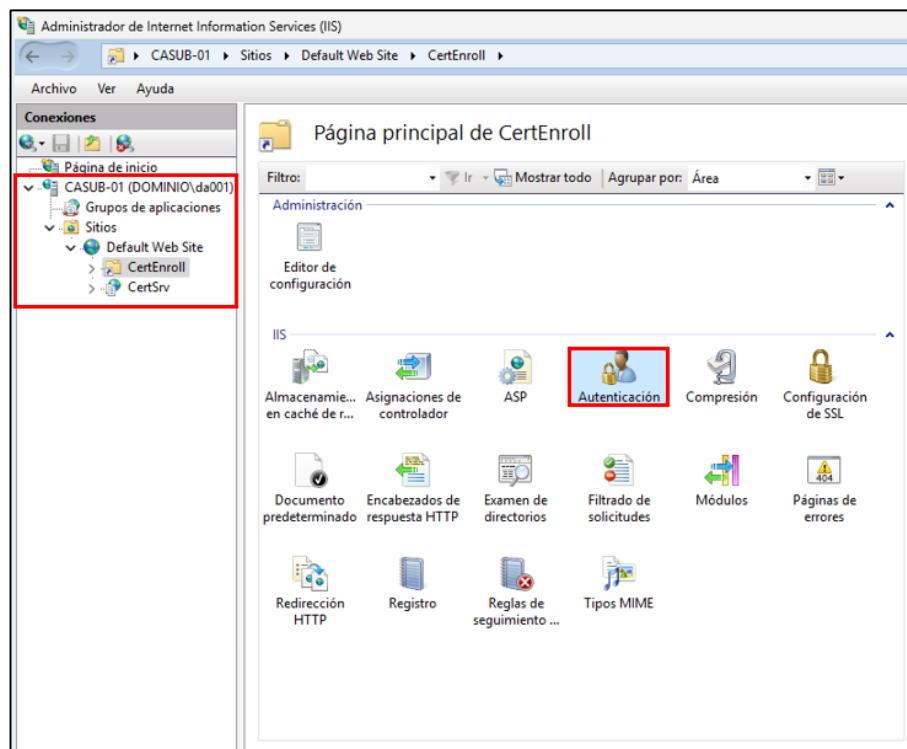


Ilustración 210 - Configuración de autenticación

131. Confirme que la autenticación anónima se encuentra “Habilitada”.

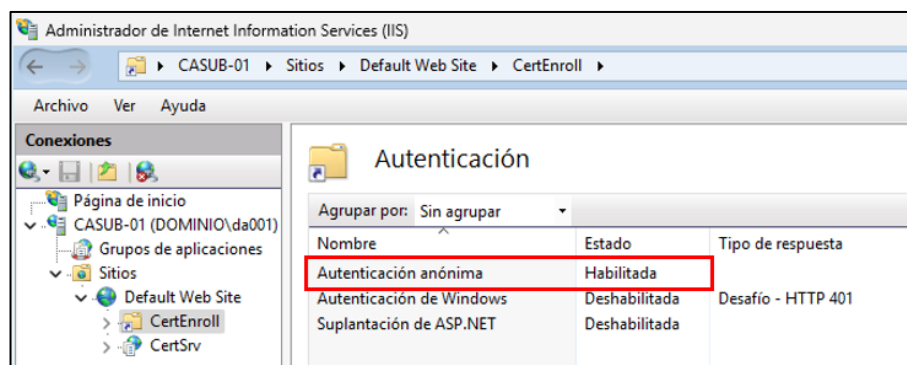


Ilustración 211 - Autenticación anónima habilitada

132. Para continuar, confirme que el directorio de CertEnroll está vinculado al directorio C:\Windows\System32\CertSrv\CertEnroll haciendo clic derecho sobre el acceso directo y posteriormente en “Explorar”.

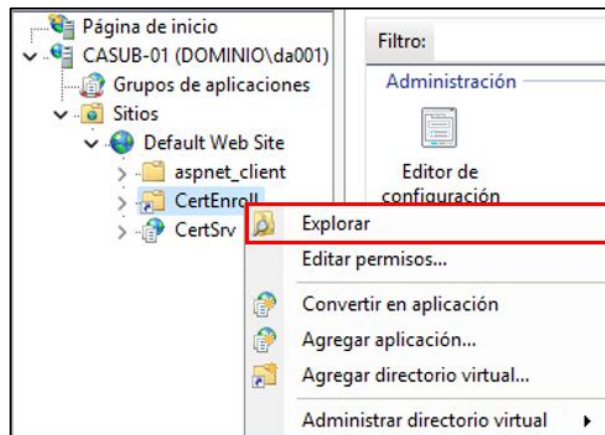


Ilustración 212 - Explorar directorio virtual

El directorio que debe aparecer es el indicado anteriormente.

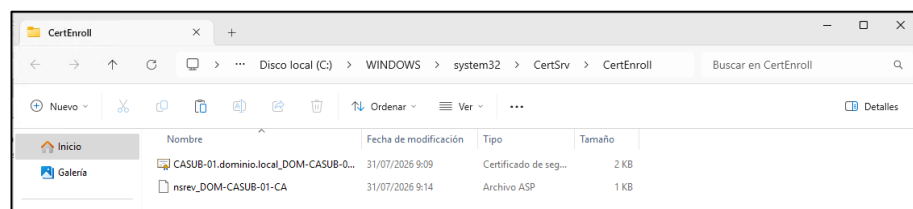


Ilustración 213 - Directorio virtual de C:\Windows\System32\CertSrv\CertEnroll

Nota: Si se ha instalado de manera manual el servicio Web, será necesario crear el directorio virtual manualmente, haciendo clic derecho sobre “Default Web Site” y seleccionando “Agregar directorio virtual...”

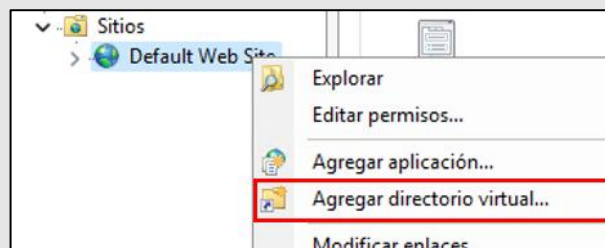
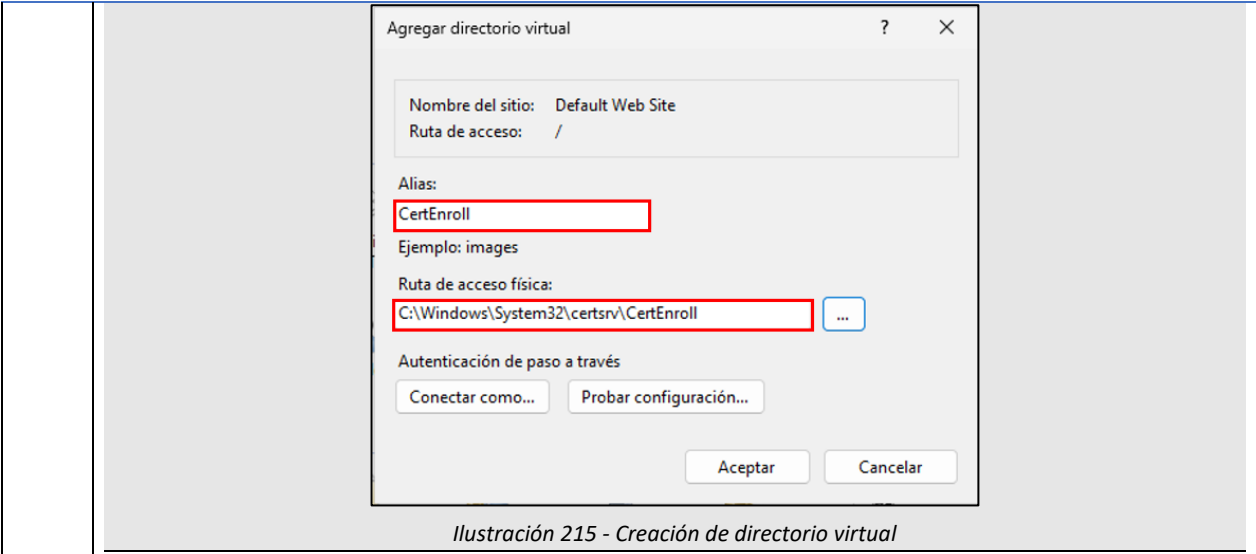
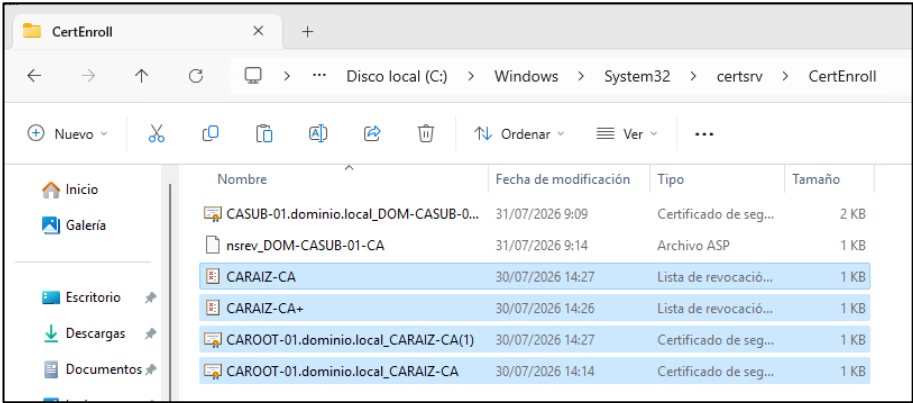
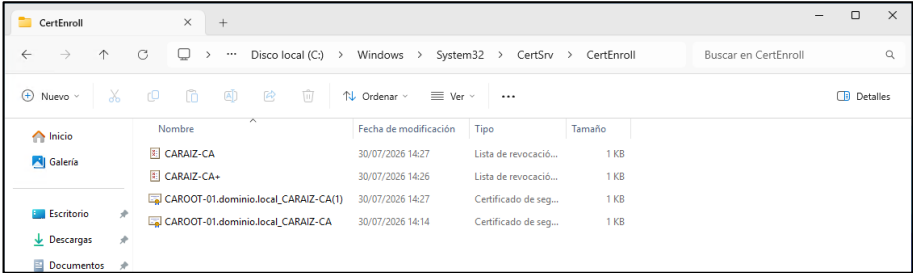


Ilustración 214 - Agregar directorio virtual

A continuación, cree el directorio CertEnroll configurando el acceso físico a la ruta C:\Windows\System32\certsrv\CertEnroll.



133. En dicho directorio, copie los ficheros importados de la entidad de certificación raíz en pasos anteriores.



134. A continuación, puede cerrar el explorador de archivos y la consola de “Administración de Internet Information Services”.

135. De nuevo en el panel de administración del servidor de la entidad de certificación subordinada, inicie la consola de administración de “Entidad de certificación”.

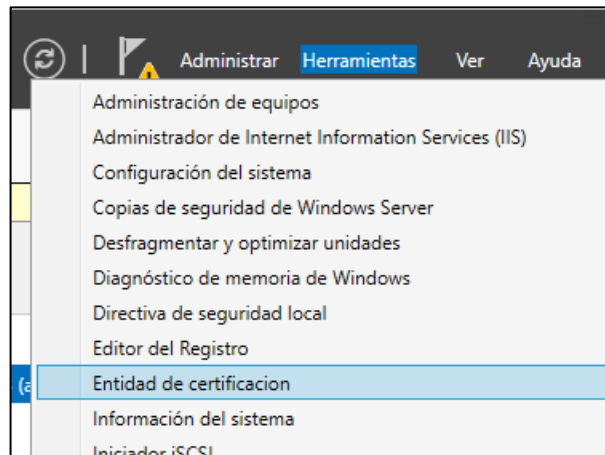


Ilustración 218 - Iniciar consola de administración de CA

136. Pulse sobre la entidad subordinada con el botón derecho y a continuación, diríjase a “Todas las tareas > Instalar el certificado de CA”.

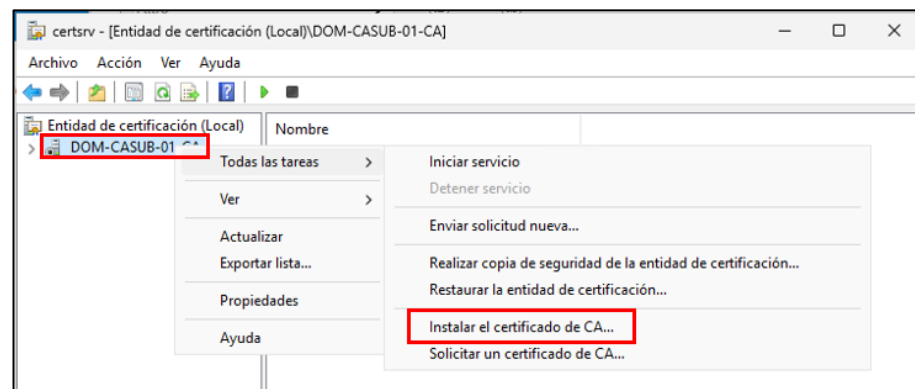


Ilustración 219 - Instalar certificado de CA

137. Navegue hasta la ruta donde se ha almacenado el certificado, y seleccionando “Todos los archivos (*.*)” en el menú contextual, seleccione el certificado.

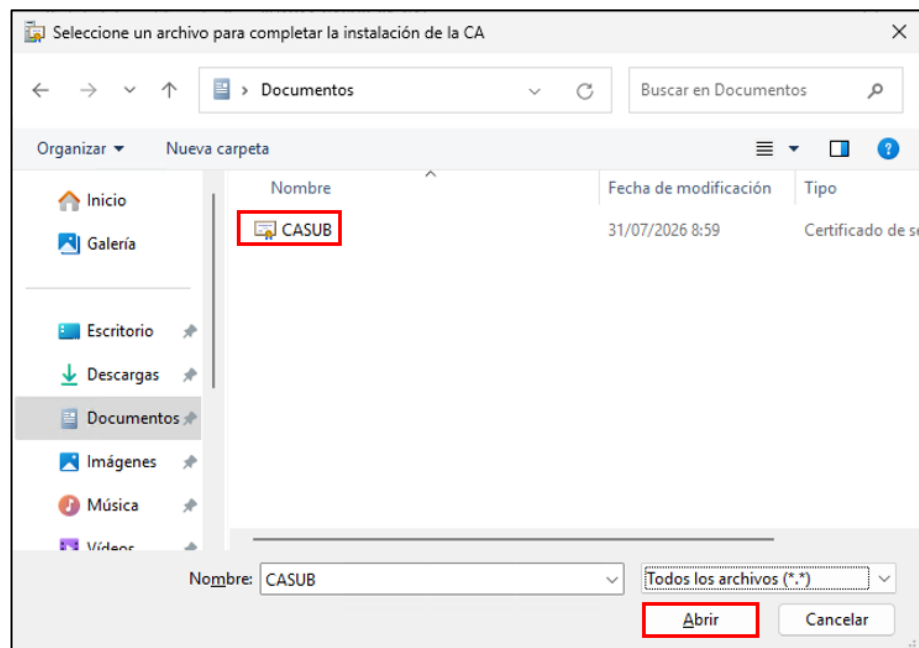


Ilustración 220 - Instalación de certificado de CA

138. En la advertencia que muestra la siguiente ilustración, pulse en “Aceptar”. De este modo, se permitirá confiar en el certificado de la entidad de certificación raíz.



Ilustración 221 - Permitir confiar en la cadena de certificación

139. A continuación, se observará que el servicio de la entidad subordinada de certificación no está iniciado.

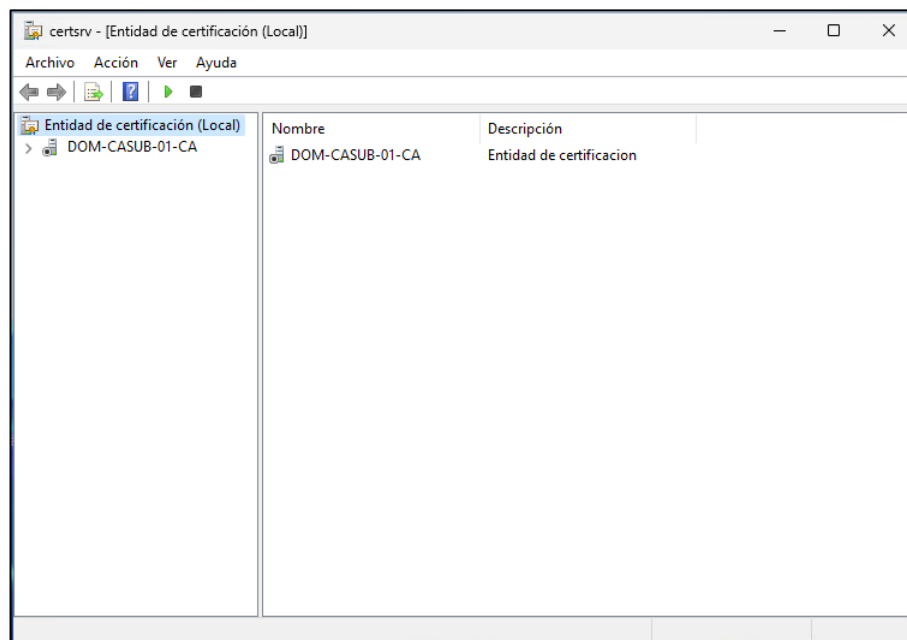


Ilustración 222 - Consola de administración de CA

140. Pulse con el botón derecho sobre el nombre de la entidad de certificación, y a continuación, pulse en "Todas las tareas > Iniciar servicio".

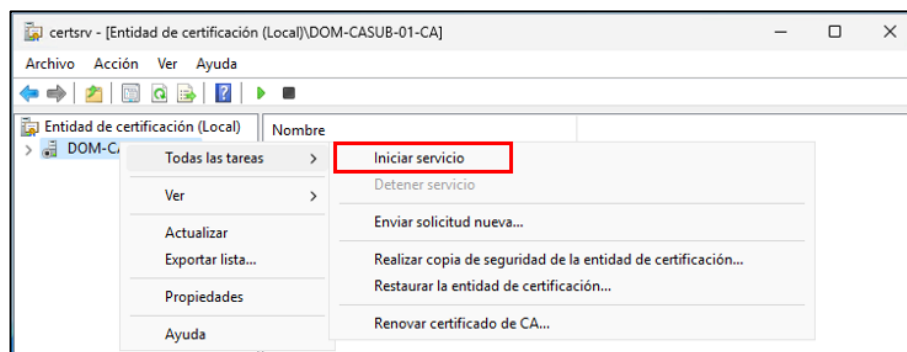


Ilustración 223 - Iniciar servicio de Entidad de certificación

141. Si la configuración es correcta, el servicio iniciará con normalidad.

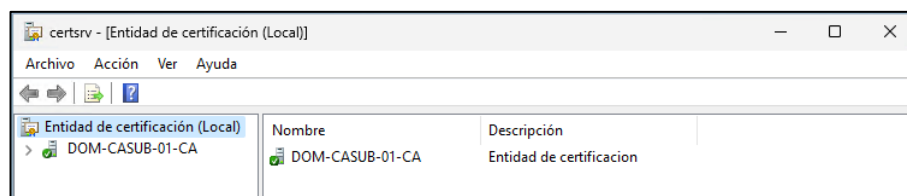


Ilustración 224 - Servicio de CA iniciado correctamente

142. A continuación, pulse con el botón derecho sobre la entidad de certificación subordinada y seleccione “Propiedades”.

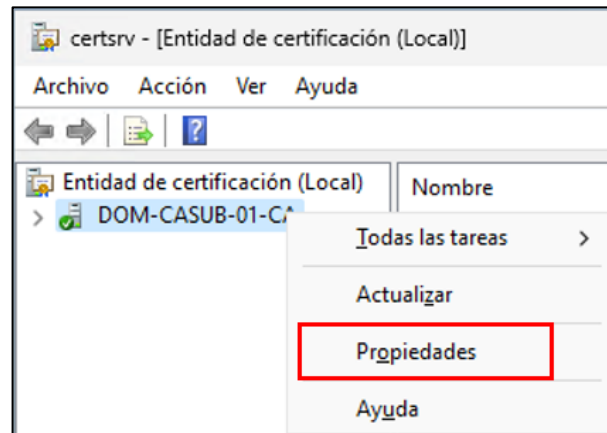


Ilustración 225 - Propiedades de CA

143. Diríjase a la pestaña “Extensiones” y, manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, revise la publicación de CRLs mediante la ruta local seleccionando “C:\Windows\System32\CertSrv\CertEnroll\<nombre de CA>< sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.

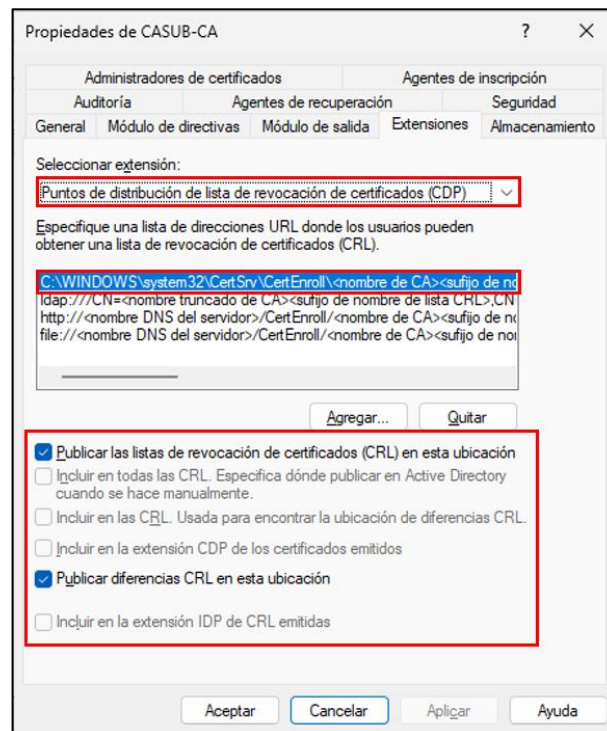


Ilustración 226 - Configuración de extensiones

144. A continuación, deshabilite la publicación de CRLs mediante LDAP seleccionando “ldap://CN=<nombre truncado de CA>< sufijo de nombre de lista CRL>,CN=nombre corto del servidor>,CN=CDP,CN=Public Key Services,<contenedor de configuración><clase de objeto CDP>” y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.

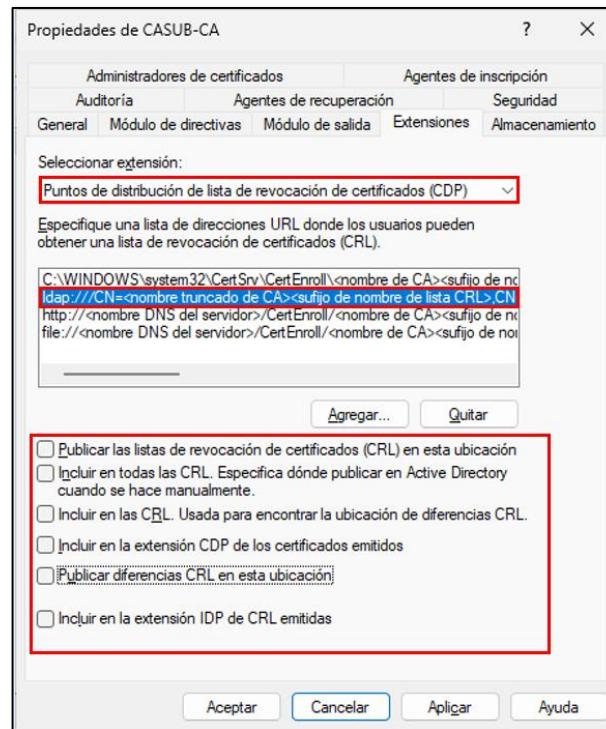


Ilustración 227 - Configuración de extensión LDAP

145. Seleccione “file://<nombre DNS del servidor>/CertEnroll/<nombre de CA>/sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y confirme que todas las opciones se encuentran como muestra la siguiente figura.

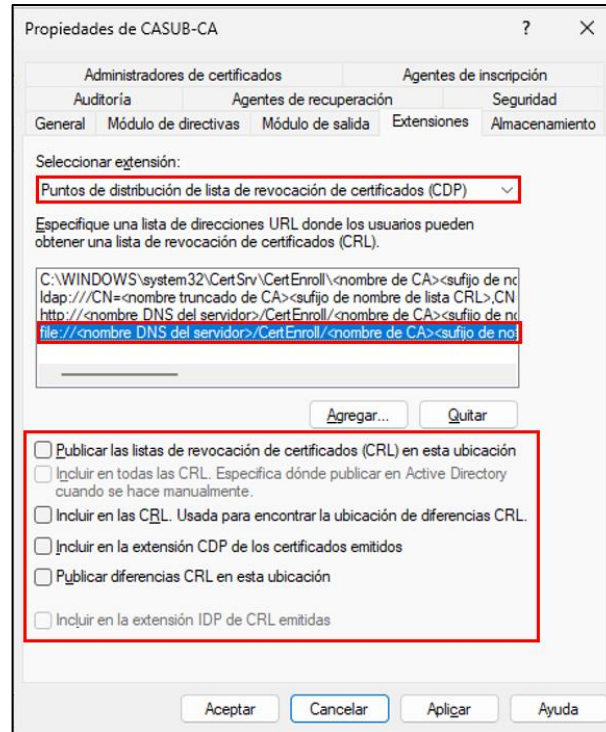


Ilustración 228 - Configuración de extensión file

146. De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y pulse “Control + C”, para copiar el objeto.

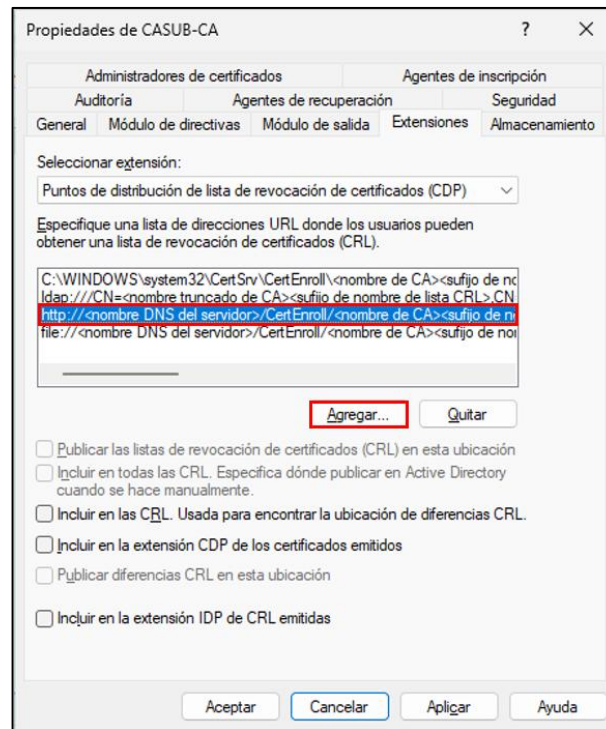


Ilustración 229 - Agregar nueva extensión http

A continuación, pulse en “Agregar”.

147. En el campo “Ubicación”, pegue la ruta copiada en el paso anterior.

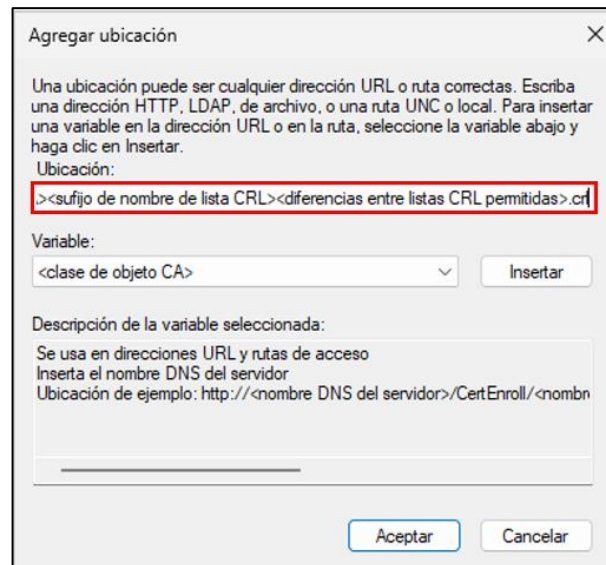


Ilustración 230 - Agregar ubicación

Nota: No pulse todavía sobre el botón “Aceptar”.

148. Sustituya “<Nombre del servidor>” por el CNAME correspondiente a la entidad subordinada de certificación.

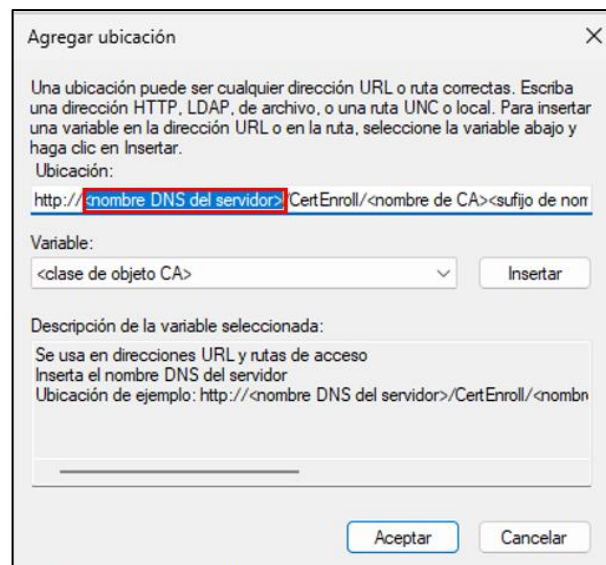


Ilustración 231 - Sustitución de nombre DNS

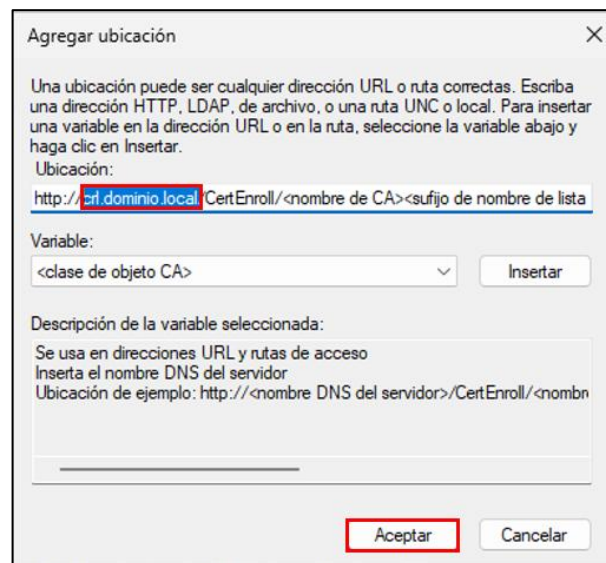


Ilustración 232 - Sustitución de nombre DNS

A continuación, pulse en “Aceptar”.

149. Marque las opciones como muestra la siguiente ilustración.

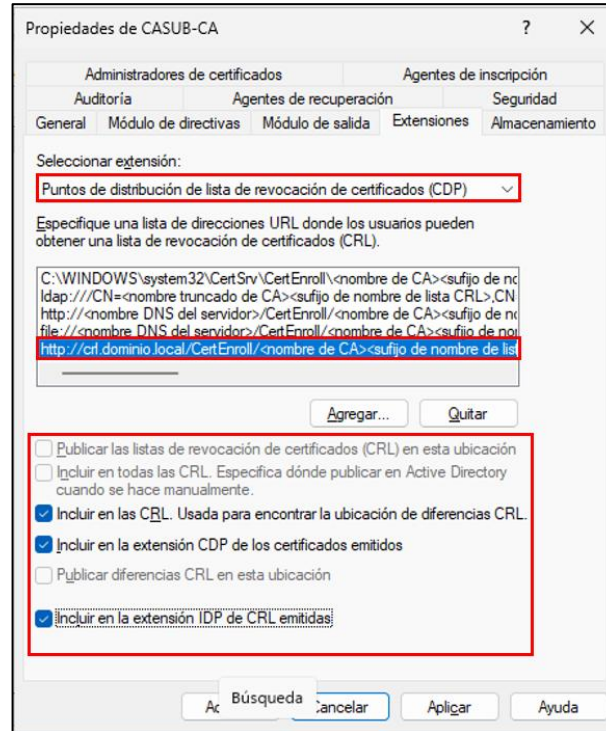


Ilustración 233 - Configuración de nueva extensión

150. A continuación, seleccione la extensión “Acceso a la información de entidad (AIA)” en el desplegable.

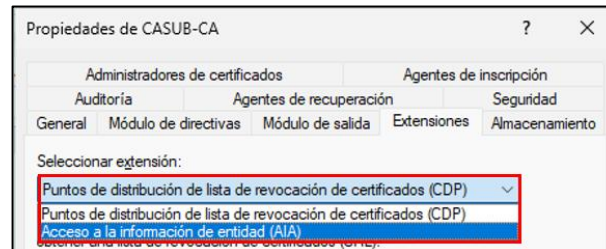


Ilustración 234 - Selección de Acceso a la información de entidad (AIA)

151. Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\

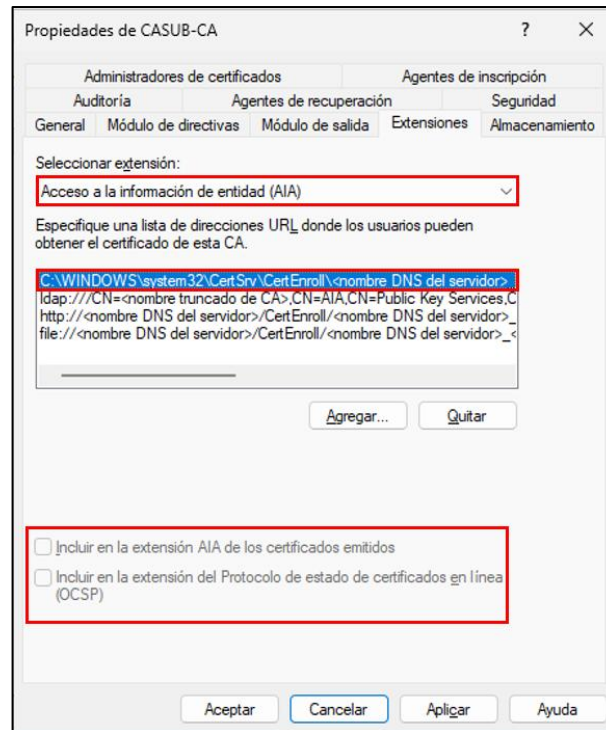


Ilustración 235 - Confirmación de configuración

152. A su vez, desmarque en el objeto “ldap://CN=<nombre truncado de CA>,CN=AIA,CN=Public Key Services,CN=Services,<contenedor de configuración><clase de objeto CA>” todas las casillas.

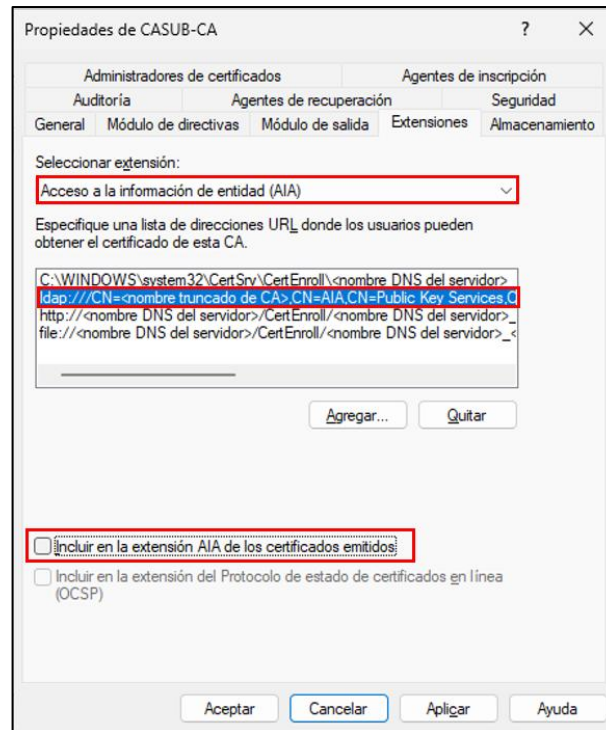


Ilustración 236 - Configuración de extensión LDAP

153. Seleccione ahora “file://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y compruebe que todas las casillas se encuentran desmarcadas.

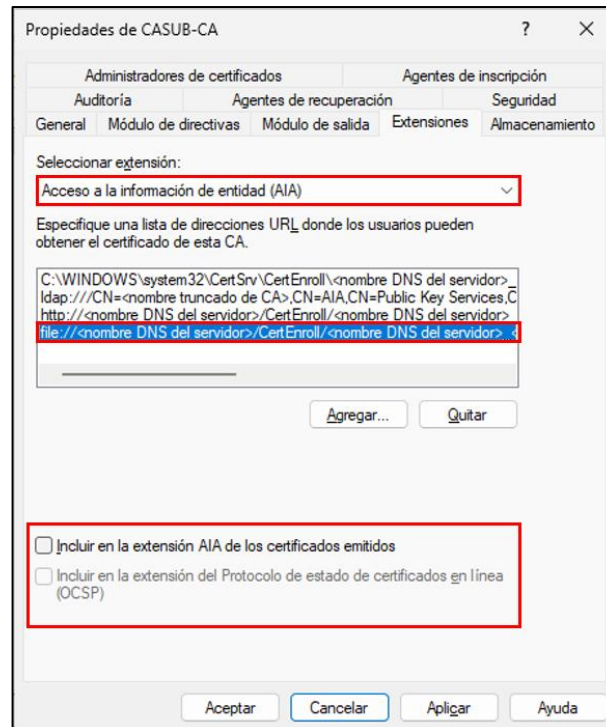


Ilustración 237 - Configuración de extensión file

154. Seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y copie el elemento mediante la combinación de teclas “Control + C”.

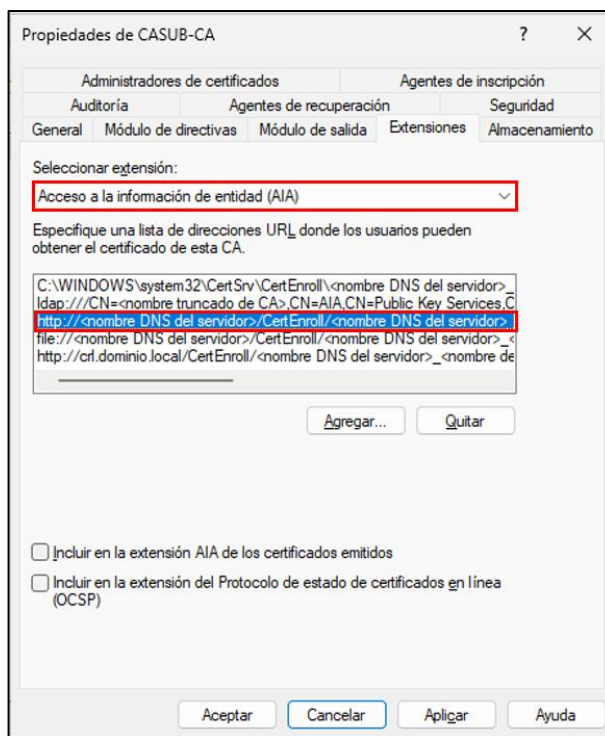


Ilustración 238 - Copiar entrada http

A continuación, pulse en “Agregar”.

155. Pegue en el campo de ubicación la ruta anterior.

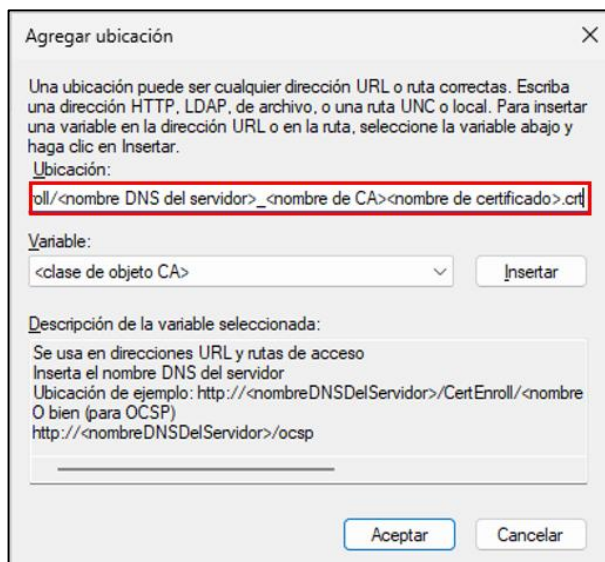


Ilustración 239 - Pegar entrada http

156. Sustituya “<nombre DNS del servidor>” por el CNAME generado al inicio de este procedimiento.

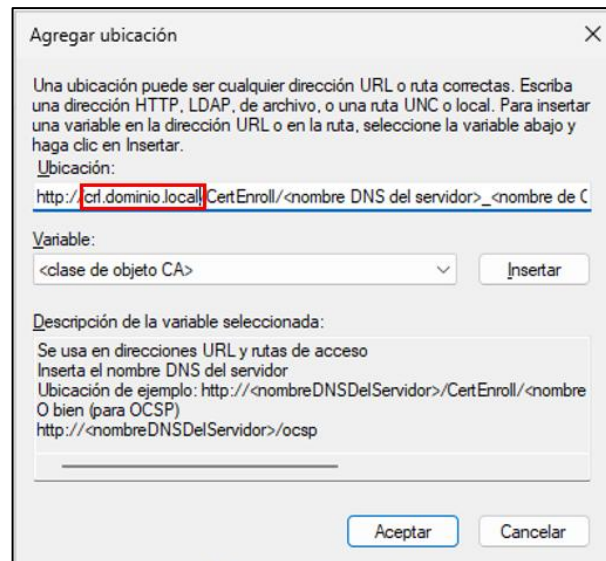


Ilustración 240 - Sustituir valor de crl

157. A continuación, marque la opción “Incluir en la extensión AIA de los certificados emitidos”.

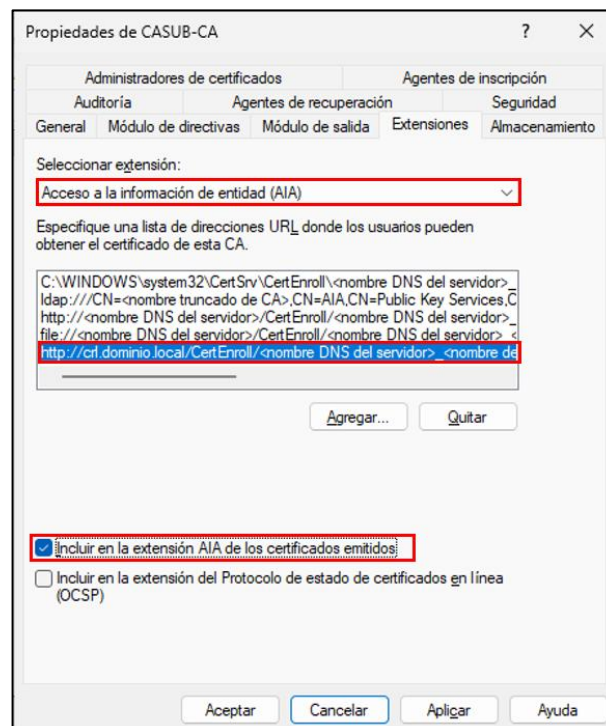
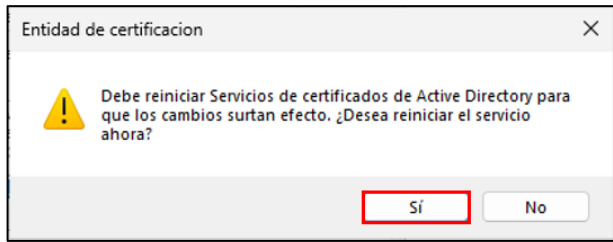
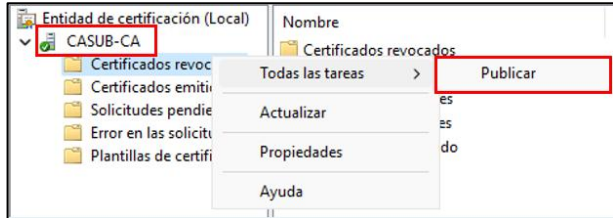
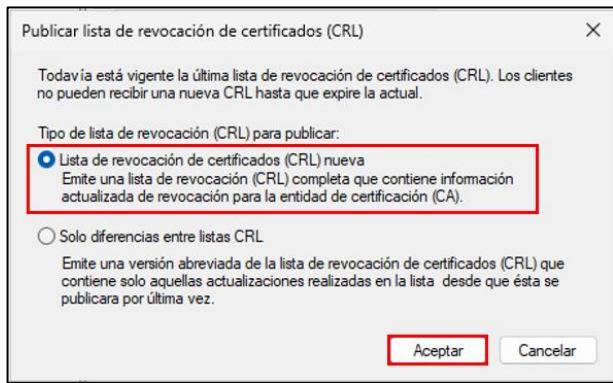


Ilustración 241 - Configuración de nueva extensión

158.	Haga clic sobre “Aplicar” y “Aceptar”. A continuación, el servicio solicitará reiniciarse.  <i>Ilustración 242 - Reiniciar servicios</i> Pulse en “Sí” para finalizar con esta configuración.
159.	Por último, publique de nuevo la lista de revocación haciendo clic derecho sobre Certificados Revocados, y a continuación, pulse en “Todas las tareas > Publicar”.  <i>Ilustración 243 - Publicación de nueva CRL</i>
160.	En el asistente, mantenga la “Lista de revocación de certificados (CRL) nueva” y pulse en Aceptar.  <i>Ilustración 244 - Publicar nueva lista de revocación de certificados</i>
161.	La nueva entidad de certificación subordinada estará disponible para configurar nuevas plantillas y emitir certificados incluyendo toda la cadena de certificación.
162.	Por último, se deberá desvincular o deshabilitar la GPO “CCN-STIC-598A25 Incremental shell remoto”. Para ello, inicie sesión en un controlador de dominio con un usuario perteneciente al grupo “Admins. del dominio”.

163. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

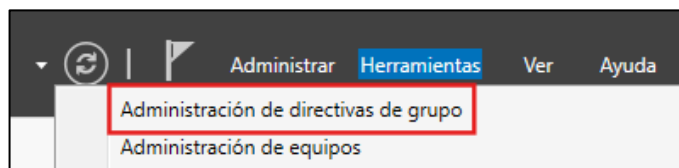


Ilustración 245 - Administración de directivas de grupo

164. Diríjase a la OU “Servidores Entidad de Certificación”, haga clic derecho sobre la GPO “CCN-STIC-598A25 Incremental shell remoto” y haga clic sobre “Vínculo habilitado” para deshabilitar el vínculo”.

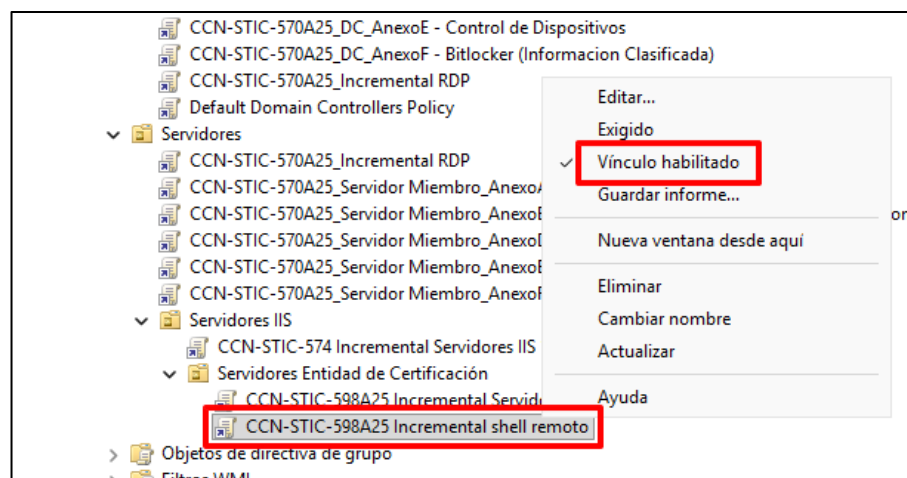


Ilustración 246 - Desvinculación de GPO incremental shell remoto

165. Habrá finalizado la configuración.

Nota: En este momento, podrá apagar la entidad de certificación raíz, ya que su única función legítima es firmar certificados para entidades de certificación subordinadas. De este modo, reducirá la superficie de exposición y evitará que la jerarquía PKI pueda verse comprometida. Desde este momento, todas las plantillas de certificados generadas en la entidad de certificación subordinada permitirán la generación de nuevos certificados de dominio.

6.2.6. PASO A PASO DE FUNCIONAMIENTO

Paso	Descripción
166.	Inicie sesión en un equipo miembro del dominio donde se va a solicitar un certificado.

167.a Sobre la barra de búsqueda, escriba “certlm.msc”.

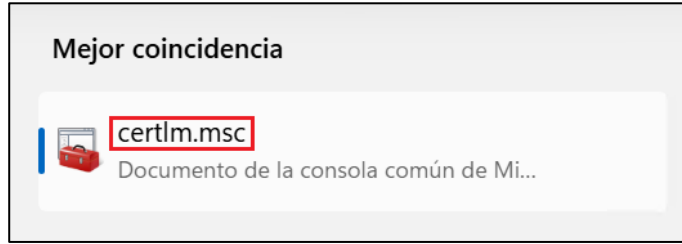


Ilustración 247 – Ejecución de consola de certificados

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

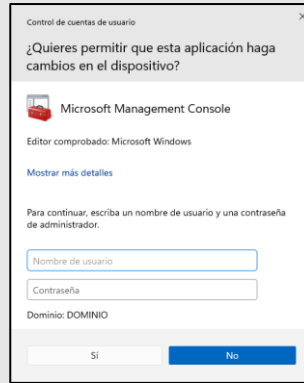


Ilustración 248 - Introducir credenciales de administrador

168. Diríjase a “Certificados – Equipo local > Personal” y posteriormente, pulse en “Buscar certificados... > Solicitar un nuevo certificado”.

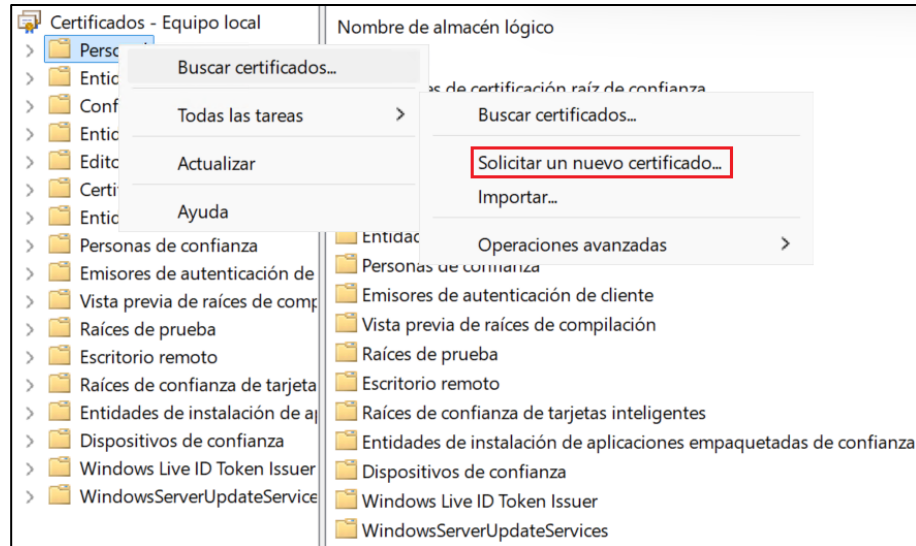


Ilustración 249 – Solicitar un nuevo certificado

169. En la primera ventana, pulse en “Siguiente”.

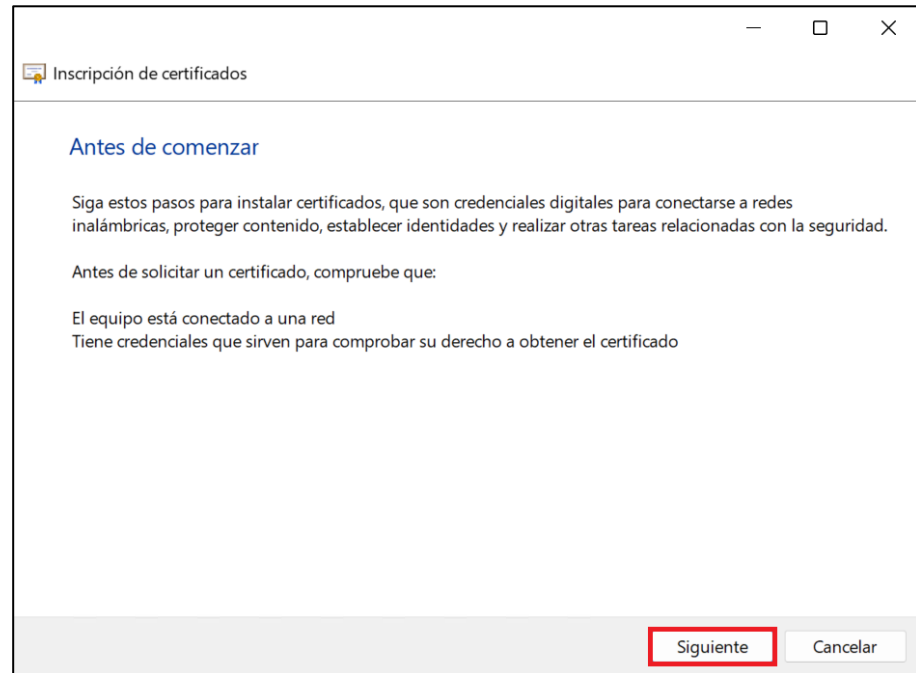


Ilustración 250 – Ventana de inscripción de certificados

170. A continuación, observe que se seleccionará automáticamente la directiva de inscripción de certificados del dominio. Pulse en “Siguiente”.

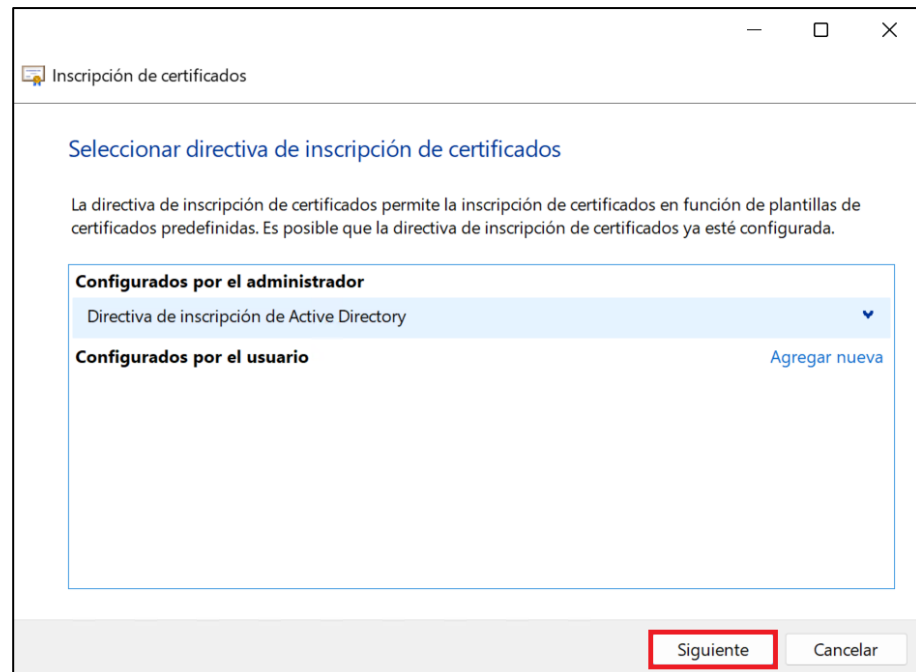


Ilustración 251 – Selección de directiva de inscripción de certificados

171. En la ventana de la imagen aparecerá las distintas plantillas de inscripción de certificados automáticos. Seleccionar una de las plantillas generadas en la entidad subordinada de certificación. En este caso, plantilla de certificados de máquina “Equipo”. Seguidamente, pulse en “Inscribir”.

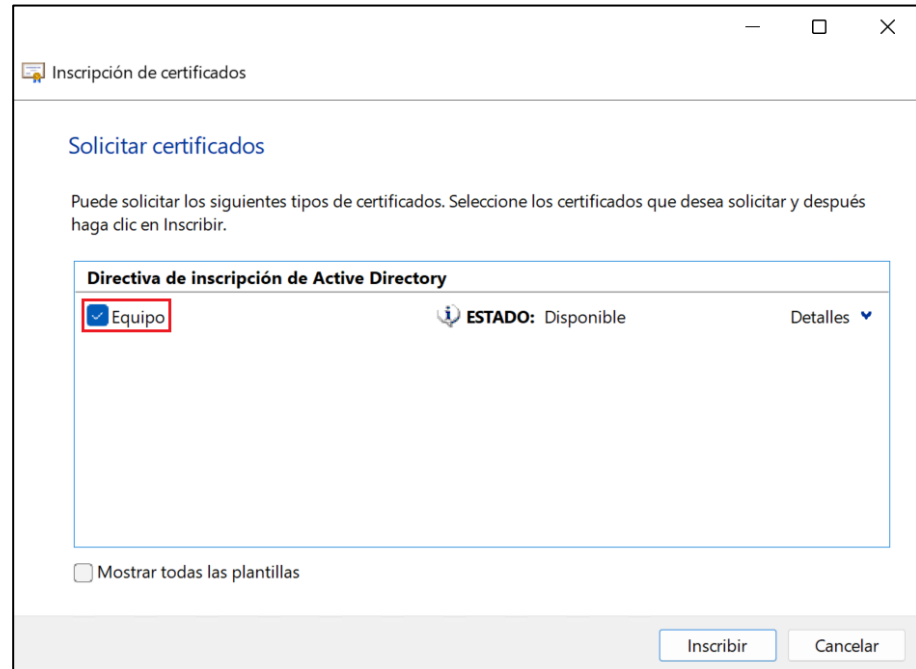


Ilustración 252 – Selección de plantilla

Nota: En caso de no aparecer plantillas disponibles, es necesario añadir el certificado de la entidad de certificación raíz en la directiva CCN-STIC-598A25 Incremental Dominio. Para ello, se ha de importar el certificado de la CA Raíz en la sección “Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de clave pública > Entidades de certificación raíz de confianza”.

172. Si todo el proceso se ha hecho correctamente, aparecerá la siguiente ventana. Finalmente, pulse en “Finalizar”.

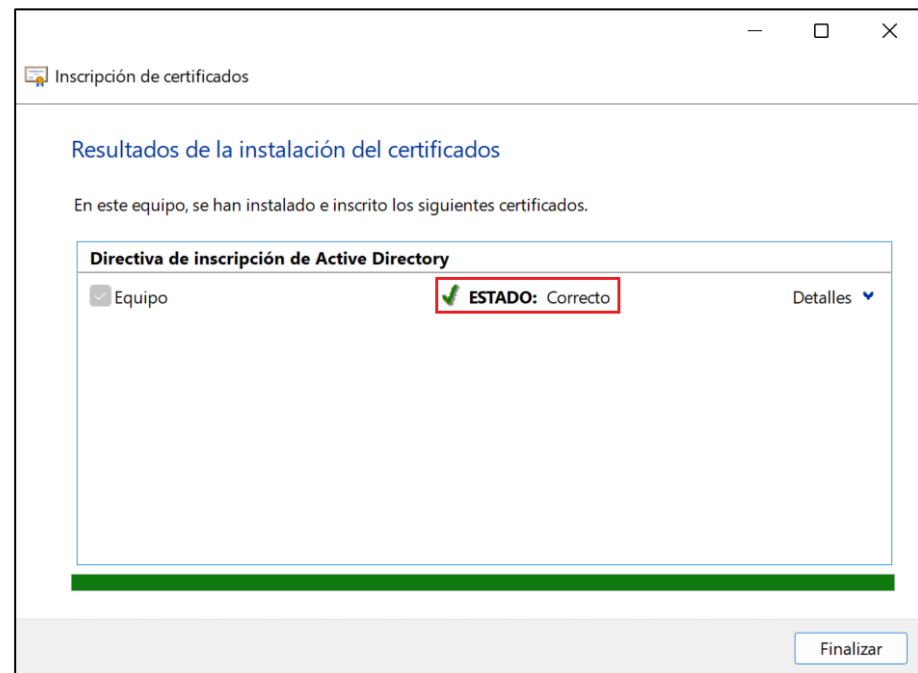


Ilustración 253 – Resultado de instalación

Nota: En caso de que su configuración corresponda a una entidad de certificación raíz y una entidad de certificación subordinada en dominio, puede continuar con la revisión del “Anexo 7. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN”

6.3. OPCIÓN C. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA CON ENTIDAD RAÍZ INDEPENDIENTE

Este apartado presenta el procedimiento de configuración de seguridad, descrito de manera ordenada y detallada, en un entorno formado por un Controlador de Dominio, un Servidor Miembro de Dominio que asumirá el rol de Entidad de Certificación Subordinada y un Servidor Aislado que asumirá el rol de Entidad de Certificación Raíz.

Antes de iniciar con el proceso de configuración, es necesario disponer de los siguientes elementos:

- a) Un servidor **controlador de dominio** Windows Server 2025 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A25.
- b) Un servidor miembro de dominio Windows Server 2025 que ejercerá como **Entidad de Certificación subordinada** siguiendo la guía de seguridad CCN-STIC-570A25. Este contendrá el servicio Web Internet Information Services instalado y preparado, y seguirá la guía CCN-STIC-574A25.
- c) Un servidor aislado Windows Server 2025 que ejercerá como **Entidad de Certificación raíz** siguiendo la guía de seguridad CCN-STIC-570B.

6.3.1. 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. Inicie la consola “Administrador del servidor” con privilegios de administración.

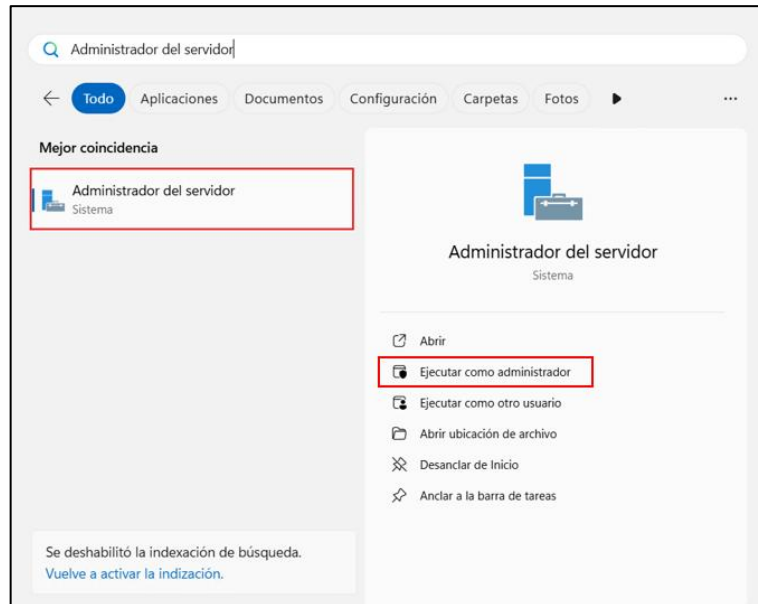


Ilustración 254 - Iniciar consola de administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

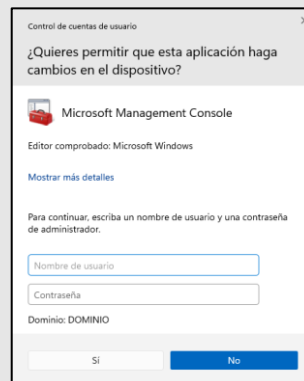


Ilustración 255 - Introducir credenciales de administrador

3. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

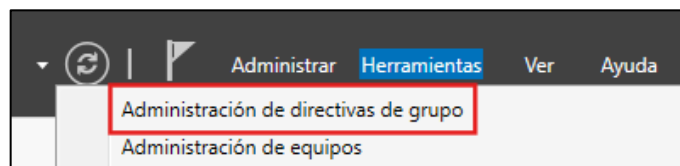


Ilustración 256 - Administración de directivas de grupo

4. Despliegue en el panel izquierdo hasta llegar a la OU “Domain Controllers”.

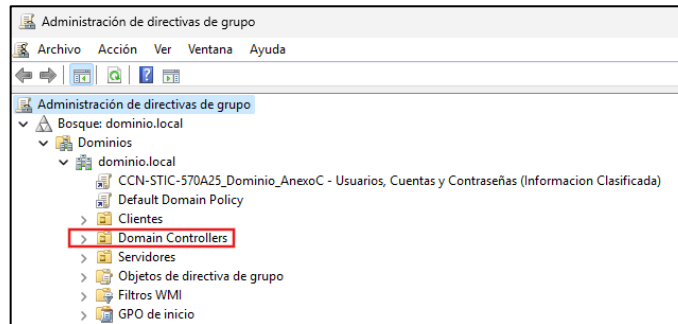


Ilustración 257 – Unidad Organizativa de Domain Controllers

5. Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

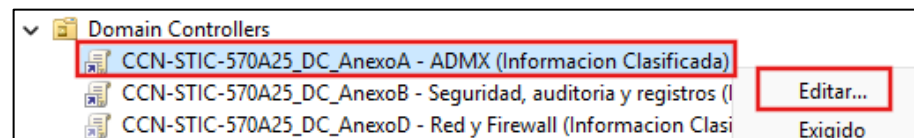


Ilustración 258 – Directiva CCN-STIC-570A25

6. 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.

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 259 – Directivas de PowerShell

7. Haga doble clic sobre la política “Activar la ejecución de scripts”.

8. En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”.

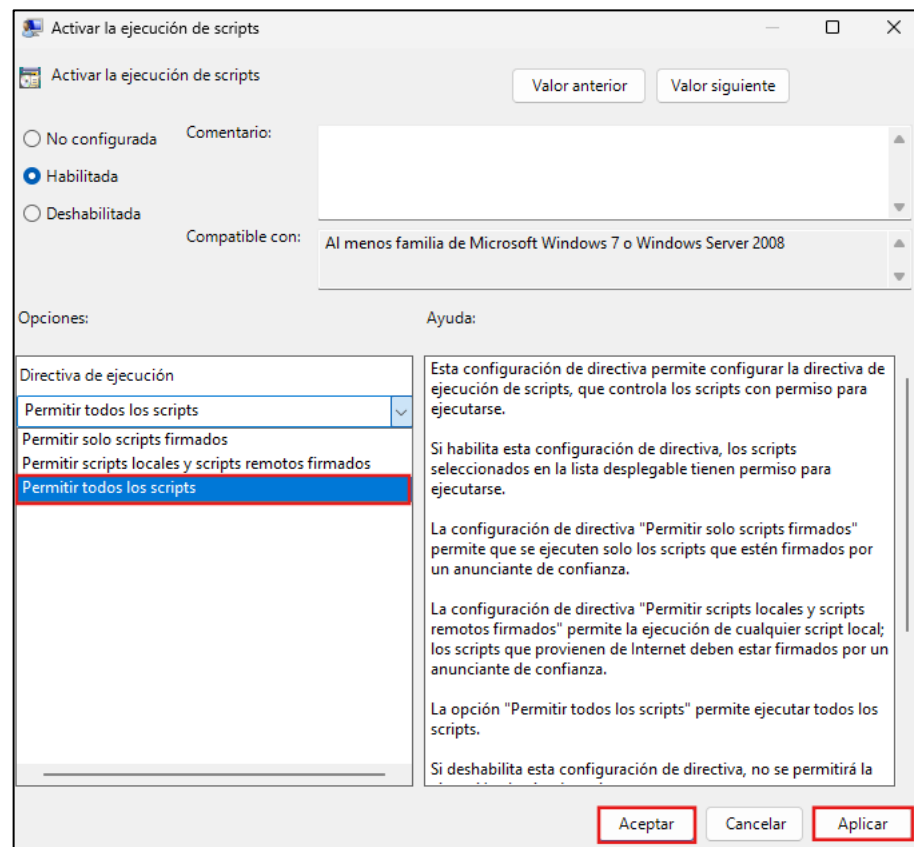


Ilustración 260 – Permitir todos los scripts

9. Reinicie el controlador de dominio para que se aplique la configuración correctamente. De nuevo, inicie sesión en el controlador de dominio con un usuario con privilegios de administración.

10. Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta.

Verifique que en su interior se encuentran los siguientes archivos:

- Directorio: CA INCREMENTAL DOMINIO
- Directorio: CA SERVIDORES
- Directorio: CA SERVIDORES – SHELL REMOTO
- Directorio: IIS
- Fichero: CCN-STIC-598A25_IncrementalServidorCA.ps1

	CA INCREMENTAL DOMINIO	24/07/2026 13:40	Carpeta de archivos
	CA SERVIDORES	24/07/2026 13:48	Carpeta de archivos
	CA SERVIDORES - SHELL REMOTO	24/07/2026 14:15	Carpeta de archivos
	IIS	24/07/2026 13:40	Carpeta de archivos
	CCN-STIC-598A25_EntidadCertificacion	24/07/2026 14:05	Script de Window...

Ilustración 261 - Copia de ficheros necesarios

11. Sobre la barra de búsqueda, escriba “PowerShell”:

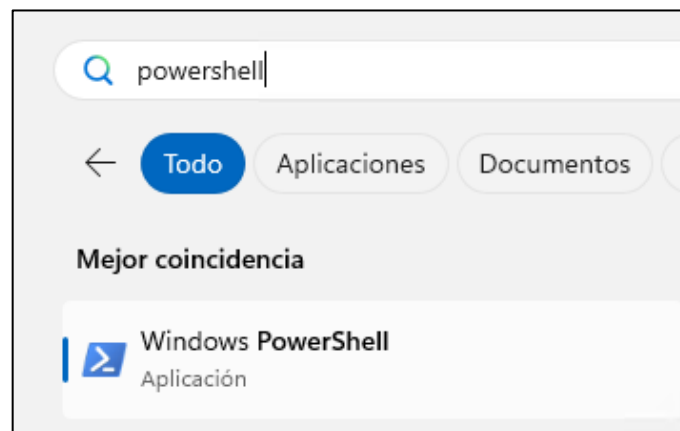


Ilustración 262 - Windows PowerShell

12. Haga clic derecho, y seleccione “Ejecutar como administrador”:

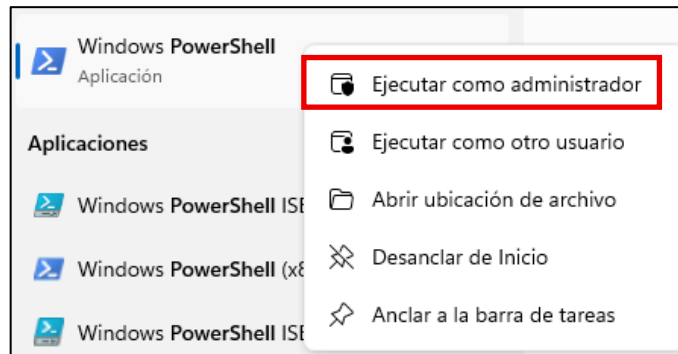


Ilustración 263 - Ejecución como administrador

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. Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

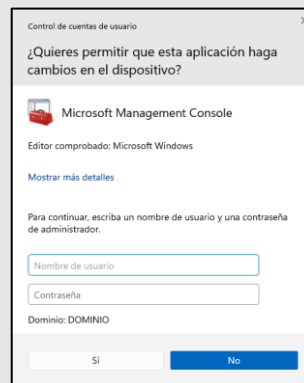


Ilustración 264 - Introducir credenciales de administrador

13. 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”.

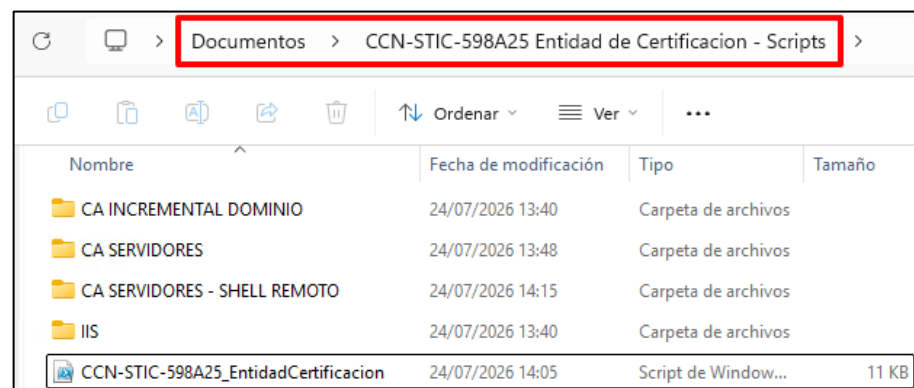
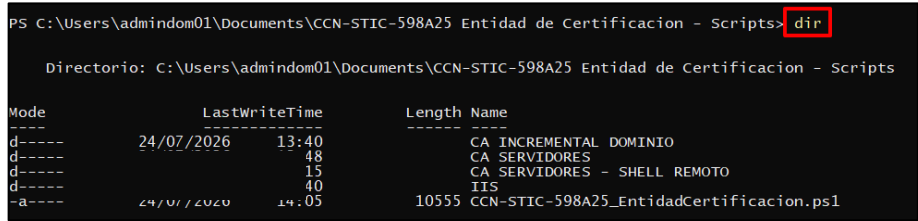
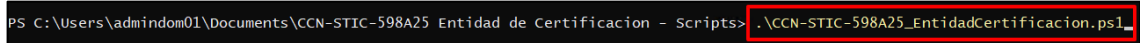
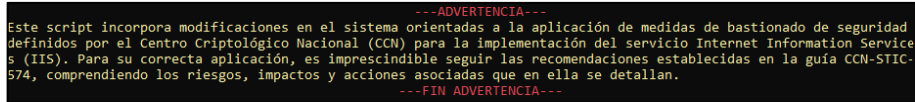
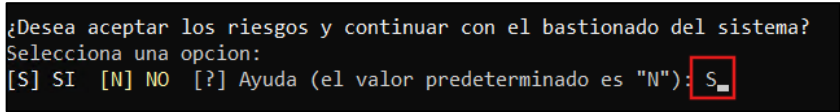


Ilustración 265 - Copia de ruta

14.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  <i>Ilustración 266 - Acceso a la ruta</i>
15.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  <i>Ilustración 267 - Contenido de la carpeta</i>
16.	Ejecute el archivo “CCN-STIC-598A25_EntidadCertificacion.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  <i>Ilustración 268 - Ejecución del script</i>
17.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  <i>Ilustración 269 - Advertencia</i>
18.	Escribir “S” y pulsar “Enter”.  <i>Ilustración 270 - Aceptación de advertencia</i>

19. En primer lugar, el script verificará que si se encuentra aplicada la GPO de IIS a la Unidad Organizativa de “Servidores IIS”. Como el Controlador de Dominio sólo tiene aplicada la guía 570A25, escriba “S” y pulse “Enter”.

```
Comprobando Unidad Organizativa: OU=Servidores,DC=dominio,DC=local
La Unidad Organizativa 'Servidores' ya existe.

Comprobando Unidad Organizativa: OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local
Creando Unidad Organizativa 'Servidores IIS' en 'OU=Servidores,DC=dominio,DC=local'...
Unidad Organizativa 'Servidores IIS' creada.

Comprobando Unidad Organizativa: OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local
Creando Unidad Organizativa 'Servidores Entidad de Certificación' en 'OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local'...
Unidad Organizativa 'Servidores Entidad de Certificación' creada.

Jerarquía de OUs preparada correctamente:
- OU=Servidores,DC=dominio,DC=local
- OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local
- OU=Servidores Entidad de Certificación,OU=Servidores IIS,OU=Servidores,DC=dominio,DC=local

Comprobando si existe la GPO 'CCN-STIC-574 Incremental Servidores IIS'...
ADVERTENCIA: No se ha encontrado la GPO 'CCN-STIC-574 Incremental Servidores IIS'.

Se procederá a importar y vincular la GPO 'CCN-STIC-574 Incremental Servidores IIS'. ¿Desea continuar?

Confirmacion
Seleccione una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S
```

Ilustración 271 – Verificación UO IIS

Nota: Si se ha implementado previamente la guía CCN-STIC-574A25 para IIS, el presente paso se omitirá.

20. A continuación, se importará la GPO Incremental en dominio. Escriba “S” y pulse “Enter”.

```
IIS / 574 aplicado correctamente.

Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental Dominio'. ¿Desea continuar?

Confirmacion
Seleccione una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S
```

Ilustración 272 - Implementación Incremental Dominio

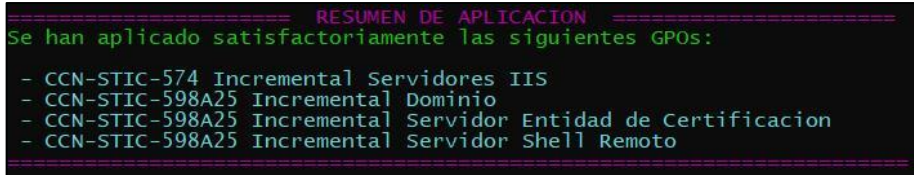
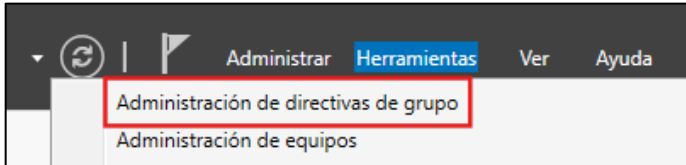
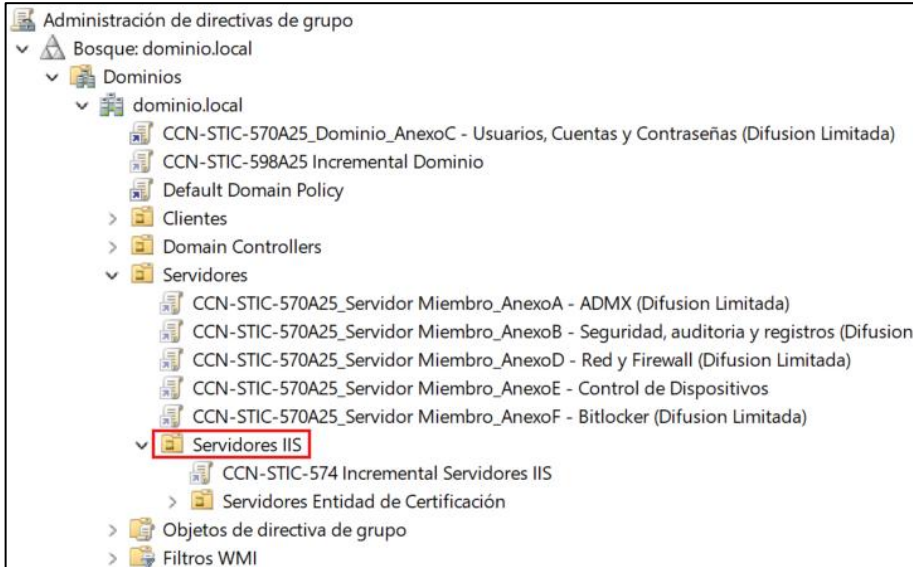
21. Finalmente, se importará la GPO Incremental de Servidores Entidad de Certificación a la Unidad Organizativa correspondiente. Escriba “S” y pulse “Enter”.

```
CA INCREMENTAL DOMINIO aplicado correctamente.

Se procederá a importar y vincular la GPO 'CCN-STIC-598A25 Incremental Servidor Entidad de Certificación'. ¿Desea continuar?

Confirmacion
Seleccione una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S
```

Ilustración 273 - Implementación Incremental Servidores CA

22.	Espera a que finalice la ejecución; al terminar, se mostrará un mensaje indicando las GPO que se han vinculado correctamente a las Unidades Organizativas correspondientes. Cierre el terminal de Powershell.  <i>Ilustración 274 - GPOs aplicadas correctamente</i>
23.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  <i>Ilustración 275 - Administración de directivas de grupo</i>
24.	Despliegue la lista del menú izquierdo hasta localizar el dominio y, a continuación, acceda a la Unidad Organizativa de “Servidores IIS”.  <i>Ilustración 276 - OU Servidores IIS</i>

25. Despliegue la OU y haga clic derecho sobre el GPO “CCN-STIC-574 Incremental Servidores IIS 10”. Seleccione la opción “Vínculo habilitado”.



Ilustración 277 - Habilitar GPO

26. Despliegue la OU de “Servidores Entidad de Certificación” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Servidores Entidad de Certificación”. Seleccione la opción “Vínculo habilitado”. Repita esta acción para la directiva “CCN-STIC-598A25 Incremental Shell remoto”.

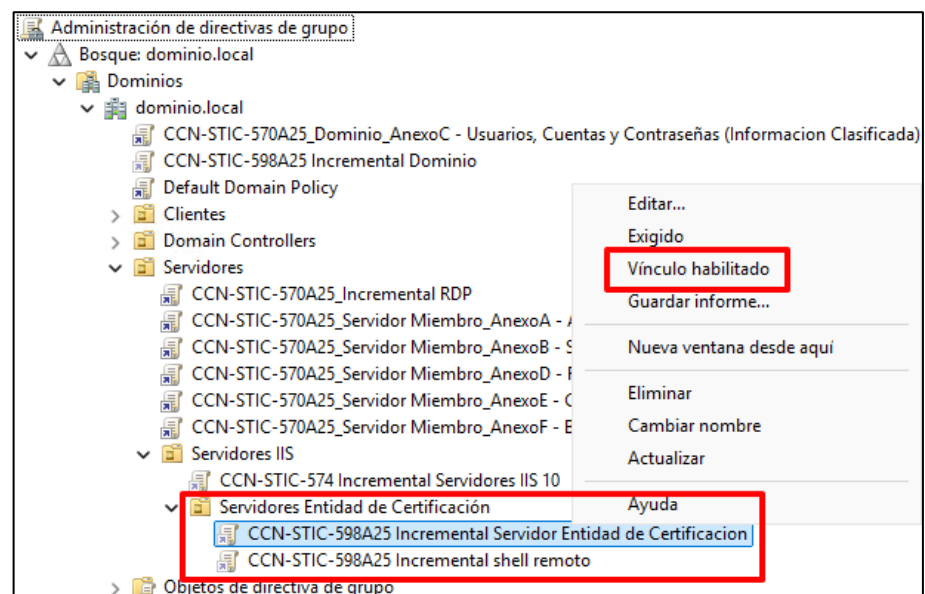


Ilustración 278 - Habilitar GPO CA

27. Diríjase a “dominio.local” y haga clic derecho sobre el GPO “CCN-STIC-598A25 Incremental Dominio”. Seleccione la opción “Vínculo habilitado”.

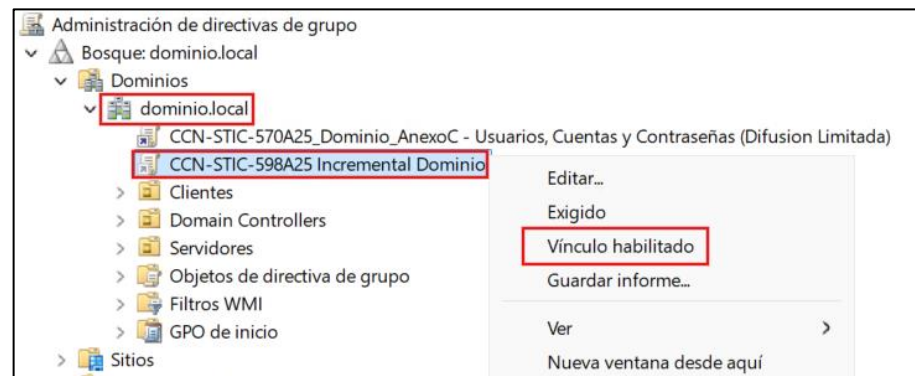


Ilustración 279 - Habilitar GPO Dominio

28. En la parte derecha del Administrador de directivas de grupo asegúrese de que la GPO “CCN-STIC-598A25 Incremental Dominio” se encuentra en primer lugar.

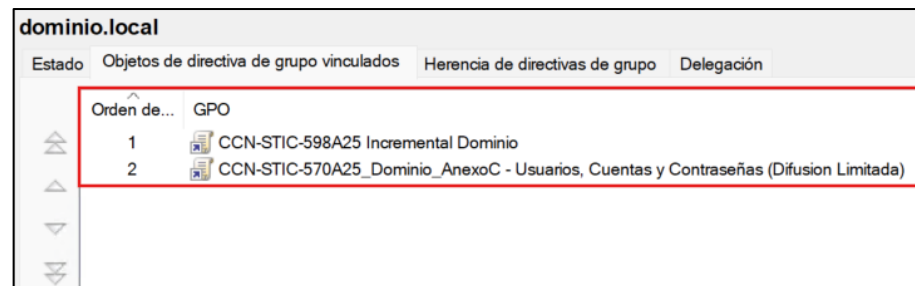


Ilustración 280 - Orden de las GPOs

29. De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior, y seleccione “Usuarios y equipos de Active Directory”.

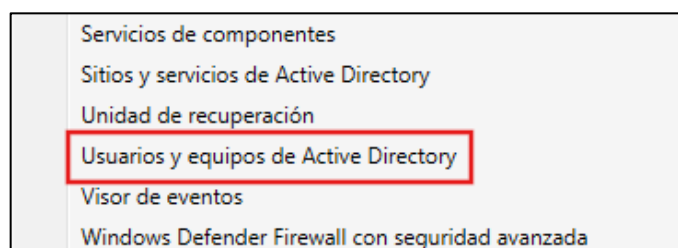


Ilustración 281 - Usuarios y equipos de Active Directory

30. Despliegue la lista del panel izquierdo hasta visualizar la OU “Servidores Entidad de Certificación”.



Ilustración 282 - OU Servidores Entidad de Certificación

31. Haga clic sobre la carpeta “Computers” y seleccione el servidor de Entidad de Certificación subordinada que se utilizará en todo el procedimiento.

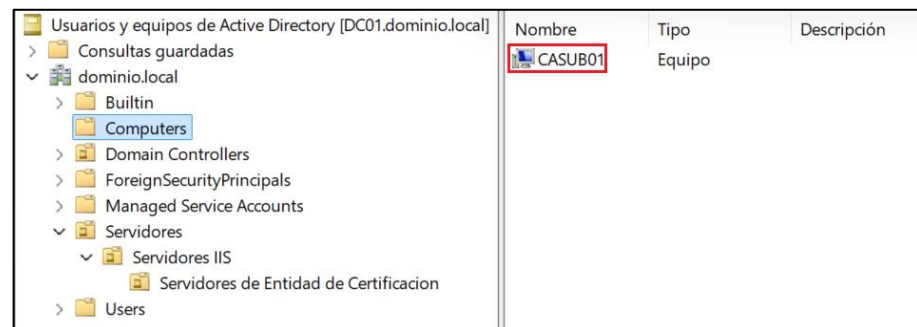


Ilustración 283 - Selección del servidor.

32. Arrástrelo a la OU “Servidores Entidad de Certificación”. Aparecerá una advertencia. Haga clic en “Sí”.

Puede cerrar la ventana de “Usuarios y equipos de Active Directory”.

33. De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

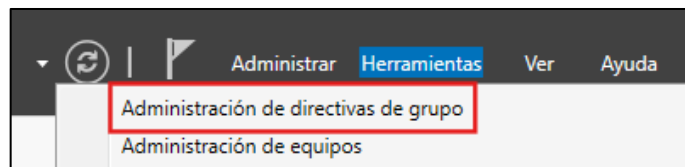


Ilustración 284 - Administración de directivas de grupo

34. Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.

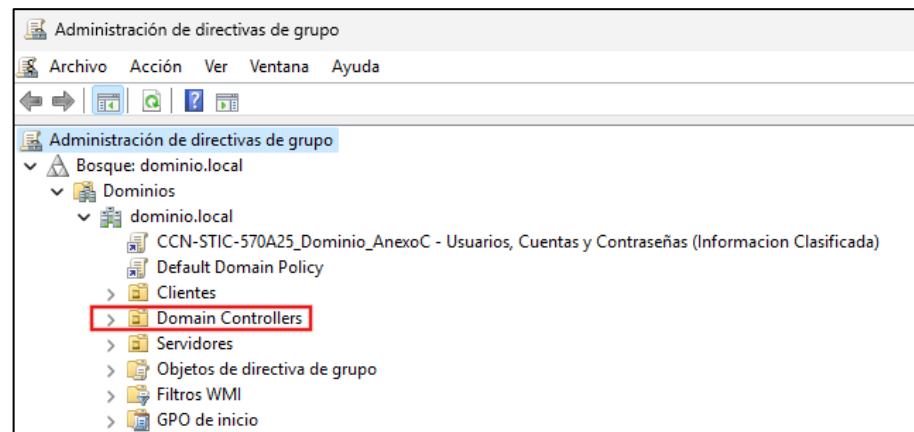


Ilustración 285 - OU Domain Controllers

35. Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

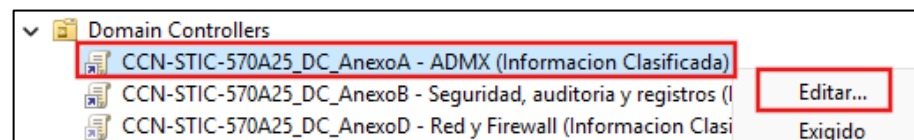


Ilustración 286 - Edición ADMX 570A25

36. 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.

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 287 - Políticas de PowerShell

37. Haga doble clic sobre la política “Activar la ejecución de scripts”.

38. En el desplegable de la política, seleccione “Permitir solo scripts firmados”, y haga clic en “Aplicar” y “Aceptar”.

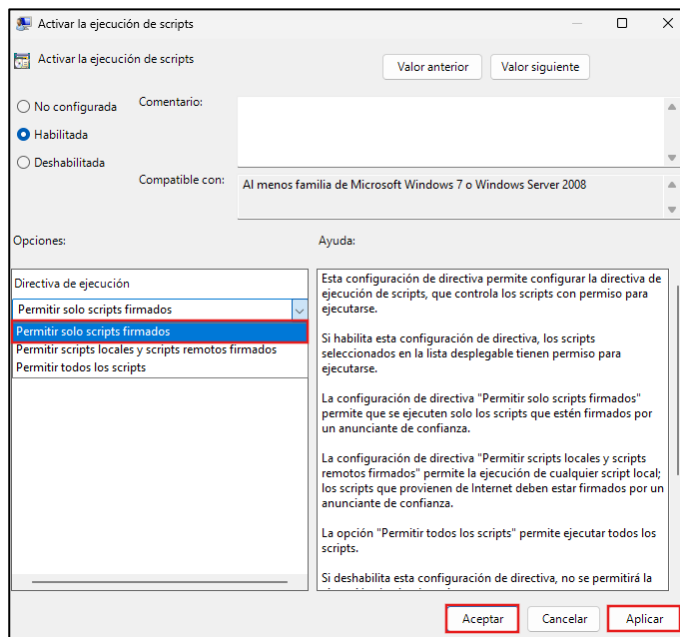


Ilustración 288 - Selección de "Permitir solo scripts firmados"

39. Reinicie el controlador de dominio para que se aplique la configuración correctamente.

6.3.2. PASO A PASO DE INSTALACIÓN Y CONFIGURACIÓN DE SEGURIDAD EN ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE

Los pasos que se describen a continuación se realizarán en el servidor Entidad de Certificación Raíz independiente al dominio.

Nota: Si su entidad de certificación raíz ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
40.	Inicie sesión en el equipo donde se va a instalar el servidor Entidad de Certificación raíz fuera de dominio.
41.	Durante la aplicación de medidas de la guía CCN-STIC-570B, algunos de los servicios y herramientas administrativas del sistema serán bloqueados. Para poder continuar con la aplicación de esta guía y configurar la entidad de certificación raíz, deberá habilitar e iniciar los siguientes servicios: - Aislamiento de claves CNG. - Administración remota de Windows (WinRM) - Servicios de certificados de Active Directory.

42. Para configurar dichos servicios, diríjase al “Administrador del servidor”. Pulse sobre “Ejecutar como administrador”.

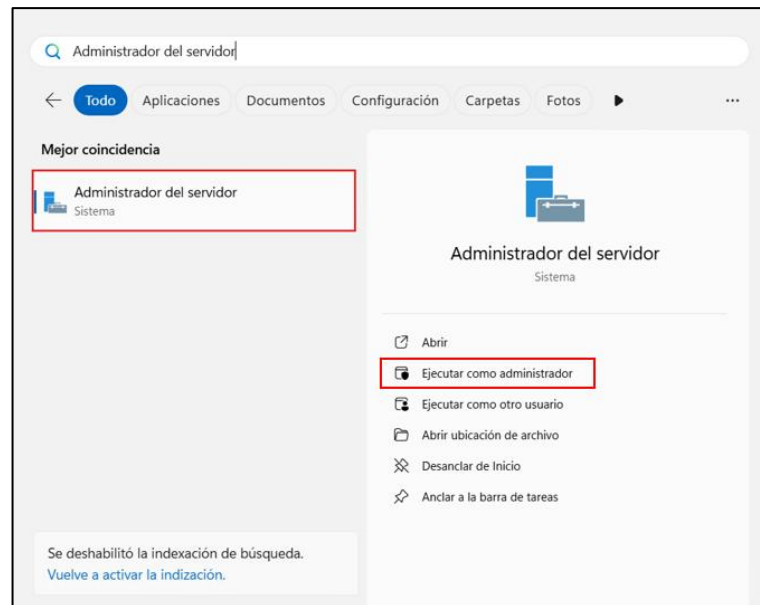


Ilustración 289 - Iniciar consola de administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

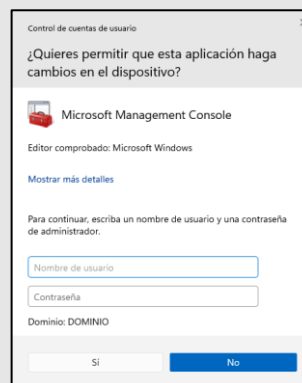


Ilustración 290 - Introducir credenciales de administrador

43. Acceda a “Herramientas > Servicios” para confirmar el estado de los servicios del sistema.

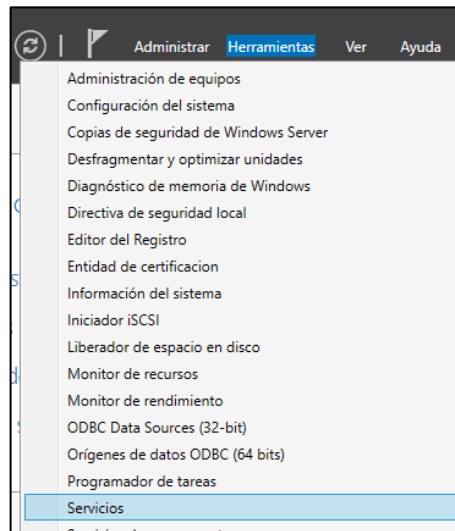


Ilustración 291 - Iniciar consola de Servicios

44. Localice cada uno de los servicios indicados en pasos anteriores, pulse con el clic derecho y seleccione “Propiedades”.

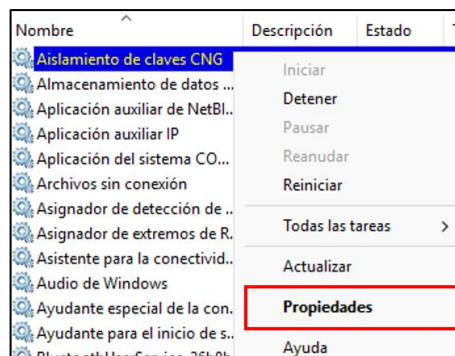


Ilustración 292 - Propiedades del servicio

45. Establezca el modo de inicio automático, y a continuación, pulse en “Iniciar”.

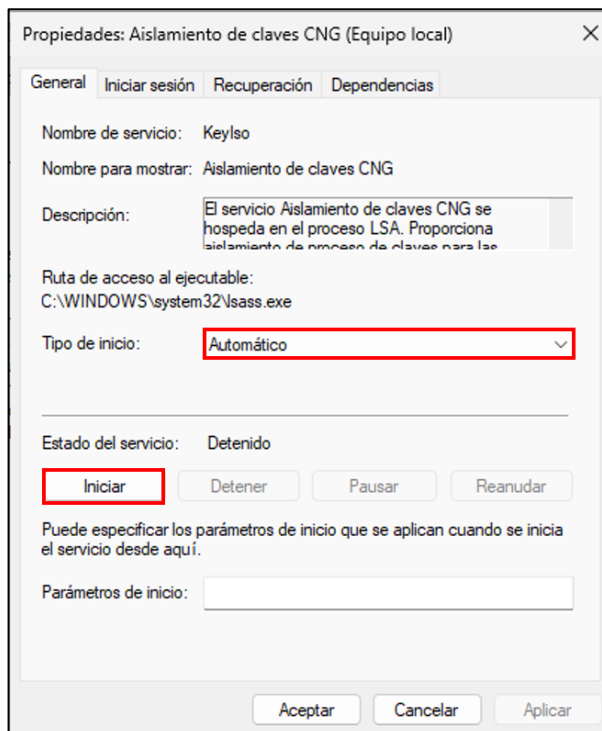


Ilustración 293 - Configuración e inicio del servicio

Nota: Repita esta configuración en los servicios indicados.

46. A su vez, las medidas de fortificación del sistema operativo impiden la utilización del “Acceso a Shell Remoto”. Para habilitarlo, deberá editar las directivas de máquina local (*gpedit.msc*) y dirigirse a “Configuración de Equipo > Plantillas administrativas > Componentes de Windows > Shell remoto de Windows”.

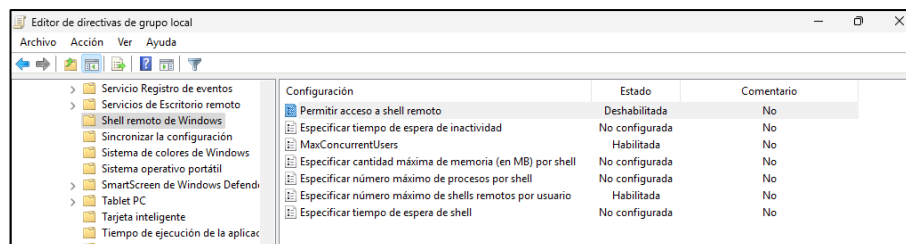


Ilustración 294 - Acceso a configuración de Shell remoto de Windows

47. Edite la directiva “Permitir acceso a shell remoto” haciendo doble clic sobre ella y configurando el modo “Habilitado”. Posteriormente, pulse en “Aplicar” y “Aceptar”.

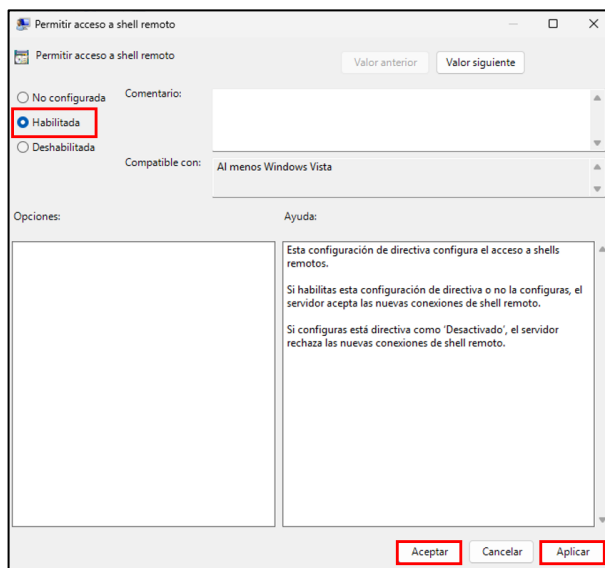


Ilustración 295 - Habilitar el acceso a Shell remoto

48. A continuación, actualice las directivas mediante la ejecución del comando “gpupdate /force” y continúe con el procedimiento.

```

Administrador: Windows PowerShell

PS C:\Users\adminlocal> gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

PS C:\Users\adminlocal>
    
```

Ilustración 296 - Ejecución de gpupdate /force

49. Para continuar con la configuración de la entidad de certificación raíz, de nuevo en la consola de “Administración del servidor”, diríjase a “Configurar Servicios de certificados de Active Directory”.



Ilustración 297 – Configurar Servicios de certificados

Nota: Si el rol de Entidad de certificación no se encuentra instalado, esta advertencia no se apreciará en el administrador del servidor. Añadir la funcionalidad desde “Administrar > Agregar roles y características”.

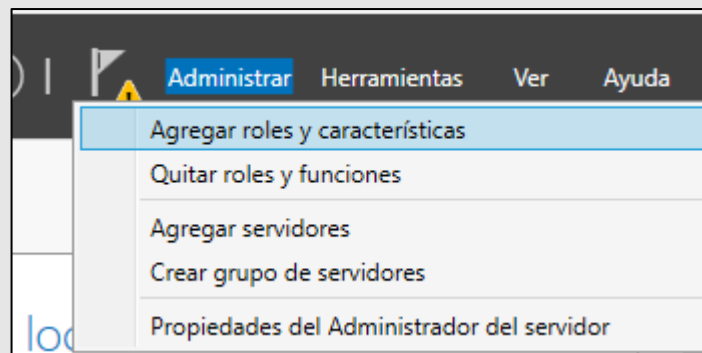


Ilustración 298 - Agregar roles y características

50. Especifique las credenciales para configurar servicios de rol. Pulse en “Siguiente”.

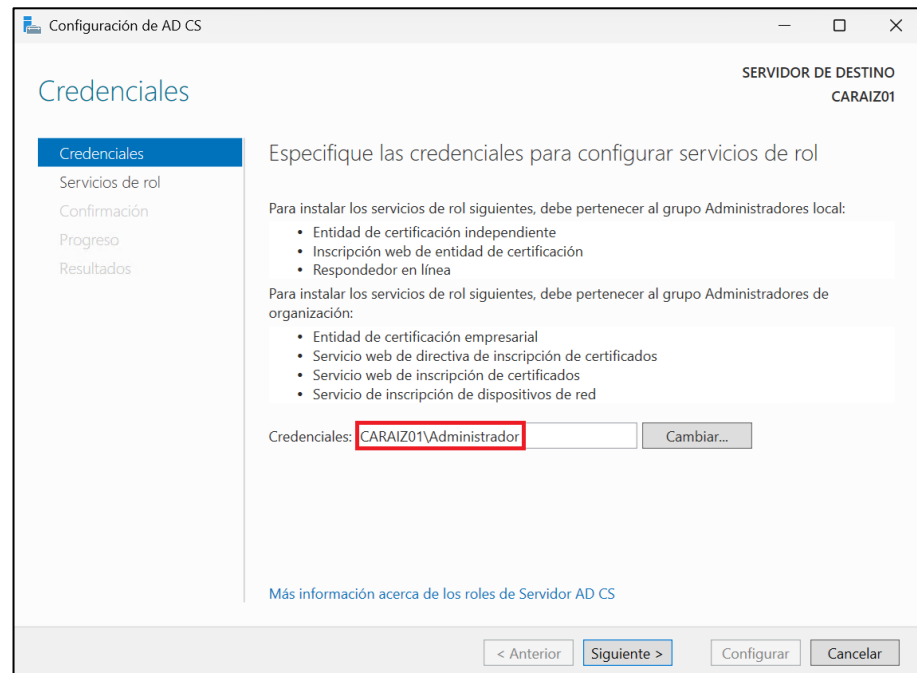


Ilustración 299 – Establecer credenciales

Nota: El usuario administrador que se utilizará en todo el escenario será **Administrador**.

51. Seleccione los servicios de rol que dispondrá el servidor de Entidad de Certificación. En el presente caso será “Entidad de certificación”. Pulse en “Siguiente”.

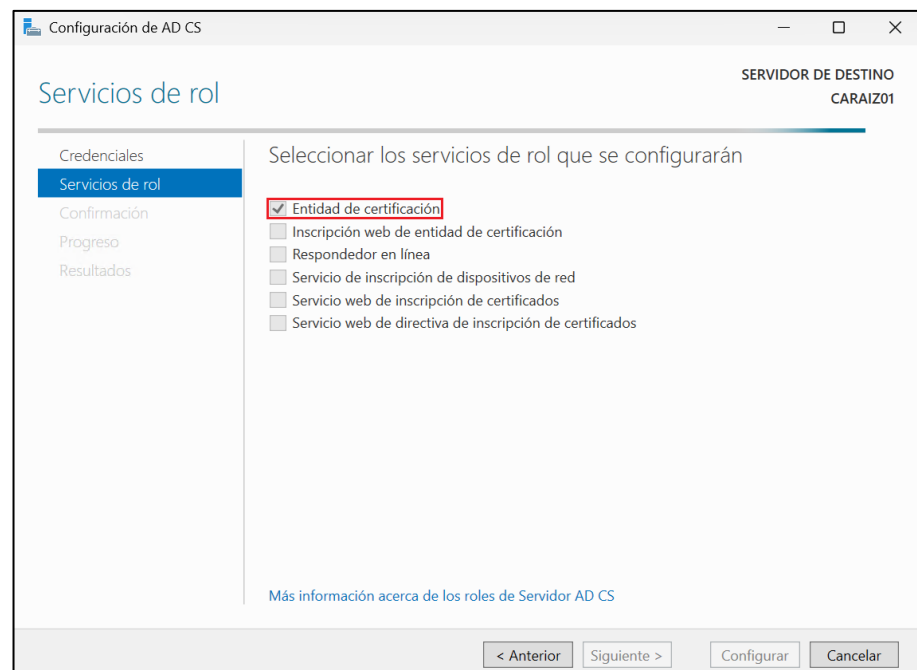


Ilustración 300 – Configurar servicio de rol

52. Especifique el tipo de instalación de la CA, seleccione “CA independiente”. Pulse en “Siguiente”.

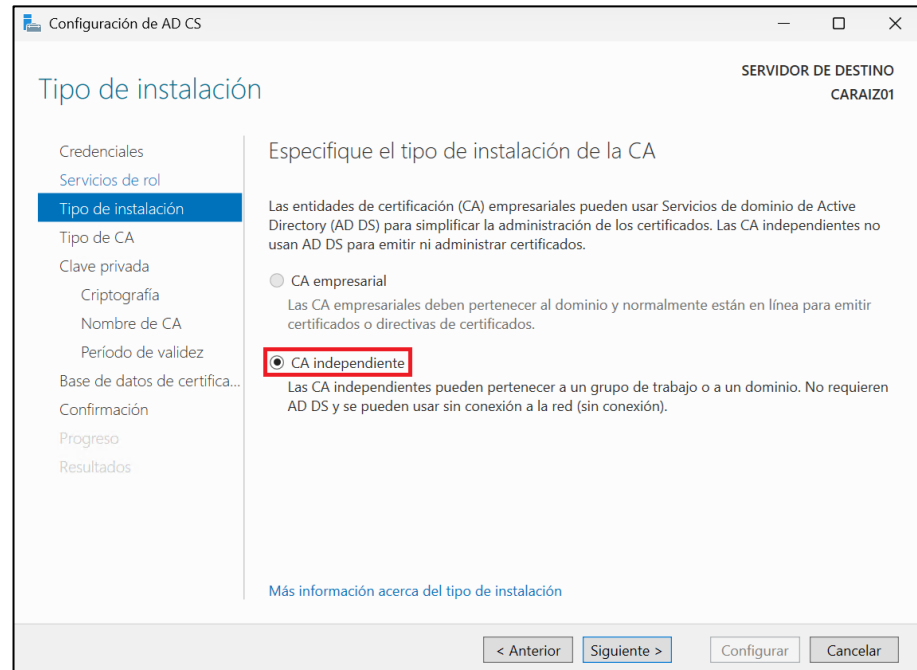


Ilustración 301 – Selección de CA independiente

53. Seleccione “CA raíz” y pulse en “Siguiente >”.

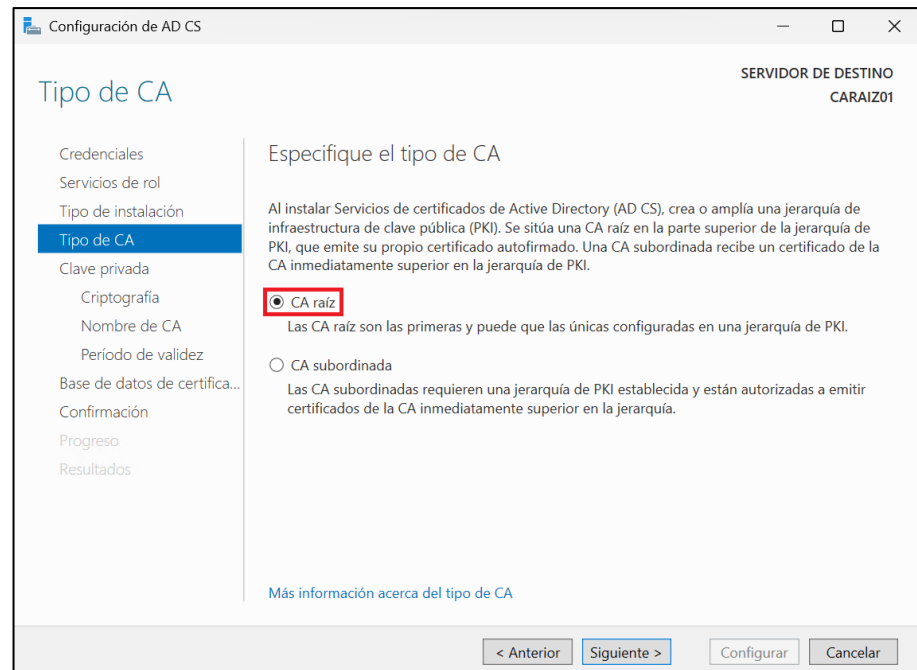


Ilustración 302 – Especificación de tipo de CA

54. Seleccione “Crear una clave privada nueva” y pulse en “Siguiente >”.

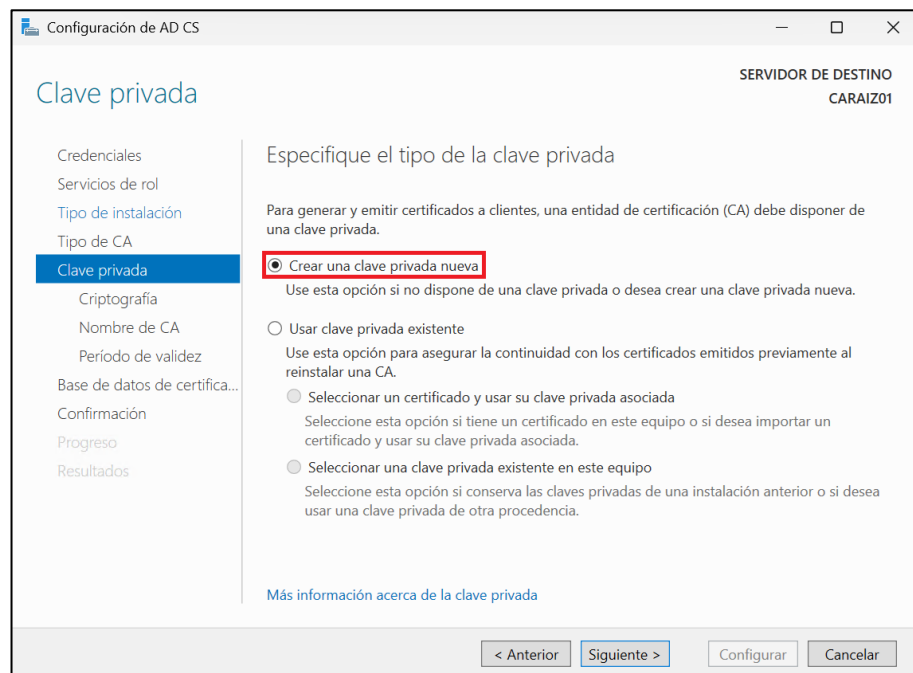


Ilustración 303 – Selección de crear clave privada

55. Las opciones criptográficas que se seleccionarán serán.

- Longitud: 2048
- Tipo de algoritmo hash: SHA256

Posteriormente, pulse en “Siguiente >”.

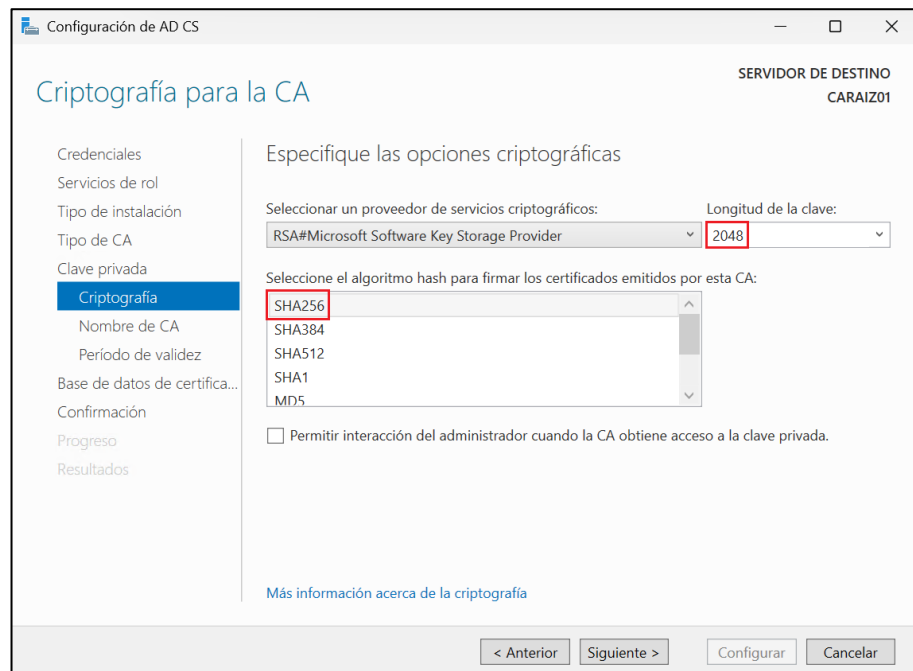
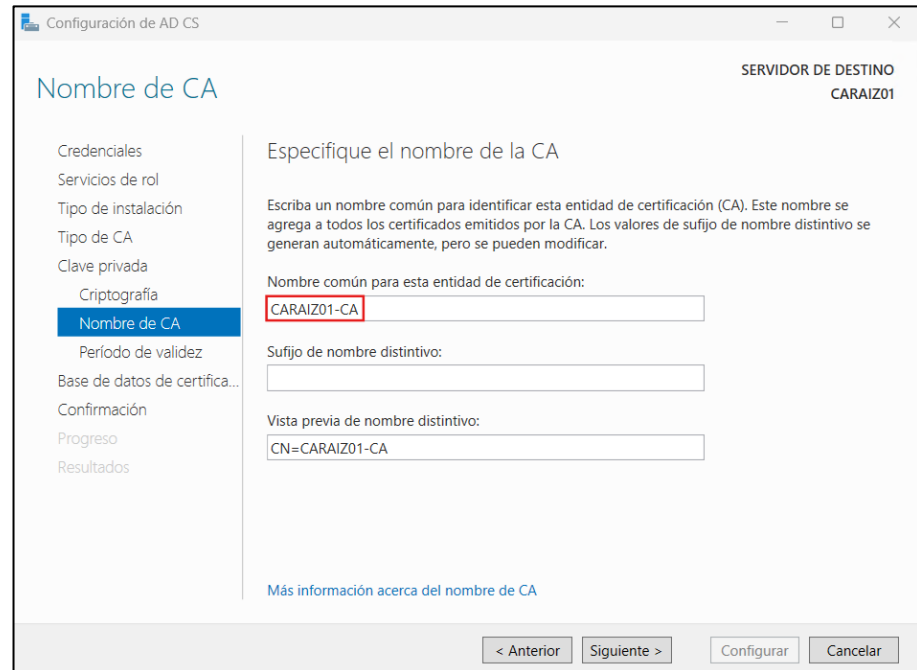


Ilustración 304 – Selección de criptografía

56. A continuación, se especificará el nombre para la entidad de certificación. En el presente caso, será “CARAIZ01-CA”. Posteriormente, pulse en “Siguiente >”.



Configuración de AD CS

SERVIDOR DE DESTINO
CARAIZ01

Nombre de CA

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Especifique el nombre de la CA

Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.

Nombre común para esta entidad de certificación:

Sufijo de nombre distintivo:

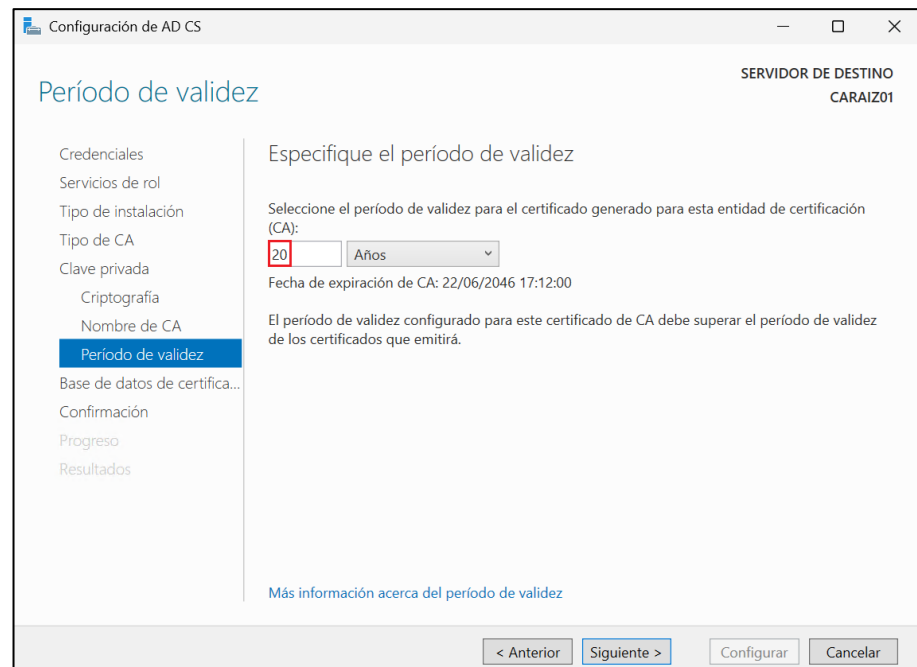
Vista previa de nombre distintivo:

[Más información acerca del nombre de CA](#)

< Anterior Siguiente > Configurar Cancelar

Ilustración 305 – Nombre de la CA

57. Especifique el período de validez para el certificado para esta entidad de certificación. Se establecerá en 20 años. Pulse en “Siguiente >”.



Configuración de AD CS

SERVIDOR DE DESTINO
CARAIZ01

Período de validez

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Especifique el período de validez

Seleccione el período de validez para el certificado generado para esta entidad de certificación (CA):
 Años

Fecha de expiración de CA: 22/06/2046 17:12:00

El período de validez configurado para este certificado de CA debe superar el período de validez de los certificados que emitirá.

[Más información acerca del período de validez](#)

< Anterior Siguiente > Configurar Cancelar

Ilustración 306 – Años de validez

58. En la siguiente página se especificará las ubicaciones donde se almacenarán los certificados. Se establecerán las carpetas por defecto. Finalmente, pulse en “Siguiente >”.

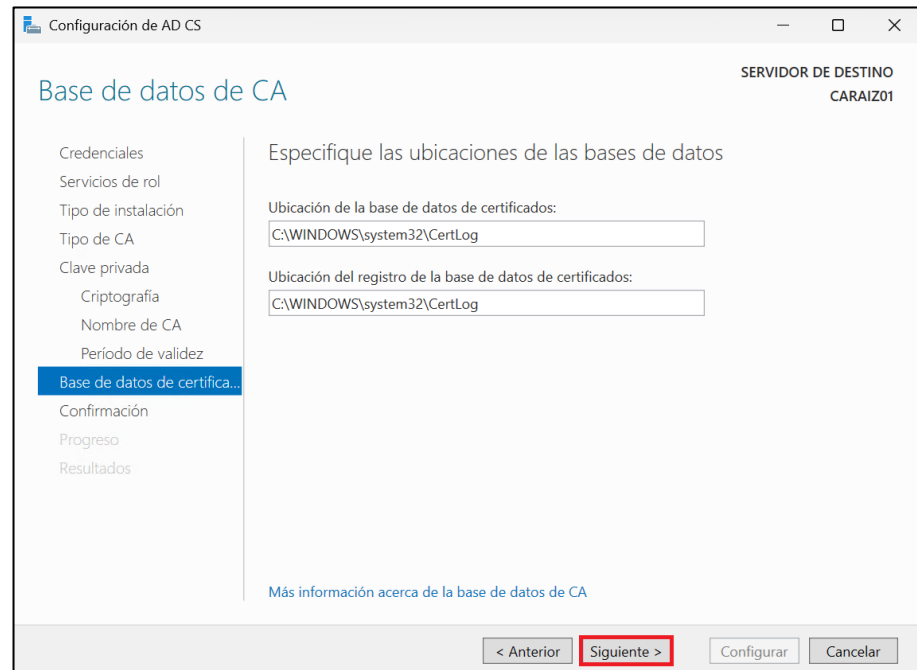


Ilustración 307 – Ubicación de base de datos

59. Finalmente, se visualiza un resumen de toda la configuración. Pulse en “Configurar”.

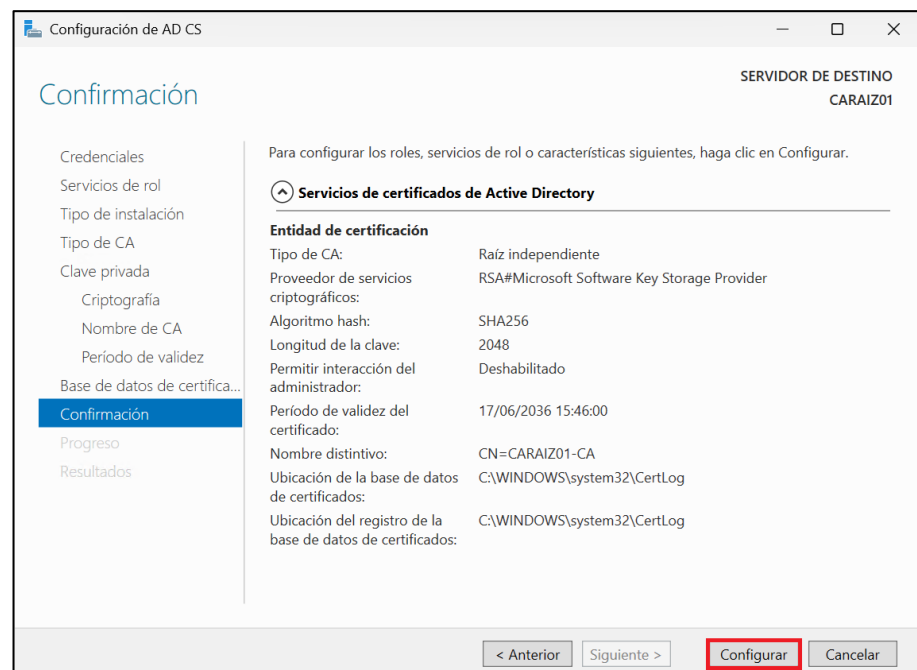


Ilustración 308 – Resumen de configuración de CA

60. Para finalizar el asistente y confirmar la configuración exitosa del servicio de Entidad de certificación, pulse en “Cerrar”.

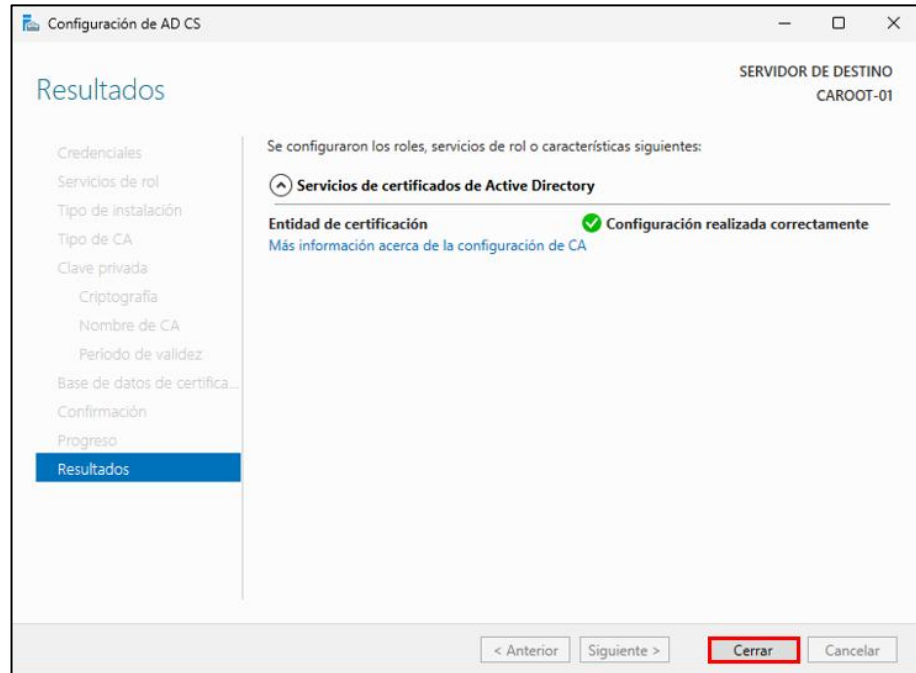


Ilustración 309 - Finalización de configuración de CA

6.3.3. CONFIGURACIÓN DE ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE A UN DOMINIO

Paso	Descripción
61.	Inicie sesión con un usuario miembro del grupo “Admins. del dominio” en el controlador de dominio del entorno donde se desea configurar la jerarquía de entidad de certificación.

62. Inicie la consola “Administrador del servidor” con privilegios de administración.

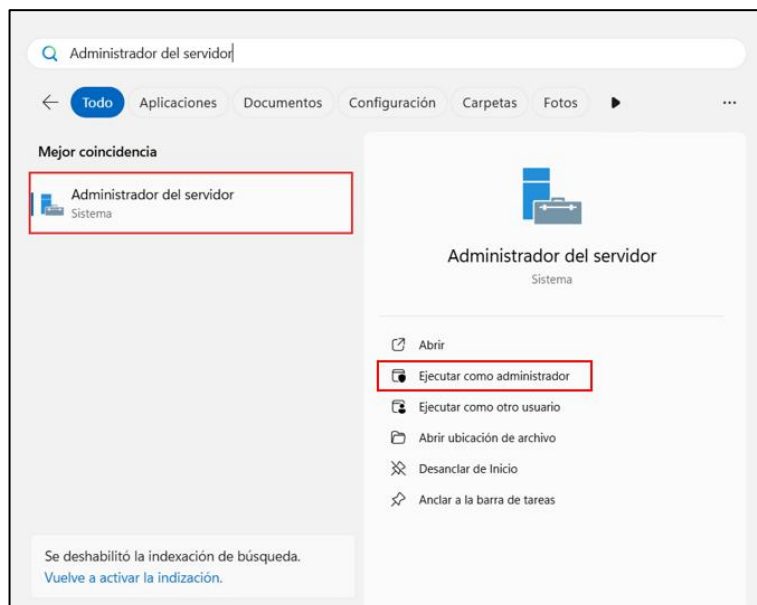


Ilustración 310 - Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

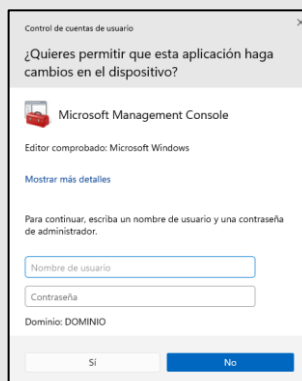


Ilustración 311 - Introducir credenciales de administrador

63. En el panel de administración del servidor, haga clic en “Herramientas” y posteriormente en “DNS” para iniciar la consola de administración del servicio de nombres.

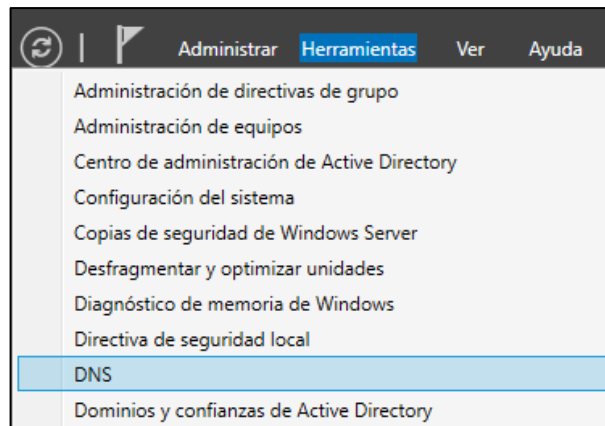


Ilustración 312 - Iniciar la consola de administración DNS

64. Despliegue el árbol de dominio y pulse con el botón derecho sobre “dominio.local”. A continuación, haga clic sobre “Alias nuevo (CNAME)”.

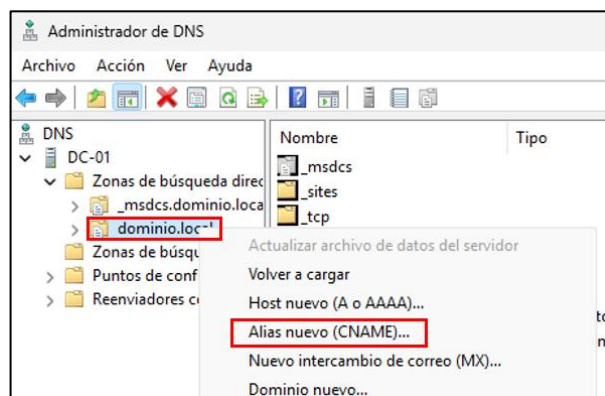


Ilustración 313 - Creación de CNAME

65. En el campo “Nombre de alias”, introduzca el nombre alternativo que se desea configurar como, por ejemplo, “crl”.

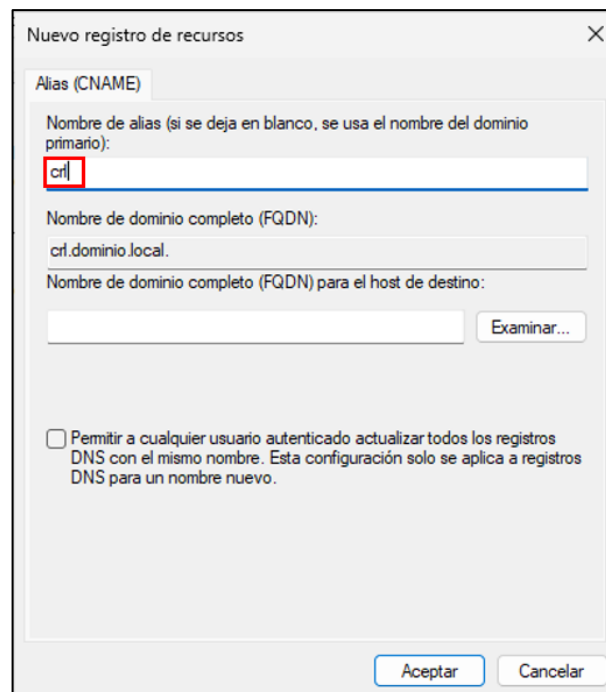


Ilustración 314 - Creación de CNAME para CRL

66. Haga clic en “Examinar” y navegue hasta el nombre de la entidad de certificación subordinada que se utilizará para publicar la CLR. A continuación, pulse en “Aceptar”.

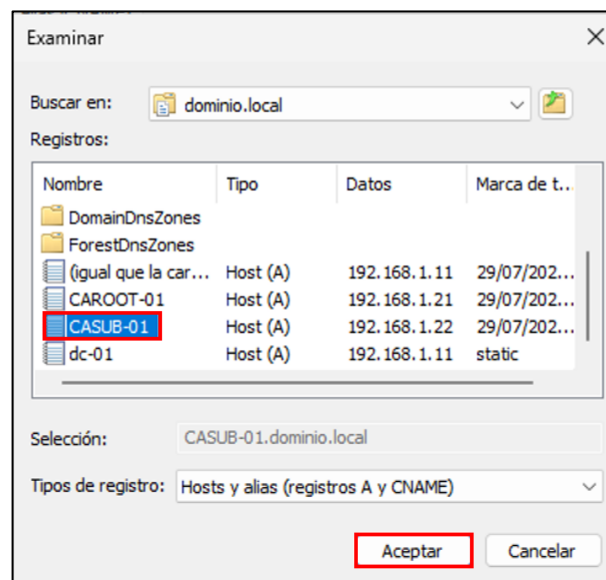


Ilustración 315 - Selección de objeto de CA Subordinada

67. De nuevo, pulse en “Aceptar” para registrar la creación del CNAME.

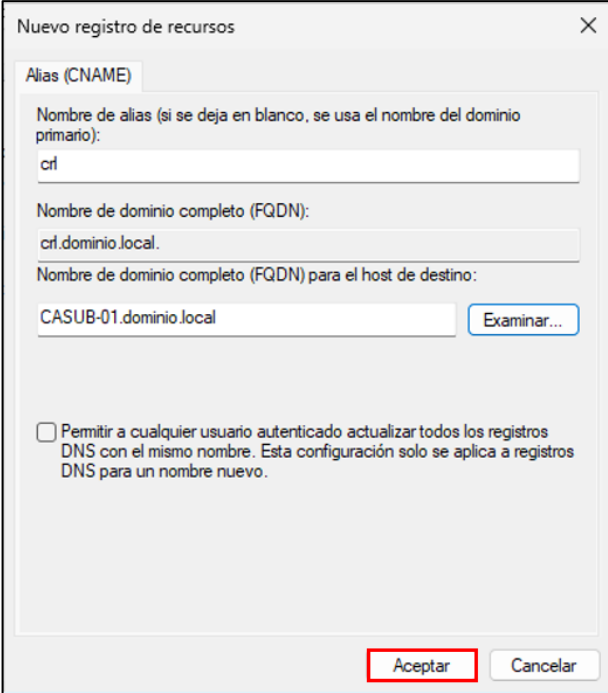


Ilustración 316 - Creación del alias (CNAME)

68. Cierre la consola de administración DNS y cierre sesión en el controlador de dominio. A continuación, inicie sesión en el servidor de entidad de certificación independiente recién configurado con un usuario administrador local.

69. En el menú de inicio, busque “Powershell” para iniciar una consola y ejecútelo como administrador.

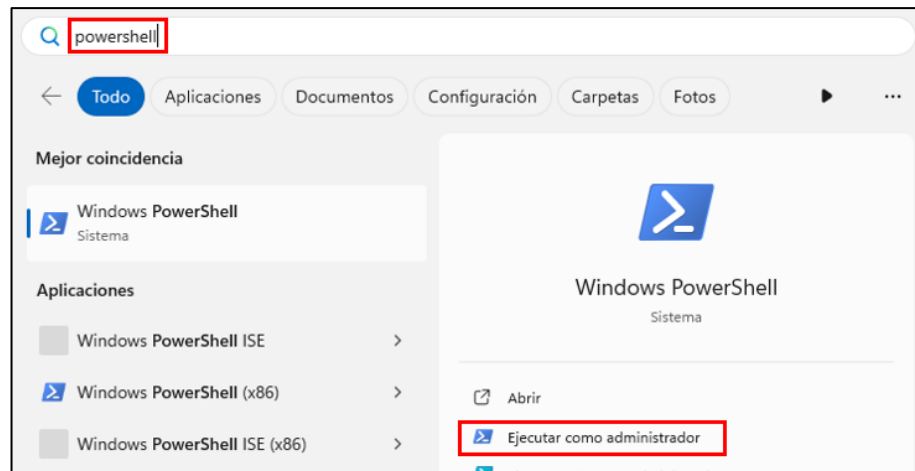


Ilustración 317 - Ejecutar PowerShell como administrador

Nota: En entornos bastionados con la guía CCN-STIC-570B, es posible que el acceso se encuentre bloqueado. Para acceder a la consola de Powershell, puede realizarlo haciendo clic desde la consola de “Administrador del servidor > Herramientas > Windows PowerShell”.

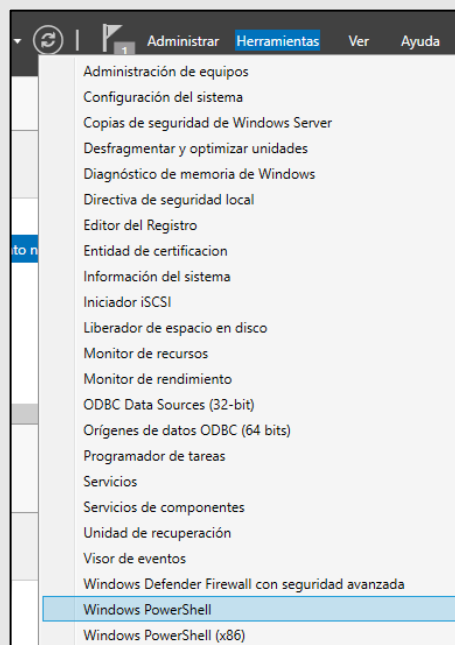


Ilustración 318 - Iniciar Windows PowerShell

70. Introduzca “regedit” para abrir la consola de edición del registro y pulse “enter”.

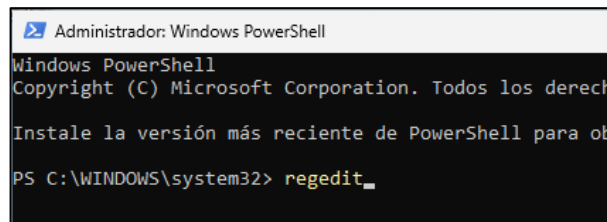


Ilustración 319 - Iniciar el editor del registro

Nota: En entornos bastionados con la guía CCN-STIC-570B, es posible que el acceso se encuentre bloqueado. Para acceder al editor del registro, puede hacer clic en “Editor del registro” en la consola de “Administrador del servidor > Herramientas”.

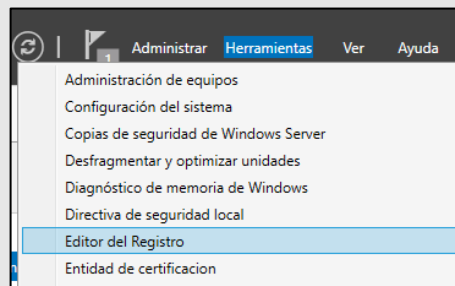


Ilustración 320 - Iniciar el editor del registro

71. Diríjase a la clave de registro “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration y acceda a clave de su ROOT CA.

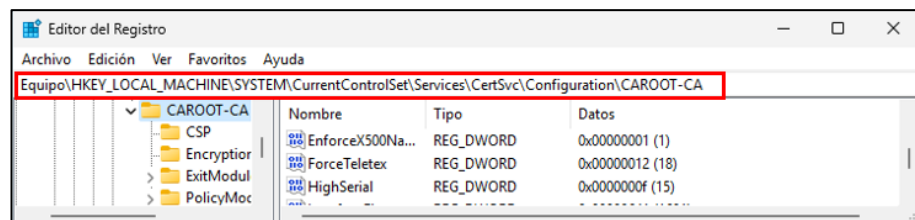


Ilustración 321 - Acceso a clave de registro de CA Raíz

72. Localice el valor “ValidityPeriodUnits” y edítelo pulsando con el botón derecho y “Modificar”.

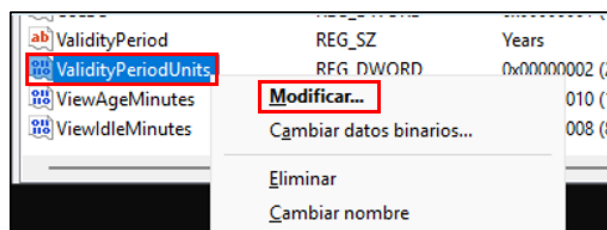


Ilustración 322 - Modificar ValidityPeriodUnits

73. Introduzca el valor “10” en el campo “Información del valor” y asegúrese que la opción “Decimal” se encuentra habilitada. A continuación, pulse en “Aceptar”.

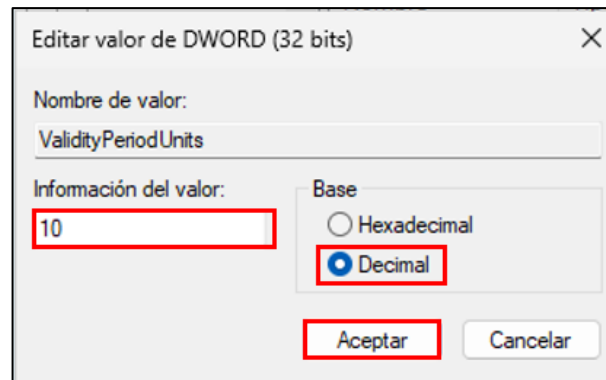


Ilustración 323 - Configuración del valor DWORD

74. Cierre el editor del registro y la consola de Powershell.

75. En el panel de administración del servidor, pulse en “Herramientas”, y a continuación “Entidad de certificación”.

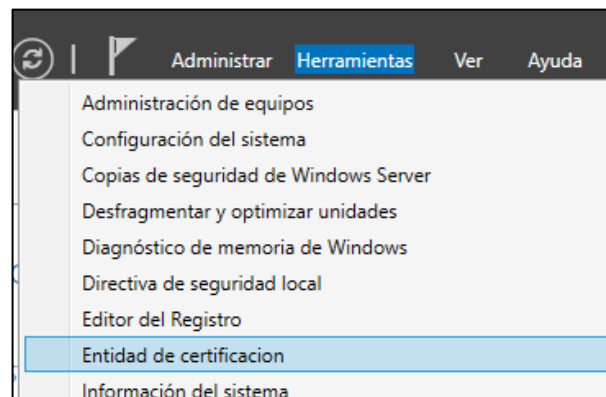


Ilustración 324 - Acceso a consola de administración de CA

76. Haga clic sobre el nombre de la entidad de certificación, y posteriormente en “Propiedades”.

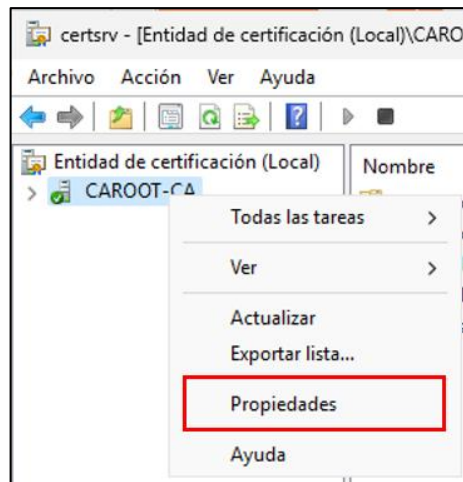


Ilustración 325 - Propiedades de CA Raíz

77. En la ventana de “Propiedades” diríjase a la pestaña “Extensiones” y, manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, revise la publicación de CRLs mediante la ruta local seleccionando “C:\Windows\System32\CertSrv\CertEnroll\<nombre de CA>< sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.

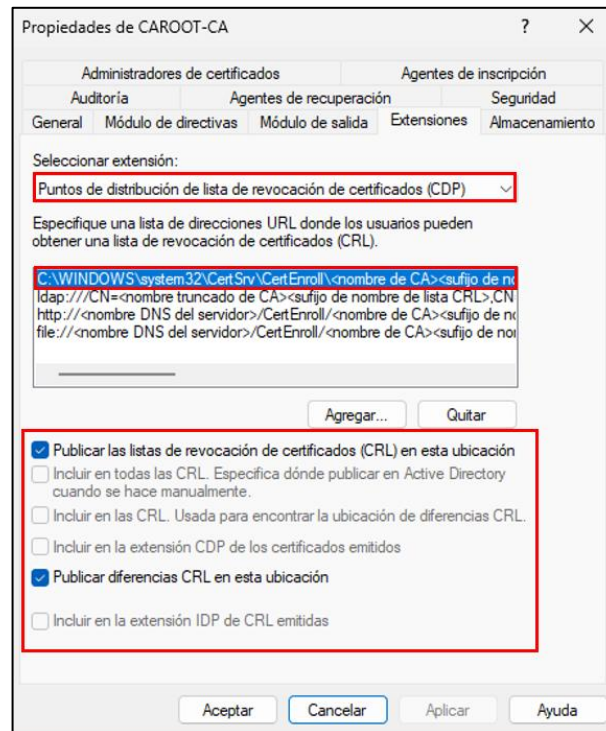


Ilustración 326 - Configuración de extensión CDP

78. A continuación, deshabilite la publicación de CRLs mediante LDAP seleccionando “ldap://CN=<nombre truncado de CA>< sufijo de nombre de lista CRL>,CN=nombre corto del servidor>,CN=CDP,CN=Public Key Services,<contenedor de configuración><clase de objeto CDP>” y desmarque todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.

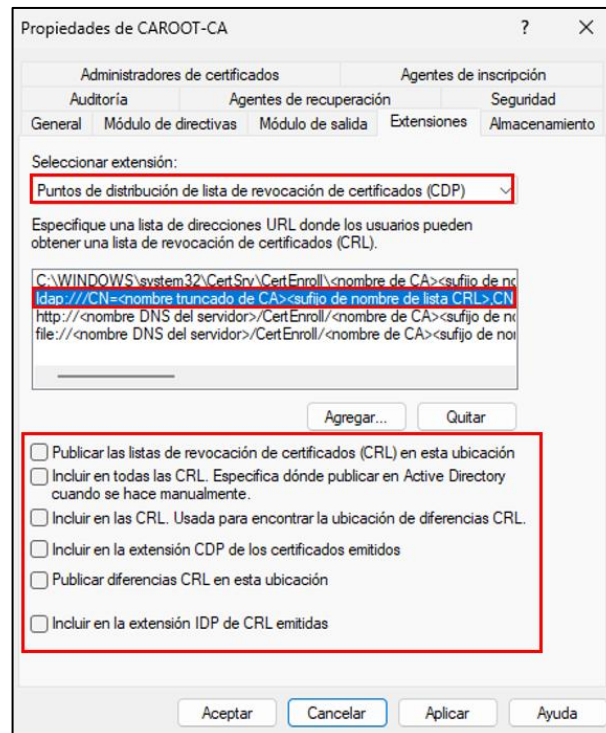


Ilustración 327 - Configuración de extensión LDAP

79. Para continuar, seleccione “file://<nombre DNS del servidor>/CertEnroll/<nombre de CA>/sufijo de nombre de lista CRL<diferencias entre listas CRL permitidas>.crl” y desmarque todas las opciones como muestra la siguiente figura.

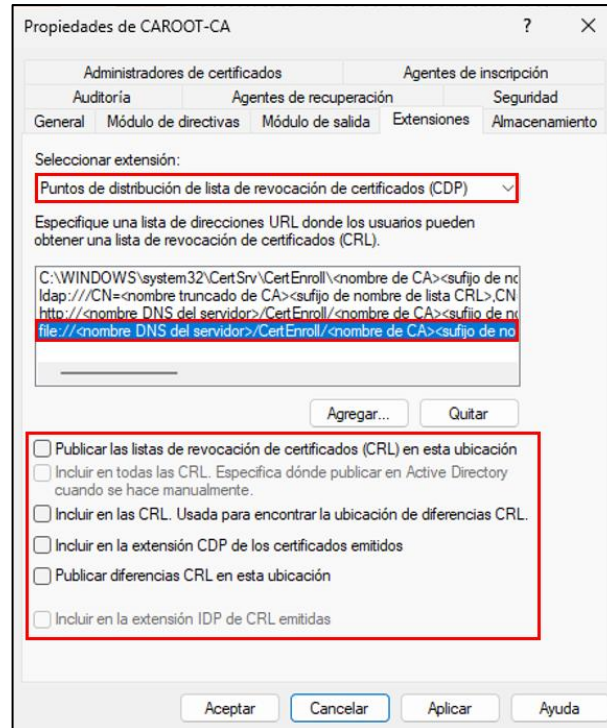


Ilustración 328 - Configuración de extensión file

80. Una vez realizada dicha configuración, seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre de CA><sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y pulse “Control + C”, para copiar el objeto.

81. Pulse en Agregar.

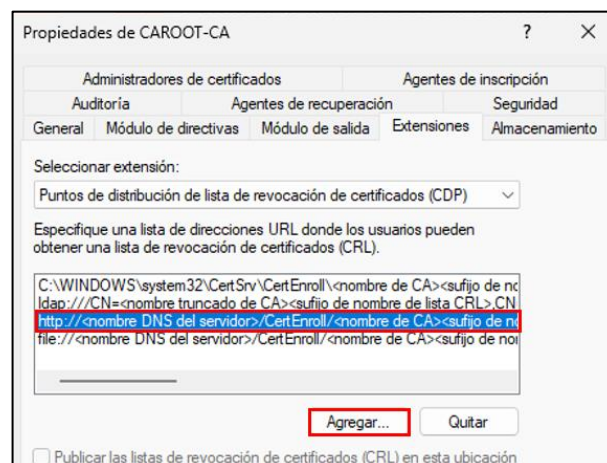
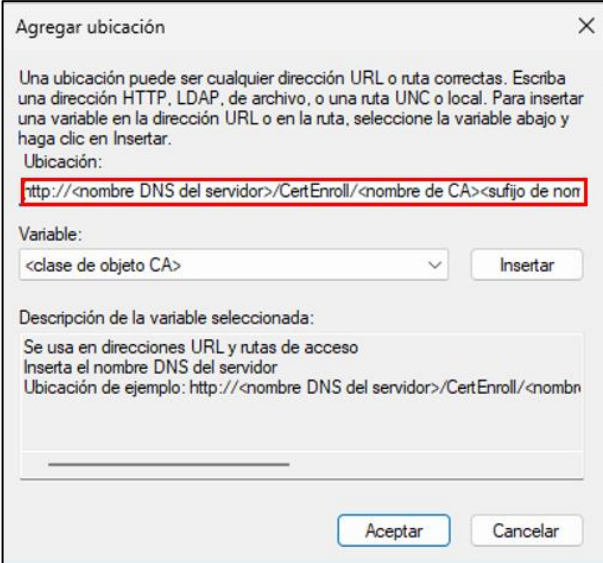


Ilustración 329 - Crear nueva extensión CDP

82. En el campo “Ubicación”, pegue la ruta copiada en el paso anterior.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de non

Variable:

<clase de objeto CA>

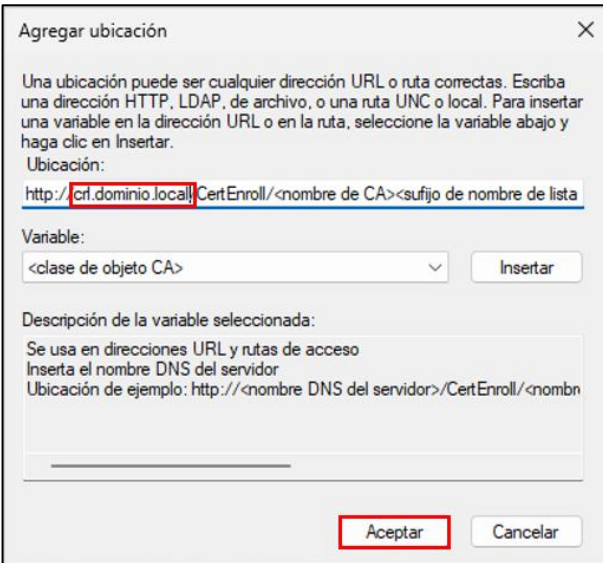
Descripción de la variable seleccionada:

Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Ilustración 330 - Pegar ruta de la extensión

Nota: No pulse el botón “Aceptar”.

83. Localice “<nombre DNS del servidor>” al inicio de la ruta, y sustitúyalo por el CNAME generado al inicio de este procedimiento.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://<rf.dominio.local>/CertEnroll/<nombre de CA>< sufijo de nombre de lista

Variable:

<clase de objeto CA>

Descripción de la variable seleccionada:

Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Ilustración 331 - Sustitución de ruta por CNAME

84. Pulse sobre el botón “Aceptar” y a continuación, seleccionando la nueva entrada, marque los siguientes componentes.

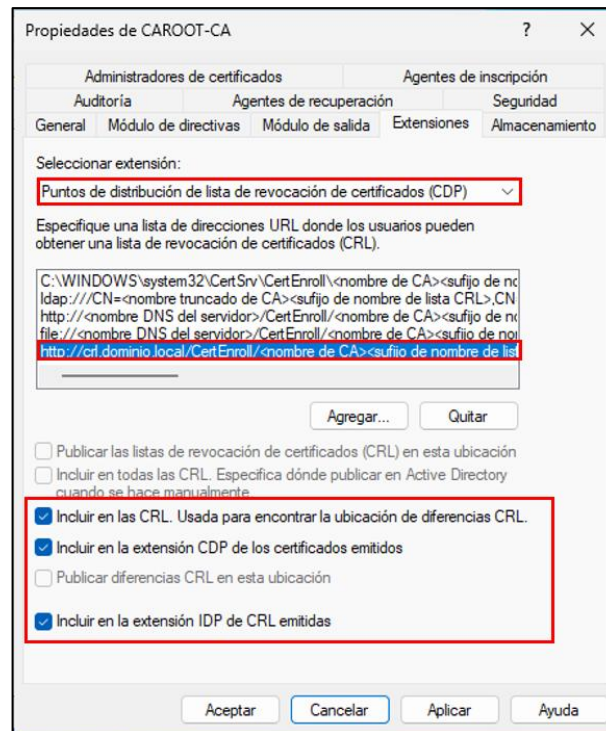


Ilustración 332 - Configuración de extensión http

85. Para continuar, en el desplegable “Seleccionar extensión”, elija “Acceso a la información de entidad (AIA)”.

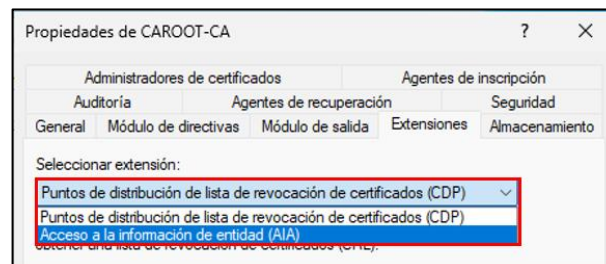


Ilustración 333 - Cambio a Acceso a la información de entidad (AIA)

86. Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\<nombre DNS del servidor>_<nombre de CA><Nombre de certificado>.crt” todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.

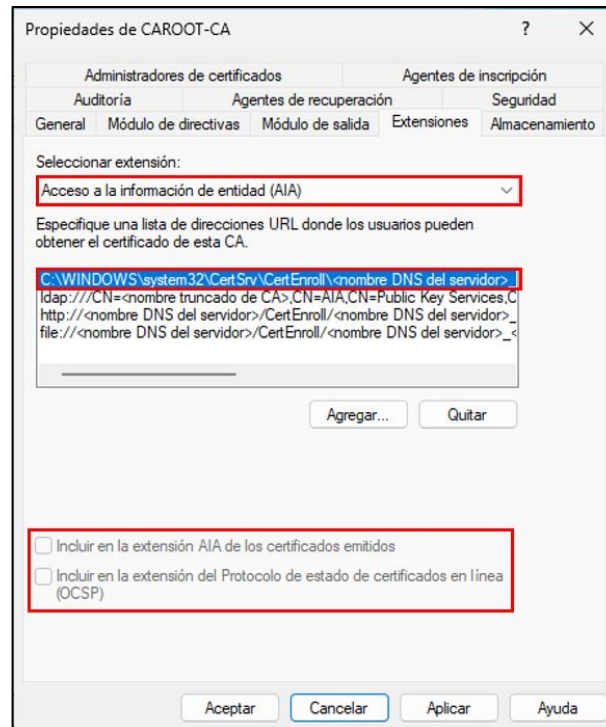


Ilustración 334 - Configuración de extensión AIA

87. Seleccione el objeto “ldap://CN=<nombre truncado de CA>,CN=AIA,CN=Public Key Services,CN=Services,<contenedor de configuración><clase de objeto CA>” y desmarque todas las casillas tal y como se muestra en la siguiente figura.

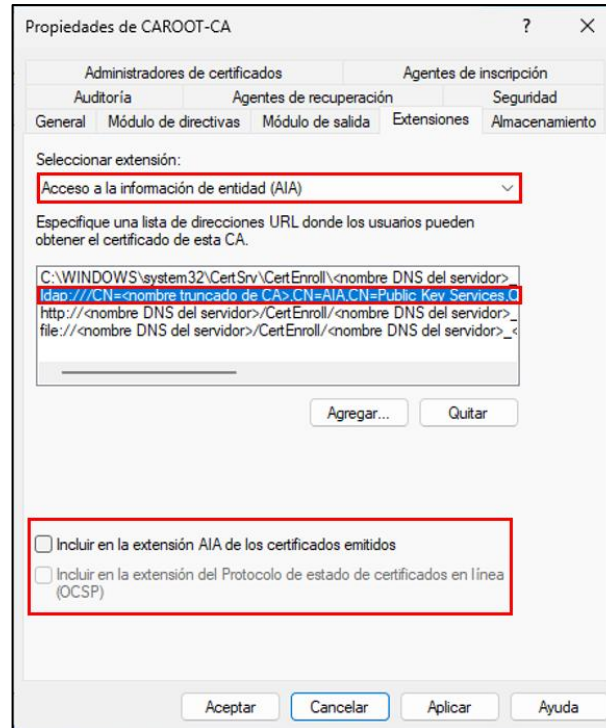


Ilustración 335 - Configuración de LDAP

88. Seleccione ahora “file://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y confirme que la opción “Incluir en la extensión AIA de los certificados emitidos” se encuentra deshabilitada.

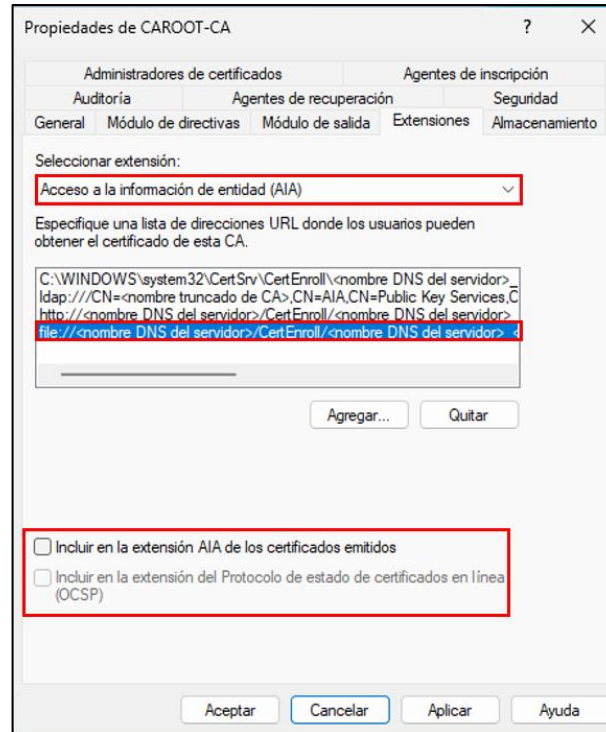


Ilustración 336 - Configuración de file

89. Seleccione ahora “http://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y copie el elemento mediante la combinación de teclas “Control + C”. A continuación, pulse en “Agregar”.

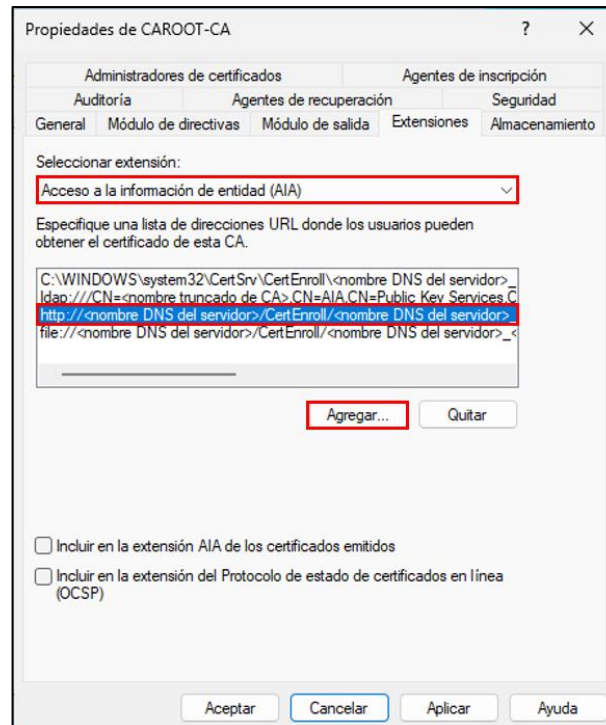


Ilustración 337 - Agregar nueva extensión

90. En el campo “Ubicación” pegue el contenido copiado.

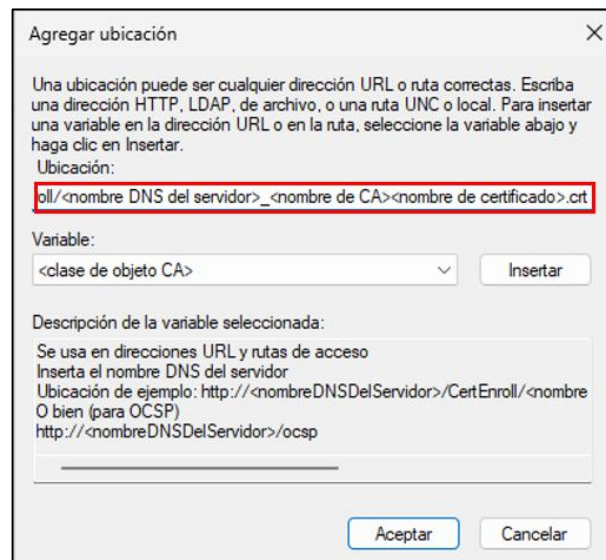


Ilustración 338 - Pegar contenido del portapapeles

Nota: Aún no pulse sobre el botón “Aceptar”.

91. Localice y sustituya el valor “<nombre DNS del servidor>” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y su alias CNAME.

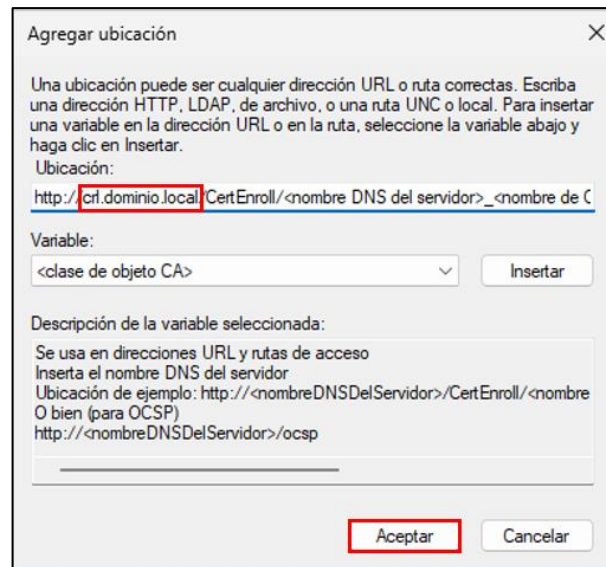


Ilustración 339 - Edición de la ruta

92. Pulse “Aceptar” y a continuación, marque la casilla “Incluir en la extensión AIA de los certificados emitidos”. A continuación, pulse en “Aplicar” y “Aceptar”.

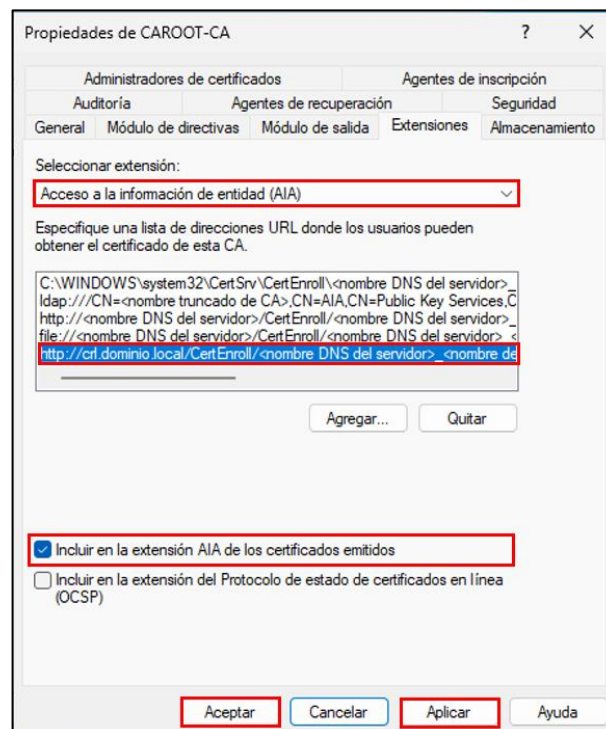


Ilustración 340 - Modificación de nueva extensión

93. El sistema solicitará reiniciar los servicios de certificados. Pulse en “Sí”.

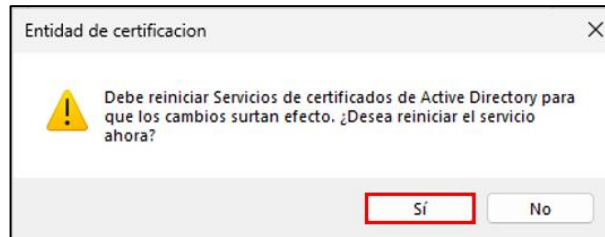


Ilustración 341 - Aceptar reiniciar el servicio

94. A continuación, se establecerá un período de caducidad para la lista de revocación de certificados (CRL). Para ello, pulse con el botón derecho sobre “Certificados revocados”, y a continuación, seleccione “Propiedades”.

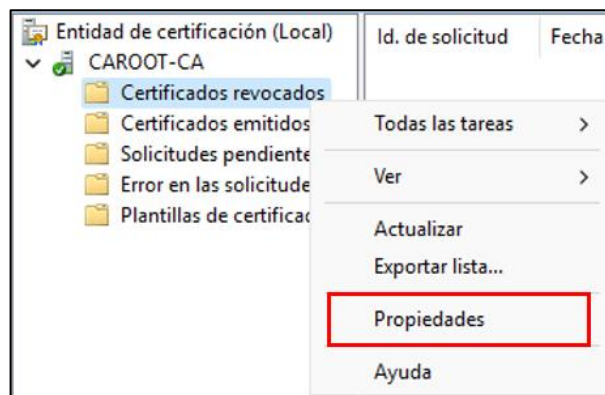


Ilustración 342 - Propiedades de lista de revocación en CA Raíz

95. Seleccione el intervalo de publicación CRL con la validez del certificado de la entidad de certificación raíz (20), y a su vez, desmarque la posibilidad de “Publicar diferencias CLR”.

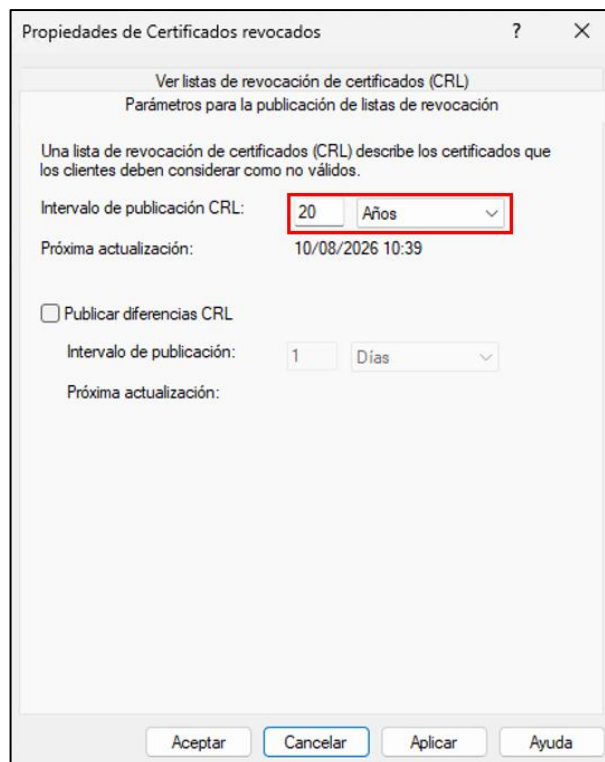


Ilustración 343 - Intervalo de publicación CRL en CA Raíz

A continuación, pulse sobre el botón “Aplicar” y “Aceptar”.

96. Una vez realizados los cambios, pulse de nuevo con el botón derecho sobre “Certificados revocados”, y seleccione “Todas las tareas > Publicar”.

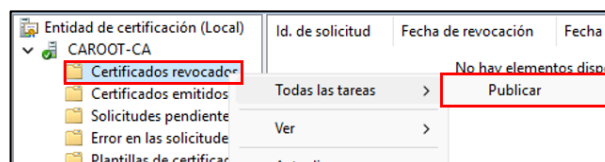


Ilustración 344 - Publicar nueva CRL en CA Raíz

97. En el asistente de publicación de lista de revocación de certificados, pulse en “Aceptar”.



Ilustración 345 - Publicar nueva CRL en CA Raíz

98. Una vez cambiados estos parámetros será necesario emitir un certificado de la entidad raíz actualizado. Para ello, sobre el objeto con el nombre de la Entidad de Certificación, pulse con el botón derecho y seleccione “Todas las tareas → Renovar certificado de CA...”.

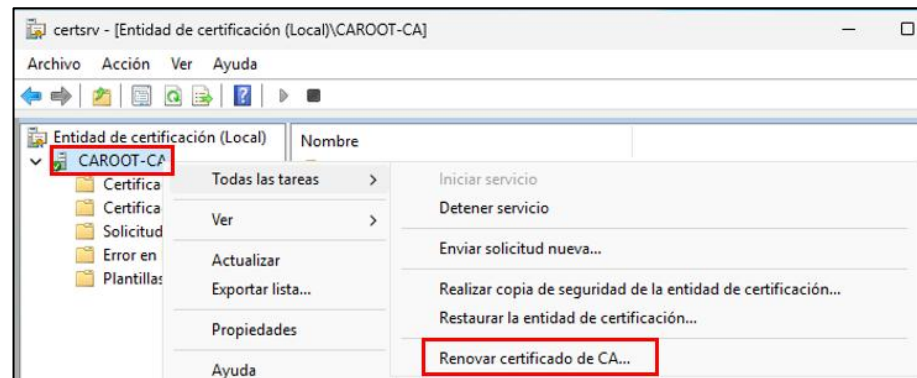


Ilustración 346 - Renovar certificado de CA

99. Pulse en “Sí” para confirmar la creación del nuevo certificado.

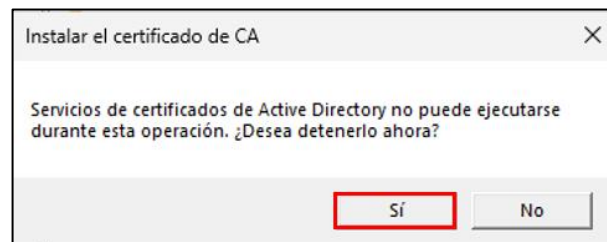


Ilustración 347 - Detener servicio de CA

100. En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.

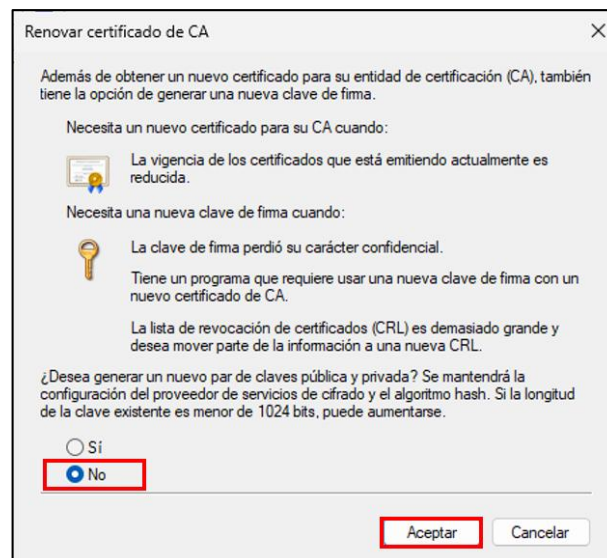


Ilustración 348 - Finalizar la renovación del certificado de CA

101. Una vez finalice el proceso, la entidad de certificación raíz estará disponible para generar el certificado de la entidad subordinada y establecer la jerarquía de certificación.

6.3.4. PASO A PASO DE INSTALACIÓN DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA EN DOMINIO

Los pasos que se describen a continuación se realizarán en el servidor Entidad de Certificación Subordinada en el dominio.

Nota: Si su entidad de certificación subordinada ya se encuentra implementada y configurada, puede obviar este procedimiento.

Paso	Descripción
102.	Inicie sesión en el equipo donde se va a instalar el servidor Entidad de Certificación subordinada del dominio.

103. A continuación, se ejecutará como administrador el “Administrador del servidor” para configurar el servidor de Entidad de Certificación.

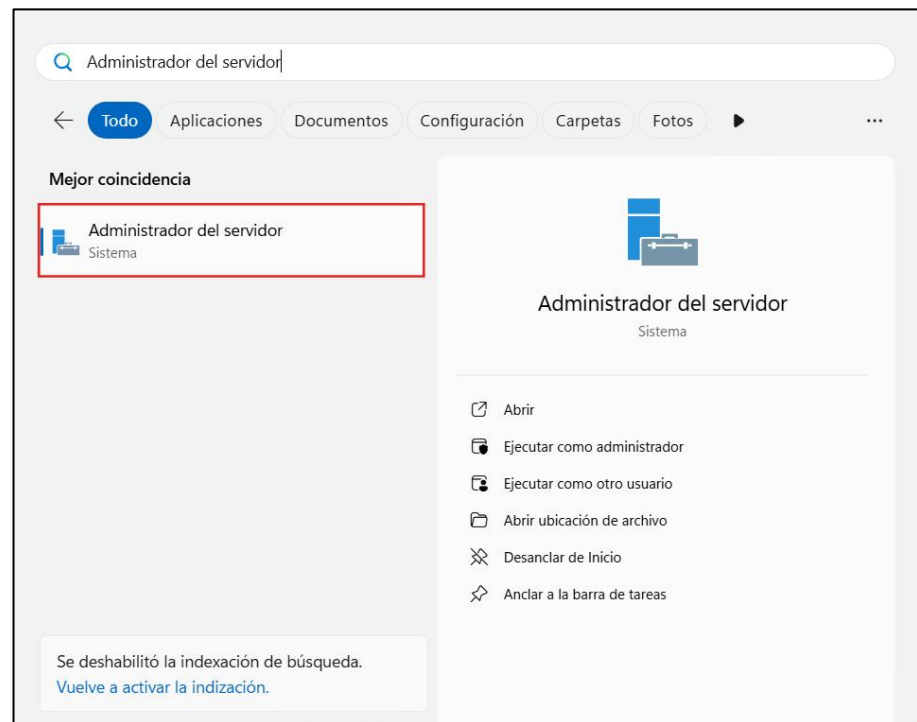


Ilustración 349 – Administrador del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

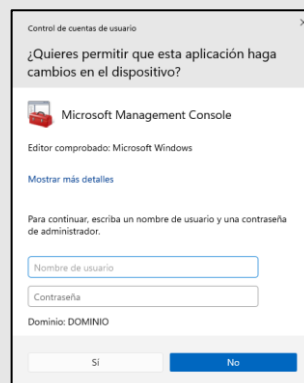


Ilustración 350 - Introducir credenciales de administrador

104. Le aparecerá una ventana para proceder con la configuración, pulse en “Configurar Servicios de certificados de Active Directory”.

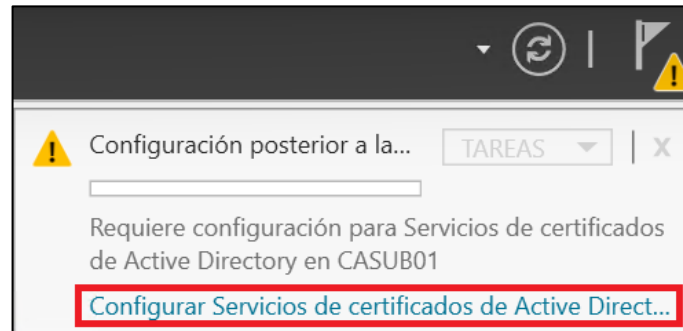


Ilustración 351 – Configurar Servicios de certificados de Active Directory

Nota: Si el rol de Entidad de certificación no se encuentra instalado, esta advertencia no se apreciará en el administrador del servidor. Añadir la funcionalidad desde “Administrar > Agregar roles y características”.

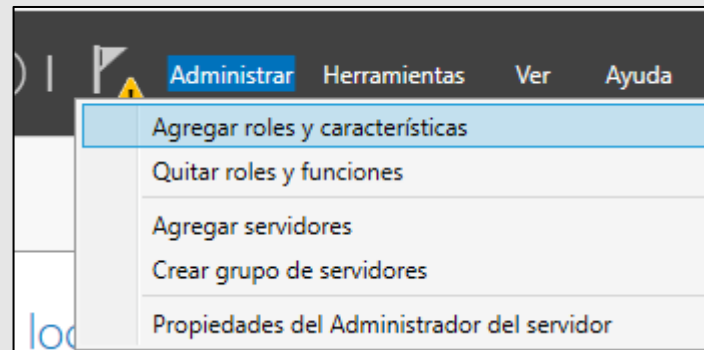


Ilustración 352 - Agregar roles y características

105. Especifique las credenciales para configurar servicios de rol. Pulse en “Siguiente”.

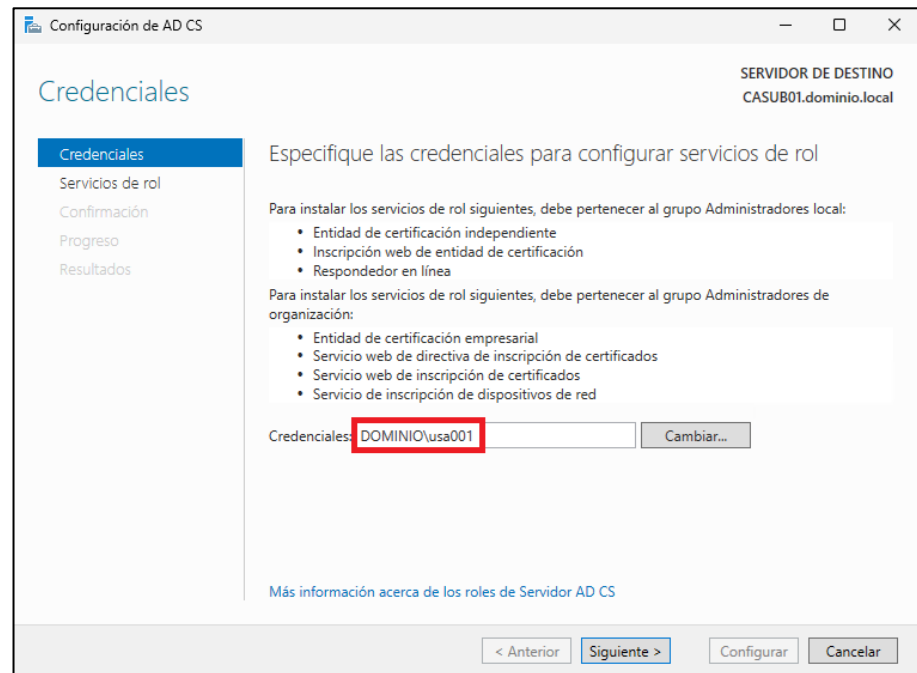


Ilustración 353 – Especificación de credenciales

Nota: El usuario administrador que se utilizará en todo el escenario será **usa001**.

106. Seleccione los servicios de rol que dispondrá el servidor de Entidad de Certificación. En el presente caso serán “Entidad de certificación” e “Inscripción web de entidad de certificación”. Pulse en “Siguiente”.

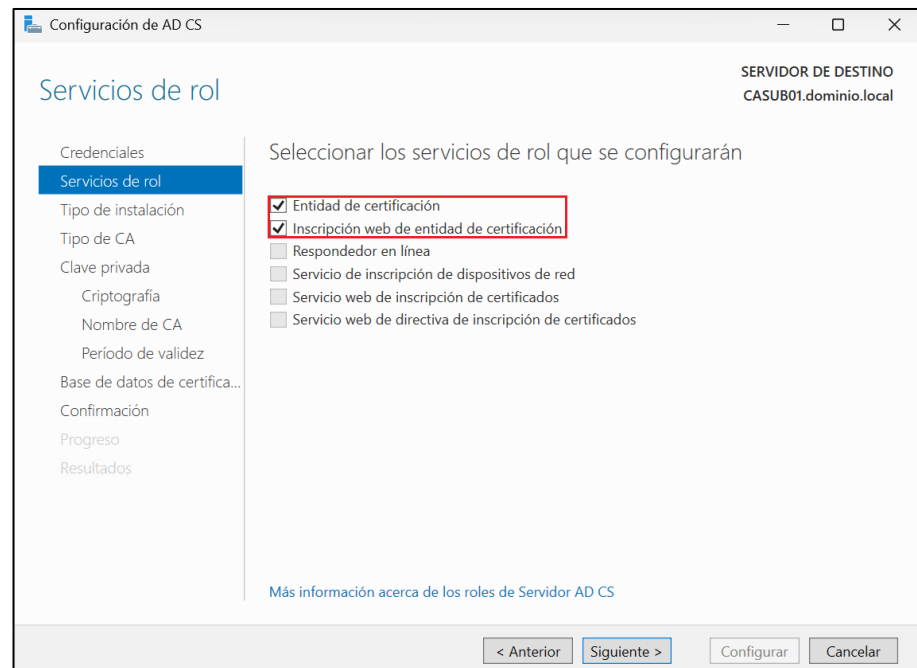


Ilustración 354 – Servicios de rol que se configurarán

107. Especifique el tipo de instalación de la CA, seleccione “CA empresarial”. Pulse en “Siguiente”.

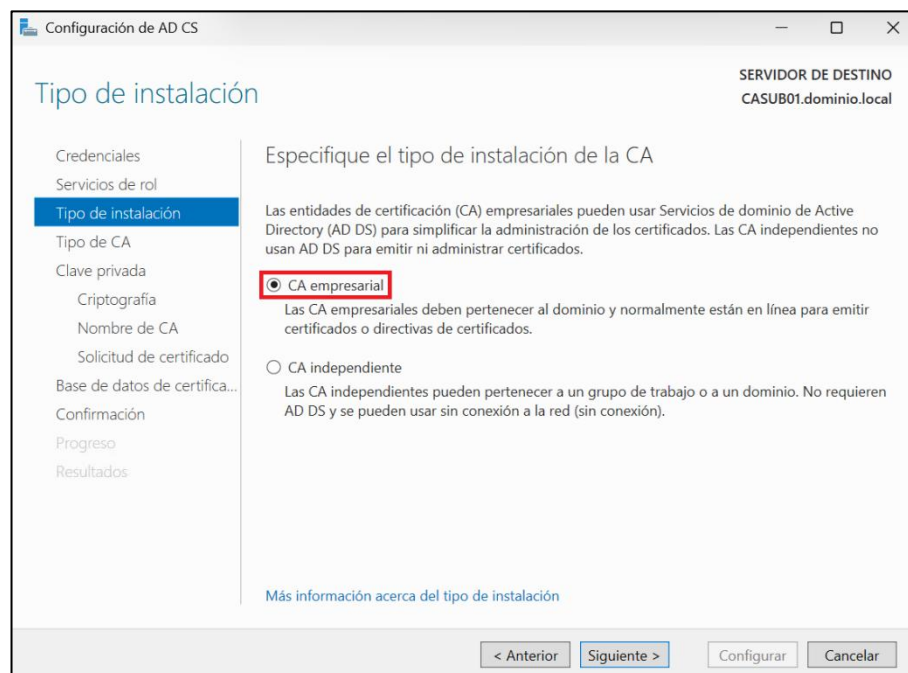


Ilustración 355 – Tipo de instalación

108. Seleccione “CA subordinada”. Pulse en “Siguiente”.

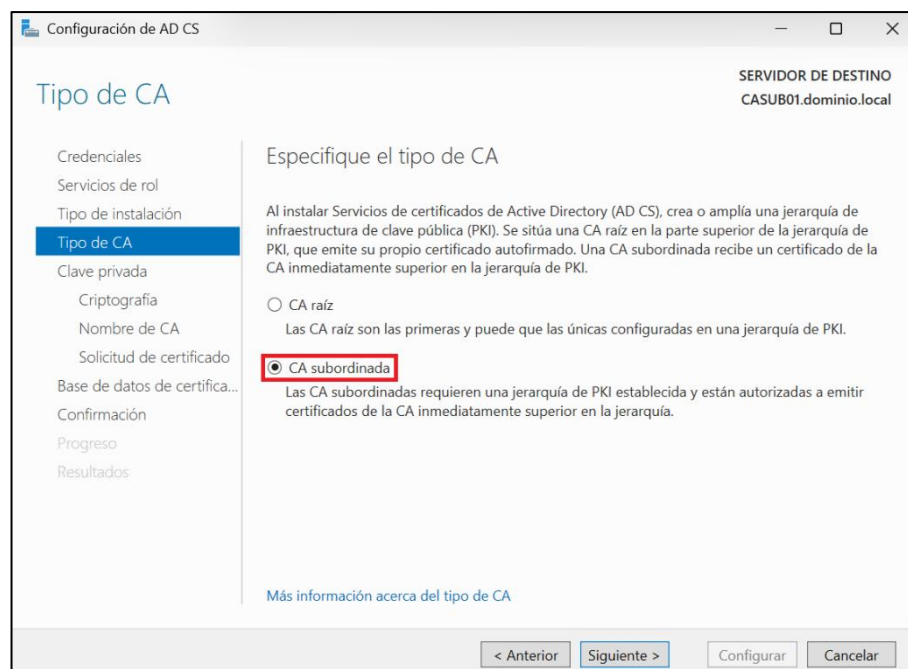


Ilustración 356 – Selección de CA Subordinada

109. A continuación, seleccione la opción de “Crear una clave privada nueva”. Pulse en “Siguiente”.

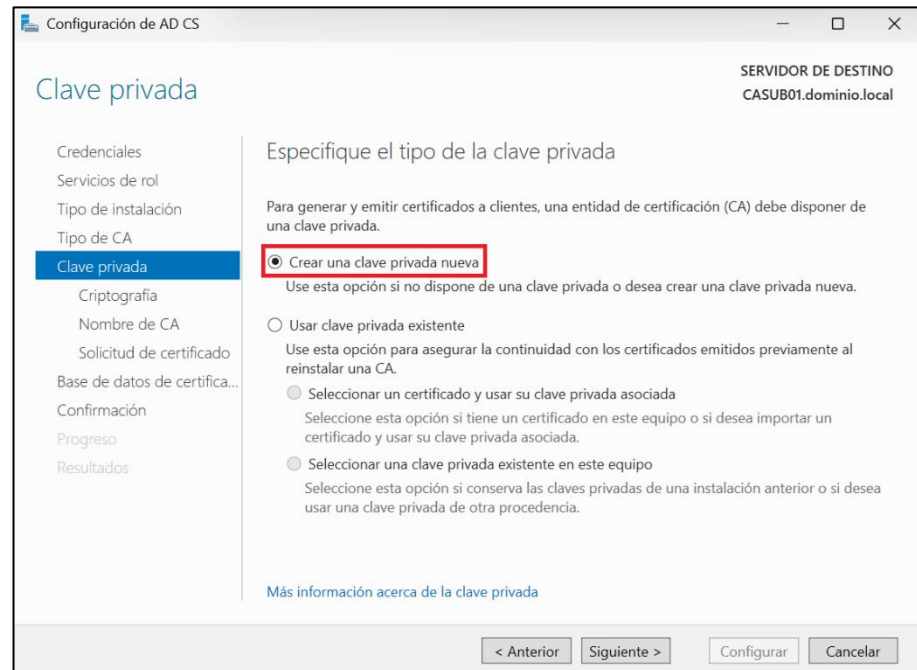


Ilustración 357 –Crear clave privada

110. Las opciones criptográficas que se seleccionarán serán.

- Longitud: 2048
- Tipo de algoritmo hash: SHA256

Posteriormente, pulse en “Siguiente”.

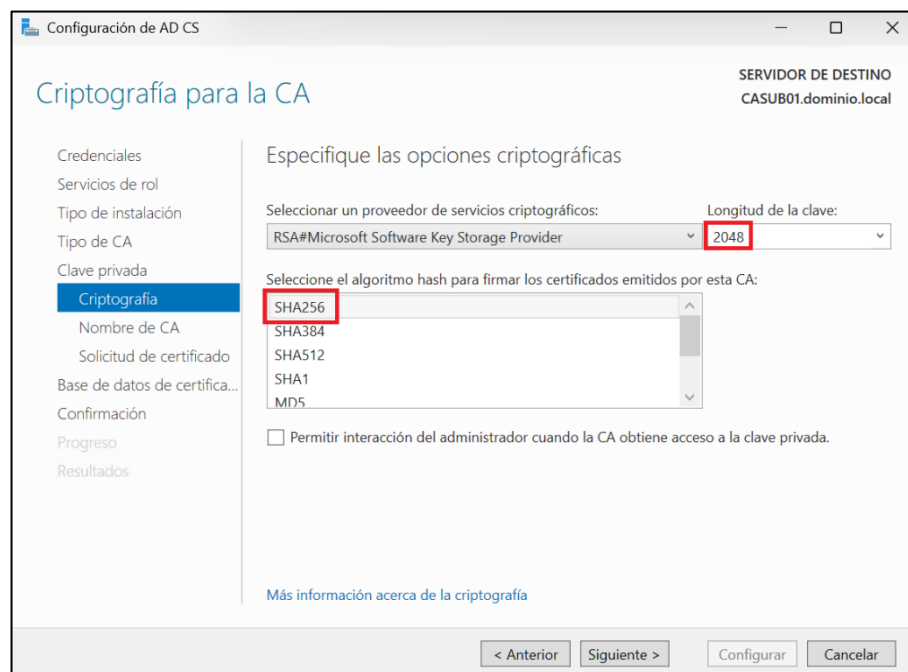
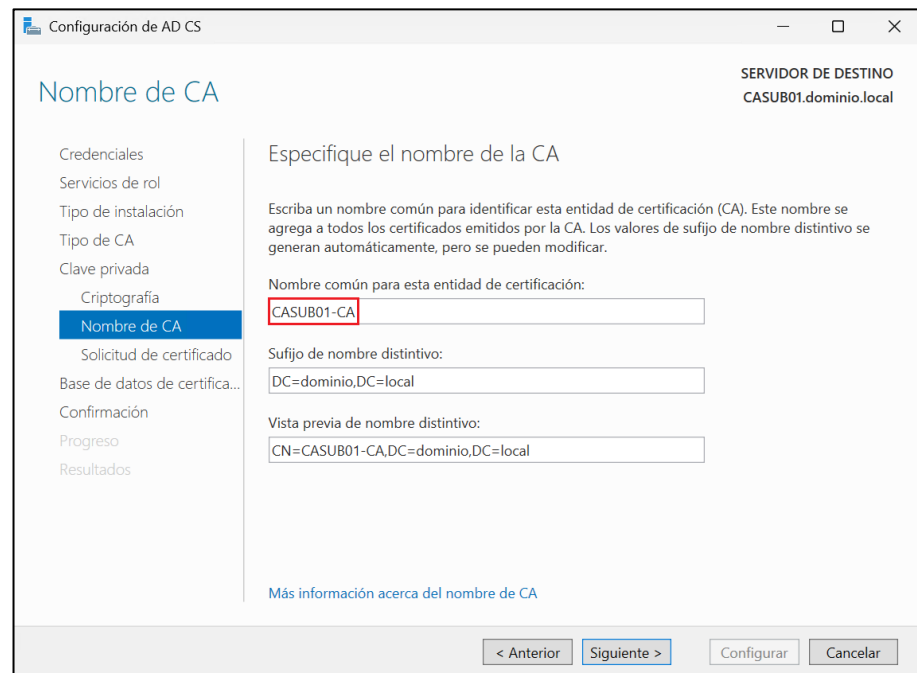


Ilustración 358 – Especificar criptografía

111. A continuación, se especificará el nombre para la entidad de certificación. En el presente caso, será “CASUB01-CA”. Posteriormente, pulse en “Siguiente”.



Configuración de AD CS

Nombre de CA

SERVIDOR DE DESTINO
CASUB01.dominio.local

Especifique el nombre de la CA

Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.

Nombre común para esta entidad de certificación:
CASUB01-CA

Sufijo de nombre distintivo:
DC=dominio,DC=local

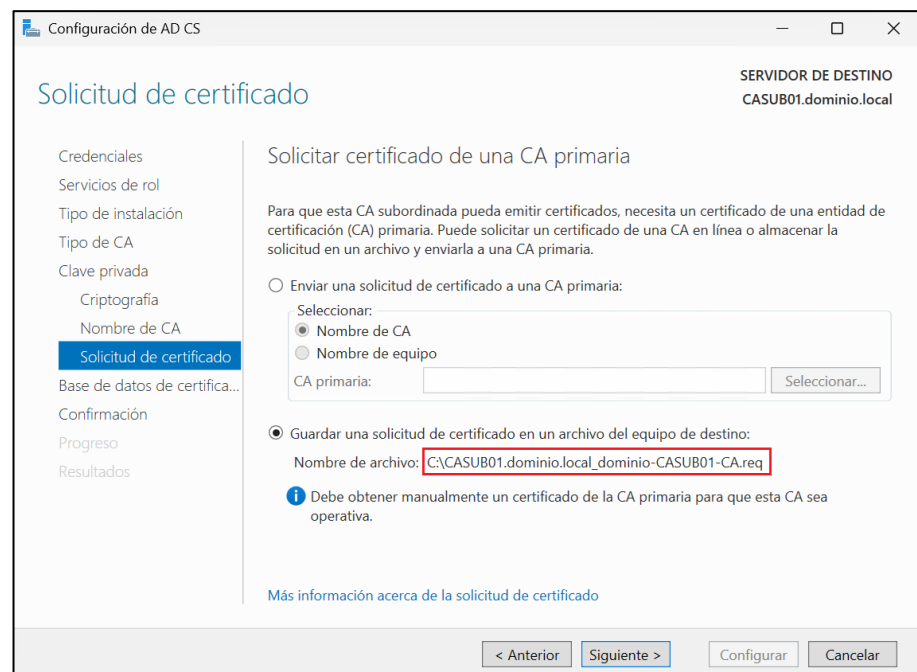
Vista previa de nombre distintivo:
CN=CASUB01-CA,DC=dominio,DC=local

Más información acerca del nombre de CA

< Anterior Siguiente > Configurar Cancelar

Ilustración 359 – Nombre de la CA Subordinada

112. A continuación, seleccione “Guardar una solicitud de certificado en un archivo del equipo de destino”, y pulse en “Siguiente”.



Configuración de AD CS

Solicitud de certificado

SERVIDOR DE DESTINO
CASUB01.dominio.local

Solicitar certificado de una CA primaria

Para que esta CA subordinada pueda emitir certificados, necesita un certificado de una entidad de certificación (CA) primaria. Puede solicitar un certificado de una CA en línea o almacenar la solicitud en un archivo y enviarla a una CA primaria.

☐ Enviar una solicitud de certificado a una CA primaria:

Seleccionar:

☒ Nombre de CA

☐ Nombre de equipo

CA primaria: Seleccionar...

☒ Guardar una solicitud de certificado en un archivo del equipo de destino:

Nombre de archivo: **C:\CASUB01.dominio.local_dominio-CASUB01-CA.req**

Debe obtener manualmente un certificado de la CA primaria para que esta CA sea operativa.

Más información acerca de la solicitud de certificado

< Anterior Siguiente > Configurar Cancelar

Ilustración 360 – Creación de petición de certificado

113. Para continuar con el asistente, modifique si es necesario la ubicación de los logs y base de datos de certificados, y posteriormente, pulse en “Siguiente”.

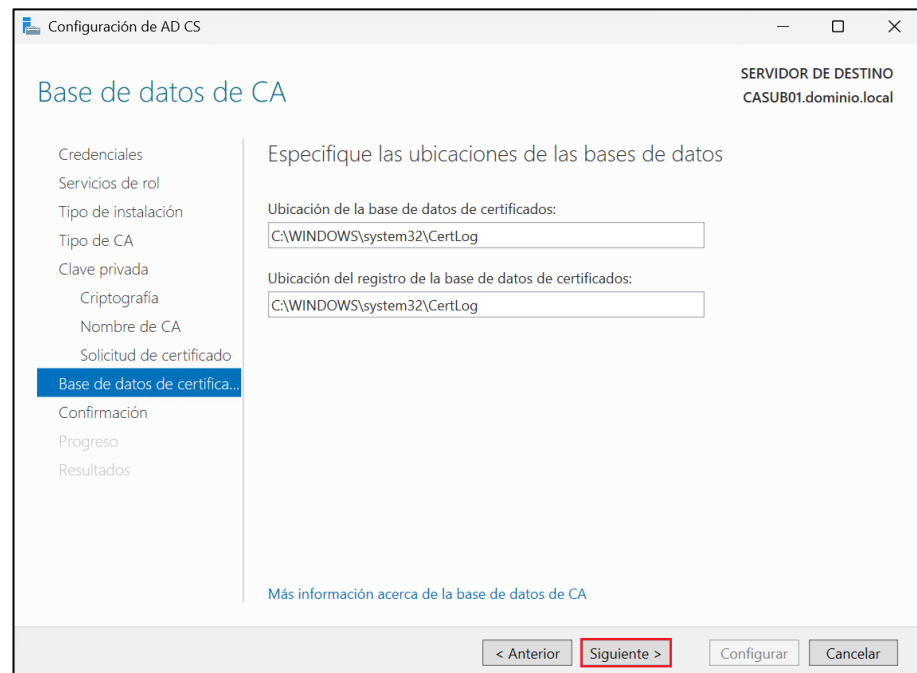


Ilustración 361 – Ubicaciones de las bases de datos

114. A continuación, pulse en “Configurar” tras la revisión del resumen de configuración de servicios de certificados de Active Directory.

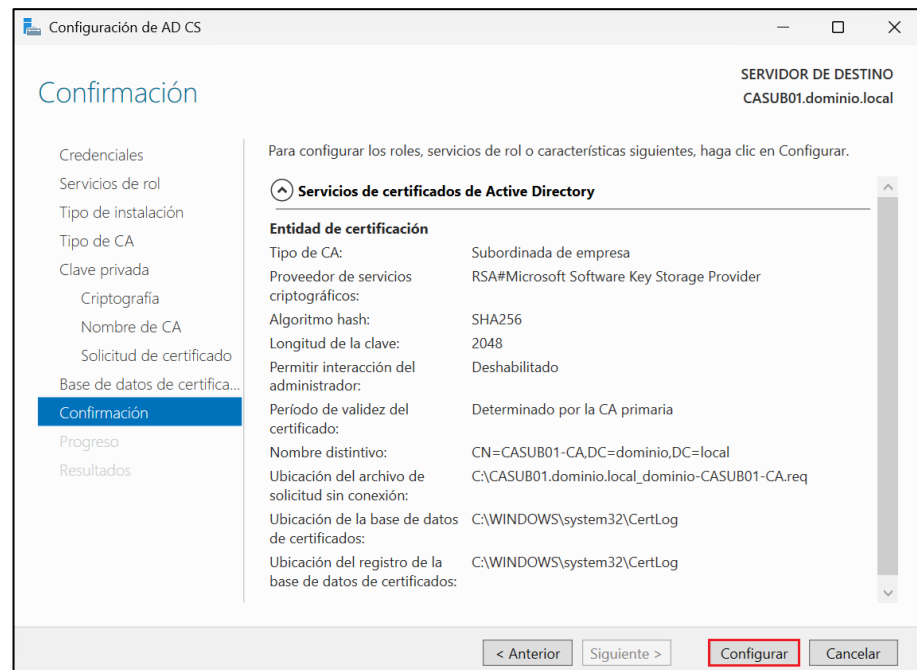


Ilustración 362 – Resumen de la configuración

115. El asistente mostrará que la configuración se realizó correctamente, pero es necesario generar el certificado de CA utilizando la petición “*.req” exportada en pasos anteriores. Para finalizar la configuración, pulse en “Cerrar”.

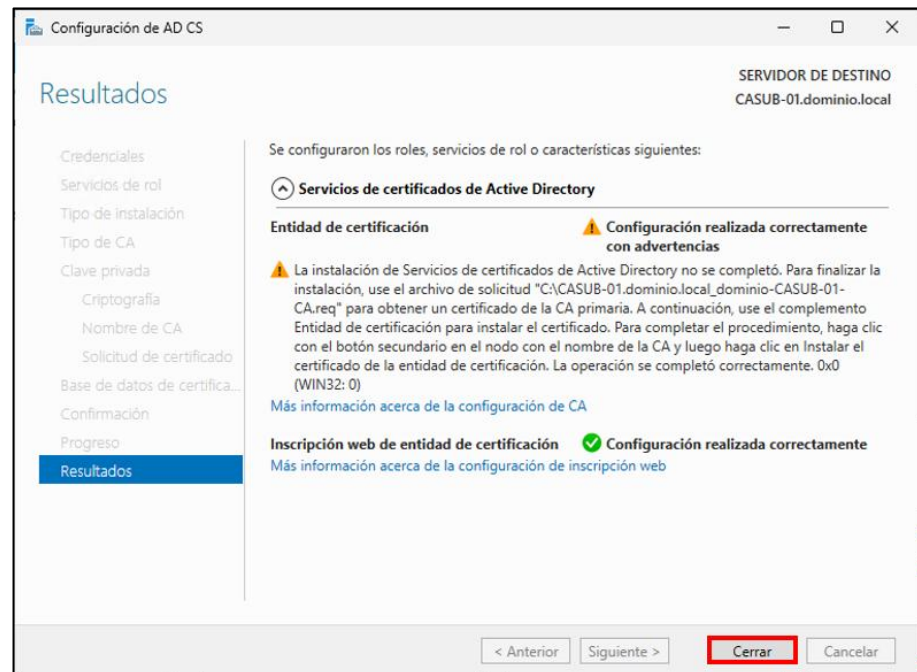


Ilustración 363 - Finalizar el asistente de configuración

6.3.5. PASO A PASO DE INTERCAMBIO DE CERTIFICADOS ENTRE LA ENTIDAD SUBORDINADA Y LA ENTIDAD RAÍZ INDEPENDIENTE DEL DOMINIO

Paso	Descripción
116.	Inicie sesión en el servidor Entidad de Certificación raíz con un usuario con privilegios de administración.
117.	Copie el fichero “*.req” generado en el apéndice anterior siguiendo los procedimientos operativos de seguridad correspondientes.

118. Sobre la barra de búsqueda, escriba “certsrv.msc”.

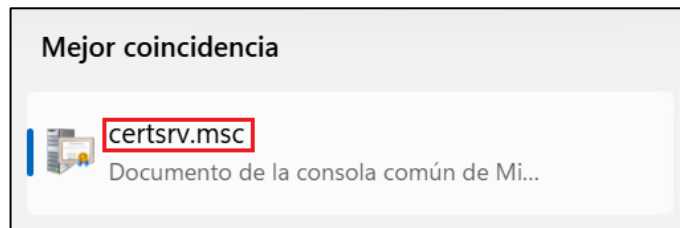


Ilustración 364 – Ejecución de Entidad de Certificación

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

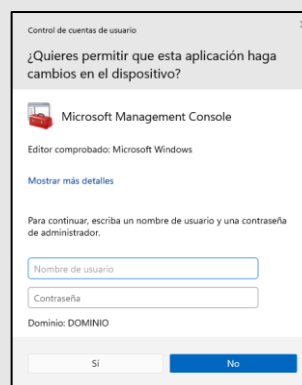


Ilustración 365 - Control de cuentas de usuario

119. Pulse sobre la entidad de certificación raíz con clic derecho y pulse sobre “Enviar solicitud nueva...”

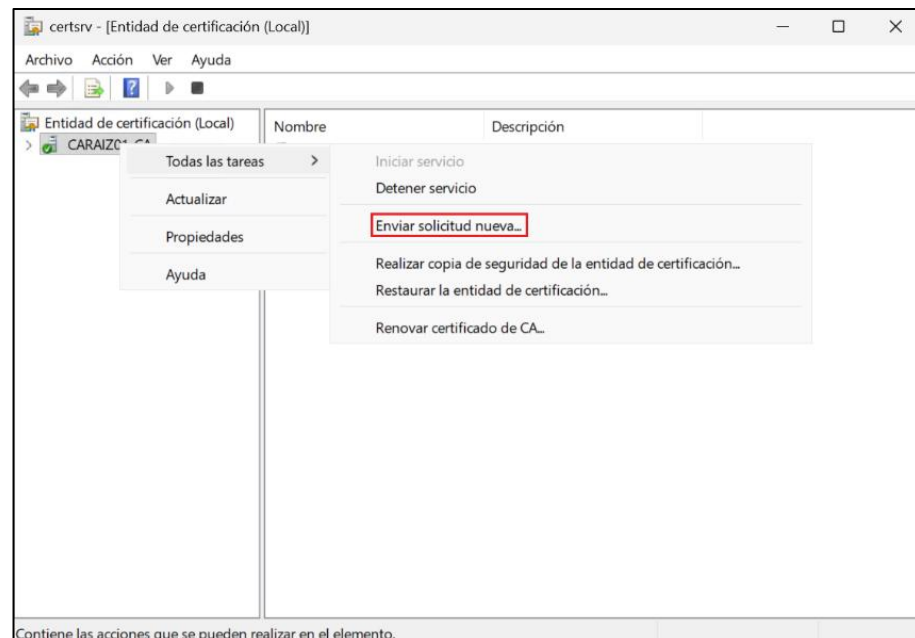


Ilustración 366 – Enviar solicitud nueva

120. Seleccione el archivo “.req” copiado en pasos anteriores. A continuación, pulse sobre el botón “Abrir”.

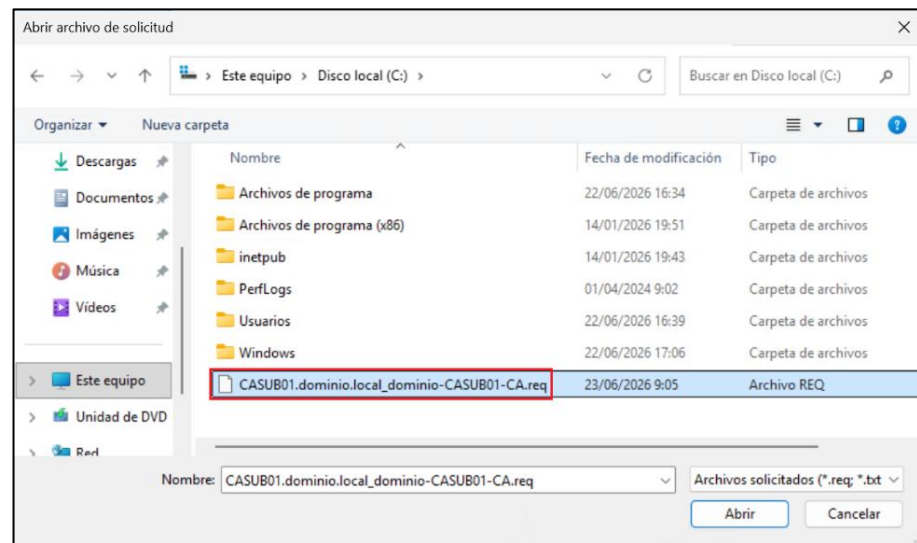


Ilustración 367 – Selección de archivo de solicitud

121. A continuación, desplácese hasta “Solicitudes pendientes”. Dentro se habrá creado una nueva solicitud, pulse sobre ella con clic derecho y pulse en “Todas las tareas > Emitir”.

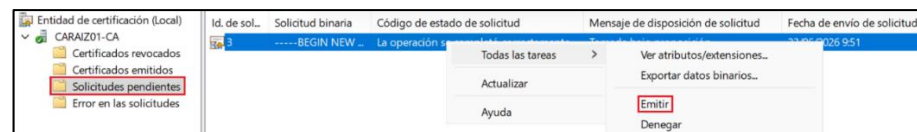


Ilustración 368 – Enviar solicitud

122. Desplácese hasta “Certificados emitidos” y sobre el certificado que aparece, pulse con clic derecho en “Abrir”.

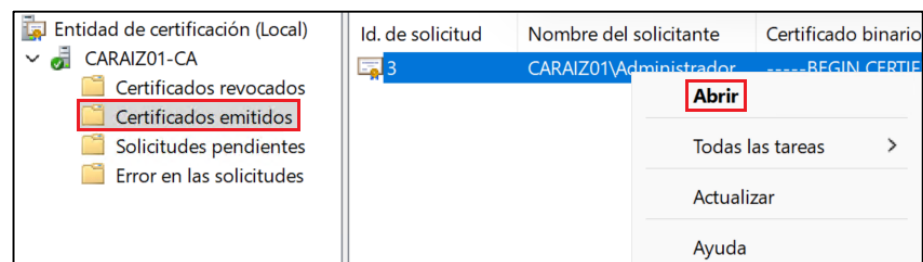


Ilustración 369 – Abrir certificado

123. Sobre la pestaña “Detalles”. Pulse en “Copiar en archivo...” para llevar a cabo la exportación del certificado.

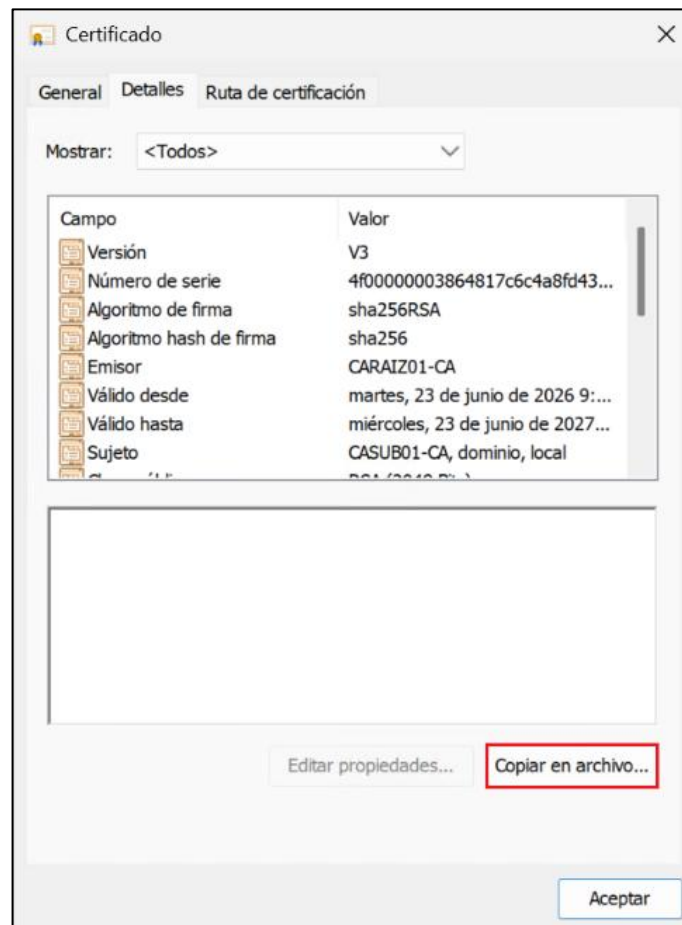


Ilustración 370 – Copia en archivo

124. Seleccione el formato de “DER binario codificado X.509 (.CER)” y pulse en “Siguiente”.

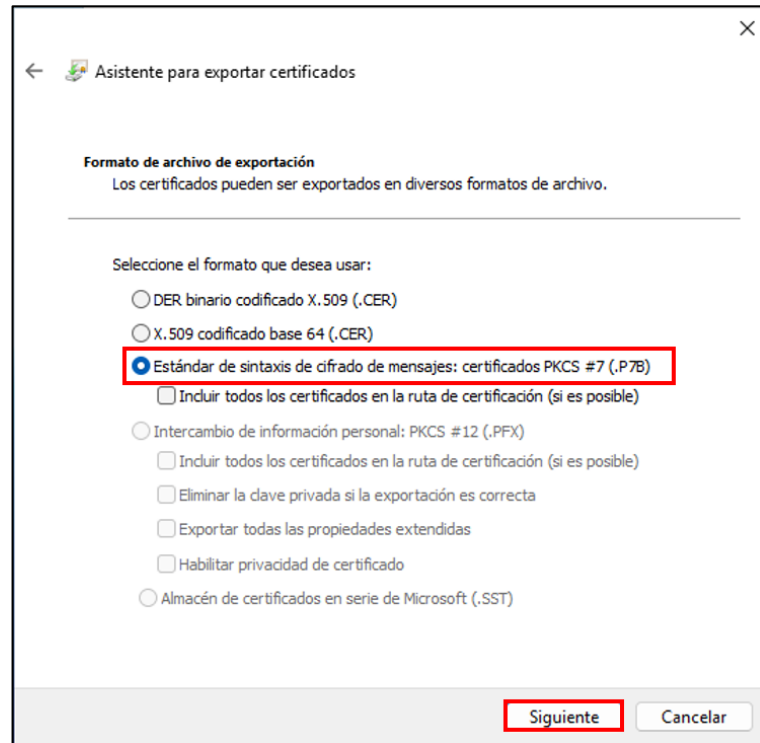


Ilustración 371 - Selección de formato del certificado

125. Haga clic sobre el botón “Examinar”.

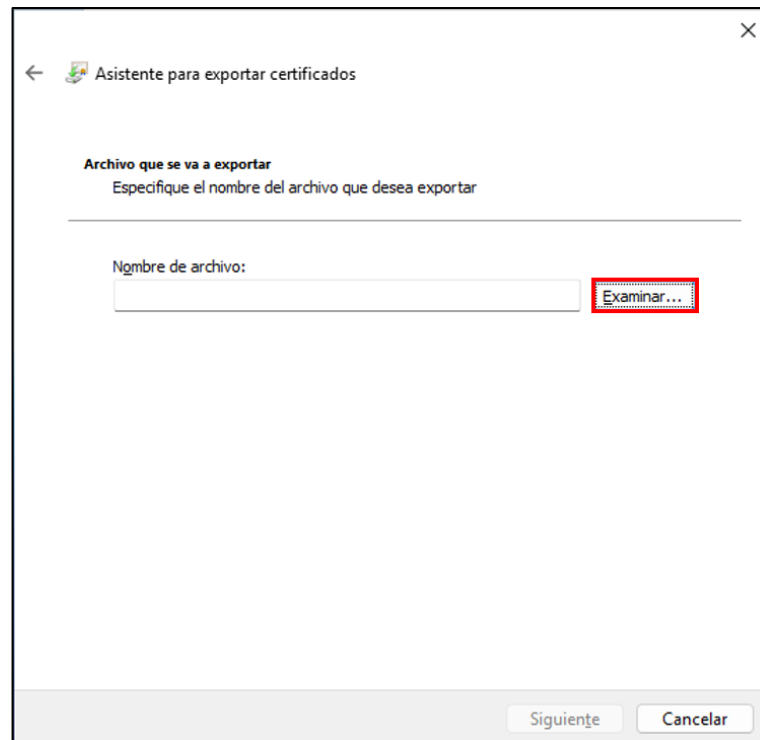


Ilustración 372 - Examinar ruta para almacenar el certificado

126. A continuación, navegue a una ruta accesible e introduzca un nombre de certificado para la exportación del fichero. En este caso, "SUBCA-Cert". Para continuar, pulse en "Guardar".

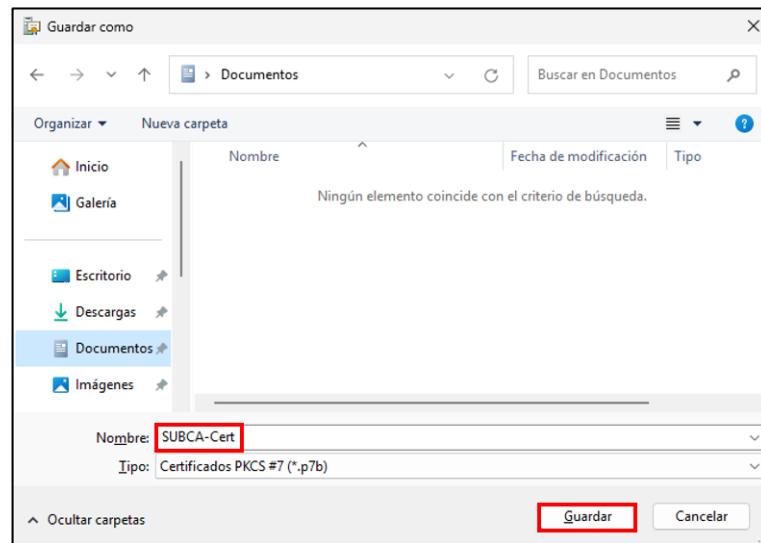


Ilustración 373 - Guardar certificado

127. Pulse en "Siguiente" para continuar con el asistente.

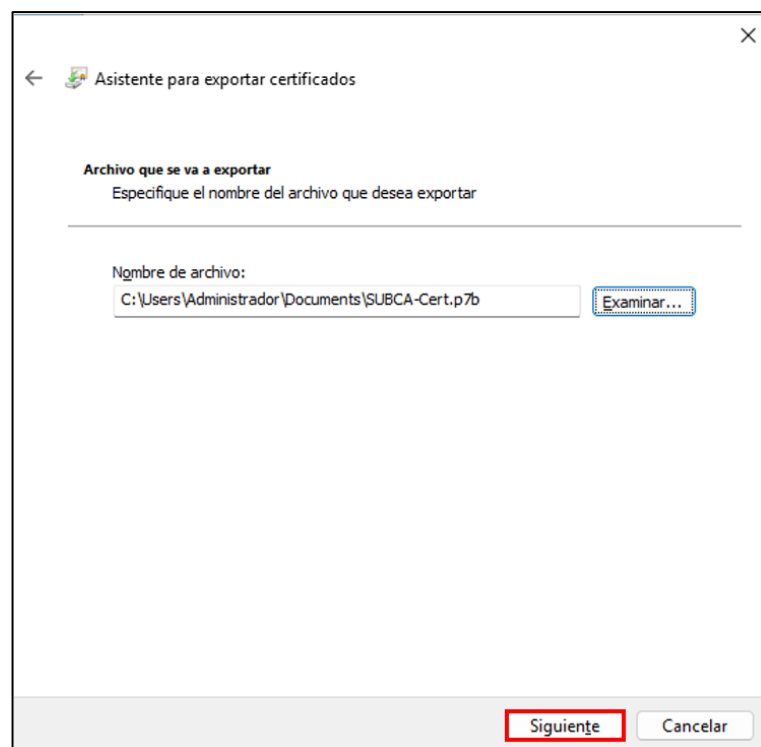


Ilustración 374 - Continuar con el asistente de exportación de certificados

128. Pulse en “Finalizar”.

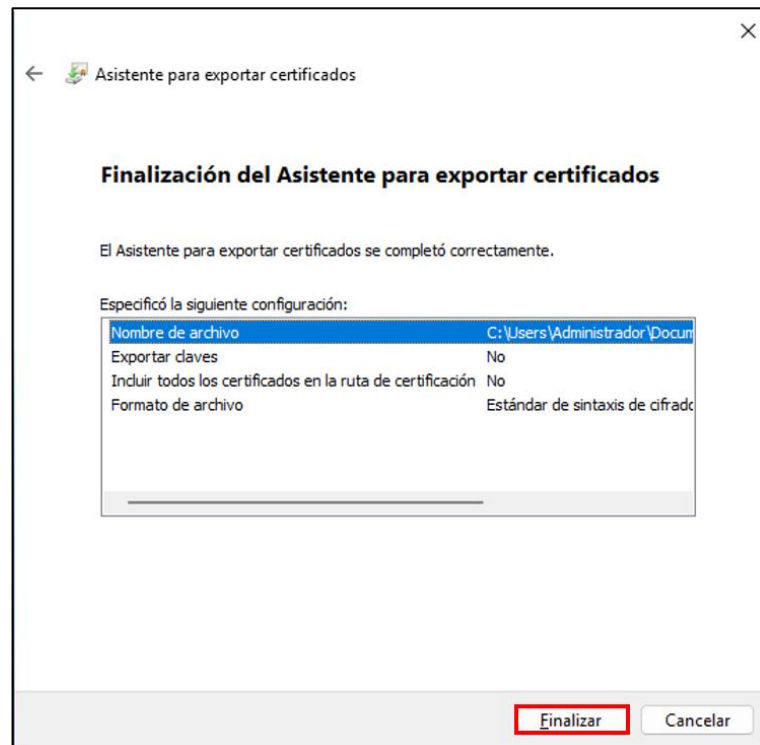


Ilustración 375 - Finalizar la exportación

129. Para terminar el proceso, pulse sobre el botón “Aceptar”.

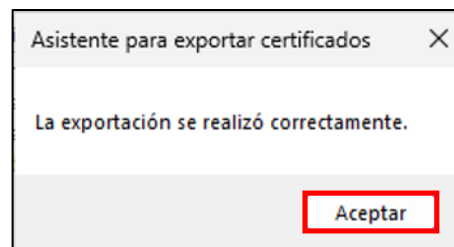


Ilustración 376 - Finalizar proceso

130. A continuación, pulse en “Aceptar” para cerrar las propiedades del certificado de CA Subordinada.

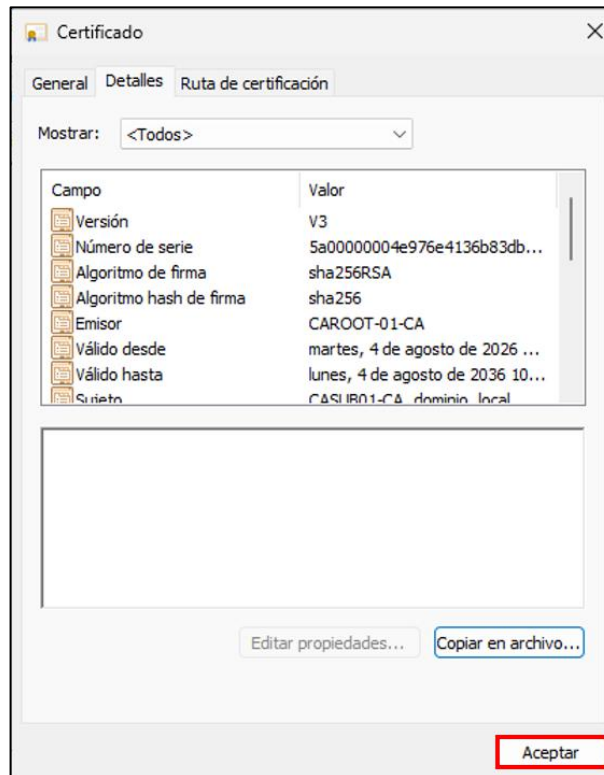


Ilustración 377 - Cerrar el certificado

131. Seguidamente, en el “Explorador de archivos”, desplácese a la ruta C:\Windows\System32\CertSrv\CertEnroll\ y copie todos los archivos al directorio donde se ha almacenado el certificado exportado en los pasos anteriores. En este caso, C:\Users\Administrador\Documentos.

- Certificados de CA Raíz.
- Lista de revocación.

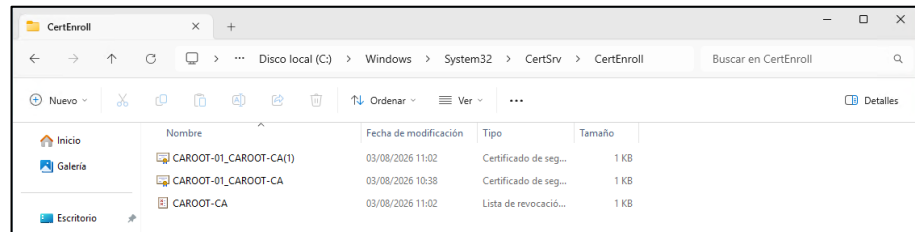


Ilustración 378 - Carpeta origen: CertEnroll

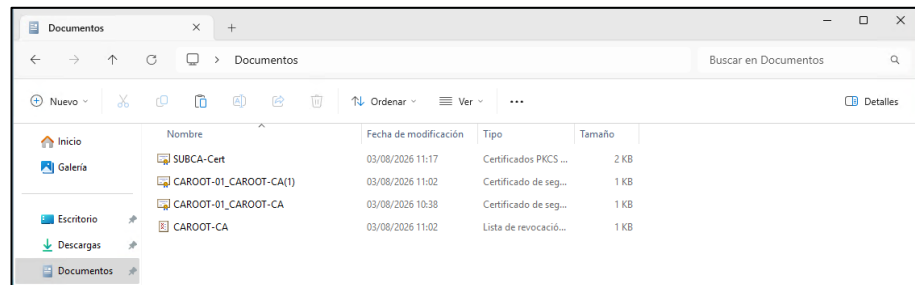


Ilustración 379 - Carpeta destino: Documentos

132. A continuación, copie todos los ficheros de la carpeta documentos al servidor Entidad de Certificación Subordinada en dominio siguiendo los procedimientos operativos de seguridad establecidos.

Nota: Una vez copiados los ficheros, la entidad de certificación independiente podrá ser apagada.

133. Inicie sesión en el servidor Entidad de Certificación subordinada del dominio con un usuario con privilegios de administración.

134. Almacene los archivos que ha copiado de la entidad de certificación raíz en la ruta “C:\Windows\System32\CertSrv\CertEnroll\”.

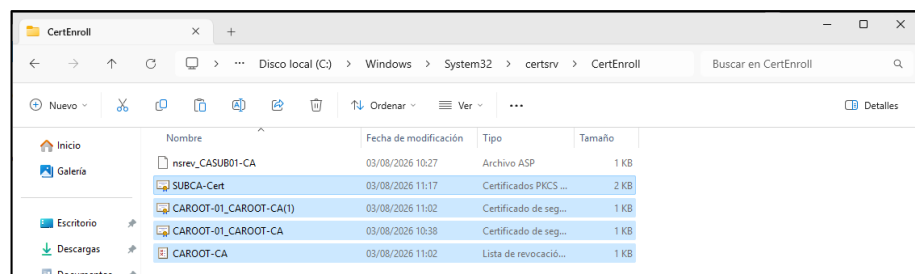


Ilustración 380 - Pegar los ficheros en CertEnroll

135. A continuación, desde la consola de “Administración del servidor”, inicie el “Administrador de Internet Information Services (IIS)” en la sección “Herramientas”.

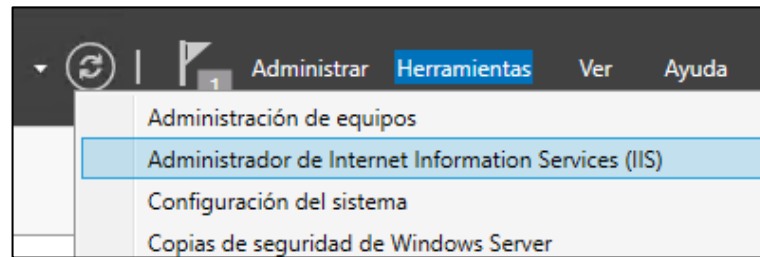


Ilustración 381 - Consola de administración de IIS

136. En el apartado de “Conexiones”, navegue hasta “CertEnroll”, y haga doble clic sobre “Autenticación”.

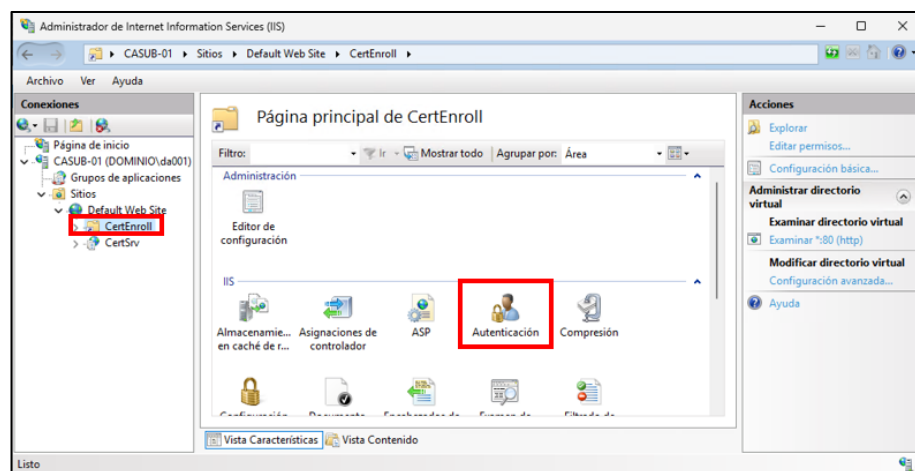


Ilustración 382 - Autenticación en CertEnroll

137. Confirme que la autenticación anónima se encuentra habilitada.

Autenticación		
Agrupar por: Sin agrupar		
Nombre	Estado	Tipo de respuesta
Autenticación anónima	Habilitada	
Autenticación de Windows	Deshabilitada	Desafío - HTTP 401
Suplantación de ASP.NET	Deshabilitada	

Ilustración 383 - Autenticación anónima habilitada

138. Para continuar, confirme que el directorio CertEnroll está vinculado con la carpeta “C:\Windows\System32\CertSrv\CertEnroll”, y que se encuentran los ficheros almacenados en los pasos anteriores. Para ello, pulse con el botón derecho sobre “CertEnroll” y seleccione “Explorar”.

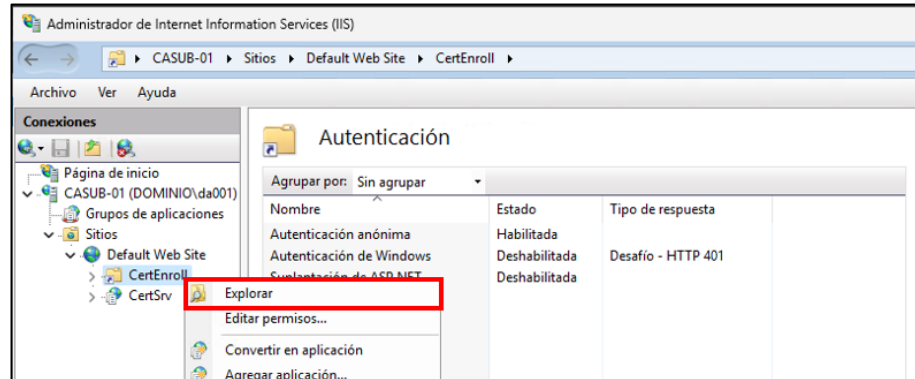


Ilustración 384 - Explorar ruta de CertEnroll en IIS

139. La carpeta mostrará los ficheros almacenados.

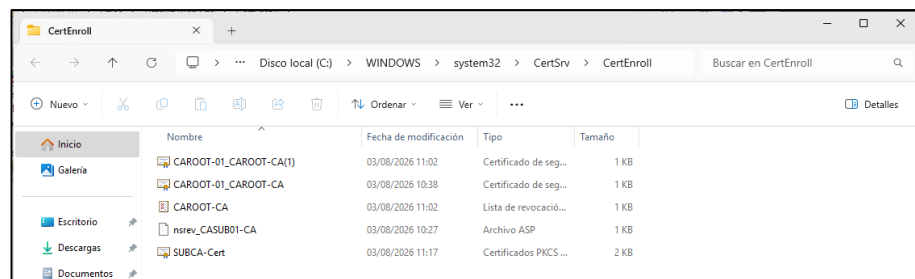


Ilustración 385 - Ruta de CertEnroll

140. Puede cerrar el explorador de archivos y la consola de administración de IIS.

141. A continuación, se importará el certificado emitido desde la CA Raíz. Sobre la barra de búsqueda, escriba “certsrv.msc”.

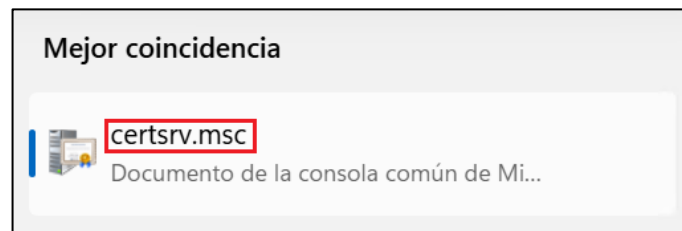


Ilustración 386 – Ejecución de consola de Entidad de certificación

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

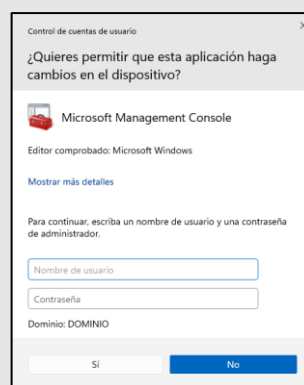


Ilustración 387 - Introducir credenciales de administrador

142. Pulse con clic derecho en “CASUB01-CA” y seleccione “Todas las tareas > Instalar el certificado de CA...”

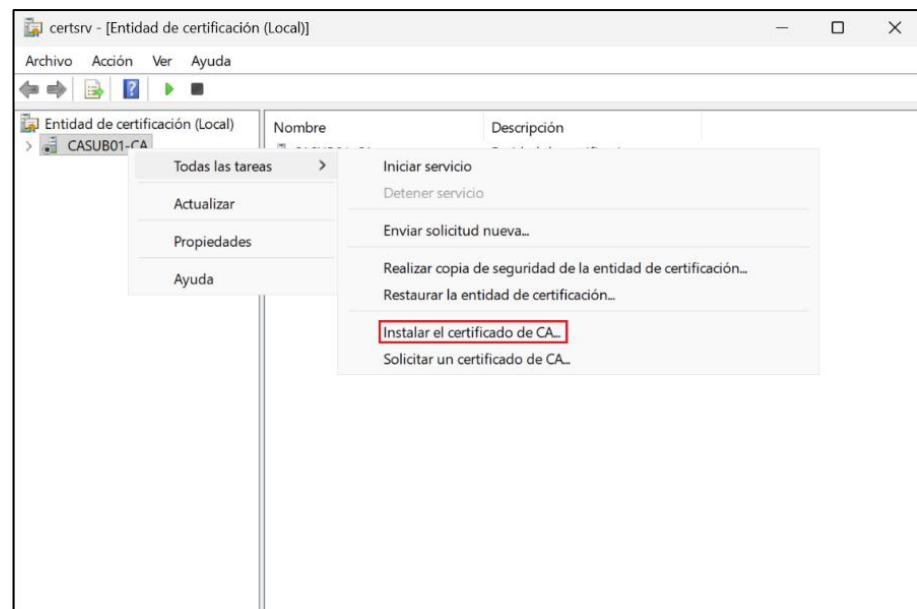


Ilustración 388 – Instalar el certificado de CA

143. Desplácese hasta la ruta donde se encuentran los archivos y seleccione “SUBCA-Cert” y pulse en “Abrir”.

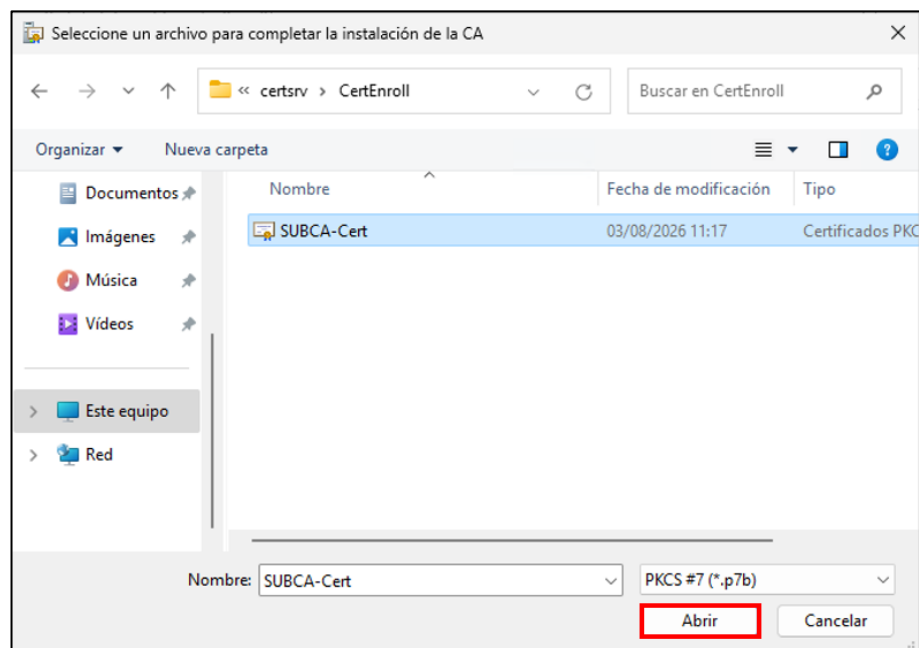


Ilustración 389 - Selección de certificado de CA Subordinada

144. Le aparecerá la siguiente ventana emergente, pulse en “Aceptar”.



Ilustración 390 - Aceptar la confianza en el certificado ROOT

145. Pulse sobre “CASUB01-CA” con clic derecho y seleccione “Todas las tareas > Iniciar servicio”.

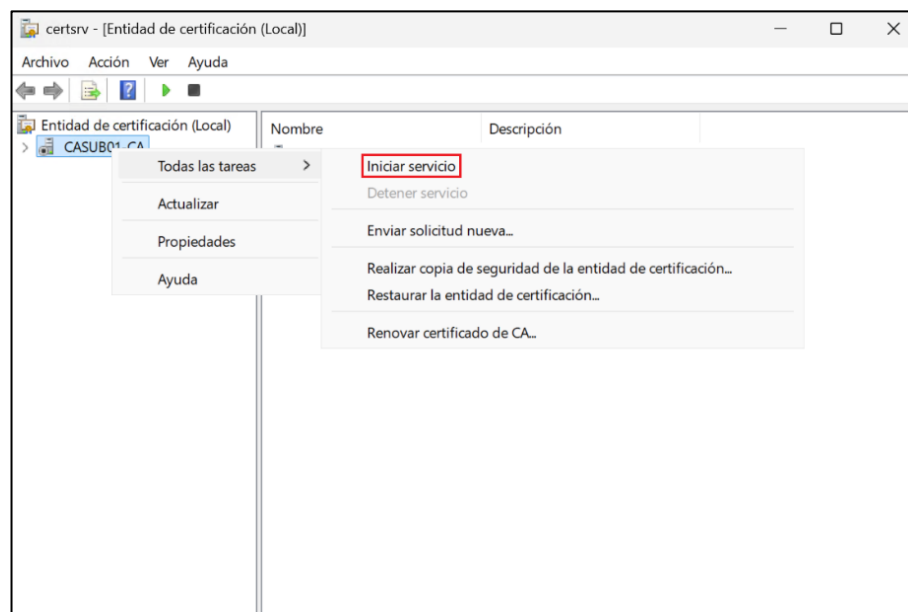


Ilustración 391 – Iniciar servicio

146. Si la configuración es correcta, el servicio iniciará con normalidad.

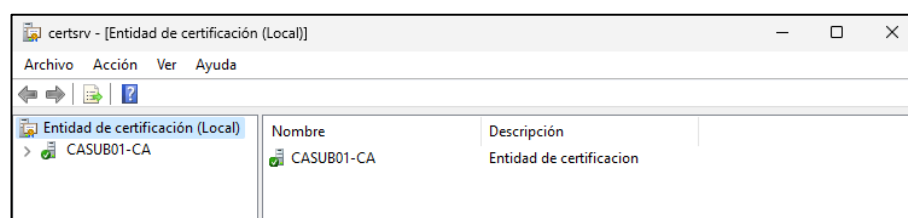


Ilustración 392 - Consola de administración de CA Subordinada

147. A continuación, pulse con el botón derecho sobre la entidad de certificación subordinada y seleccione “Propiedades”.

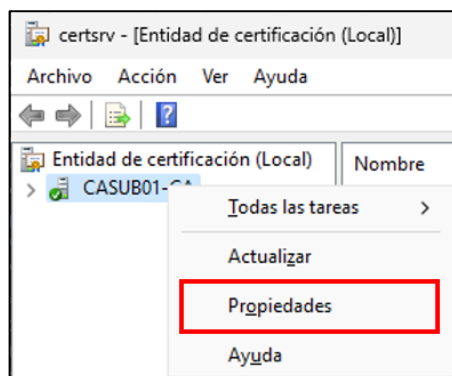


Ilustración 393 - Propiedades de CA Subordinada

148. Diríjase a la pestaña “Extensiones” y, manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, revise la publicación de CRLs mediante la ruta local seleccionando “C:\Windows\System32\CertSrv\CertEnroll\

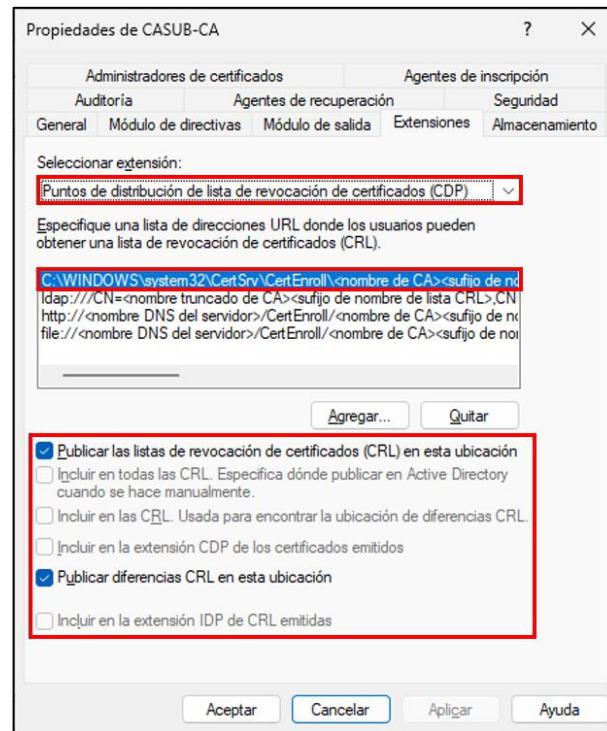


Ilustración 394 - Configuración de CDP

149. A continuación, deshabilite la publicación de CRLs mediante LDAP seleccionando “ldap://CN=<nombre truncado de CA>< sufijo de nombre de lista CRL>,CN=nombre corto del servidor>,CN=CDP,CN=Public Key Services,<contenedor de configuración><clase de objeto CDP>” y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.

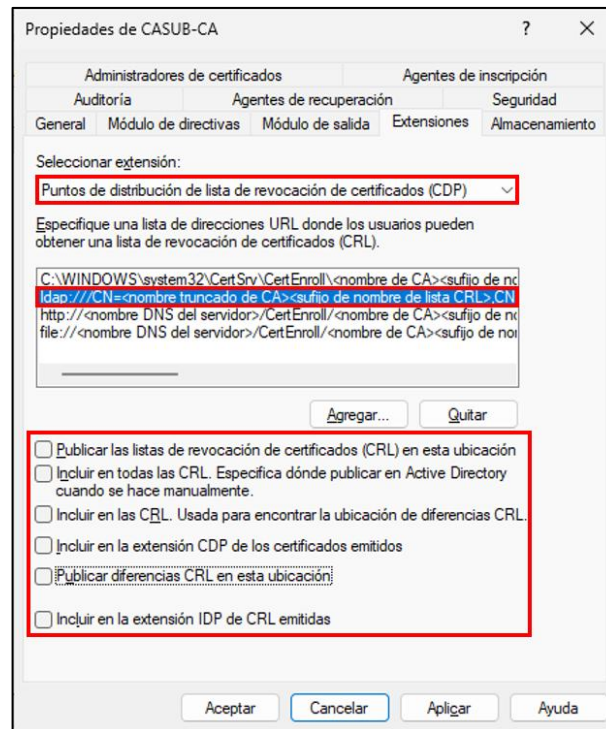


Ilustración 395 - Configuración de LDAP

150. Seleccione “file://<nombre DNS del servidor>/CertEnroll/<nombre de CA>/sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y confirme que todas las opciones se encuentran como muestra la siguiente figura.

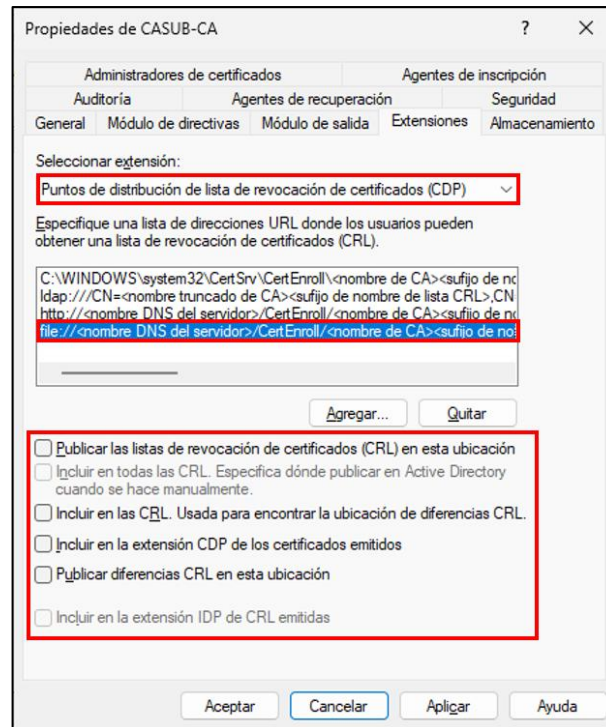


Ilustración 396 - Configuración de extensión file

151. De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de nombre de lista CRL><diferencias entre listas CRL permitidas>.crl” y pulse “Control + C”, para copiar el objeto.

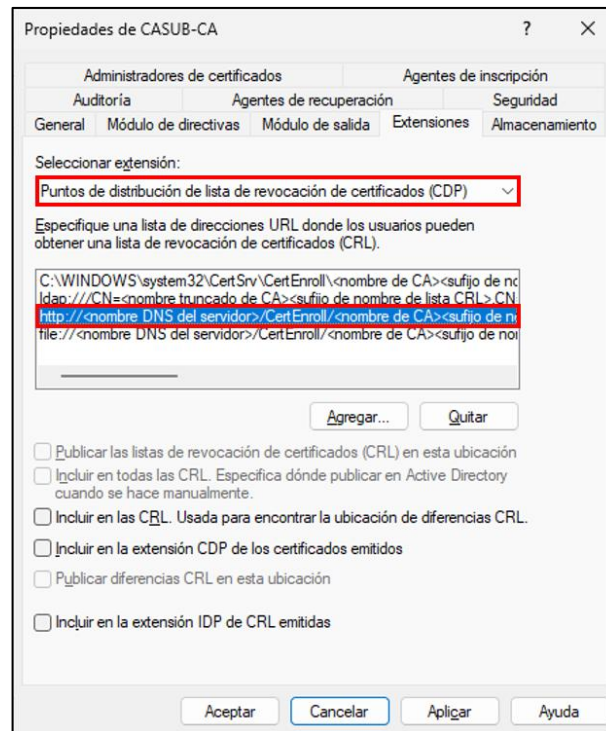


Ilustración 397 - Copiar extensión http

A continuación, pulse en “Agregar”.

152. En el campo “Ubicación”, pegue la ruta copiada en el paso anterior.

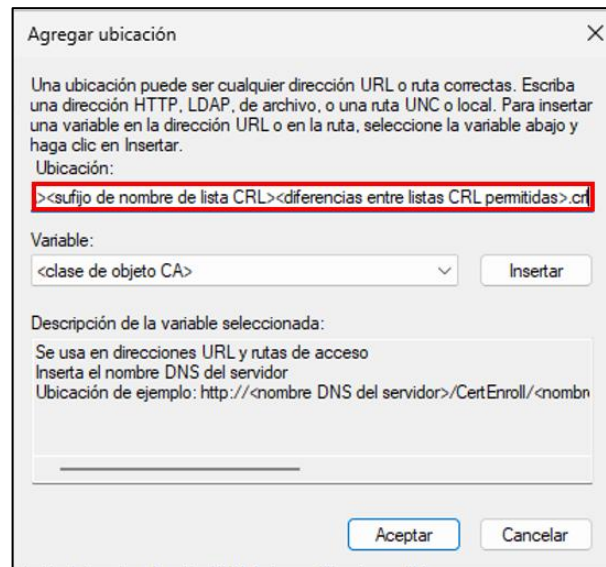
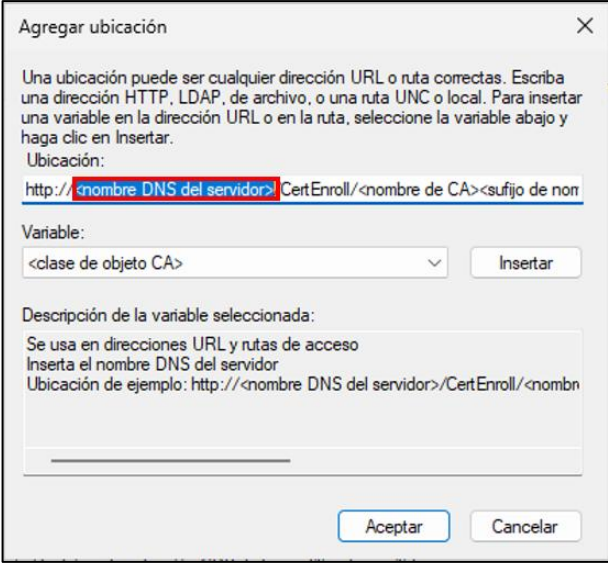


Ilustración 398 - Pegar nueva ubicación de extensión

Nota: No pulse todavía sobre el botón “Aceptar”.

153. Sustituya “<Nombre del servidor>” por el CNAME correspondiente a la entidad subordinada de certificación.



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://<nombre DNS del servidor>/CertEnroll/<nombre de CA>< sufijo de non

Variable:

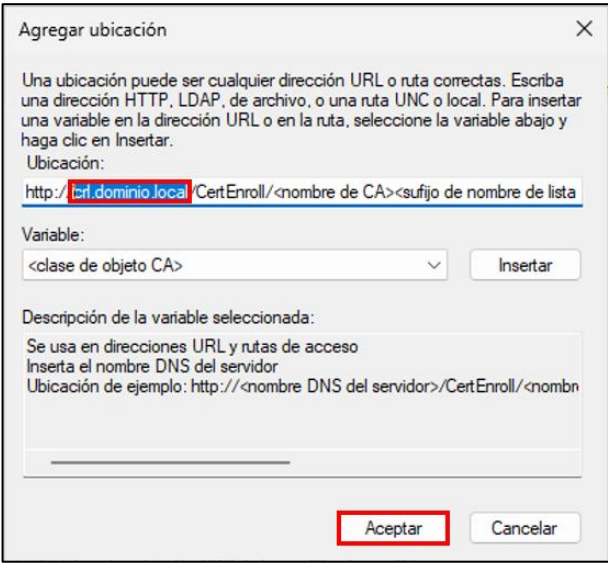
<clase de objeto CA> Insertar

Descripción de la variable seleccionada:

Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 399 - Sustituir nombre DNS



Agregar ubicación

Una ubicación puede ser cualquier dirección URL o ruta correctas. Escriba una dirección HTTP, LDAP, de archivo, o una ruta UNC o local. Para insertar una variable en la dirección URL o en la ruta, seleccione la variable abajo y haga clic en Insertar.

Ubicación:

http://<cert.dominio.local>/CertEnroll/<nombre de CA>< sufijo de nombre de lista

Variable:

<clase de objeto CA> Insertar

Descripción de la variable seleccionada:

Se usa en direcciones URL y rutas de acceso
Inserta el nombre DNS del servidor
Ubicación de ejemplo: http://<nombre DNS del servidor>/CertEnroll/<nombr

Aceptar Cancelar

Ilustración 400 - DNS con la configuración CNAME correcta

A continuación, pulse en “Aceptar”.

154. Marque las opciones como muestra la siguiente ilustración.

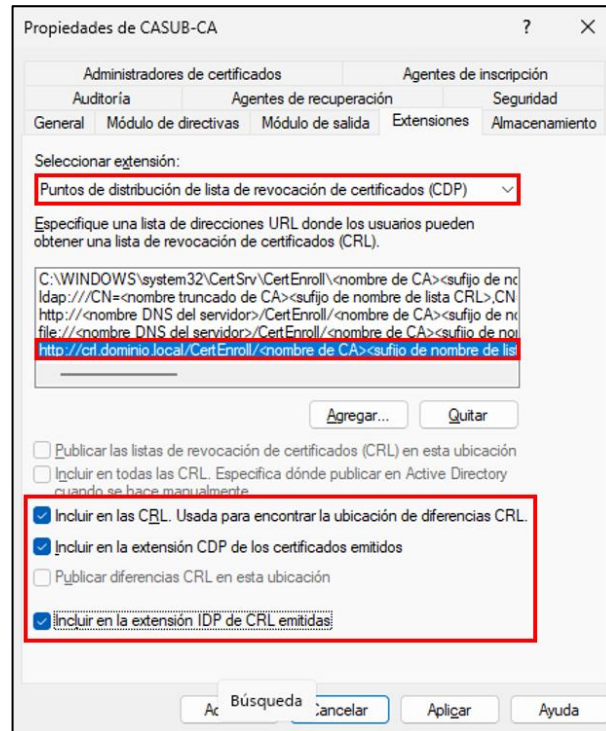


Ilustración 401 - Configuración de la nueva extensión

155. A continuación, seleccione la extensión “Acceso a la información de entidad (AIA)” en el desplegable.



Ilustración 402 - Cambio de extensión a AIA

156. Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\

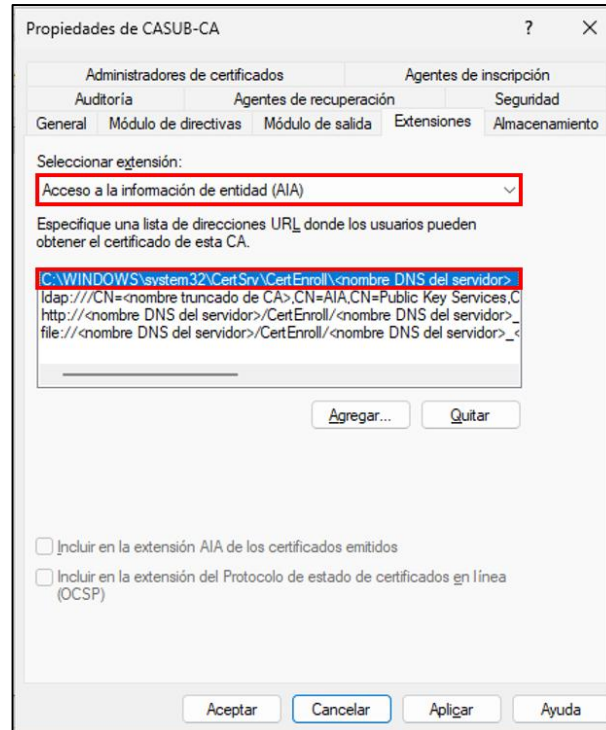


Ilustración 403 - Comprobación de extensión

157. A su vez, desmarque en el objeto “ldap://CN=<nombre truncado de CA>,CN=AIA,CN=Public Key Services,CN=Services,<contenedor de configuración><clase de objeto CA>” todas las casillas.

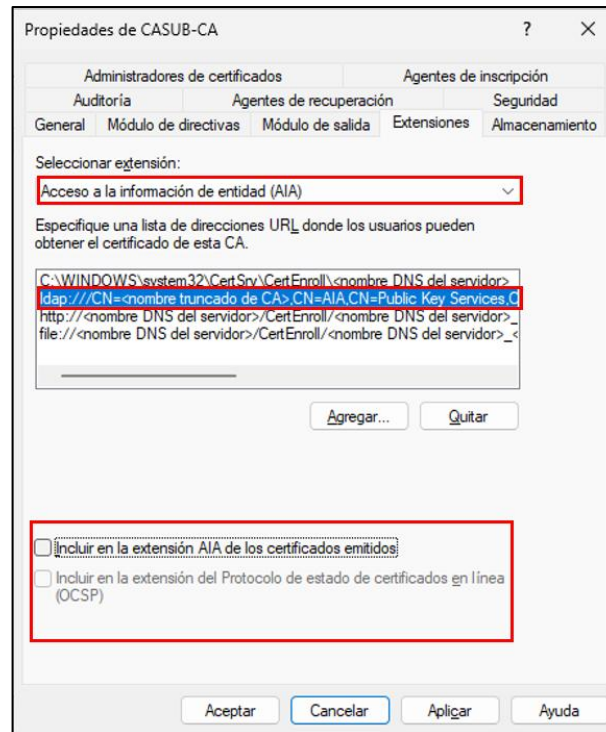


Ilustración 404 - Configuración de extensión LDAP

158. Seleccione ahora “file://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y compruebe que todas las casillas se encuentran desmarcadas.

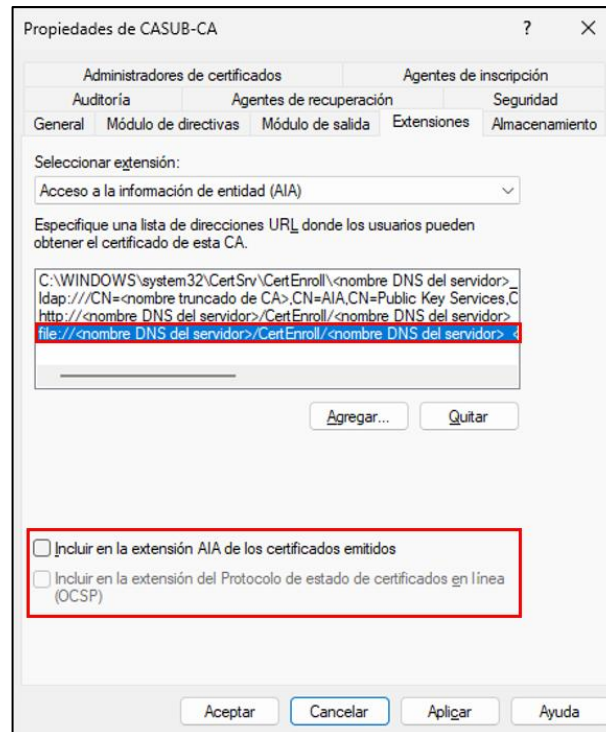


Ilustración 405 - Comprobación de extensión file

159. Seleccione “http://<nombre DNS del servidor>/CertEnroll/<nombre DNS del servidor>_<nombre de CA><nombre de certificado>.crt” y copie el elemento mediante la combinación de teclas “Control + C”.

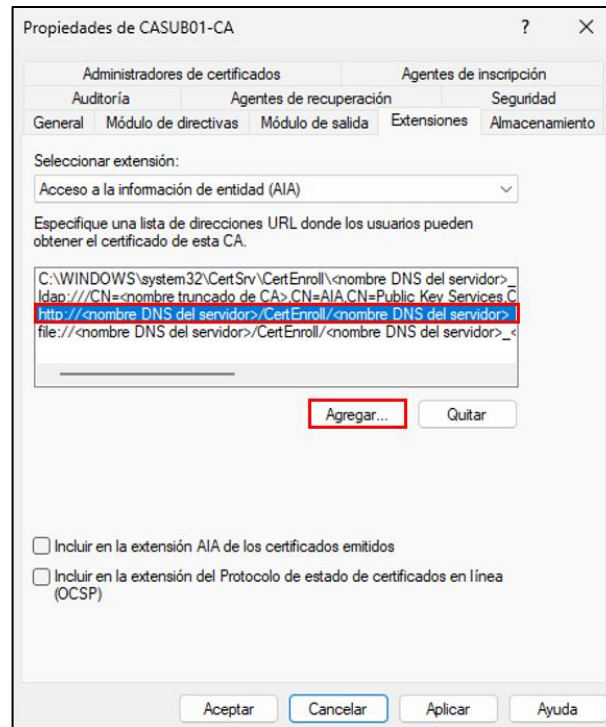


Ilustración 406 - Configuración de nueva extensión http

A continuación, pulse en “Agregar”.

160. Pegue en el campo de ubicación la ruta anterior.

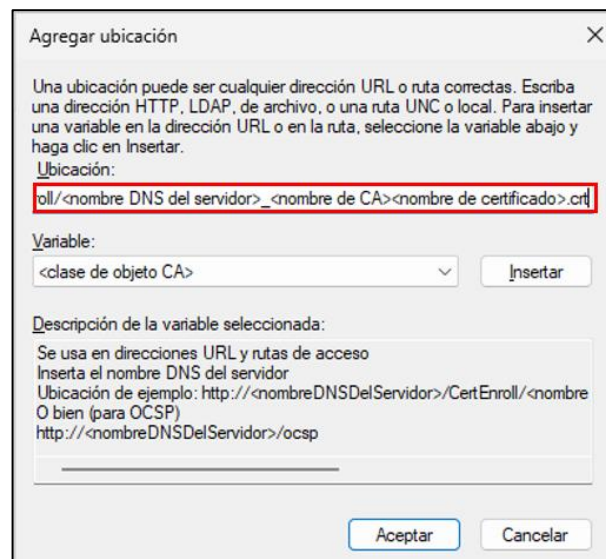


Ilustración 407 - Pegar la ruta de la nueva extensión

Nota: No pulse todavía “Aceptar”.

161. Sustituya “<nombre DNS del servidor>” por el CNAME generado al inicio de este procedimiento. A continuación, pulse en “Aceptar”.

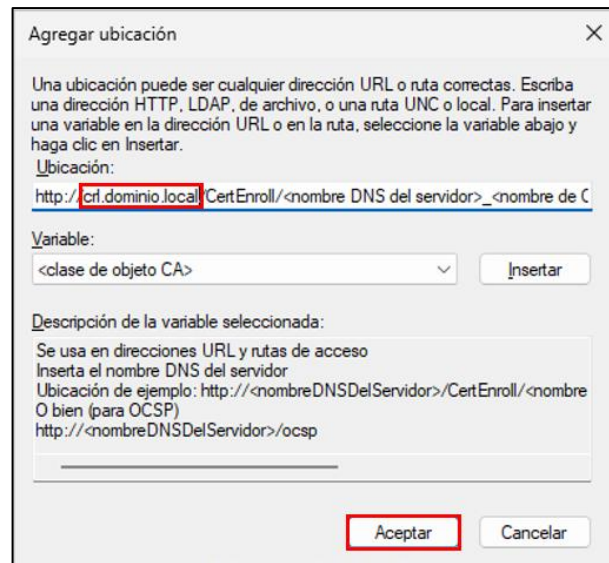


Ilustración 408 - Modificar ruta de la extensión

162. A continuación, marque la opción “Incluir en la extensión AIA de los certificados emitidos”.

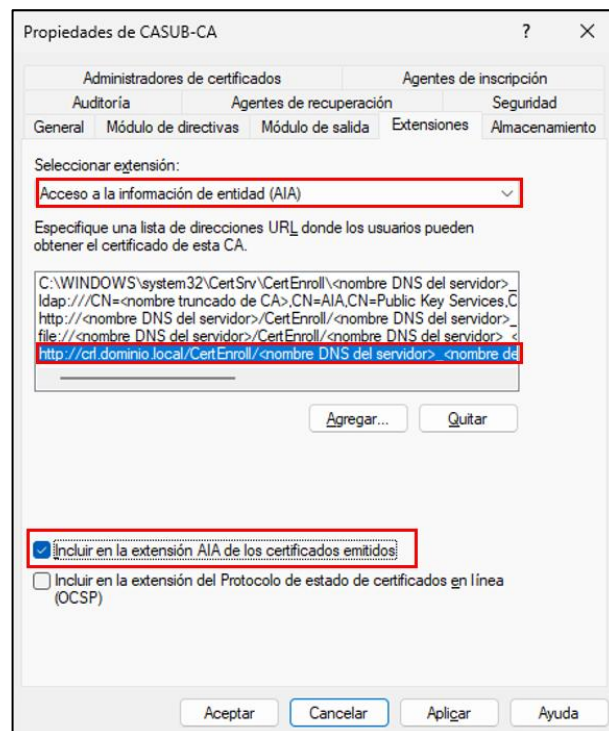


Ilustración 409 - Configuración de extensión http

163. Haga clic sobre “Aplicar” y “Aceptar”. A continuación, el servicio solicitará reiniciarse. Pulse en “Sí” para finalizar con esta configuración.

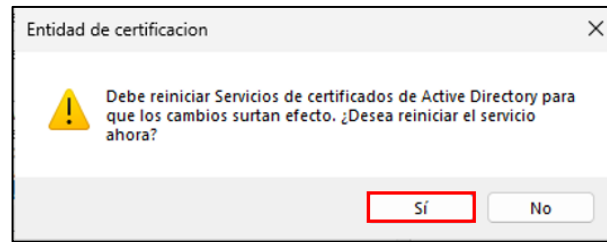


Ilustración 410 - Reiniciar el servicio

164. Por último, publique de nuevo la lista de revocación haciendo clic derecho sobre Certificados Revocados, y a continuación, pulse en “Todas las tareas > Publicar”.

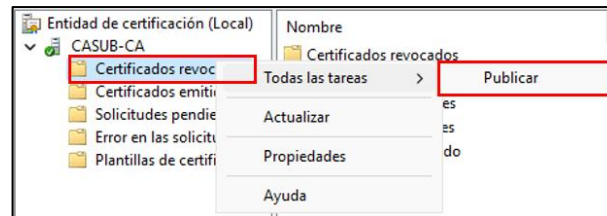


Ilustración 411 - Publicar nueva CRL

165. En el asistente, mantenga la “Lista de revocación de certificados (CRL) nueva” y pulse en Aceptar.

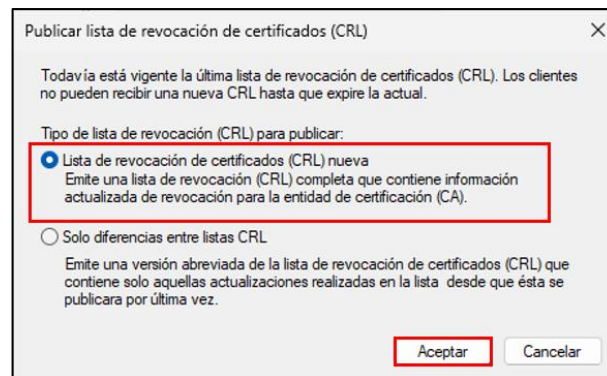


Ilustración 412 - Publicar nueva lista de revocación de certificados

166. Una vez finalizado todo el proceso, será necesario propagar el certificado de la entidad de certificación raíz en el dominio, ya que el resto de equipos no tienen confianza en ella. Para llevarlo a cabo, en la entidad de certificación subordinada, ejecute “PowerShell”.

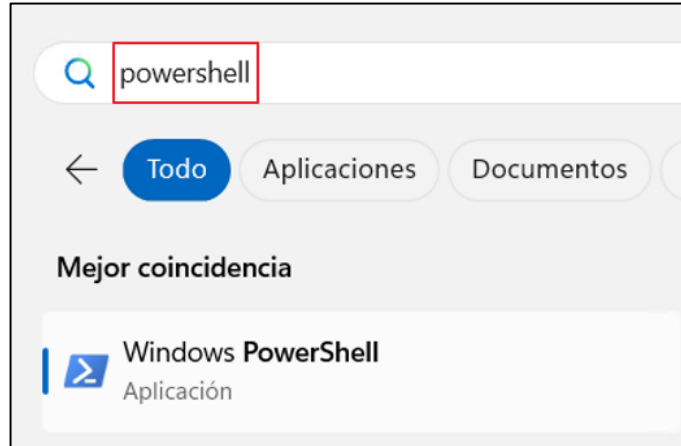


Ilustración 413 – Ejecución de Powershell

A continuación, seleccione “Ejecutar como administrador”.

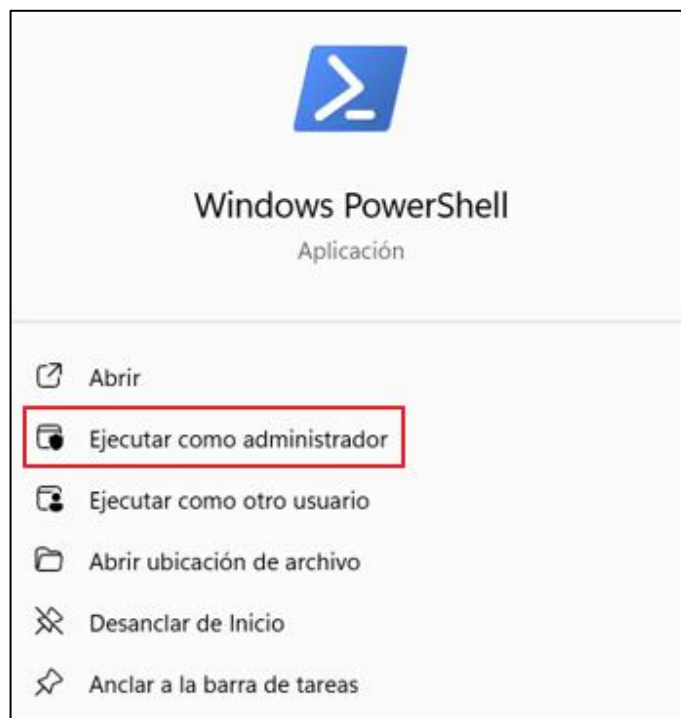


Ilustración 414 – Ejecutar como administrador

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

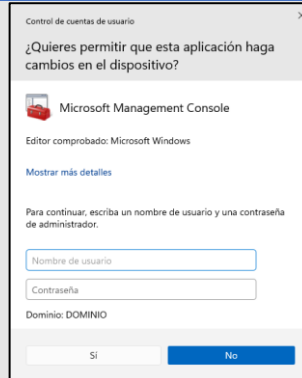


Ilustración 415 - Introducir credenciales de administrador

167. Desplácese a la ruta "C:\Windows\System32\certsrv\CertEnroll" con el comando "cd".

```
PS C:\WINDOWS\system32> cd C:\Windows\System32\certsrv\CertEnroll
```

Ilustración 416 - Acceder a la ruta CertEnroll

168. Ejecute el comando "dir" para visualizar los elementos del directorio.

```
PS C:\windows\system32\certsrv\CertEnroll> dir

Directorio: C:\windows\system32\certsrv\CertEnroll

Mode                LastWriteTime         Length Name
----                -
-a----            03/08/2026   11:02             812 CAROOT-01_CAROOT-CA(1).crt
-a----            03/08/2026   10:38             775 CAROOT-01_CAROOT-CA.crt
-a----            03/08/2026   11:02             521 CAROOT-CA.crl
-a----            03/08/2026   11:49          1051 CASUB-01.dominio.local_CASUB01-CA.crt
-a----            03/08/2026   12:13             587 CASUB01-CA+.crl
-a----            03/08/2026   12:13             642 CASUB01-CA.crl
-a----            03/08/2026   10:27             325 nsrev_CASUB01-CA.asp
-a----            03/08/2026   11:17          1098 SUBCA-Cert.p7b
```

Ilustración 417 - Visualizar elementos del directorio

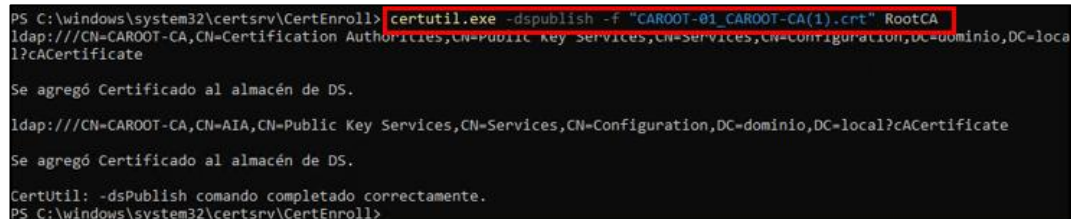
169. Seleccione el certificado de la entidad raíz con nombre "CAROOT-01_CAROOT-CA(1).crt", ya que es el último generado en la entidad de certificación, y copie el contenido pulsando la tecla "Ctrl + C".

```
Directorio: C:\windows\system32\certsrv\CertEnroll

Mode                LastWriteTime         Length Name
----                -
-a----            03/08/2026   11:02             812 CAROOT-01_CAROOT-CA(1).crt
-a----            03/08/2026   10:38             775 CAROOT-01_CAROOT-CA.crt
-a----            03/08/2026   11:02             521 CAROOT-CA.crl
-a----            03/08/2026   11:49          1051 CASUB-01.dominio.local_CASUB01-CA.crt
```

Ilustración 418 - Seleccionar y copiar el nombre del certificado

170. Introduzca el comando “`certutil.exe -dspublish -f "CAROOT-01_CAROOT-CA(1).crt" RootCA`” y a continuación, pulse la tecla “Intro”.



```
PS C:\windows\system32\certsrv\CertEnroll> certutil.exe -dspublish -f "CAROOT-01_CAROOT-CA(1).crt" RootCA
ldap:///CN=CAROOT-CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=dominio,DC=local?cACertificate
Se agregó Certificado al almacén de DS.
ldap:///CN=CAROOT-CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=dominio,DC=local?cACertificate
Se agregó Certificado al almacén de DS.
CertUtil: -dsPublish comando completado correctamente.
PS C:\windows\system32\certsrv\CertEnroll>
```

Ilustración 419 - Ejecución del comando

Nota: Si se desea evitar esta ejecución, es recomendable añadir el certificado de la entidad de certificación raíz en la directiva CCN-STIC-598A25 Incremental Dominio. Para ello, se ha de importar el certificado en la sección “Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de clave pública > Entidades de certificación raíz de confianza”.

171. La nueva entidad de certificación subordinada estará disponible para configurar nuevas plantillas y emitir certificados incluyendo toda la cadena de certificación.
172. Por último, se deberá desvincular o deshabilitar la GPO “CCN-STIC-598A25 Incremental shell remoto”. Para ello, inicie sesión en un controlador de dominio con un usuario perteneciente al grupo “Admins. del dominio”.

173. Inicie la consola “Administrador del servidor” con privilegios de administración.

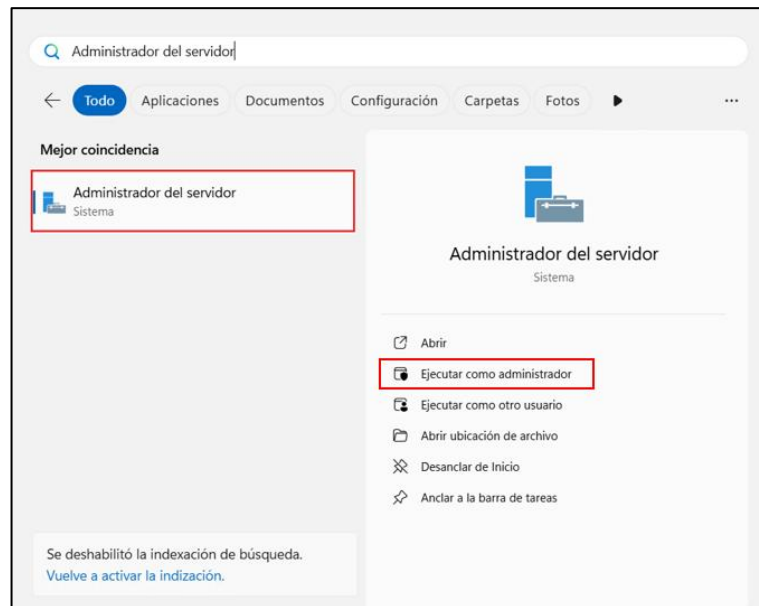


Ilustración 420 - Ejecutar como administrador

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

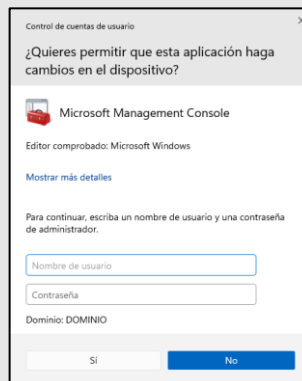


Ilustración 421 - Introducir credenciales de administrador

174. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

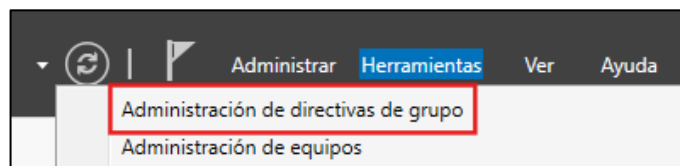


Ilustración 422 - Administración de directivas de grupo

175. Diríjase a la OU “Servidores Entidad de Certificación”, haga clic derecho sobre la GPO “CCN-STIC-598A25 Incremental shell remoto” y haga clic sobre “Vínculo habilitado” para deshabilitar el vínculo”.

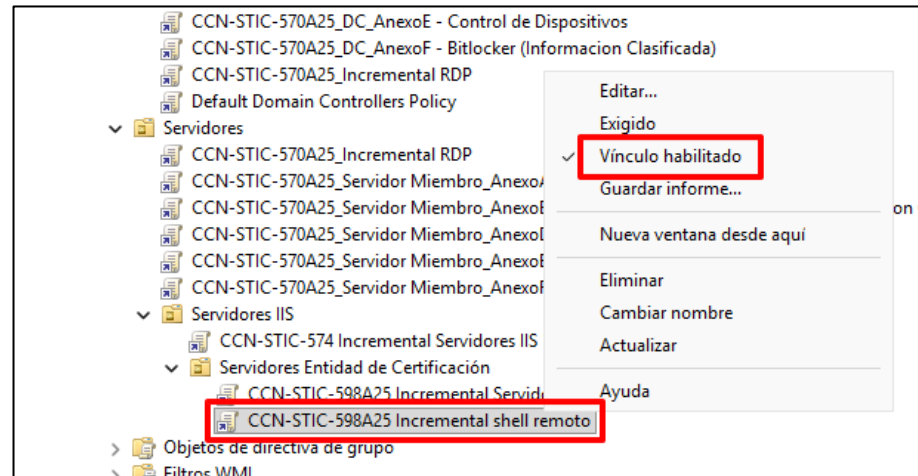


Ilustración 423 - Desvinculación de GPO incremental shell remoto

176. Habrá finalizado la configuración y la jerarquía de entidad de certificación estará disponible para emitir certificados.

6.3.6. PASO A PASO DE FUNCIONAMIENTO

Paso	Descripción
177.	Inicie sesión en un equipo miembro del dominio donde se va a solicitar un certificado.

178. Sobre la barra de búsqueda, escriba “cmd” y seleccione “Ejecutar como administrador”.

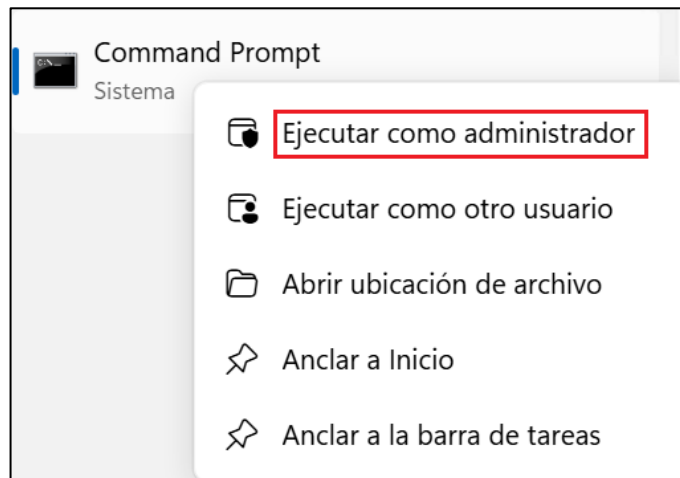


Ilustración 424 – Ejecutar consola

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

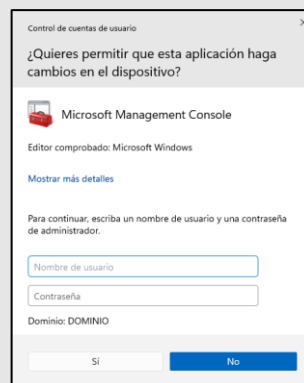


Ilustración 425 - Introducir credenciales de administrador

179. Escriba “gpupdate /force” para actualizar las directivas del dominio. Posteriormente, cierre el terminal.

```
Microsoft Windows [Versión 10.0.26100.32230]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
```

Ilustración 426 – Actualizar directivas del dominio

180. A continuación, sobre la barra de búsqueda escriba “certlm.msc” para ejecutar la consola de certificados.

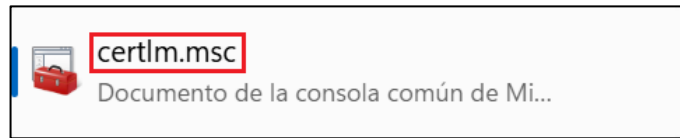


Ilustración 427 – Ejecutar consola de certificados

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

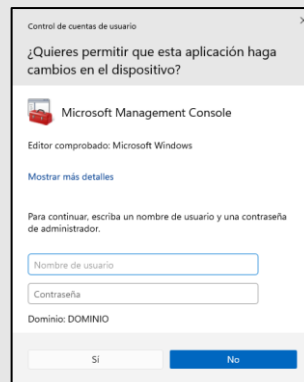


Ilustración 428 - Introducir credenciales de administrador

181. Desplácese hasta “Personal” y seleccione “Todas las tareas > Solicitar un nuevo certificado...”

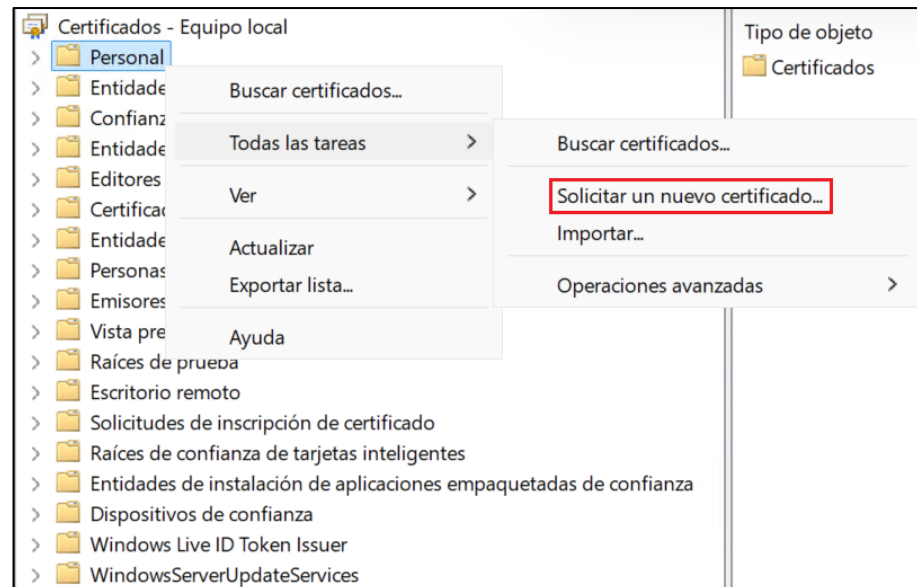


Ilustración 429 – Solicitud de certificado

182. Se ejecutará el asistente de inscripción de certificados y se seleccionará la directiva que aparece en la imagen y pulse en “Siguiente”.

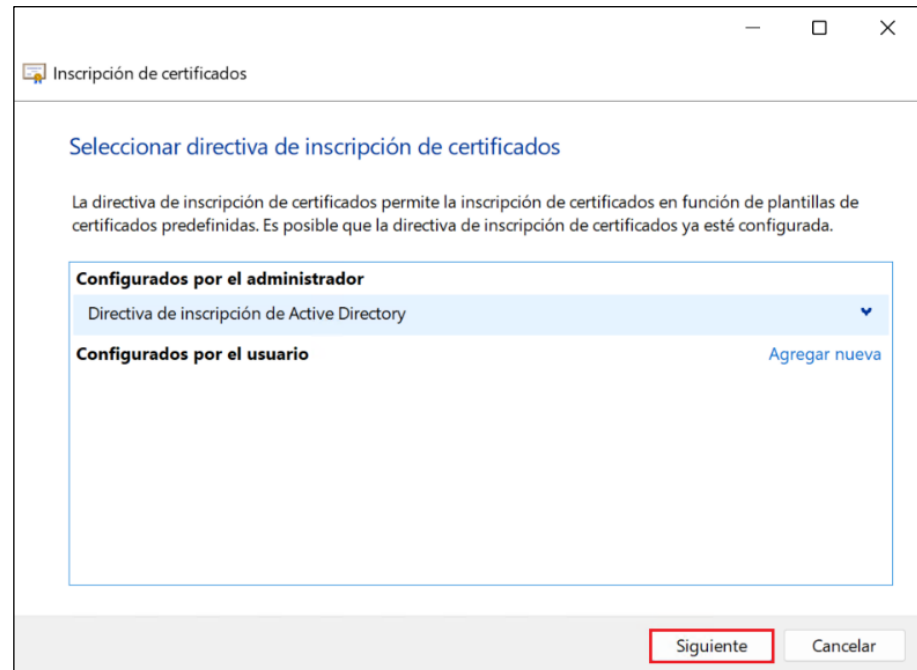


Ilustración 430 – Selección de directiva de inscripción

183. En la siguiente ventana, aparecerá la plantilla configurada como “Equipo” para solicitar un certificado de equipo. Pulse en “Inscribir”.

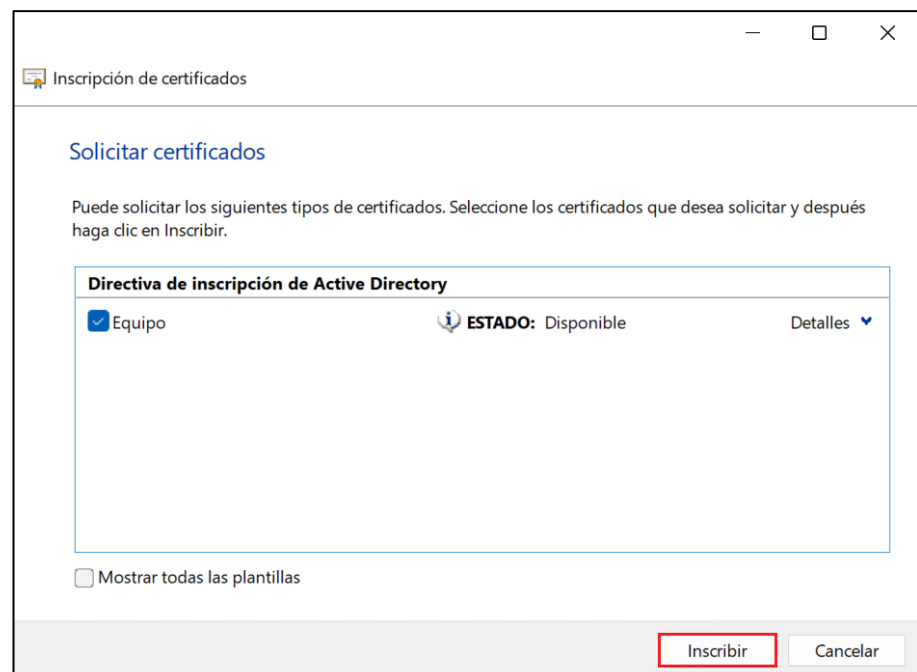


Ilustración 431 – Elegir plantilla de certificado

184. Verá que el estado se encuentra en “Correcto”, finalmente pulse en “Finalizar” y el certificado se habrá creado correctamente.

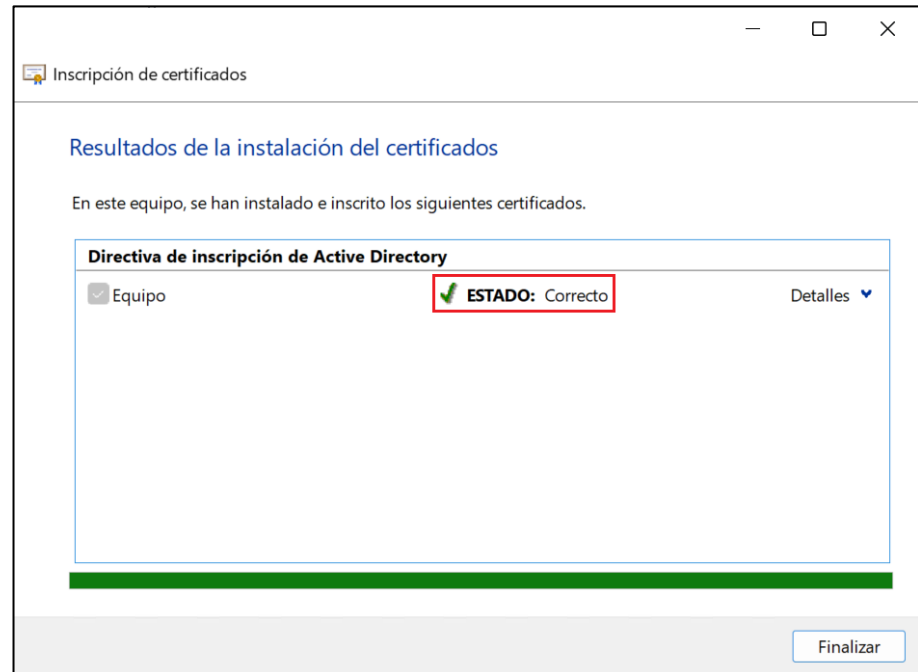
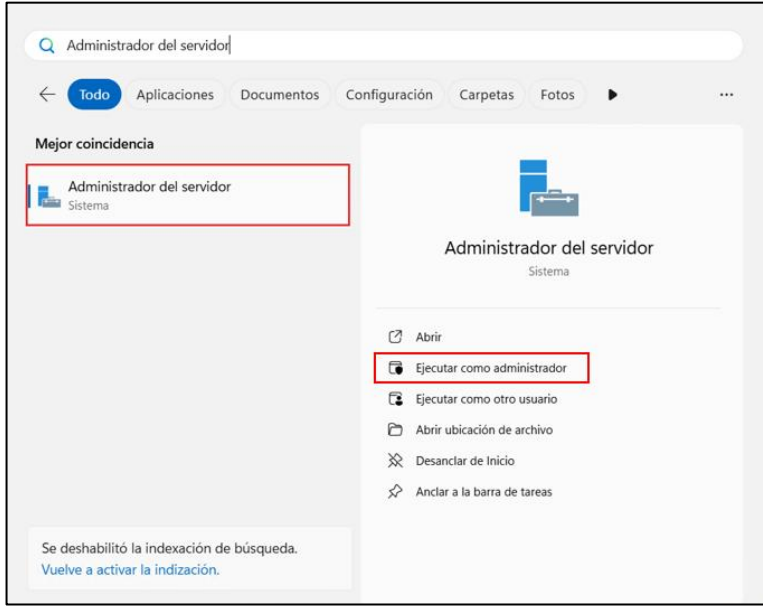
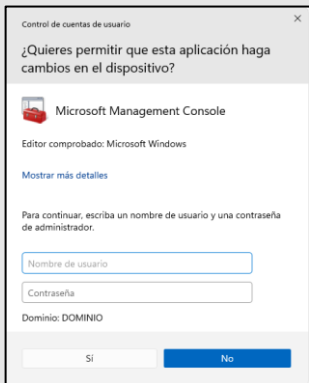


Ilustración 432 – Resultado de instalación del certificado

7. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

7.1. SEGREGACIÓN DE ROLES

Los pasos que se definen a continuación detallarán la creación de grupos de usuario para conceder o denegar permisos sobre los recursos del sistema. Esta configuración es de aplicación tanto para los servidores en dominio como los servidores independientes.

Paso	Descripción
1.	Inicie sesión con un usuario con privilegios en el controlador del dominio del entorno donde se ha configurado la jerarquía PKI.
2.	A continuación, inicie como administrador la consola de “Administrador del servidor”.  <i>Ilustración 433 - Consola de administración del servidor</i> Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 434 - Introducir credenciales de administrador</i>

3. Acceda a “Herramientas > Usuarios y equipos de Active Directory”.

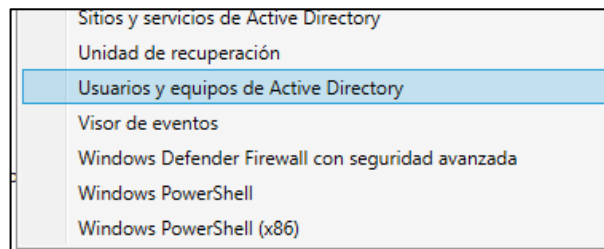


Ilustración 435 - Usuarios y equipos de Active Directory

4. Diríjase a la unidad organizativa donde desee crear el nuevo grupo de seguridad que permitirá la administración de la entidad de certificación.

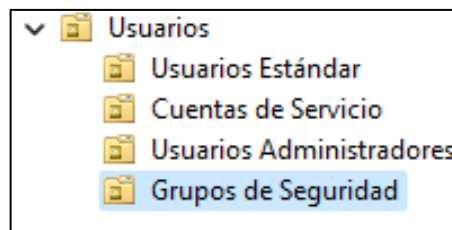


Ilustración 436 - Unidades organizativas del entorno

5. Pulse con el botón derecho sobre la OU, y a continuación, pulse en “Nuevo > Grupo”.

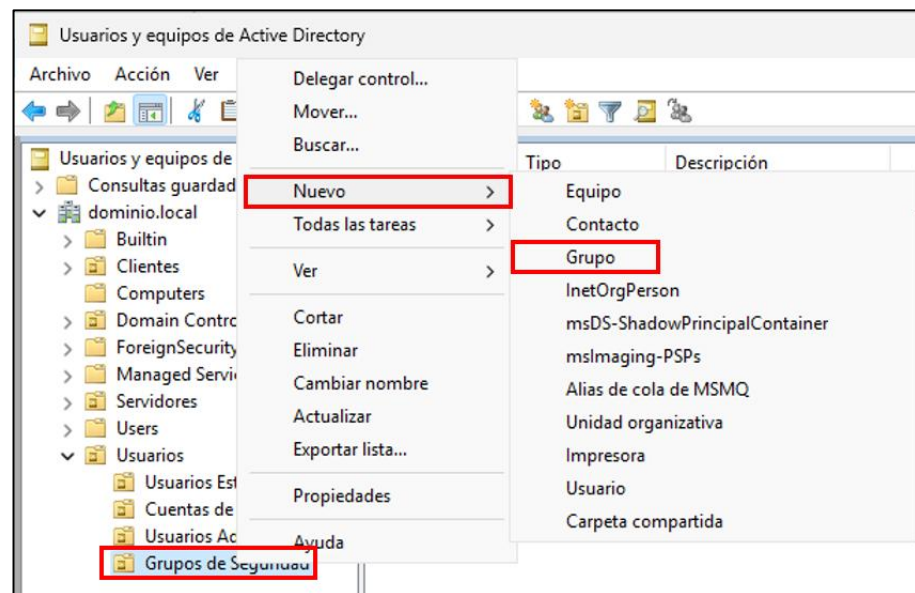


Ilustración 437 - Crear nuevo grupo

6. Indique un nombre orientativo para la administración de la entidad y a continuación, pulse “Aceptar”.

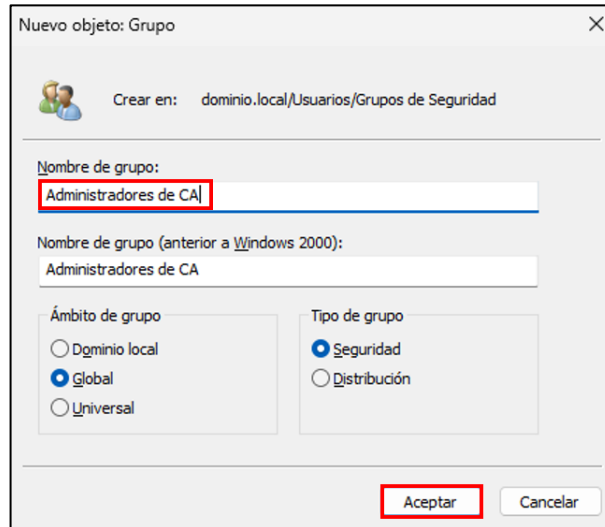


Ilustración 438 - Creación del grupo de seguridad

7. A continuación, haga doble clic sobre el grupo generado para acceder a sus propiedades.

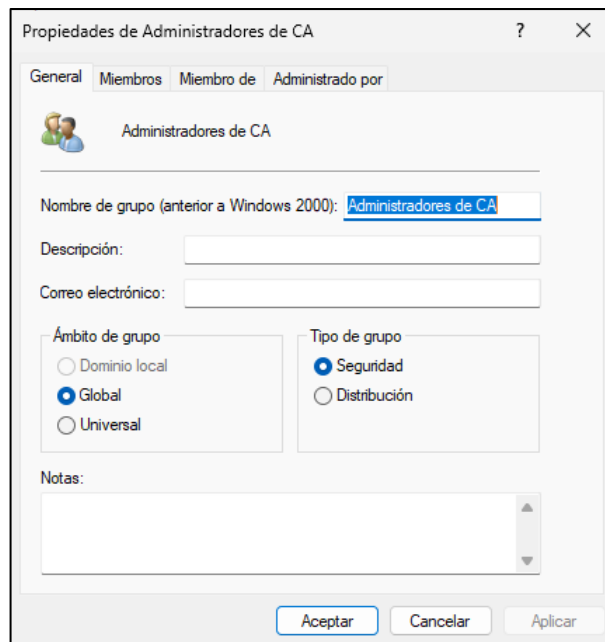


Ilustración 439 - Propiedades de grupo de seguridad

8. Pulse en la pestaña “Miembros” y, posteriormente, “Agregar”.

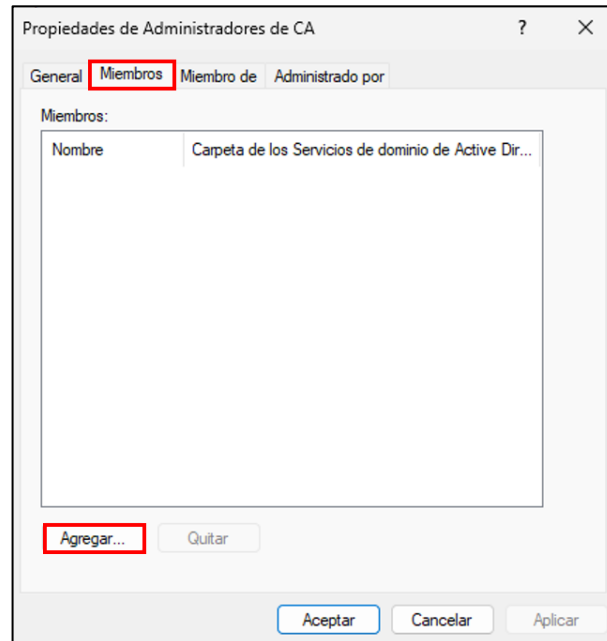


Ilustración 440 - Agregar miembros al grupo

9. Introduzca el nombre o nombres de usuario que desee incluir en el grupo. A continuación, pulse en “Aceptar”.

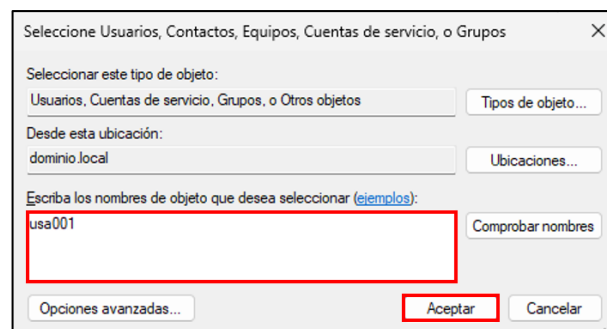


Ilustración 441 - Seleccionar miembros del grupo

10. Por último, haga clic en “Aplicar” y “Aceptar”.

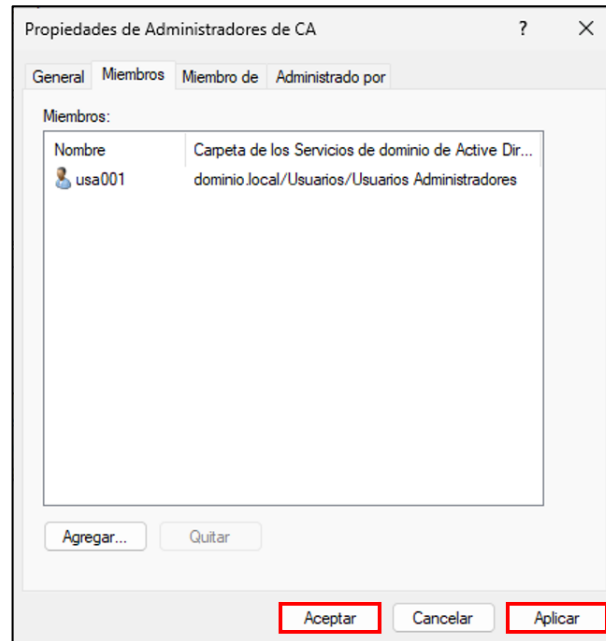


Ilustración 442 - Aplicar cambios en el grupo

11. Puede cerrar la consola de “Usuarios y equipos de Active Directory” y cerrar la sesión en el controlador de dominio.
12. A continuación, inicie sesión con un usuario con privilegios administrativos en la entidad de certificación Enterprise o subordinada en dominio.

13. Inicie como administrador la consola de “Administrador del servidor”.

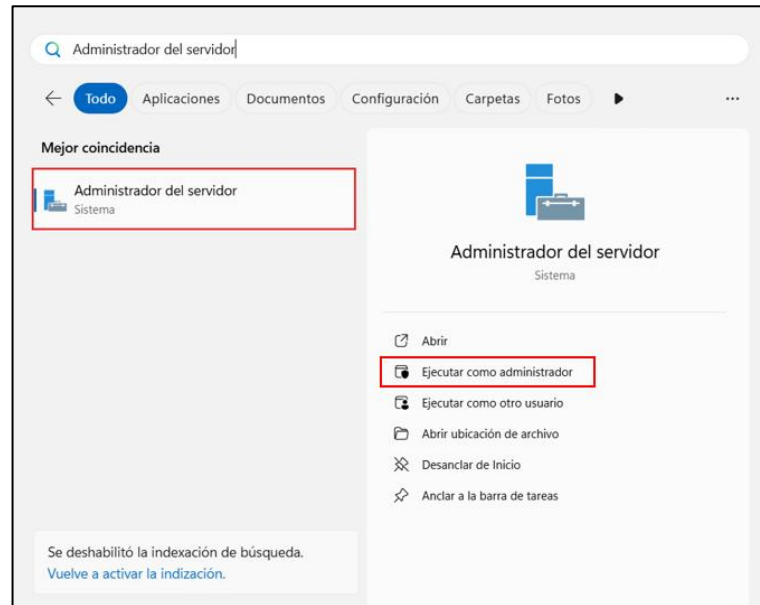


Ilustración 443 - Iniciar la administración del servidor

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

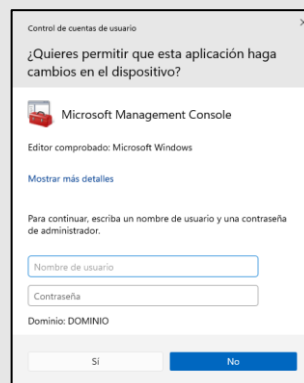


Ilustración 444 - Introducir credenciales de administrador

14. Diríjase a “Herramientas > Entidad de certificación”.

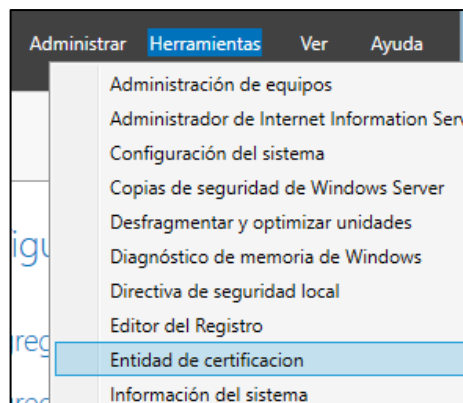


Ilustración 445 - Iniciar la consola de Entidad de Certificación

15. Haga clic derecho en el nombre de su entidad de certificación y, a continuación, pulse en “Propiedades”.

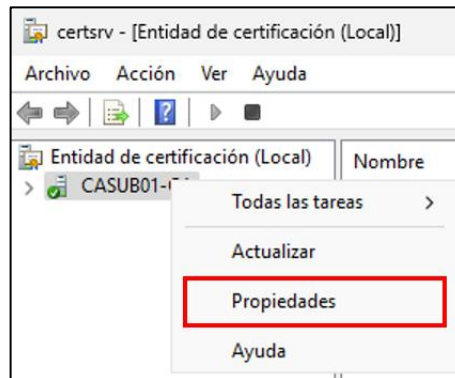


Ilustración 446 - Propiedades de la CA

16. Pulse sobre la pestaña “Seguridad” y, a continuación, pulse en “Agregar”.

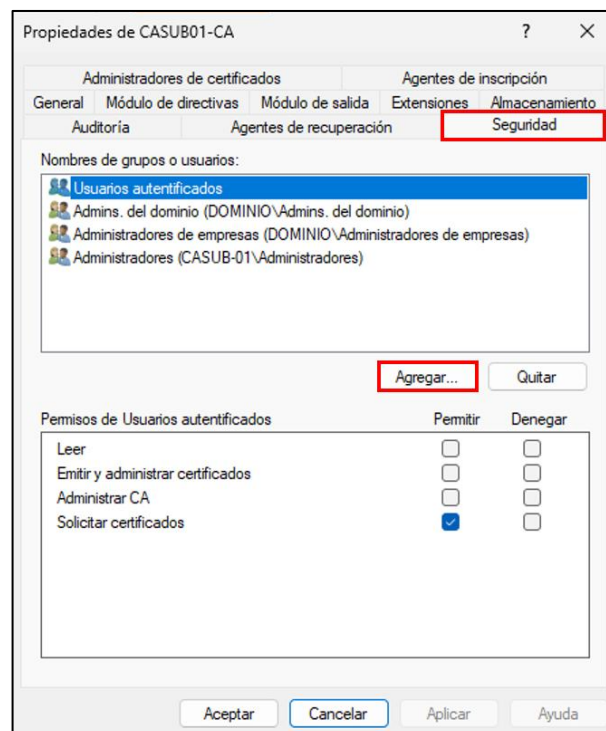


Ilustración 447 - Agregar administradores de CA

17. Introduzca el nombre del grupo generado en pasos anteriores y posteriormente, pulse en “Aceptar”.

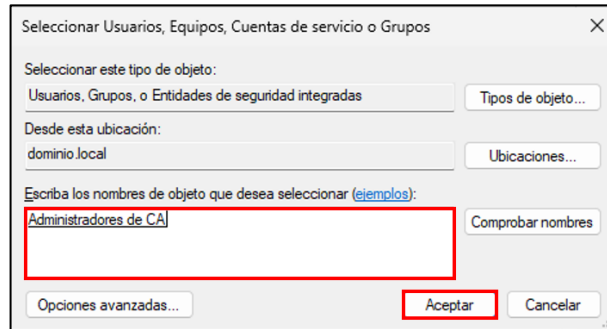


Ilustración 448 - Agregar el grupo de seguridad

18. Seleccione el grupo “Administradores de CA” y establezca los permisos deseados.

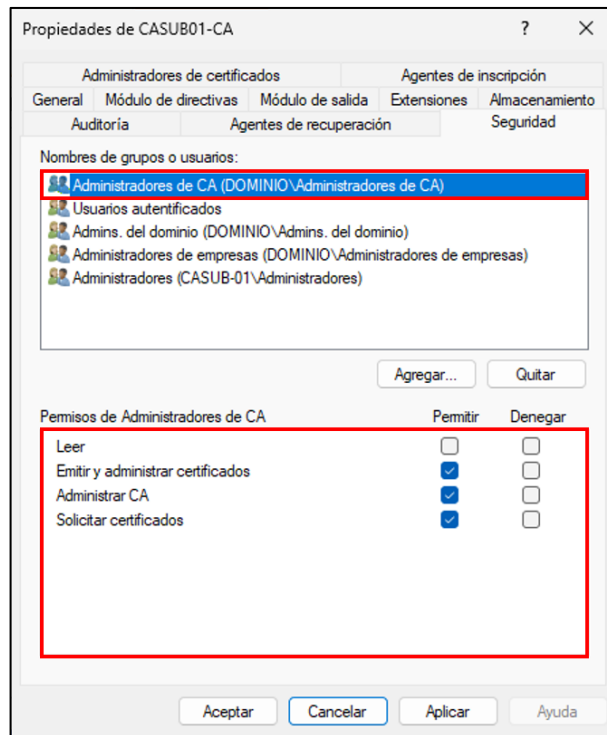


Ilustración 449 - Configurar permisos al grupo

19. A continuación, elimine aquellos grupos que no desea que dispongan de privilegios de administración, pulsando sobre cada uno de ellos y posteriormente, sobre el botón “Quitar”.

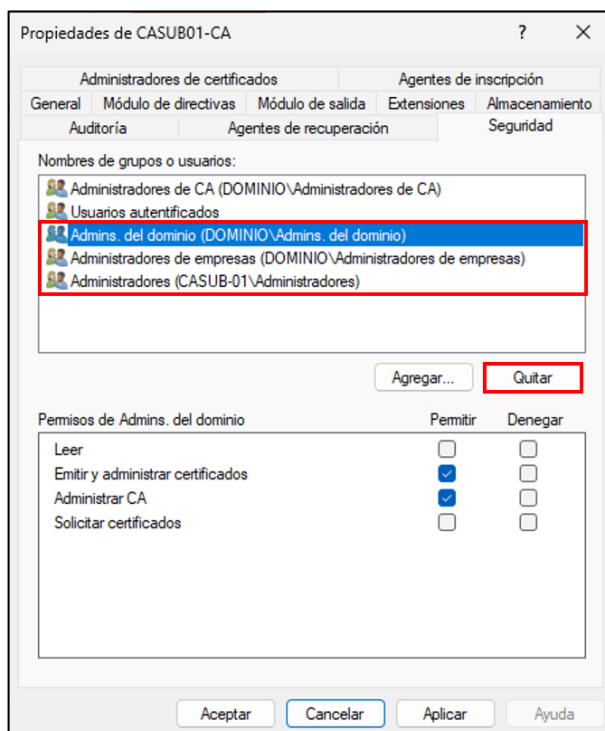


Ilustración 450 - Quitar grupos no deseados

20. Para finalizar, haga clic en “Aplicar” y “Aceptar”.

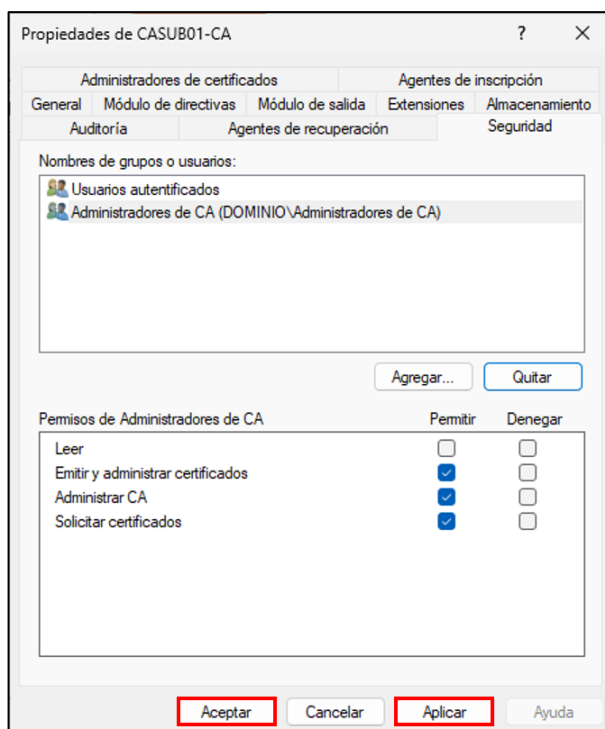


Ilustración 451 - Aplicar cambios

21. Tras el reinicio del servicio, únicamente el grupo “Administradores de CA” dispondrá de privilegios administrativos en la consola de administración de certificados de Active Directory. Para realizarlo, haga clic con el botón derecho sobre su entidad de certificación, y a continuación, pulse en “Todas las tareas > Detener servicio”.

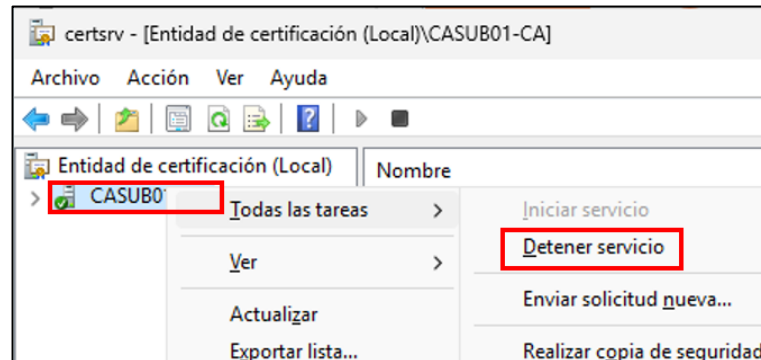


Ilustración 452 - Detener servicio

22. Una vez detenido, realice la misma operación para iniciar el servicio de nuevo, haciendo clic en “Todas las tareas > Iniciar servicio”.

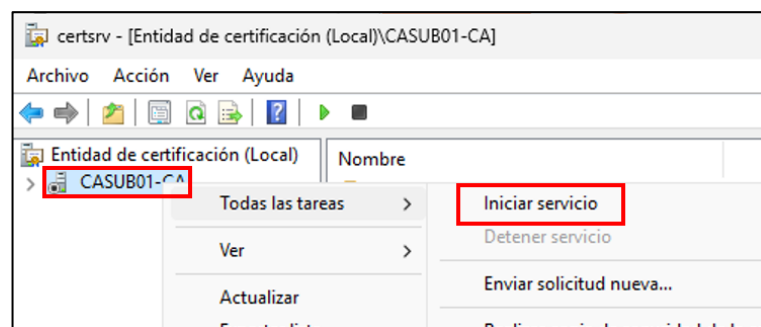


Ilustración 453 - Iniciar el servicio

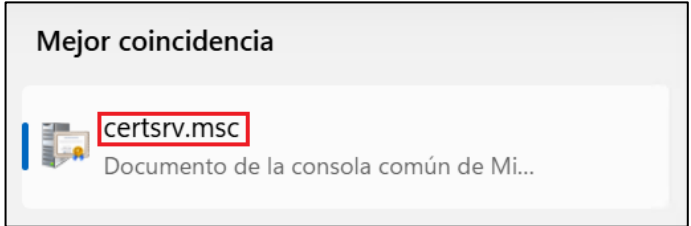
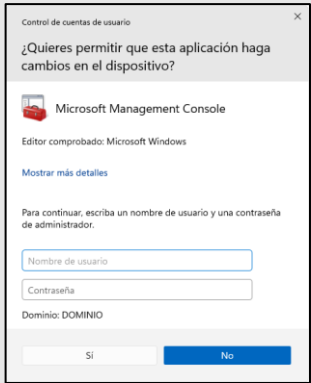
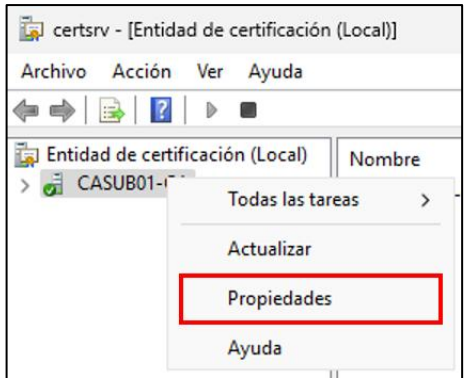
23. Por otro lado, se deberá tener en cuenta que si los servidores han sido bastionados siguiendo el procedimiento establecido en la guía CCN-STIC-570A25, existirán directivas que limitan el acceso por escritorio remoto o el inicio de sesión local a únicamente “BUILTIN\Administradores”. Para evitar pérdidas de acceso, se deberá gestionar el acceso mediante directiva de grupo o configurar “Administradores de CA” como miembro del grupo de administradores locales.

Nota: Cabe destacar que, en los servidores independientes, no podrá vincularse el grupo de dominio para realizar la administración del servicio. En este caso, podrá configurarse un grupo de seguridad local y agregar los usuarios nominales deseados.

7.2. CONFIGURACIÓN DE AUDITORÍA

Disponer de la trazabilidad de las tareas administrativas y operativas de un entorno es una de las premisas principales en infraestructuras que trabajarán con información sensible o información clasificada. El servicio de entidad de certificación dispone de configuraciones adicionales que permiten llevarlo a cabo y, que un auditor controle las

diferentes tareas realizadas en el servidor. Estos pasos se realizarán en una Entidad de Certificación, independientemente del tipo de la misma.

Paso	Descripción
1.	Inicie sesión en el equipo Entidad de Certificación raíz con credenciales de administrador.
2.	Sobre la barra de búsqueda, escriba “certsrv.msc” y ejecútelo como administrador.  <i>Ilustración 454 – Consola de entidad de certificados</i> Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 455 - Introducir credenciales de administrador</i>
3.	Haga clic derecho en el nombre de su entidad de certificación y, a continuación, pulse en “Propiedades”.  <i>Ilustración 456 - Propiedades de CA</i>

4. A continuación, pulse en la pestaña “Auditoría”.

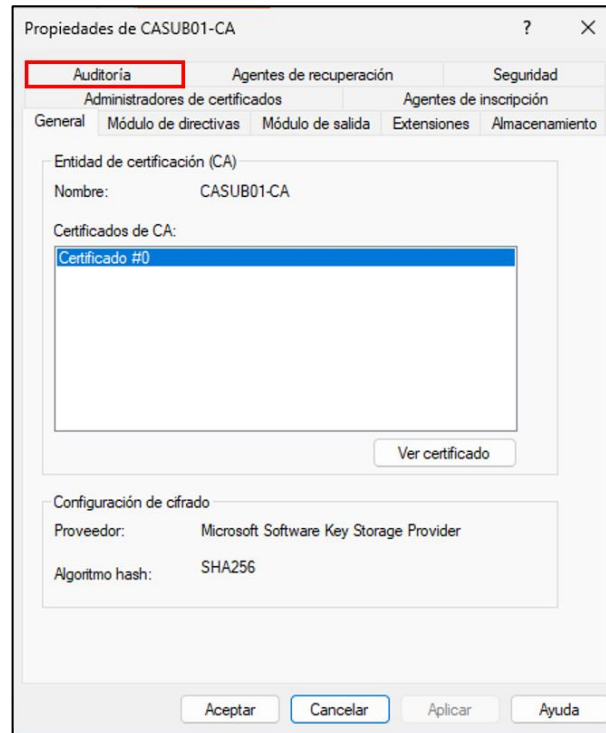


Ilustración 457 - Acceder a la auditoría de CA

5. Seleccione aquellos eventos que desee auditar. A continuación, pulse en “Aceptar” y “Aplicar”.

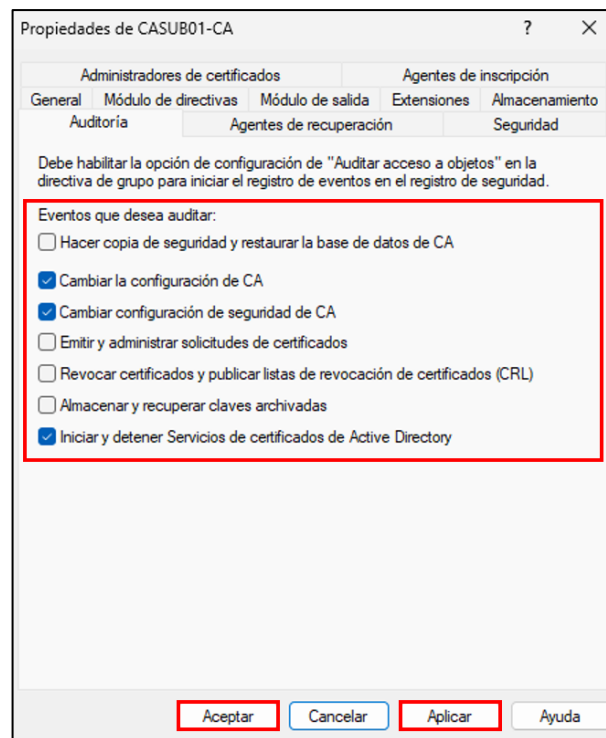


Ilustración 458 - Eventos a auditar

6. Para confirmar el cambio, haga clic con el botón derecho sobre su entidad de certificación, y a continuación, pulse en “Todas las tareas > Detener servicio”.

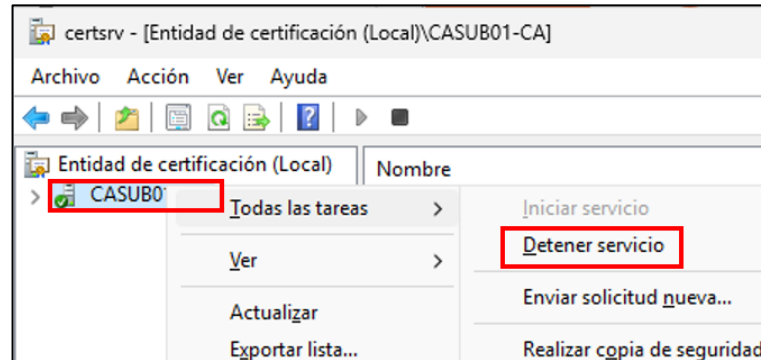


Ilustración 459 - Detener el servicio

7. Una vez detenido, realice la misma operación para iniciar el servicio de nuevo, haciendo clic en “Todas las tareas > Iniciar servicio”.

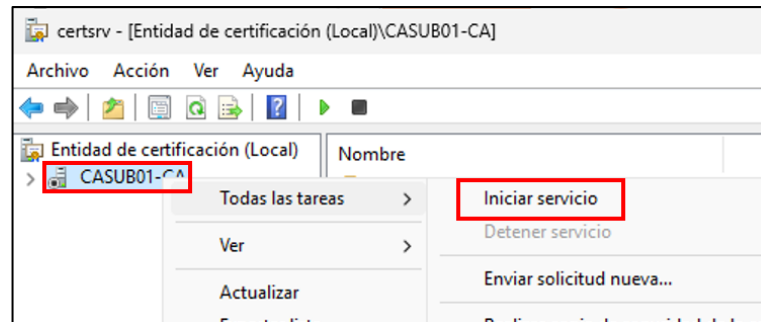


Ilustración 460 - Iniciar el servicio

8. Tras el reinicio del servicio, podrá observar los eventos registrados en el visor de eventos del servidor.

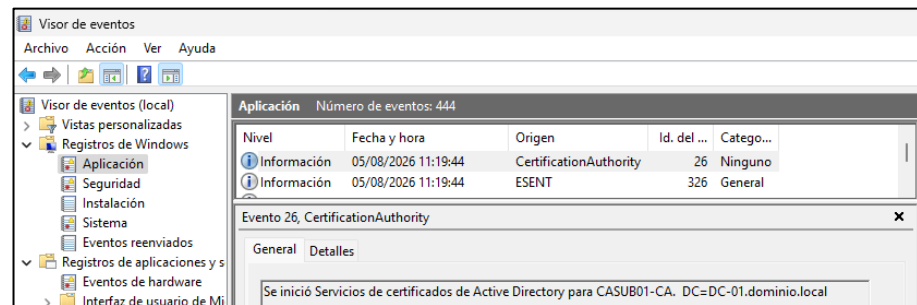
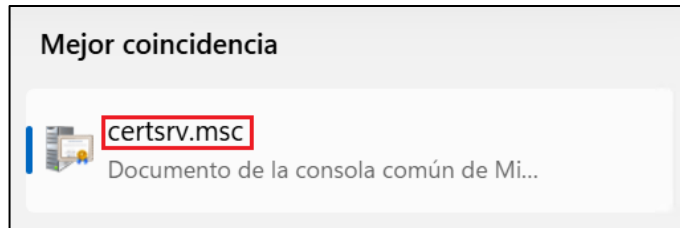
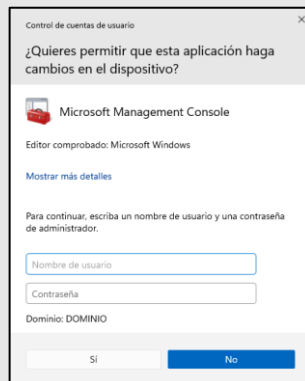


Ilustración 461 - Eventos de CA

7.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA

Los pasos que se definen a continuación comprenden la renovación de una Entidad de Certificación raíz tanto si ésta es de empresa como independiente del dominio.

Paso	Descripción
1.	Inicie sesión en el equipo Entidad de Certificación raíz con credenciales de administrador.
2.	Sobre la barra de búsqueda, escriba “certsrv.msc”.  <i>Ilustración 462 – Consola de entidad de certificados</i> Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.  <i>Ilustración 463 - Introducir credenciales de administrador</i>

3. Pulse sobre “CARAIZ01-CA” con clic derecho y seleccione “Todas las tareas > Renovar certificado de CA...”

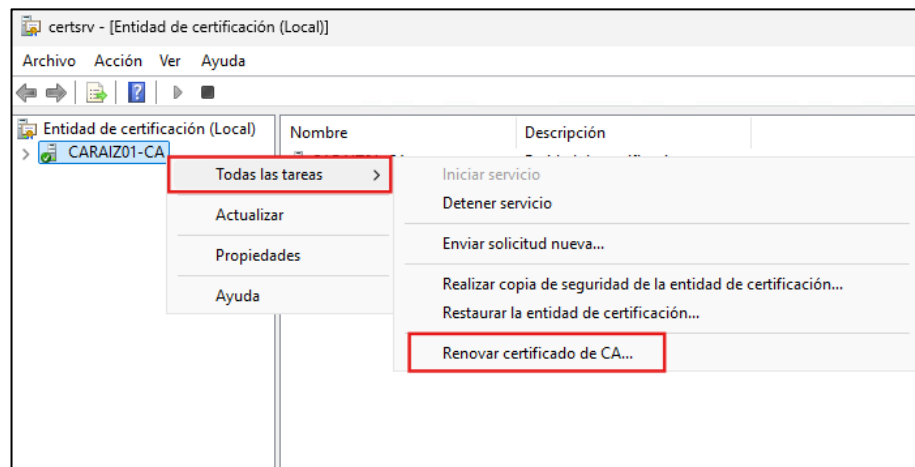


Ilustración 464 – Renovar certificado

4. Se pausará el servicio de certificados de Active Directory. Pulse en “Sí”.

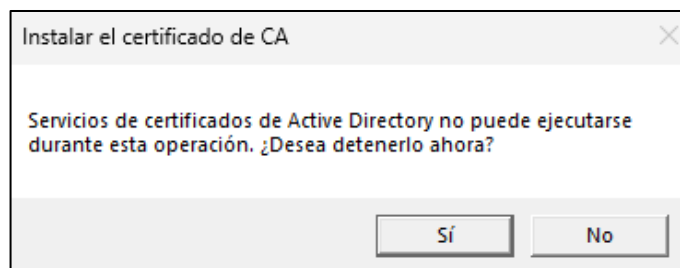


Ilustración 465 – Detener servicios

5. En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.

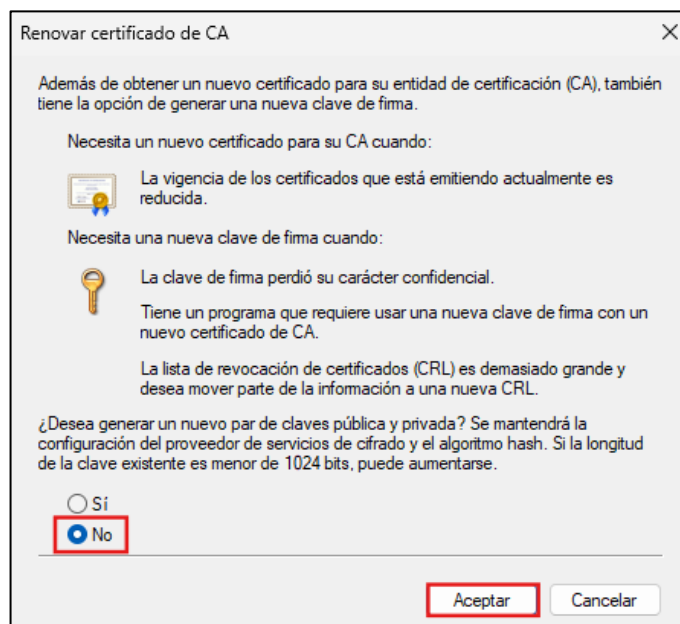


Ilustración 466 – No generar par de claves

7.4. COPIA DE SEGURIDAD Y RESTAURACIÓN DE UNA ENTIDAD DE CERTIFICACIÓN

Con el objeto de prevenir que una corrupción de la base de datos o algún otro tipo incidencia relacionado con la información contenida en la Entidad de Certificación, que conlleve la pérdida del servicio se recomienda la realización de una copia de seguridad preventiva. Ésta se realizará tanto de la base de datos, como del registro de transacciones correspondiente.

Los procedimientos operacionales del servicio permiten la recuperación tanto de la base de datos como del fichero de registro sobre el mismo servidor o sobre otro diferente. La sección siguiente describe el proceso para generar una copia de seguridad de la Entidad de Certificación, así como la restauración sobre el mismo servidor.

7.4.1. COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN

Paso	Descripción
1.	Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado.

2. Sobre la barra de búsqueda, escriba “certsrv.msc”.

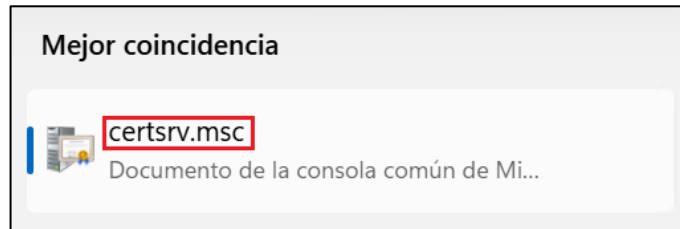


Ilustración 467 – Ejecución de entidad de certificación

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

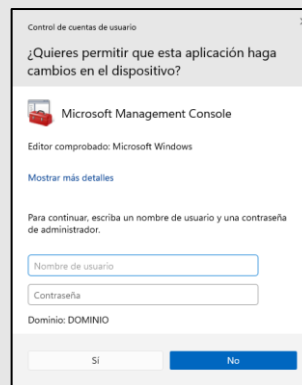


Ilustración 468 - Introducir credenciales de administrador

3. Pulse sobre “CARAIZ01-CA” con clic derecho y seleccione “Todas las tareas > Realizar copia de seguridad de la entidad de certificación...”

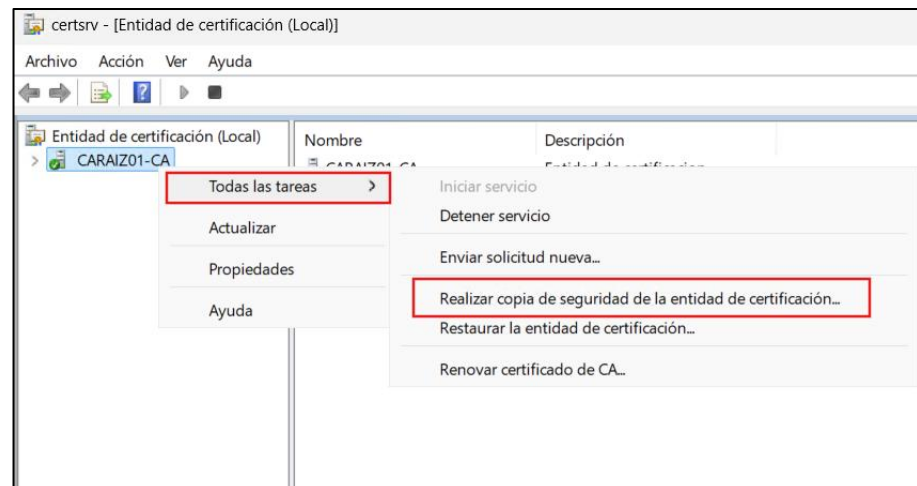


Ilustración 469 – Realizar copia de seguridad de la entidad de certificación

4. En el “Asistente para copia de seguridad de Entidad de Certificación” pulse “Siguiente >” para continuar.



Ilustración 470 – Asistente de copia de seguridad

5. En “Elementos para incluir en copia de seguridad” existe la opción de hacer salvaguarda solamente de la base de datos (completa o incremental) o también de la clave privada y el certificado de la Entidad de Certificación. En el ejemplo, se hace una copia completa. Para ello, marque las opciones “Clave privada y certificado de CA” y “Base de datos de certificados emitidos y registro de base de datos de certificados”. Pulse “Examinar” para continuar.

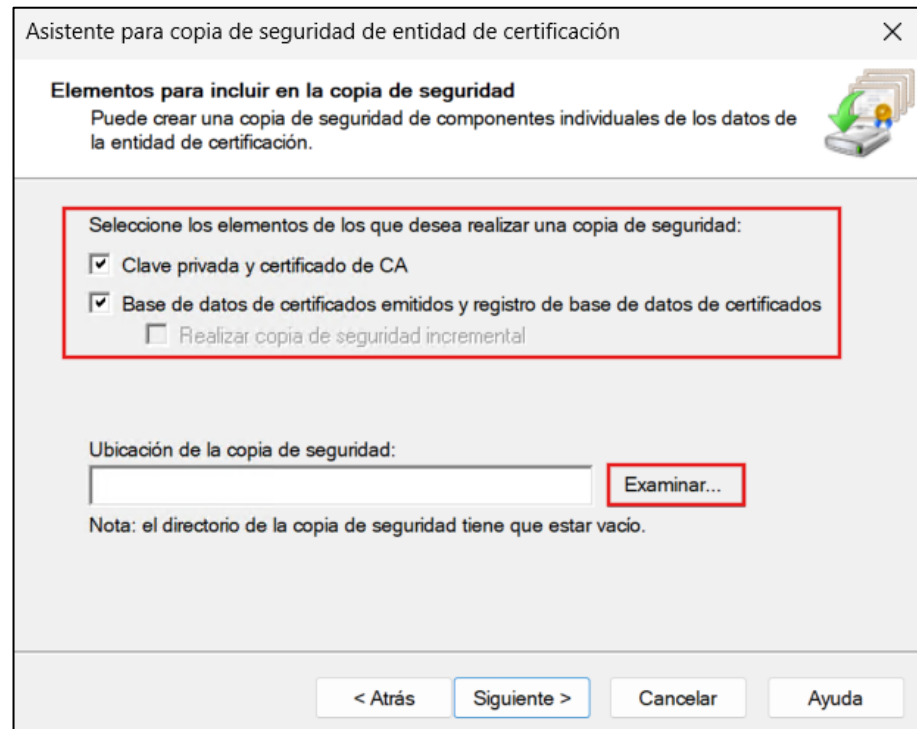


Ilustración 471 – Elementos a realizar una copia de seguridad

6. Seleccione un directorio vacío para realizar la copia de seguridad y pulse “Aceptar”.

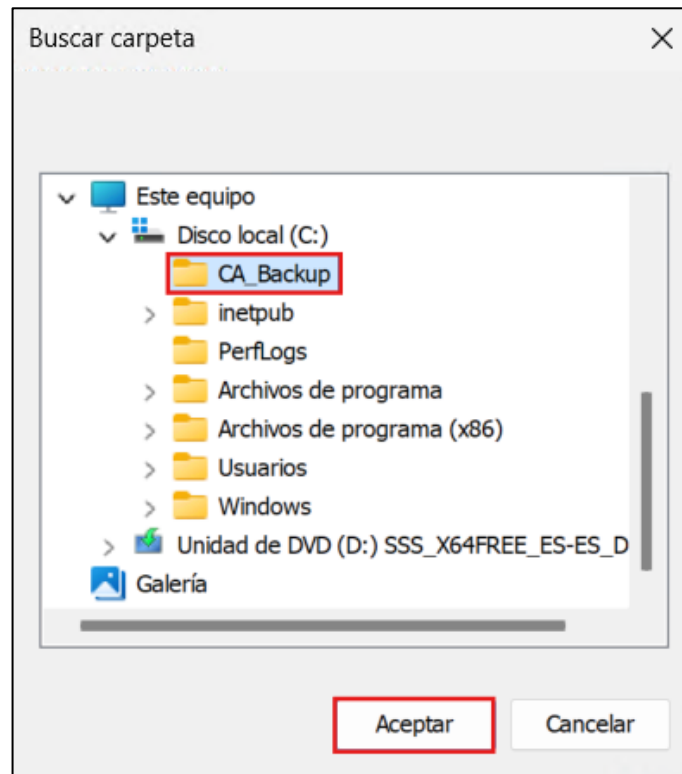


Ilustración 472 – Selección de directorio

7. Pulse “Siguiente >” para continuar.

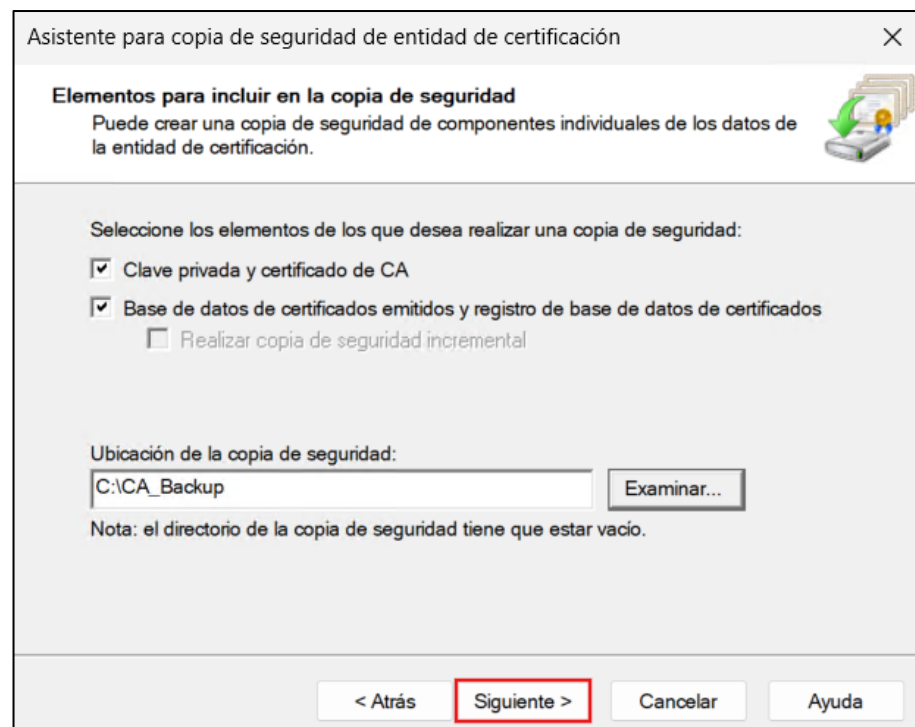


Ilustración 473 – Asistente de copia de seguridad configurado

8. Establezca una contraseña escribiéndola por duplicado en los campos correspondientes y pulse “Siguiente >”.

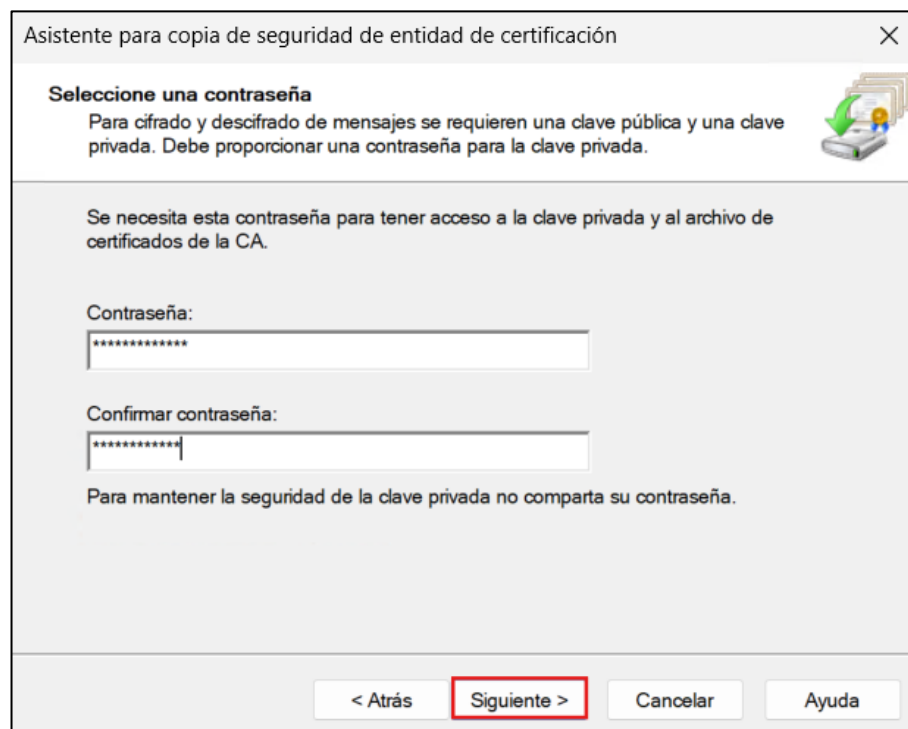


Ilustración 474 – Contraseña del archivo de certificado

9. Pulse “Finalizar” para cerrar el asistente.

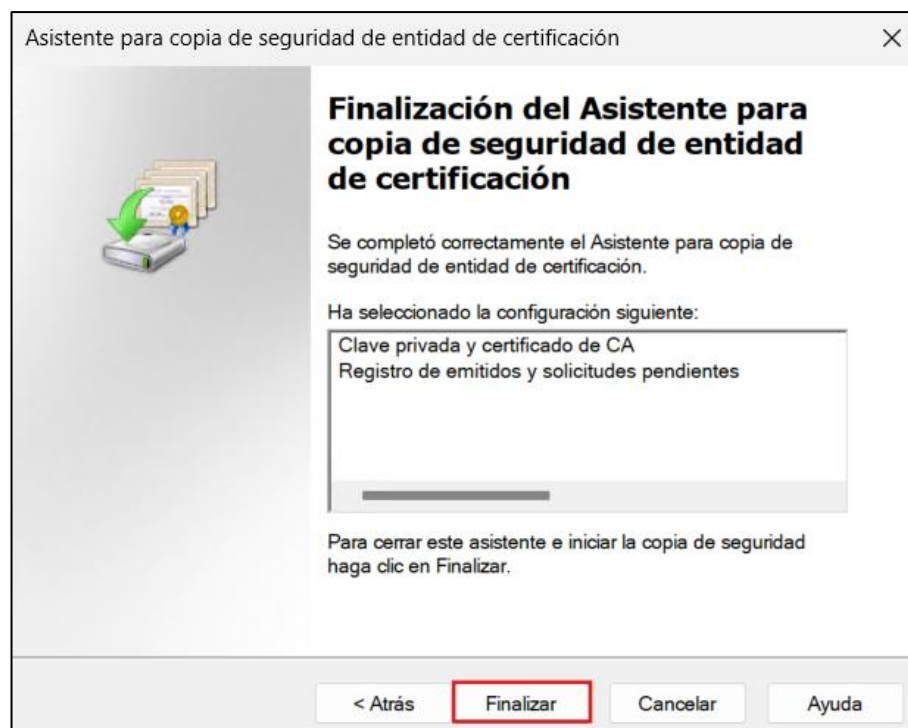


Ilustración 475 – Finalización del Asistente

10. En la carpeta podrá encontrar tanto el certificado de la CA como los ficheros de la base de datos.

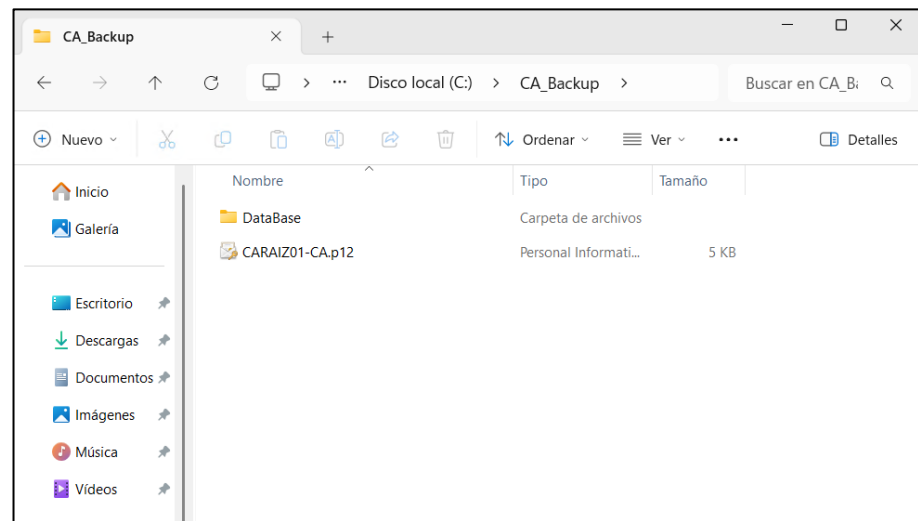


Ilustración 476 – Visualización de certificado de la CA

7.4.2. RESTAURACIÓN DE COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN

Paso	Descripción
11.	Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado.

12. Sobre la barra de búsqueda, escriba “certsrv.msc”.

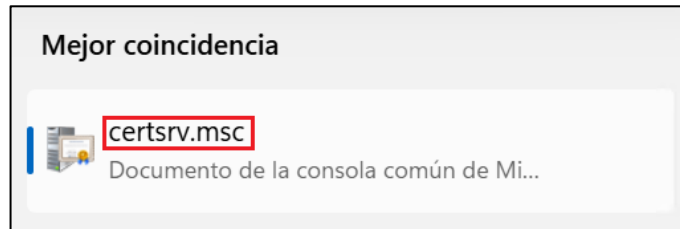


Ilustración 477 – Consola de Entidad de certificación

Nota: Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.

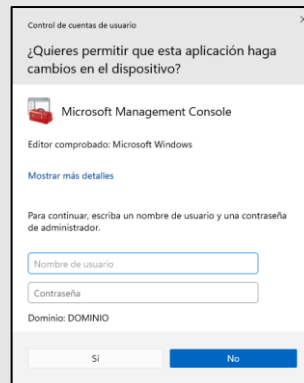


Ilustración 478 - Introducir credenciales de administrador

13. Pulse sobre “CARAI01-CA” con clic derecho y seleccione “Todas las tareas > Restaurar la entidad de certificación...”

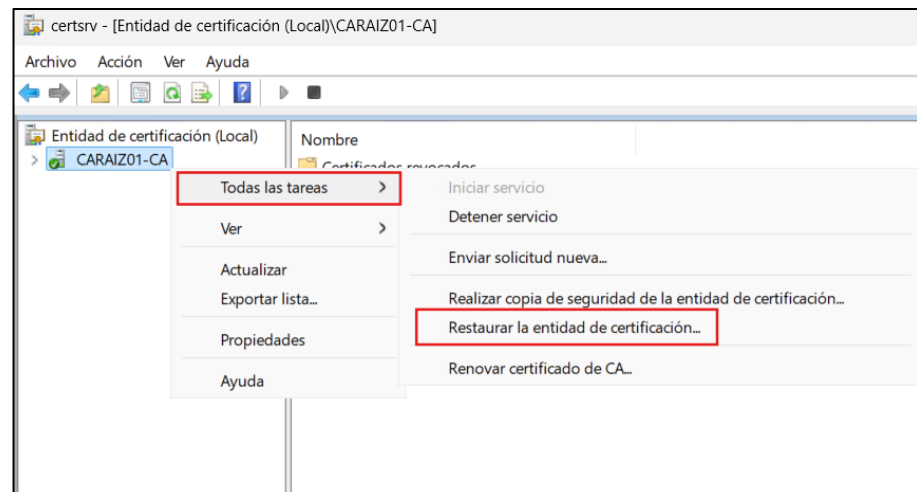


Ilustración 479 – Restaurar la entidad de certificación

14. El servicio de Entidad de Certificación está en funcionamiento, por lo que le solicitará detenerlo. En este caso pulse “Aceptar” para permitir al sistema detener el servicio de Entidad de Certificación de Directorio Activo.

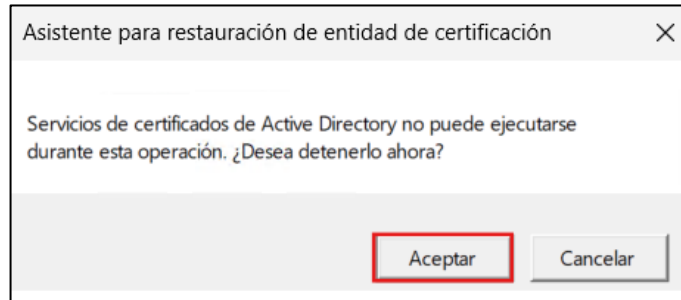


Ilustración 480 – Detener servicios de certificados

15. En el “Asistente para copia de seguridad de Entidad de Certificación” pulse “Siguiente >” para continuar.

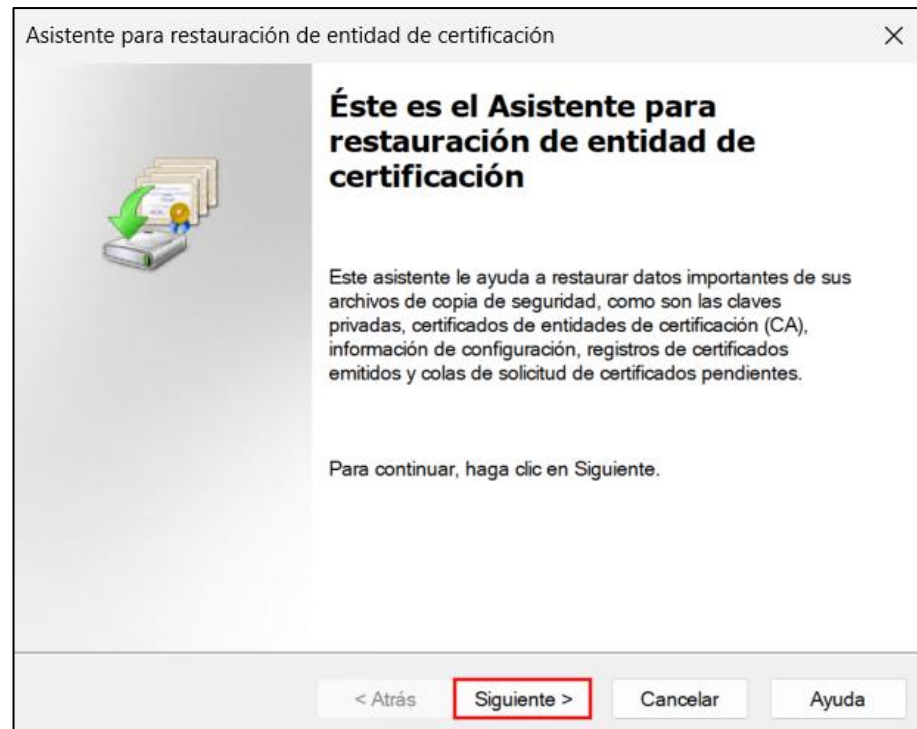


Ilustración 481 – Asistente de restauración

16. Es posible recuperar tanto la base de datos como la clave privada y el certificado. En el ejemplo se selecciona restaurar la base de datos solamente. Para ello, marque la opción “Base de datos de certificados emitidos y registro de base de datos de certificados”. Pulse “Examinar” para continuar.

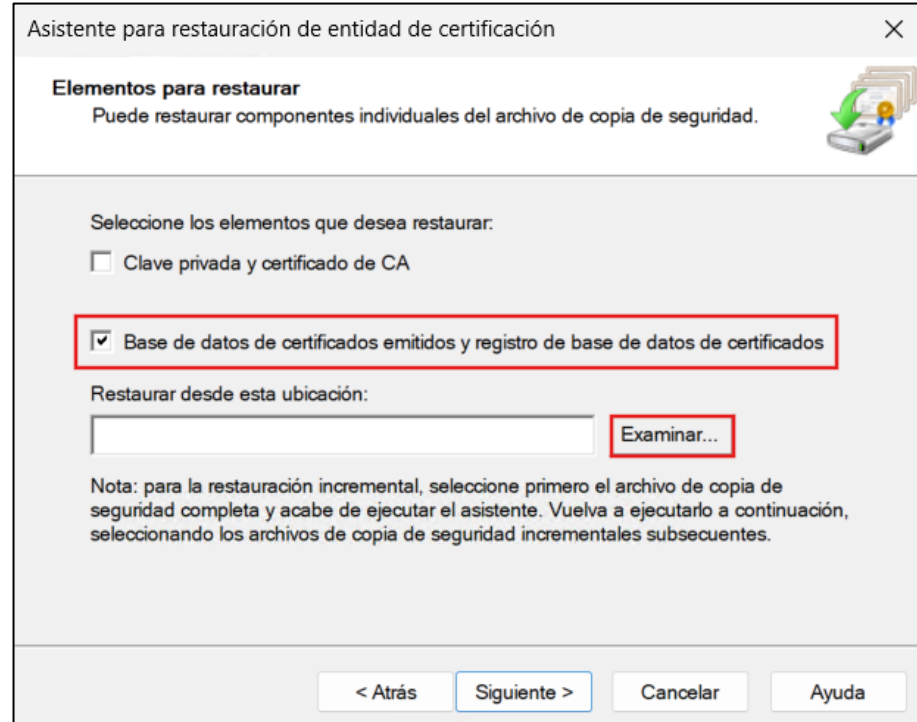


Ilustración 482 – Ruta a guardar

17. Localice la carpeta que contiene la base de datos y pulse “Aceptar”.

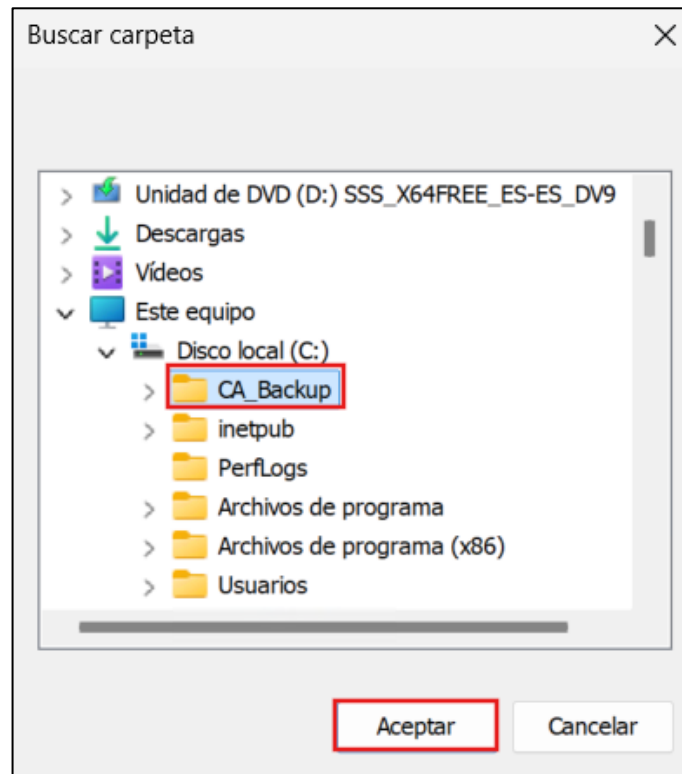


Ilustración 483 – Localización de carpeta

18. Pulse “Siguiente >” para continuar.

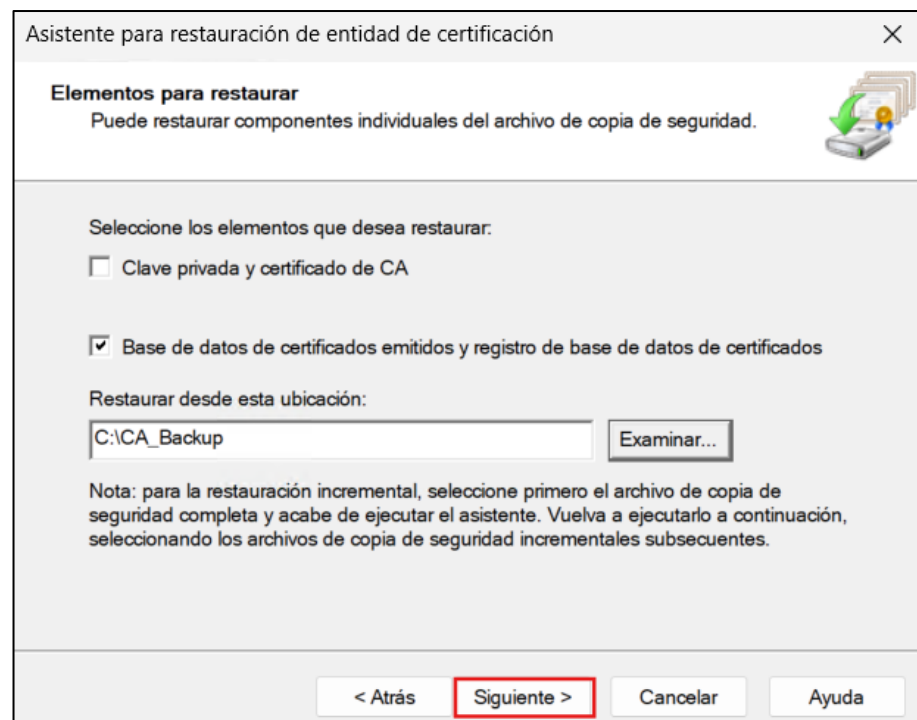


Ilustración 484 – Resumen del Asistente

19. Pulse “Finalizar” para cerrar el asistente.

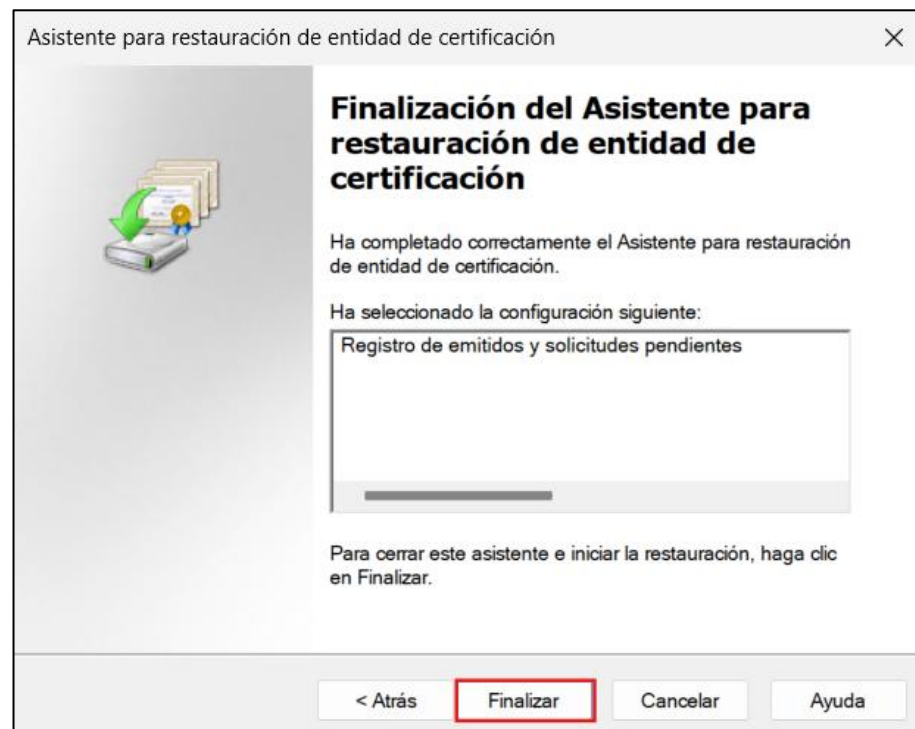


Ilustración 485 – Finalización Asistente

20. Ante el mensaje que indica que la operación se completó y que se iniciará el servicio de nuevo pulse “Sí”.

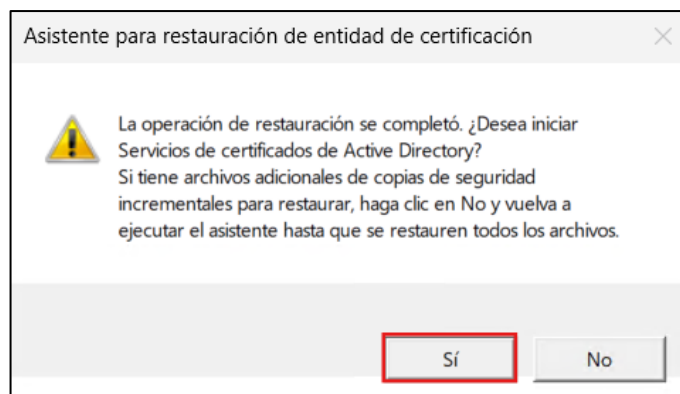


Ilustración 486 - Confirmar