

## Guía de Seguridad de las TIC CCN-STIC 598

# IMPLEMENTACIÓN DEL ENS EN ENTIDAD DE CERTIFICACIÓN SOBRE WINDOWS SERVER 2016



JUNIO 2020

Edita:



© Centro Criptológico Nacional, 2020  
NIPO: 083-20-144-0

Fecha de Edición: junio de 2020

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

#### **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.

## PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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

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

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

junio de 2020



Paz Esteban López  
Secretaria de Estado  
Directora del Centro Criptológico Nacional

## **ANEXOS**

|                                                                                                                                                                                                 |          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>ANEXO A. CONFIGURACIÓN SEGURA DE ENTIDAD DE CERTIFICACIÓN EN EL ENS .....</b>                                                                                                                | <b>8</b> |
| ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SOBRE MICROSOFT WINDOWS SERVER 2016.....                                                                                      | 8        |
| 1. APLICACIÓN DE MEDIDAS EN ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                      | 8        |
| 1.1. MARCO OPERACIONAL .....                                                                                                                                                                    | 9        |
| 1.1.1. CONTROL DE ACCESO .....                                                                                                                                                                  | 9        |
| 1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO .....                                                                                                                                                 | 9        |
| 1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS .....                                                                                                                                    | 10       |
| 1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO.....                                                                                                                              | 11       |
| 1.1.2. EXPLOTACIÓN.....                                                                                                                                                                         | 12       |
| 1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD.....                                                                                                                                            | 12       |
| 1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN .....                                                                                                                                          | 12       |
| 1.1.2.3. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS.....                                                                                                                                 | 13       |
| 1.2. MEDIDAS DE PROTECCIÓN.....                                                                                                                                                                 | 13       |
| 1.2.1. MP.INFO.9. COPIAS DE SEGURIDAD .....                                                                                                                                                     | 13       |
| 2. RESUMEN Y APLICACIÓN DE MEDIDAS EN ENTIDAD DE CERTIFICACIÓN SOBRE WINDOWS SERVER 2016 .....                                                                                                  | 14       |
| ANEXO A.2. CATEGORÍA BÁSICA.....                                                                                                                                                                | 15       |
| ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS ..... | 15       |
| 1. PREPARACIÓN DEL DOMINIO.....                                                                                                                                                                 | 15       |
| 2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN .....                                                                                                                       | 32       |
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                                | 32       |
| 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA.....                                                                                                                          | 37       |
| 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA .....                                                                                                                                 | 47       |
| ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO.....             | 50       |
| 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO .....                                                                                                                                               | 50       |
| 2. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN .....                                                                                                                              | 55       |
| ANEXO A.2.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS .....       | 58       |
| 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DEL DOMINIO.....                                                                                          | 58       |
| 2. CONFIGURACIONES DE SEGURIDAD SOBRE EL DOMINIO .....                                                                                                                                          | 61       |

|                                                                                                                                                                                               |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                              | 61  |
| 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL).....                                                                                                                          | 67  |
| 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO .....                                                                                                                                                  | 81  |
| 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.....                                                                                                | 99  |
| ANEXO A.2.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE .....       | 110 |
| 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ.....                                                                                                             | 110 |
| 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO .....                                                                                                                                          | 112 |
| 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA .....                                                                                                                | 117 |
| ANEXO A.3. CATEGORÍA MEDIA .....                                                                                                                                                              | 119 |
| ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS..... | 119 |
| 1. PREPARACIÓN DEL DOMINIO.....                                                                                                                                                               | 120 |
| 2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN .....                                                                                                                     | 137 |
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                              | 138 |
| 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA.....                                                                                                                        | 142 |
| 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA .....                                                                                                                               | 152 |
| 2.4. SEGREGACIÓN DE ROLES .....                                                                                                                                                               | 154 |
| 2.5. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                        | 164 |
| ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO.....            | 168 |
| 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO .....                                                                                                                                             | 168 |
| 2. COMPROBACIONES EN SERVIDOR MIEMBRO.....                                                                                                                                                    | 174 |
| ANEXO A.3.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS.....       | 177 |
| 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DE DOMINIO .....                                                                                        | 178 |
| 1.1. SEGREGACIÓN DE ROLES .....                                                                                                                                                               | 180 |
| 1.2. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                        | 185 |
| 2. CONFIGURACIONES DE SEGURIDAD SOBRE EL DOMINIO .....                                                                                                                                        | 189 |
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                              | 189 |
| 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL).....                                                                                                                          | 194 |
| 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO .....                                                                                                                                                  | 208 |
| 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.....                                                                                                | 227 |

|                                                                                                                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 2.5. SEGREGACIÓN DE ROLES .....                                                                                                                                                                                     | 238 |
| 2.6. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                              | 248 |
| ANEXO A.3.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE .....                              | 252 |
| 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ.....                                                                                                                                   | 252 |
| 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO .....                                                                                                                                                                | 254 |
| 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA .....                                                                                                                                      | 258 |
| ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....                                                                                                                                                                  | 261 |
| ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA .....    | 261 |
| 1. PREPARACIÓN DEL DOMINIO.....                                                                                                                                                                                     | 262 |
| 2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN .....                                                                                                                                                             | 281 |
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                                                    | 281 |
| 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA.....                                                                                                                                              | 286 |
| 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA .....                                                                                                                                                     | 297 |
| 2.4. SEGREGACIÓN DE ROLES .....                                                                                                                                                                                     | 299 |
| 2.5. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                              | 305 |
| ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO ..... | 309 |
| 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO .....                                                                                                                                                                   | 309 |
| 2. COMPROBACIONES EN SERVIDOR MIEMBRO.....                                                                                                                                                                          | 315 |
| ANEXO A.4.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS .....  | 318 |
| 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DEL DOMINIO.....                                                                                                              | 319 |
| 1.1. SEGREGACIÓN DE ROLES .....                                                                                                                                                                                     | 322 |
| 1.2. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                              | 327 |
| 2. CONSIDERACIONES DE SEGURIDAD SOBRE EL DOMINIO .....                                                                                                                                                              | 331 |
| 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN .....                                                                                                                                                    | 332 |
| 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL).....                                                                                                                                                | 337 |
| 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO .....                                                                                                                                                                        | 350 |
| 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.....                                                                                                                      | 370 |

|                                                                                                                                                                                                              |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 2.5. SEGREGACIÓN DE ROLES .....                                                                                                                                                                              | 381 |
| 2.6. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                       | 391 |
| ANEXO A.4.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE ..... | 396 |
| 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ.....                                                                                                                            | 396 |
| 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO .....                                                                                                                                                         | 398 |
| 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                           | 402 |
| ANEXO A.5. TAREAS DE ADMINISTRACIÓN DE SERVIDORES DE ENTIDAD DE CERTIFICACIÓN.....                                                                                                                           | 405 |
| 1. CONFIGURACIÓN DE PROPIEDADES DE LA ENTIDAD DE CERTIFICACIÓN.....                                                                                                                                          | 405 |
| 2. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                     | 407 |
| 2.1. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ .....                                                                                                                              | 408 |
| 2.2. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN SUBORDINADA .....                                                                                                                       | 410 |
| 3. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS .....                                                                                                                                    | 413 |
| 3.1. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (CRL) MEDIANTE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA .....                                                                      | 413 |
| 3.2. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (CRL) MEDIANTE UNA ENTIDAD DE CERTIFICACIÓN SUBORDINADA A UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE .....                        | 416 |
| 4. GENERACIÓN DE PLANTILLAS DE CERTIFICADO.....                                                                                                                                                              | 420 |
| 4.1. CREACIÓN DE PLANTILLAS DE CERTIFICADO.....                                                                                                                                                              | 421 |
| 4.2. PUBLICACIÓN DE UNA PLANTILLA DE CERTIFICADOS EN LA ENTIDAD DE CERTIFICACIÓN .                                                                                                                           | 428 |
| 5. PROCEDIMIENTOS DE SOLICITUD Y ADMINISTRACIÓN DE CERTIFICADOS.....                                                                                                                                         | 431 |
| 5.1. SOLICITUD DE CERTIFICADOS.....                                                                                                                                                                          | 431 |
| 5.1.1. DESDE LA CONSOLA MMC.....                                                                                                                                                                             | 431 |
| 5.1.2. DESDE EL SERVICIO DE INTERNET INFORMATION SERVICES (IIS) .....                                                                                                                                        | 436 |
| 5.2. EMISIÓN DE SOLICITUDES PENDIENTES DE CERTIFICADOS .....                                                                                                                                                 | 440 |
| 5.3. EXPORTACIÓN DE CERTIFICADOS .....                                                                                                                                                                       | 441 |
| 5.4. IMPORTACIÓN DE CERTIFICADOS .....                                                                                                                                                                       | 445 |
| 5.5. REVOCACIÓN DE CERTIFICADOS .....                                                                                                                                                                        | 450 |
| 5.6. RENOVACIÓN DE CERTIFICADOS.....                                                                                                                                                                         | 453 |
| 6. COPIA DE SEGURIDAD Y RESTAURACIÓN DE UNA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                   | 458 |
| 6.1. COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN.....                                                                                                                                                 | 458 |
| 6.2. RESTAURACIÓN DE COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN .....                                                                                                                                | 462 |

## ANEXO A. CONFIGURACIÓN SEGURA DE ENTIDAD DE CERTIFICACIÓN EN EL ENS

### ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE ENTIDAD DE CERTIFICACIÓN SOBRE MICROSOFT WINDOWS SERVER 2016

#### 1. APLICACIÓN DE MEDIDAS EN ENTIDAD DE CERTIFICACIÓN

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de entidad de certificación sobre servidores con Microsoft Windows Server 2016 y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un operador de una organización para hacerlas efectivas.

**Nota:** Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará uso de la aplicación de medidas de seguridad descritas en el “ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA”.

La aplicación de medidas de seguridad atenderá a las siguientes condiciones de implantación de infraestructuras:

- a) Aplicación de seguridad en el entorno de Entidad de Certificación sobre Microsoft Windows Server 2016 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.
- b) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows Server 2016 implementados siguiendo la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para entidad de certificación, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

Esta guía, por tanto, no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo o las funcionalidades que el propio rol pueda aportar. Por ejemplo, aunque es condición indispensable la implementación de un antivirus en los servidores, se establece que esta medida atiende a un criterio general de la organización y que, no siendo algo que pueda aportar el propio sistema operativo, se encontrará excluido del análisis e implementación.

Para un mejor entendimiento de las medidas éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a los niveles que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

## 1.1. MARCO OPERACIONAL

### 1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema, de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Por lo tanto, se requiere una menor exigencia de seguridad para la categoría básica mientras que en la categoría media y alta se requiere una mayor exigencia.

#### 1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la de necesidad proteger los recursos del sistema (certificados, ubicación de la base de datos de certificados) con algún mecanismo que impida su utilización, salvo a usuarios o perfiles de usuario que disfruten de los derechos de acceso suficientes.

Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad de la organización, a través de la persona responsable de dicha determinación y haciendo uso de las tecnologías necesarias.

Así mismo dicha persona responsable será la encargada de aprobar solicitudes de revocación e inscripción de certificados, así como poder administrar dichos certificados.

Desde el punto de vista tecnológico, esta medida abarca un gran número de actividades, de tal forma que los puntos de control para restringir o conceder un acceso son abundantes. Realizar la administración del Directorio Activo, acceder a un fichero o una carpeta o imprimir en un recurso, son acciones que pueden ser controladas y determinar para ello los permisos asignados.

La plantilla de seguridad recoge una serie de permisos que serán asignados con objeto de limitar las acciones por parte de usuarios y administradores. De esta forma y controlando los requisitos de acceso, se reducirán todos aquellos riesgos del uso habitual de administración de un puesto de trabajo.

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia. La siguiente dirección URL facilita la información que proporciona el fabricante sobre los controles y vigilancia de acceso para Microsoft Windows Server 2016, incluyendo los controles de acceso dinámicos.

#### 1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS

Aplicable a partir de la categoría media. Se considera un requerimiento importante para una organización la segregación de funciones en base a la actividad. De esta forma se establece cadenas de autorización y control enfocadas a evitar la existencia de una única persona autorizada y que ésta pueda abusar de sus derechos para cometer alguna acción ilícita.

Desde el punto de vista formal la segregación de funciones deberá realizarse al menos para las siguientes tareas.

- a) Desarrollo de operación.
- b) Configuración y mantenimiento del sistema de operación.
- c) Auditoría o supervisión de otra función.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona Microsoft Windows Server 2016. Conforme a las necesidades planteadas en los dos primeros elementos, desarrollo de operaciones y la configuración, así como el mantenimiento del sistema de operación, el operador deberá tomar en consideración lo establecido en la última revisión de la guía CCN-STIC-570A. En dicho documento, además de otras cuestiones relativas a mejoras en la seguridad y procesos, se recogen los procedimientos que pueden ser llevados a cabo para la segregación de tareas, de tal forma que se pueden conceder determinados privilegios a usuarios concretos sin necesidad de facultarles de derechos completos. Así, se muestran ejemplos para delegar las tareas de agregar equipos al dominio a determinados usuarios, sin que estos tengan la necesidad de ser administradores del dominio o bien atribuirles los permisos para poder gestionar las cuentas del Directorio Activo con la misma premisa de no ser administradores.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía “CCN-STIC-859 de recolección y consolidación de eventos” que aun habiendo sido emitida para Windows Server 2008 R2 es igualmente aplicable a sistemas Windows Server 2016. Aunque será mencionada a lo largo de la presente guía, en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en Windows Server 2016 y sus servicios, a través del sistema de Suscripción de eventos con el que Microsoft ya dotó a Windows Server 2008.

Así mismo es importante la creación de grupos a la hora de conceder permisos sobre un recurso. Esto permitirá una gestión más global y sencilla sobre el acceso a los recursos evitando modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

Por ende, es interesante que los usuarios que pertenezcan al grupo que Administrador de CA sean usuarios que no pertenezcan al grupo de administradores del dominio, administradores de empresas, ni sean cuentas locales de administración. Estos roles de administración se asignarán mediante el complemento de Entidad de Certificación.

#### 1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Altamente vinculado al punto “1.1.1.1 OP. ACC. 2. REQUISITOS DE ACCESO”, este proceso requiere consolidación de los derechos de acceso, de tal forma que:

- a) Exista la aplicación del mínimo privilegio. Los privilegios de cada recurso se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.
- b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
- c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

Como ya se comentó previamente, Microsoft Windows Server 2016 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

En la navegación a Internet, acceso a recursos o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administrador para poder utilizarlos. Así y sin darse cuenta podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, que descargados de Internet u otras fuentes de dudosa confianza con máximos privilegios.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña. Se establece por lo tanto a nivel de los recursos, el aplicar mecanismos de ACL para permitir la visualización de contenido o edición del mismo a los usuarios que los requieran exclusivamente.

De esta forma el principio de mínima exposición y menor privilegio se puede materializar de forma extensiva a los propios administradores de los servidores y servicios que gestiona la organización.

Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso para alterar el contenido de una carpeta no por ello implica que sea necesario que posea el permiso de “Control total”. Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS.

### 1.1.2. EXPLOTACIÓN

Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define a través de ellas una serie de procesos tanto para el control, como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

#### 1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que Entidad de Certificación debe configurarse previamente a su entrada en producción teniendo en cuenta las siguientes directrices:

- a) Se retiren cuentas y contraseñas estándar.
- b) Se aplique la regla de mínima funcionalidad.

Se considera indispensable que el sistema no proporcione funcionalidades gratuitas. Solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán, mediante el control de la configuración, aquellas funciones que no sean necesarias e incluso aquellas que sean inadecuadas al fin que se persigue.

Para el cumplimiento en este sentido, las diferentes plantillas de seguridad se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad. Adicionalmente, se protegerán los más importantes de tal forma que quedarán configurados, a través de las políticas de grupo que correspondieran, por categorías. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

#### 1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN

Se deberá tener en consideración la configuración de los componentes del sistema que se gestione de forma que:

- a) Se mantenga en todo momento la regla de funcionalidad mínima y seguridad por defecto.
- b) El sistema debe adaptarse a las nuevas necesidades las cuales previamente han sido autorizadas y probadas en un entorno de test antes de la puesta en producción.
- c) El sistema debe reaccionar ante vulnerabilidades reportadas e incidentes.

### 1.1.2.3. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS

Aplicable en las categorías altas de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

- a) Quién realiza la actividad, cuándo la realiza y sobre qué.
- b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.
- c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.
- d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.
- e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

Una Entidad de Certificación implementa mecanismos para la auditoría de acceso a objetos. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. Ya comentado previamente, la guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoría desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

## 1.2. MEDIDAS DE PROTECCIÓN

Las medidas de protección se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

### 1.2.1. MP.INFO.9. COPIAS DE SEGURIDAD

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Entidad Certificadora ofrece la posibilidad de almacenar la clave privada y el certificado de CA, además de los datos de certificados emitidos y el registro de la base de datos de los certificados.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

- a) Información de trabajo de la organización.
- b) Aplicaciones en explotación, incluyendo los sistemas operativos.
- c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
- d) Claves utilizadas para preservar la confidencialidad de la información.

## 2. RESUMEN Y APLICACIÓN DE MEDIDAS EN ENTIDAD DE CERTIFICACIÓN SOBRE WINDOWS SERVER 2016

A continuación, se establece un cuadro resumen con las diferentes medidas a aplicar, así como los mecanismos que se implementarán para su aplicación. Dichas implementaciones podrán provenir de la revisión de otras guías de seguridad de la serie CCN-STIC-500, de la serie CCN-STIC-800 o bien la aplicación de políticas de seguridad a nivel de dominio o bien localmente.

| Control     | Medida                                   | Mecanismo de aplicación                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OP. ACC. 2  | Requisitos de acceso                     | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |
| OP. ACC. 3  | Segregación de funciones y tareas        | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |
| OP. ACC. 4  | Proceso de gestión de derechos de acceso | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |
| OP. EXP. 2  | Configuración de seguridad               | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |
| OP. EXP. 3  | Gestión de la configuración              | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |
| OP. EXP. 8  | Registro de actividad de los usuarios    | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica. Revisión e implementación guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2. |
| MP. INFO. 9 | Copias de seguridad                      | Revisión e implementación de guía CCN-STIC-598, adaptándolos a la organización.                                                                                                                                                                                                                                                                                                                           |

## ANEXO A.2. CATEGORÍA BÁSICA

### ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Microsoft Windows Server 2016 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

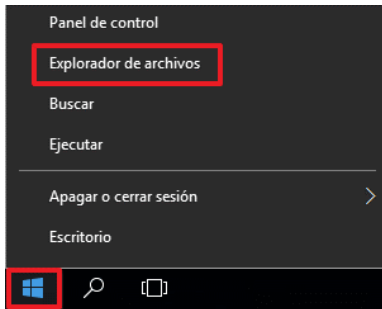
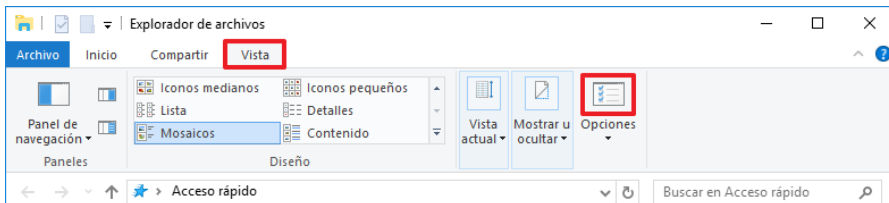
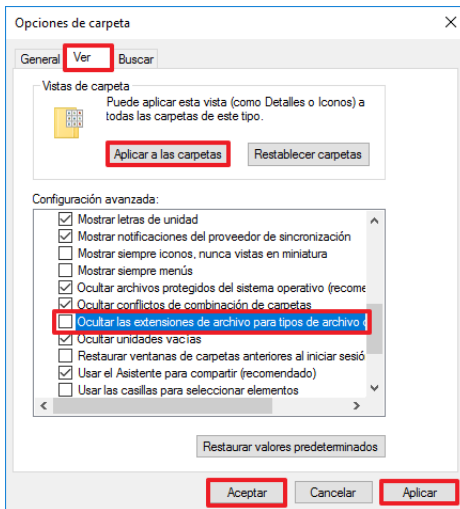
Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

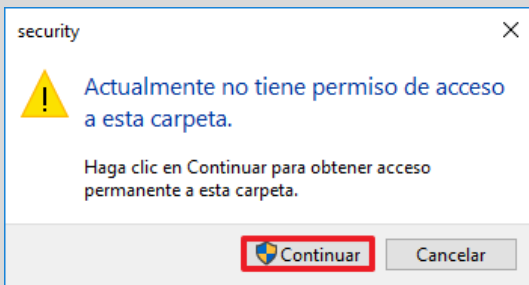
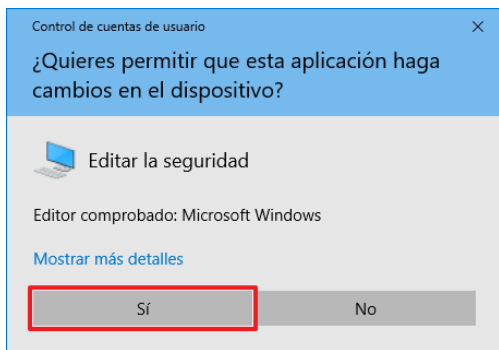
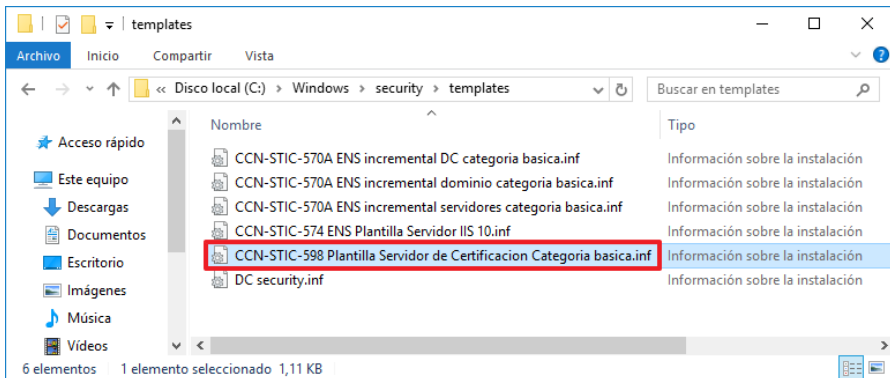
- a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad básica.
- b) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad básica.

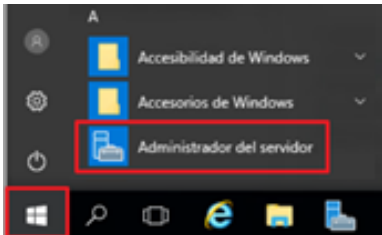
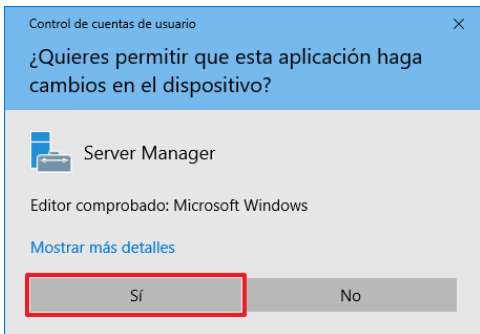
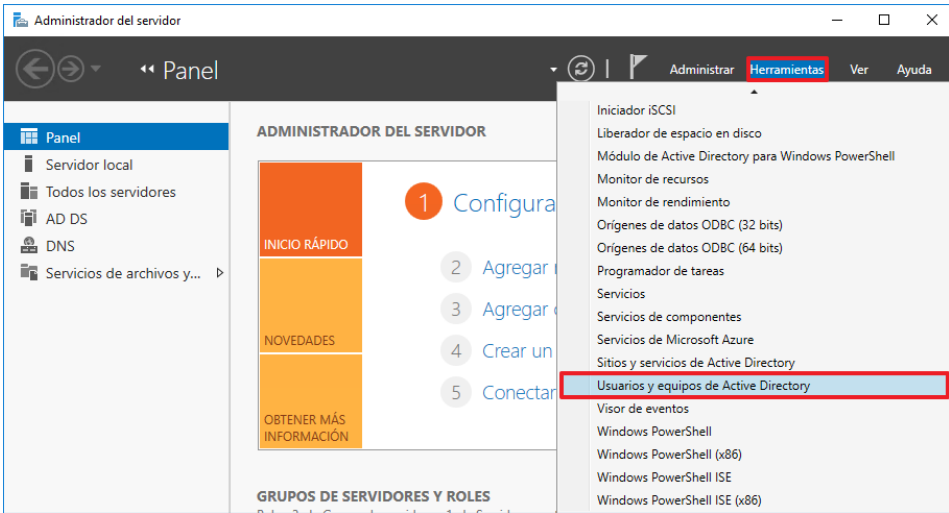
## 1. PREPARACIÓN DEL DOMINIO

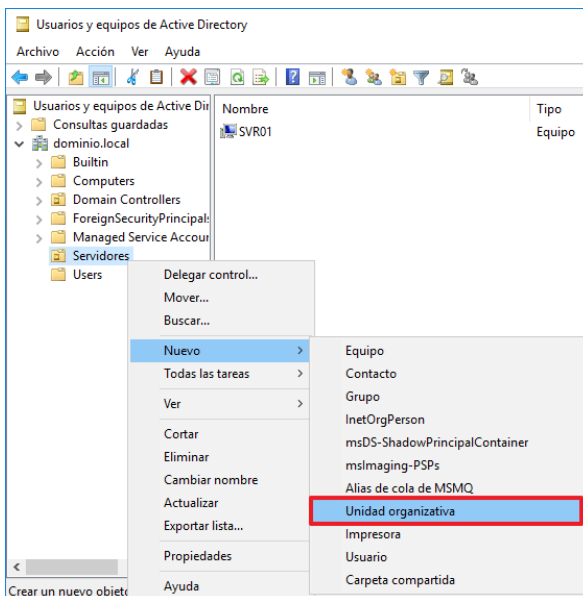
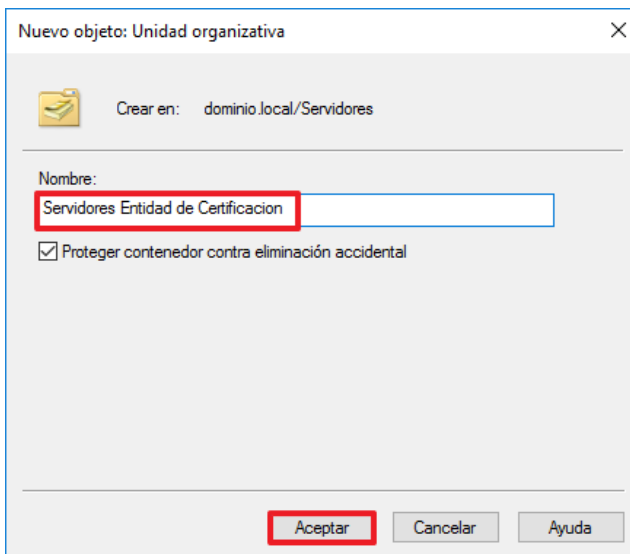
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor de Entidad de Certificación.

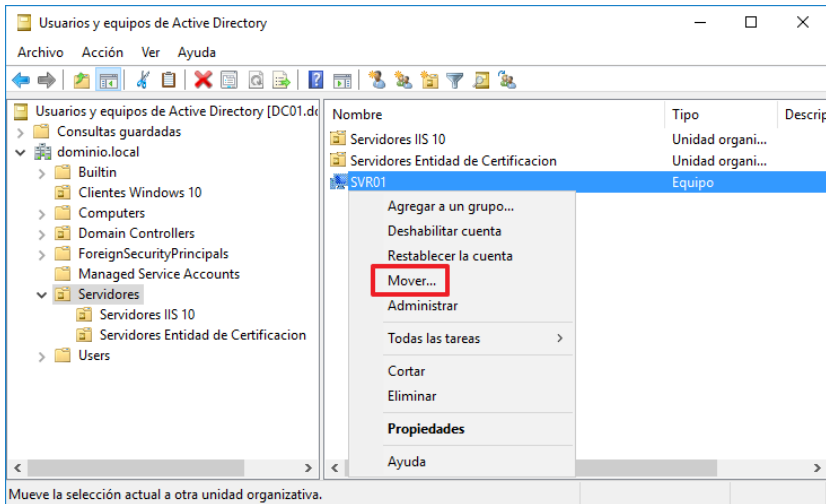
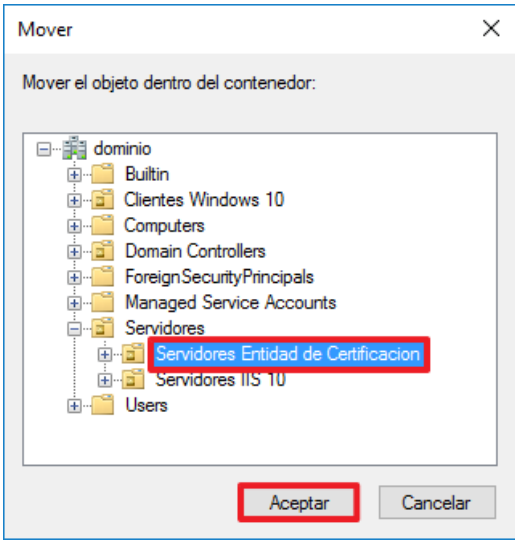
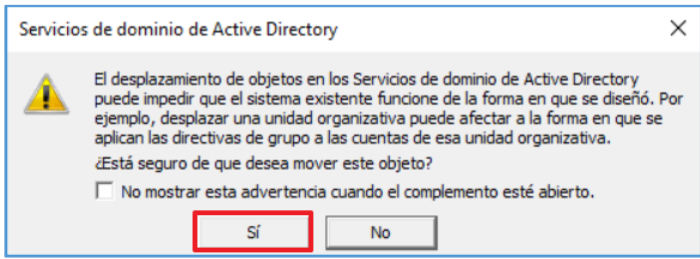
| Paso                                                                         | Descripción                                                                                                                                                                                             |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.                                                                           | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  |
| <b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio. |                                                                                                                                                                                                         |

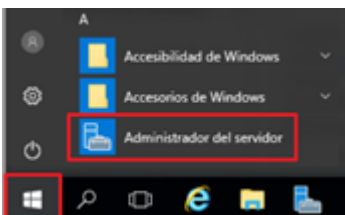
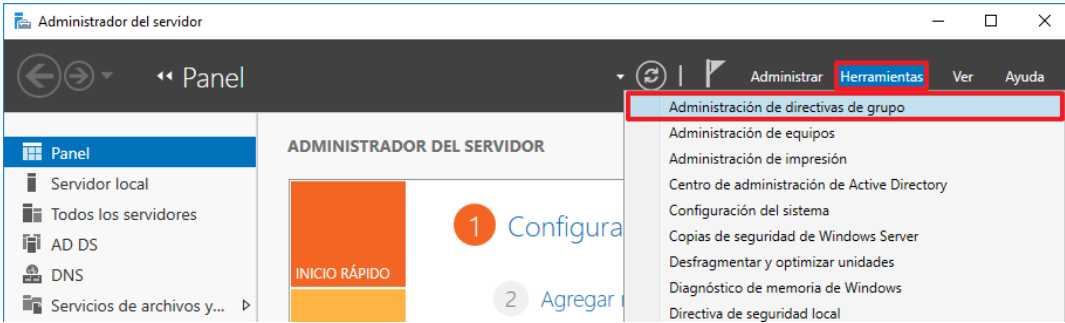
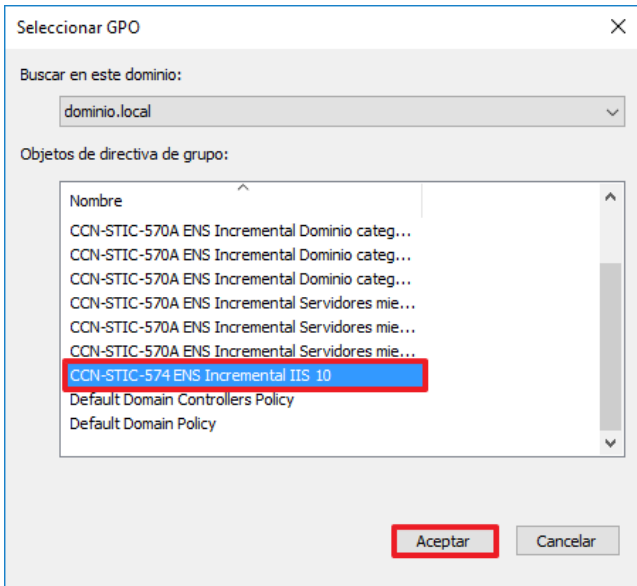
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.   | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                                                                                                                                                                                         |
| 3.   | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                                                                                                                                                                                                                                         |
| 4.   | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>                         |
| 5.   | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                                          |
| 6.   | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |

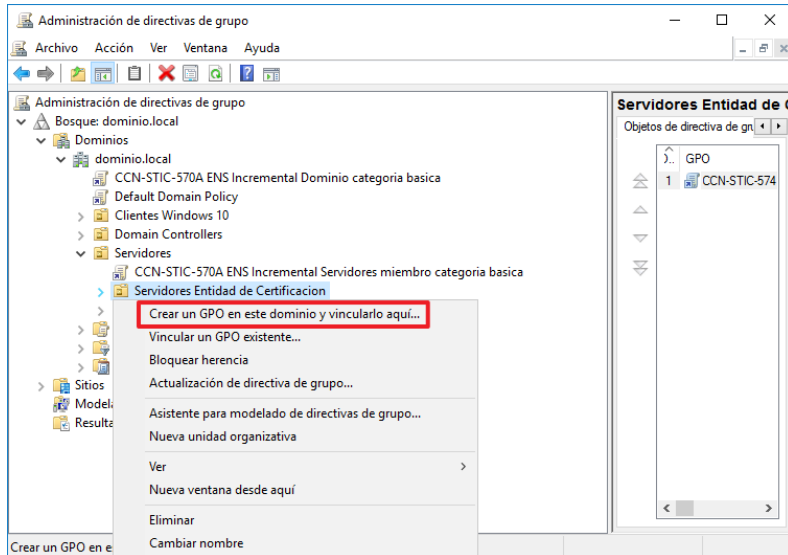
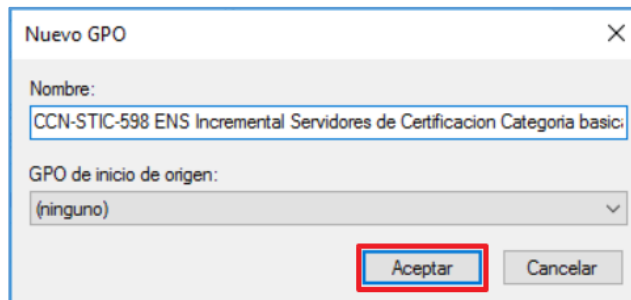
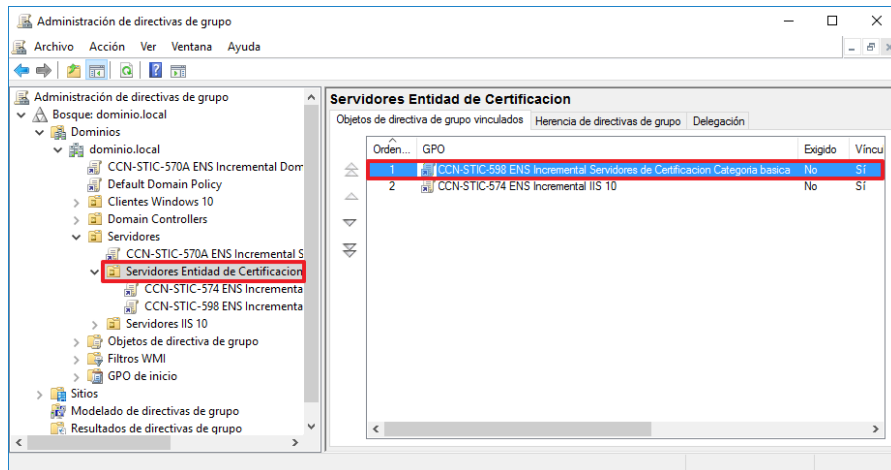
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.   | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                                                                                                                                                                                                                             |
| 8.   | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |
| 9.   | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría básica.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>                                                                                                                                                                                                                                                                                                                                                                                   |

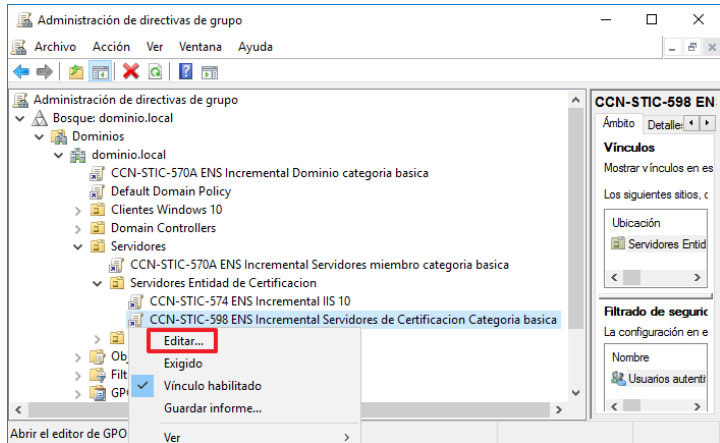
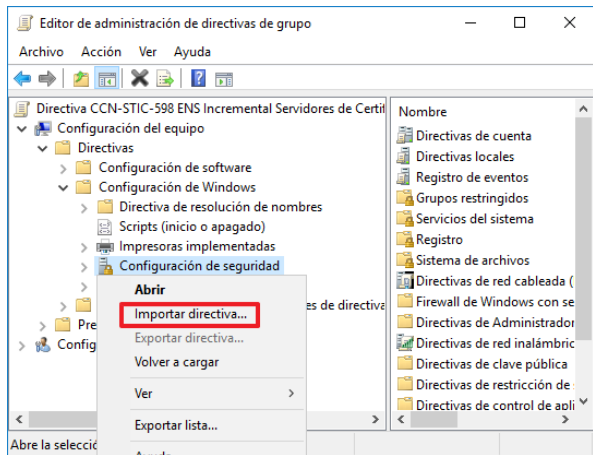
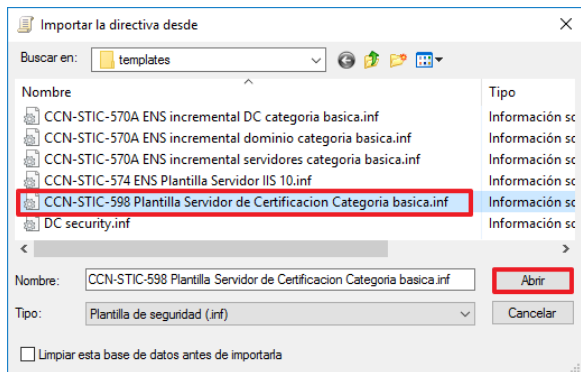
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el icono correspondiente en el menú de Inicio de Windows.</p>                                                                                                                 |
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                             |
| 12.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione “Herramientas → Usuarios y equipos de Active Directory”.</p>  |

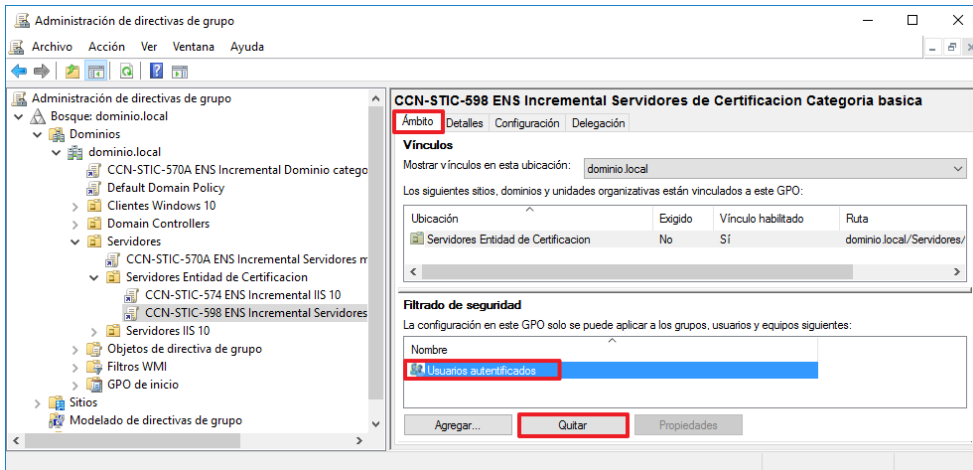
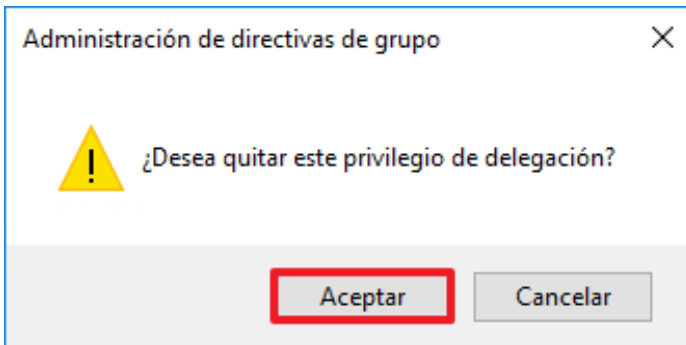
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo “&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local → Servidores”.</p> |
| 14.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

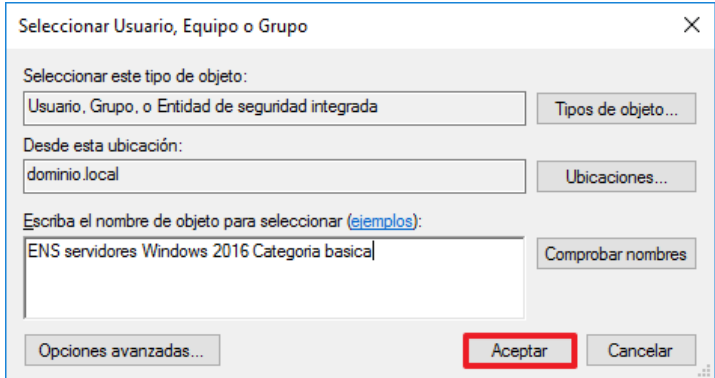
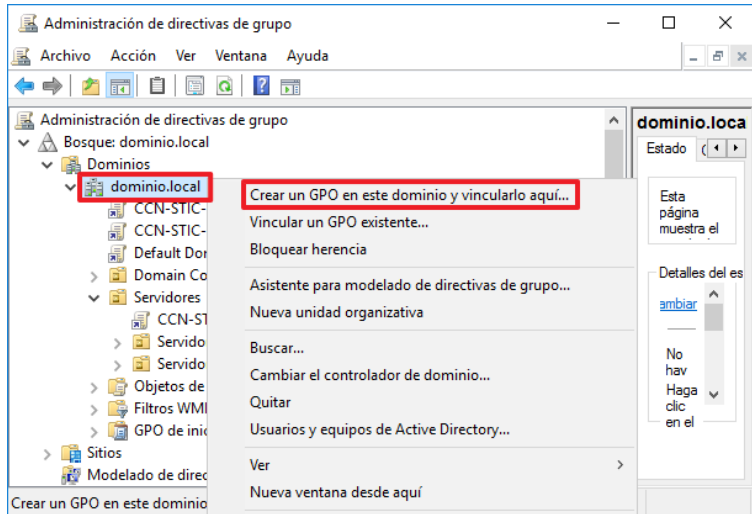
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores de entidad de certificación a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |
| 16.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                            |
| 17.  | <p>Acepte el mensaje de advertencia</p>                                                                                                                                                                                                                                                                                                            |
| 18.  | <p>Cierre la herramienta de “Usuarios y equipos de Active Directory”.</p>                                                                                                                                                                                                                                                                                                                                                              |

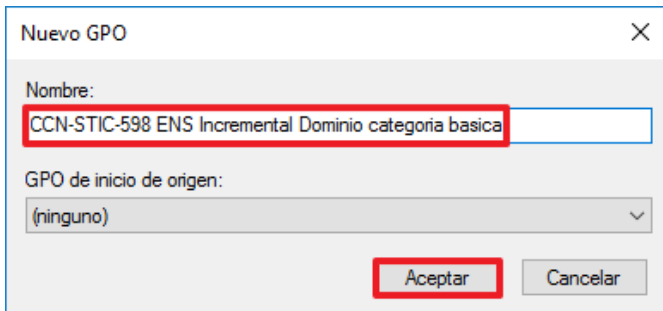
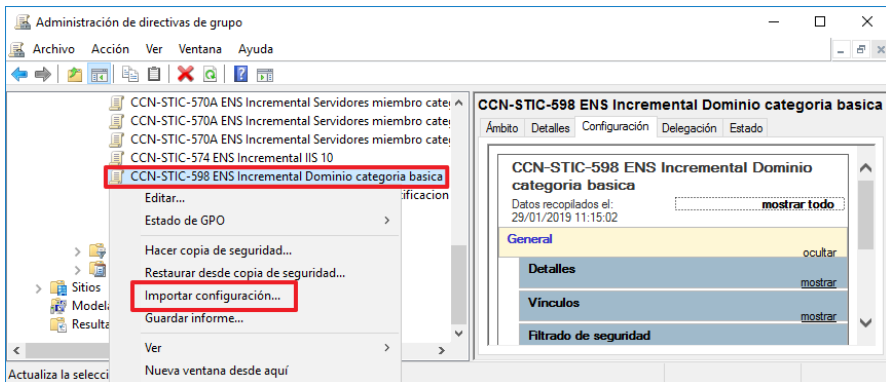
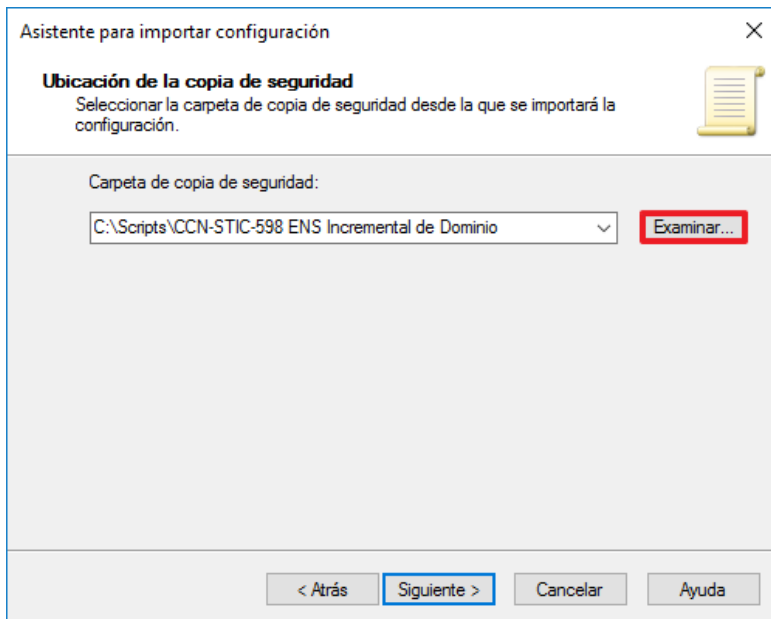
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.  | <p>A continuación, abra el “Administrador del servidor”.</p>                                                                                                                                                                                             |
| 20.  | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón “Herramientas → Administración de directivas de grupo”.</p>                                                                                                 |
| 21.  | <p>A continuación, despliegue el nodo “Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p>               |
| 22.  | <p>Seleccione “Vincular un GPO existente...” y vincule el objeto de directiva de grupo “CCN-STIC-574 ENS Incremental IIS 10” a la nueva unidad organizativa “Servidores Entidad de Certificación”, haciendo clic con el botón derecho sobre ella.</p>  |

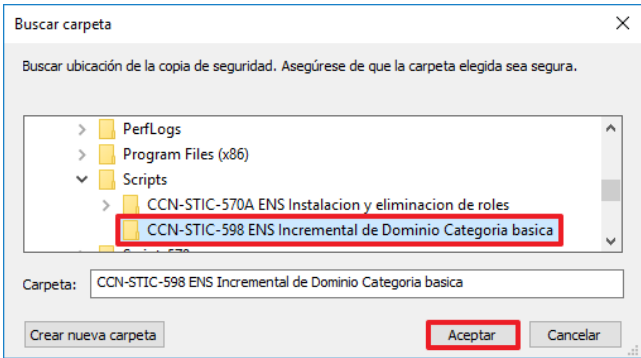
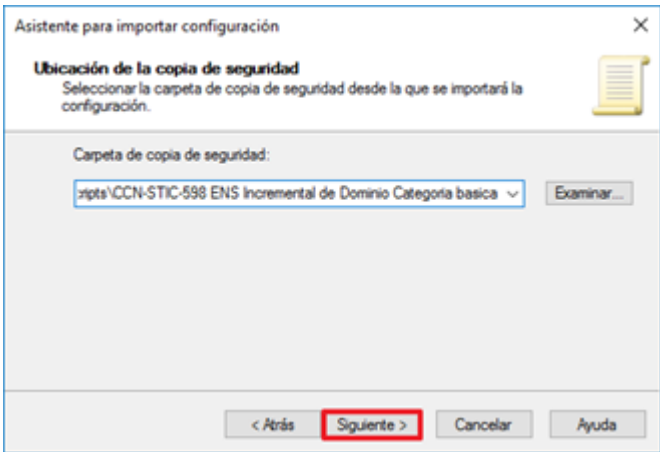
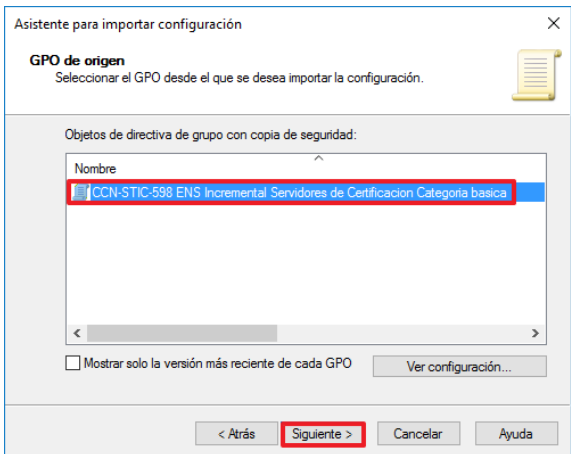
| Paso     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |         |         |         |   |                                                                           |    |    |   |                                     |    |    |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|---------|---------|---|---------------------------------------------------------------------------|----|----|---|-------------------------------------|----|----|
| 23.      | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                           |          |         |         |         |   |                                                                           |    |    |   |                                     |    |    |
| 24.      | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica” y haga clic en el botón “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |         |         |         |   |                                                                           |    |    |   |                                     |    |    |
| 25.      | <p>Seleccione la unidad organizativa “<b>Servidores Entidad de Certificación</b>”. En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  <table><thead><tr><th>Orden...</th><th>GPO</th><th>Exigido</th><th>Vínculo</th></tr></thead><tbody><tr><td>1</td><td>CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica</td><td>No</td><td>SI</td></tr><tr><td>2</td><td>CCN-STIC-574 ENS Incremental IIS 10</td><td>No</td><td>SI</td></tr></tbody></table> | Orden... | GPO     | Exigido | Vínculo | 1 | CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica | No | SI | 2 | CCN-STIC-574 ENS Incremental IIS 10 | No | SI |
| Orden... | GPO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Exigido  | Vínculo |         |         |   |                                                                           |    |    |   |                                     |    |    |
| 1        | CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | No       | SI      |         |         |   |                                                                           |    |    |   |                                     |    |    |
| 2        | CCN-STIC-574 ENS Incremental IIS 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | No       | SI      |         |         |   |                                                                           |    |    |   |                                     |    |    |

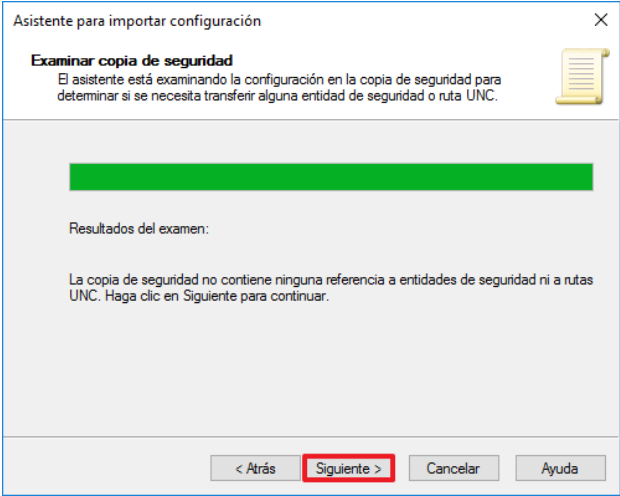
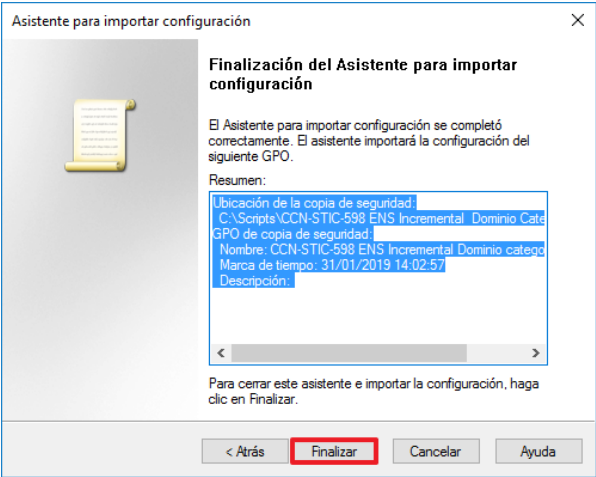
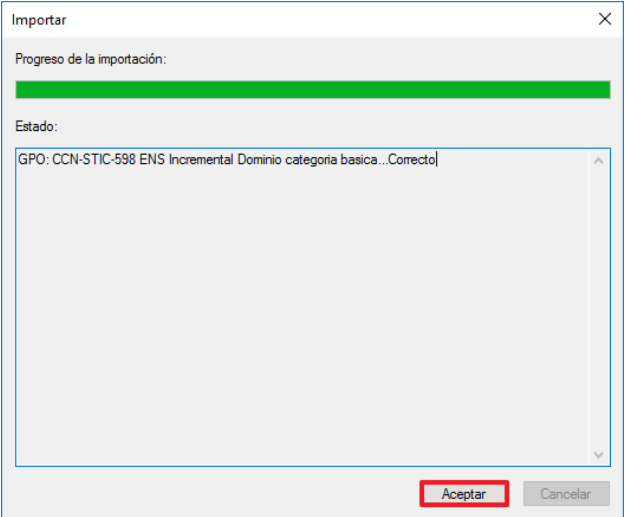
| Paso | Descripción                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.  | De esta forma, se garantiza que la directiva se aplica correctamente.                                                                                                                                                                                     |
| 27.  | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción “Editar”.</p>                              |
| 28.  | <p>Expanda el nodo “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad”.</p>                                                                                                                                   |
| 29.  | <p>Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.</p>                                                  |
| 30.  | <p>Seleccione la plantilla “C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría básica.inf”. Haga clic en el botón “Abrir”.</p>  |

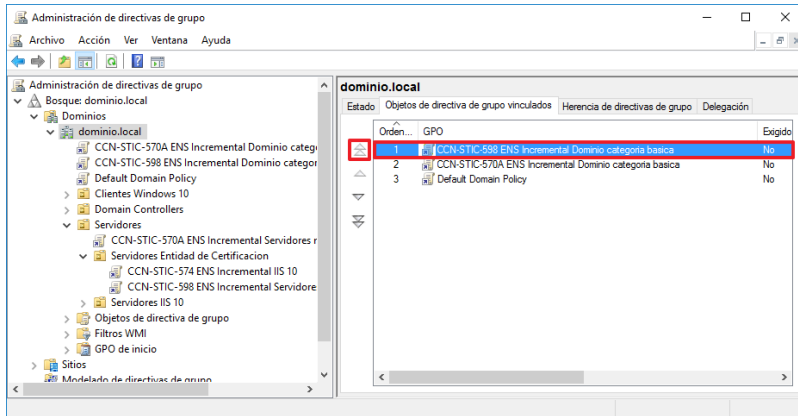
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31.  | Cierre el “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                                                                                      |
| 32.  | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>                                                            |
| 33.  | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34.  | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidor Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoría básica” que contiene el servidor con el rol “Servidor Entidad de Certificación”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 35.  | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 36.  | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

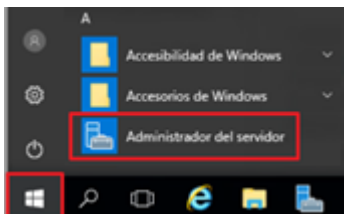
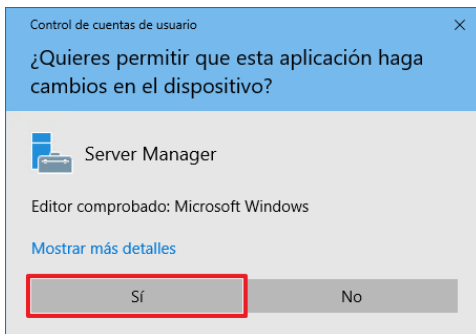
| Paso | Descripción                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 37.  | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 Incremental Dominio categoria basica” y pulse el botón “Aceptar”.</p>                                                       |
| 38.  | <p>Vaya al contenedor “Objetos de directiva de grupo” y edite la GPO recién creada haciendo clic con el botón derecho en ella y seleccionando la opción “Importar configuración”.</p>  |
| 39.  | <p>Haga clic en “Siguiente &gt;” en el “Asistente para importar configuración”.</p>                                                                                                                                                                                       |
| 40.  | <p>Haga clic en “Examinar...”.</p>                                                                                                                                                    |

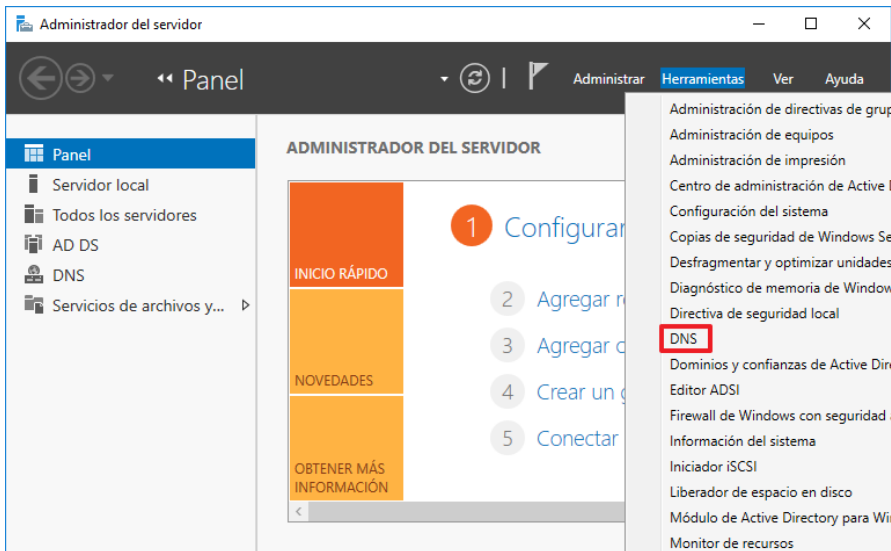
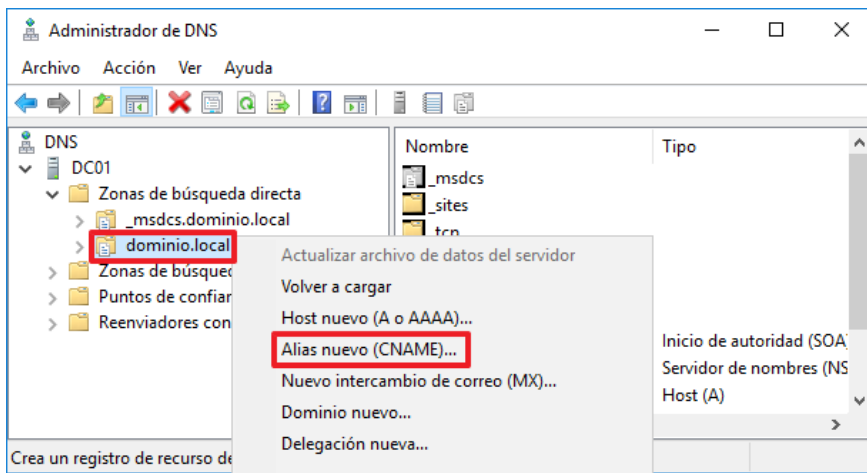
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 41.  | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoria basica” y pulse “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                  |
| 42.  | <p>Pulse “Siguiete &gt;” para continuar con la importación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 43.  | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio Categoria basica” y pulse “Siguiete &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |

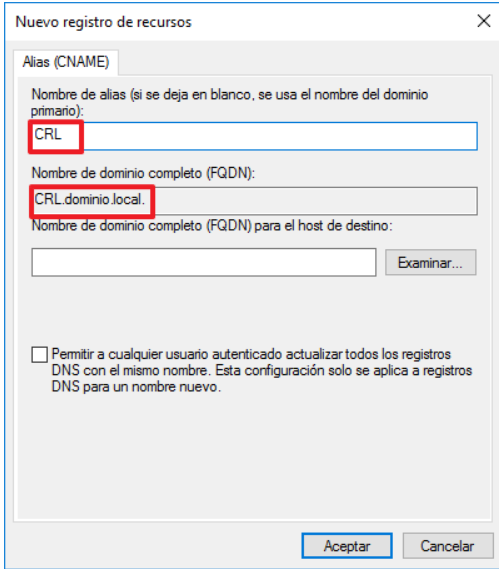
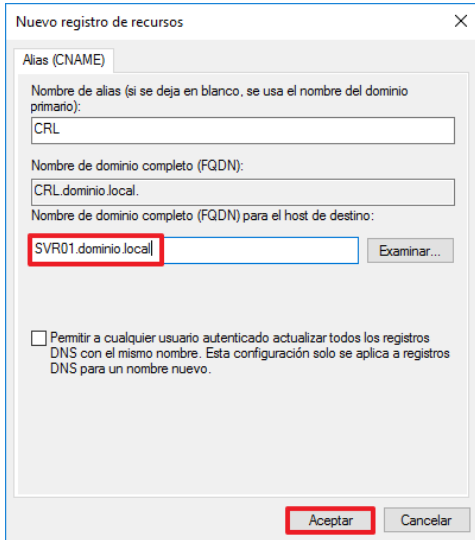
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 44.  | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>                                                                                                 |
| 45.  | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                                                                                                                   |
| 46.  | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>  |

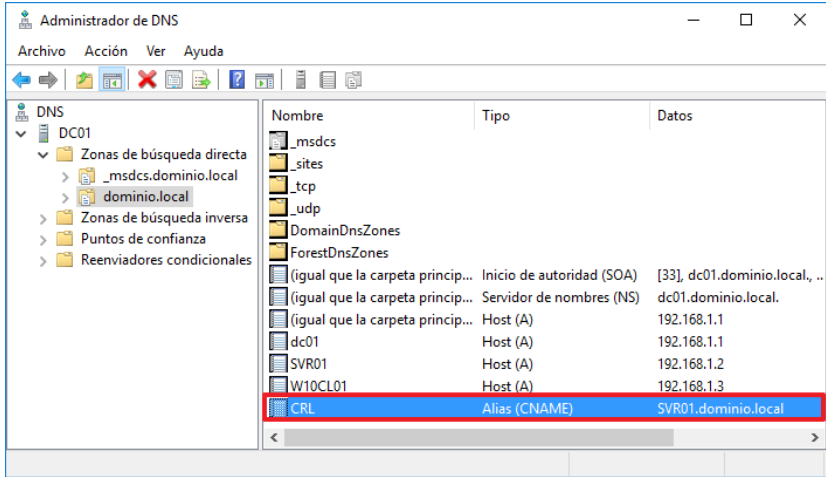
| Paso | Descripción                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 47.  | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>  |
| 48.  | Cierre la ventana “Administración de directivas de grupo”.                                                                                                                                                                                                                                                  |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

| Paso | Descripción                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 49.  | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p>Nota: Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>           |
| 50.  | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 51.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                    |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>                                                                                                                                                    |
| 53.  | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: “&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”.</p> <p>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 54.  | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |
| 55.  | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación subordinada de empresa y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p>         |

| Paso | Descripción                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 56.  | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>  |

## 2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría básica.

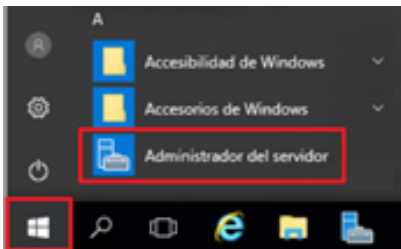
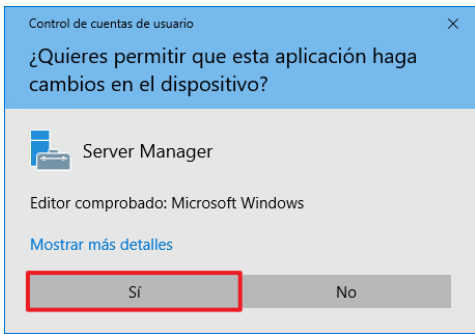
No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

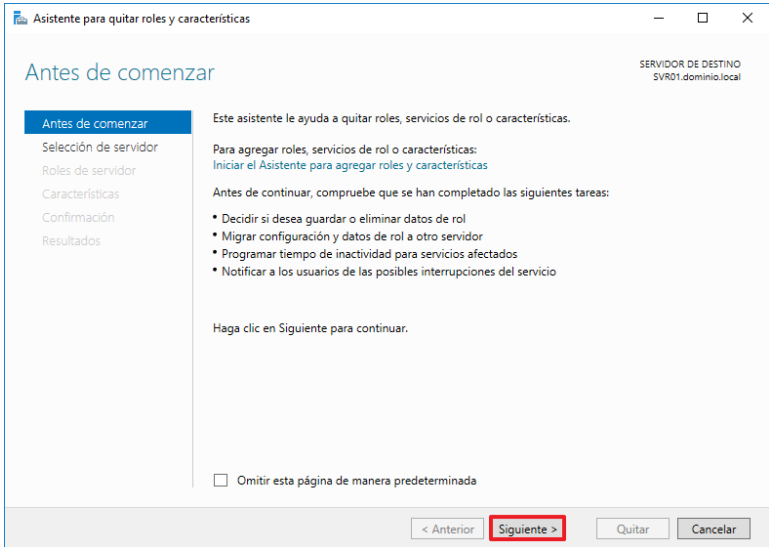
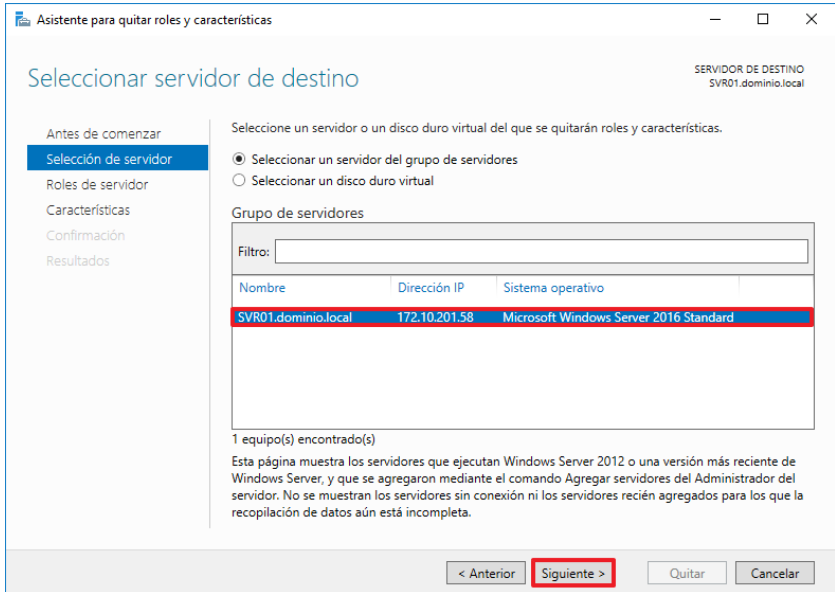
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

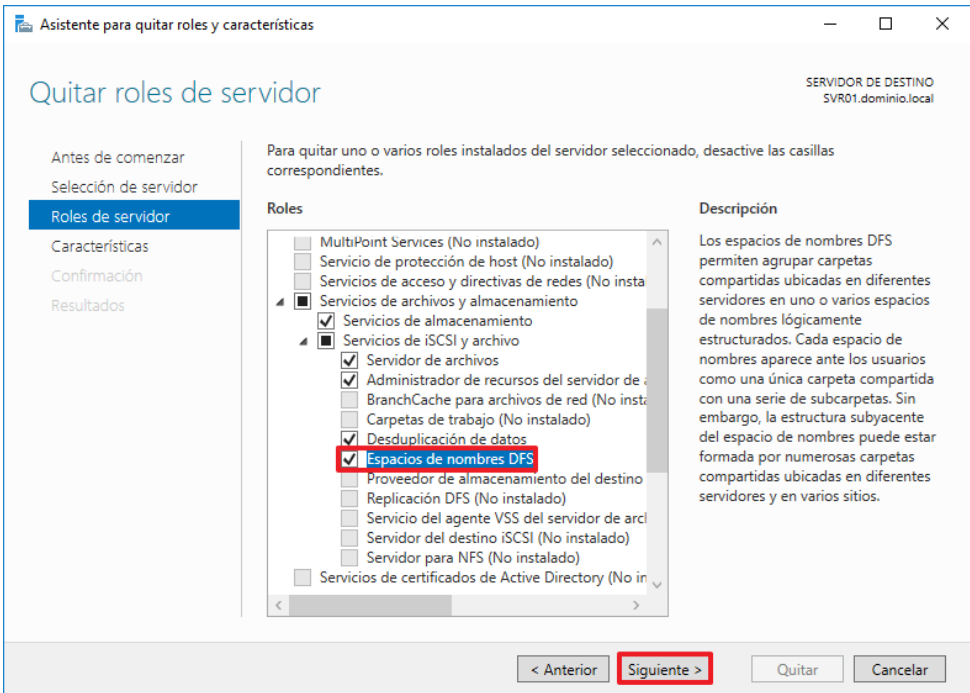
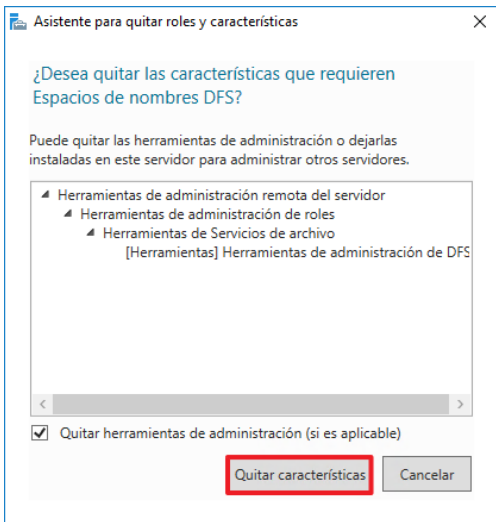
### 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

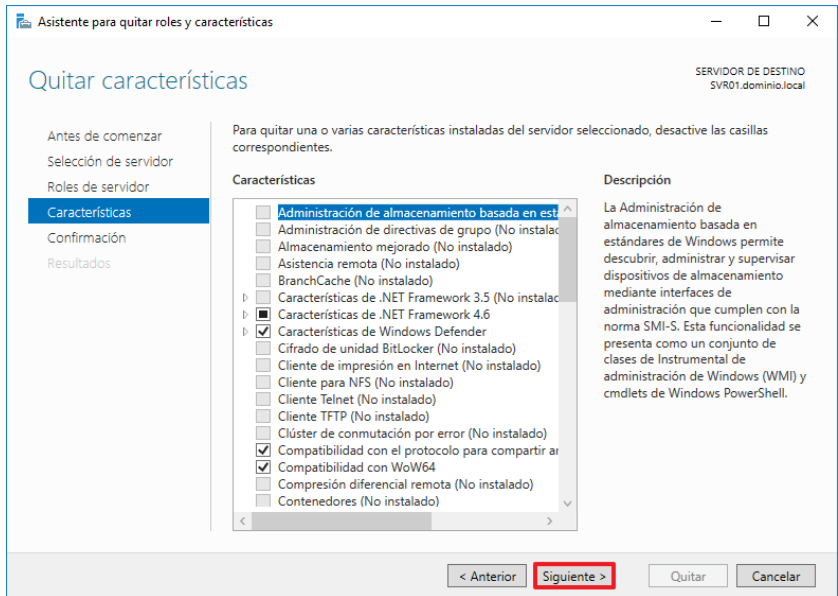
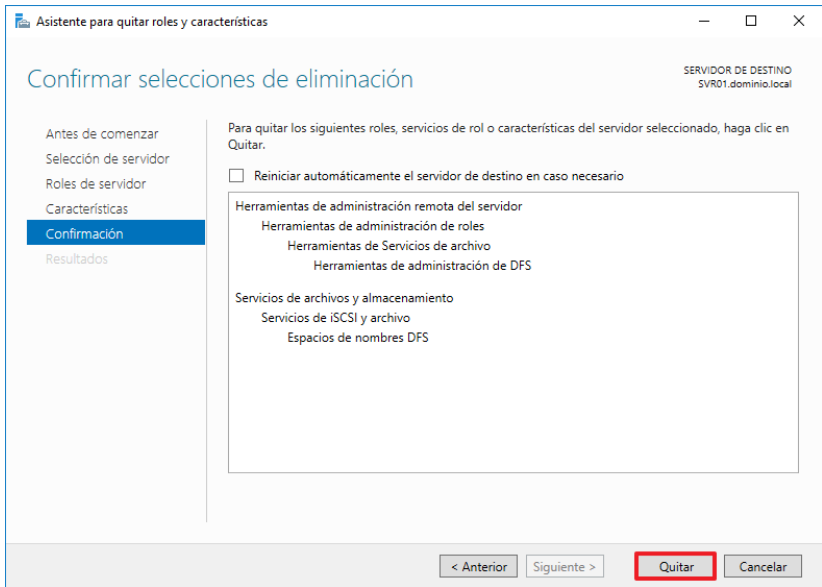
Uno de los aspectos que marca el ENS, desde su requisito de la categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

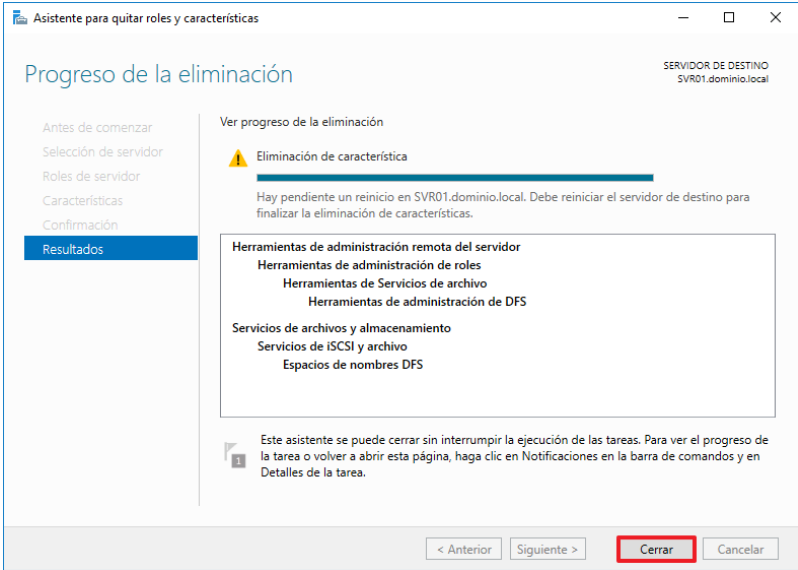
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de Certificación.

| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor Entidad de Certificación .</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 58.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                |
| 59.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                  |
| 60.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>                                                                                                                     |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 61.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>                                                                              |
| 62.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p> |

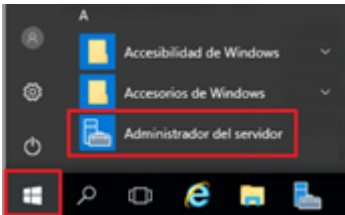
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 63.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |
| 64.  | <p>En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p>     |

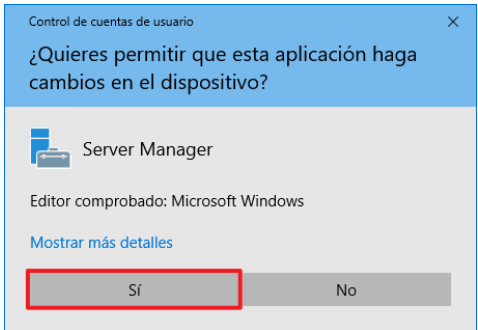
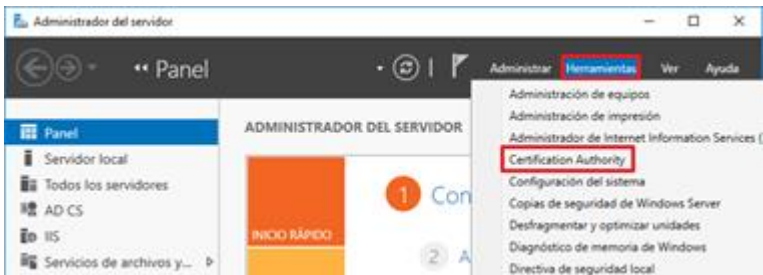
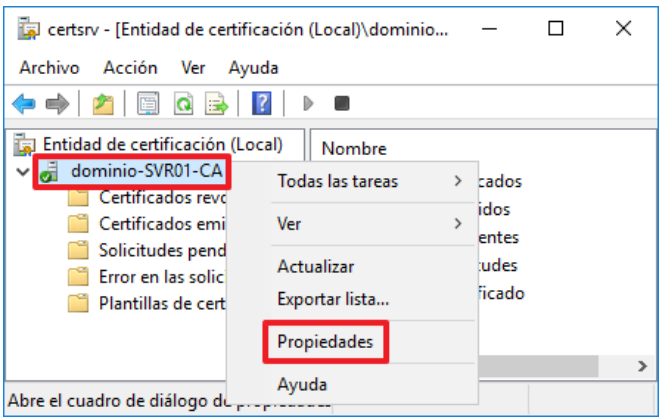
| Paso | Descripción                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 65.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>  |
| 66.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                                                                |

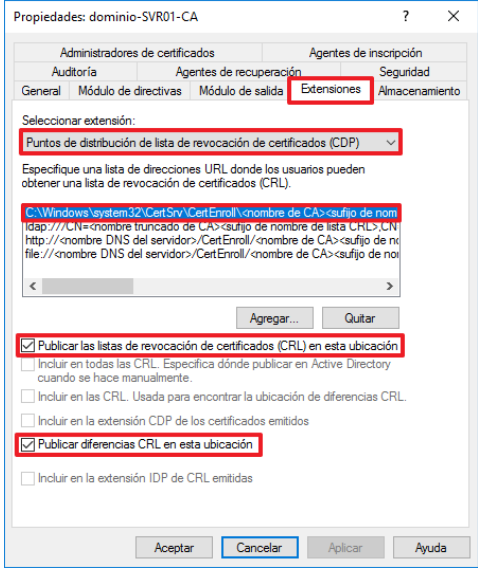
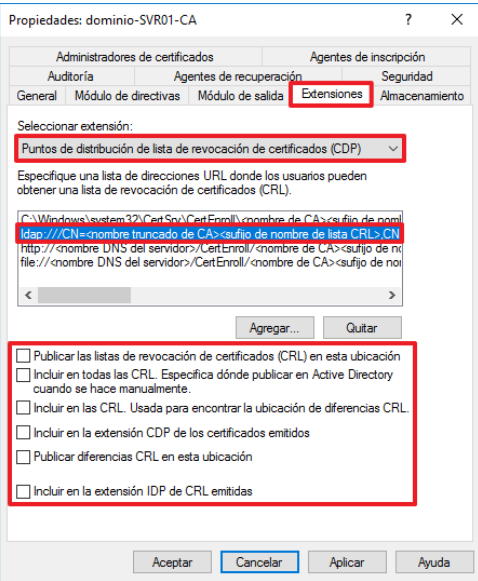
| Paso | Descripción                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 67.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 68.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                  |

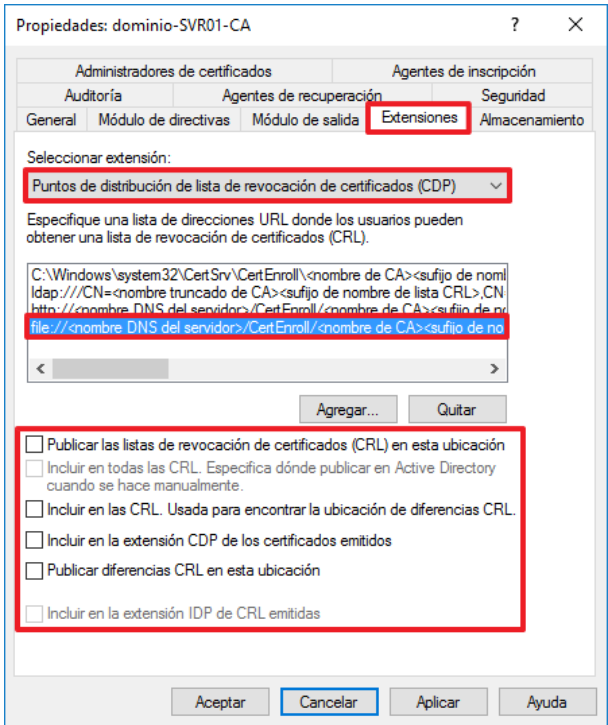
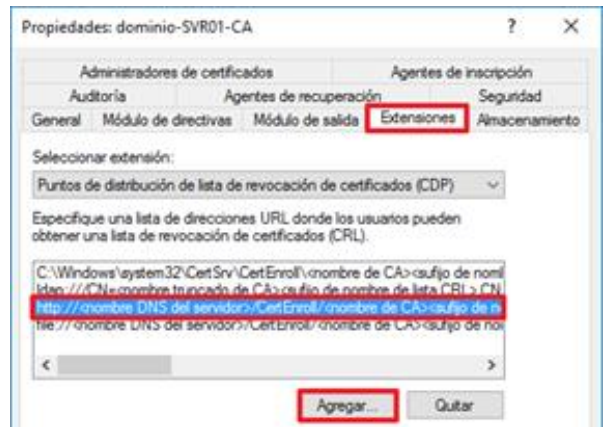
## 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA

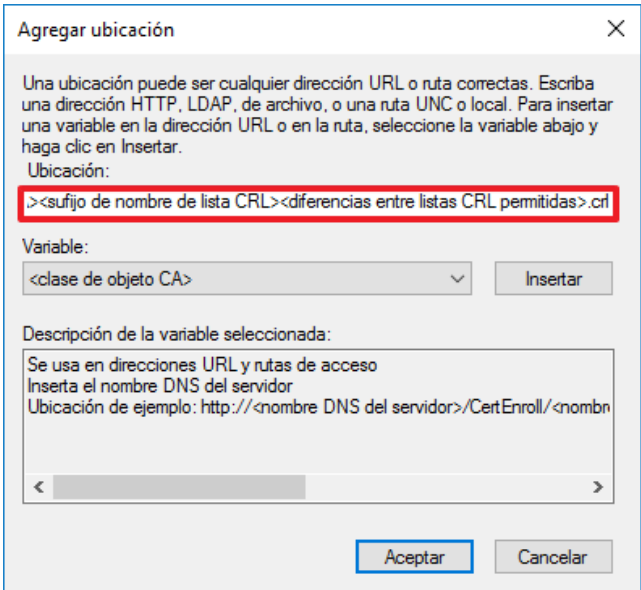
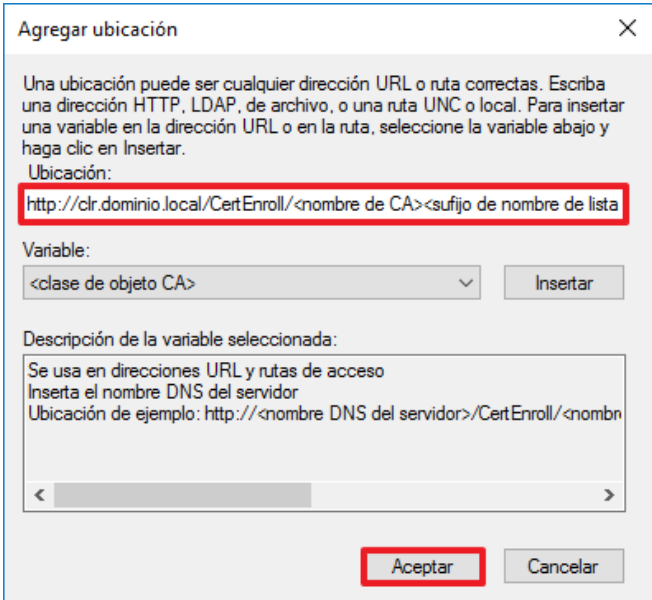
En este apartado, se establecerá la configuración que permite que un sitio web mantenga las CRLs de modo que sean accesibles por todos los clientes de la Entidad de Certificación.

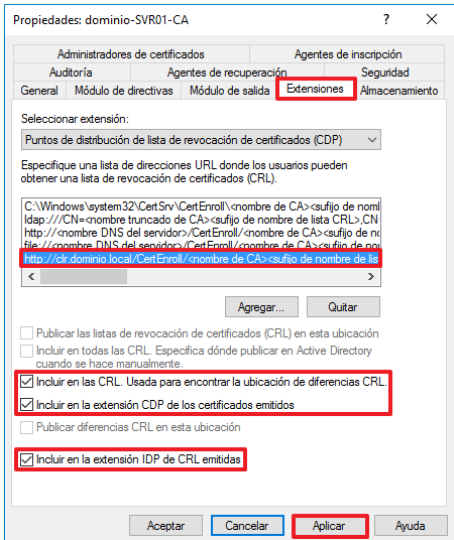
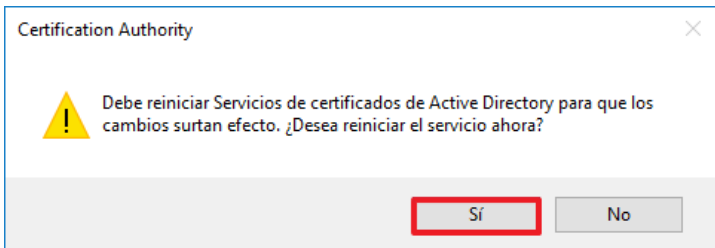
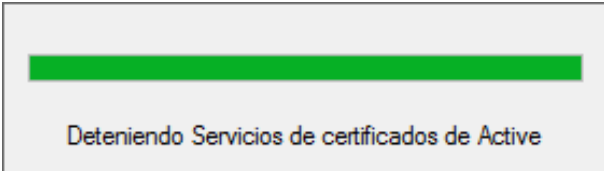
| Paso | Descripción                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 69.  | <p>Inicie sesión en el equipo que posea la Entidad de Certificación raíz de empresa.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p> |
| 70.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>               |

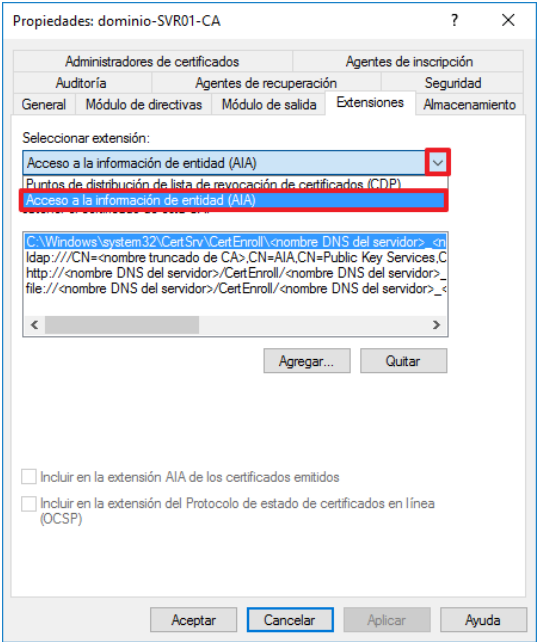
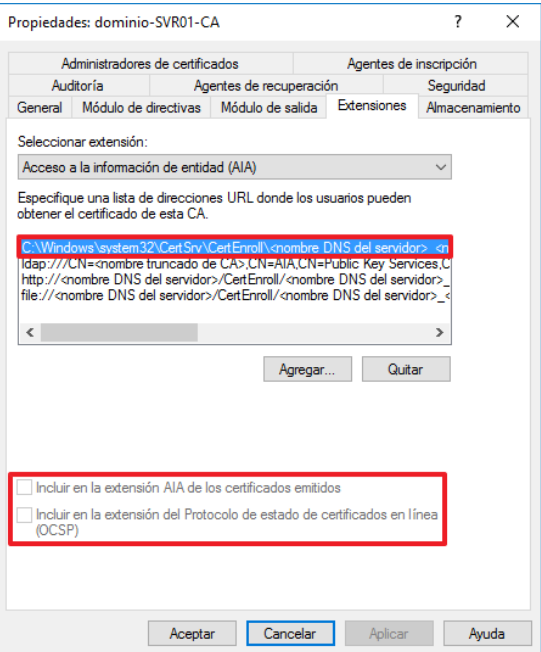
| Paso | Descripción                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 71.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                                                                                          |
| 72.  | <p>En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                                         |
| 73.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado de la Entidad de Certificación y, con el botón derecho del ratón selecciónela, y pulse la opción “Propiedades”.</p>  |

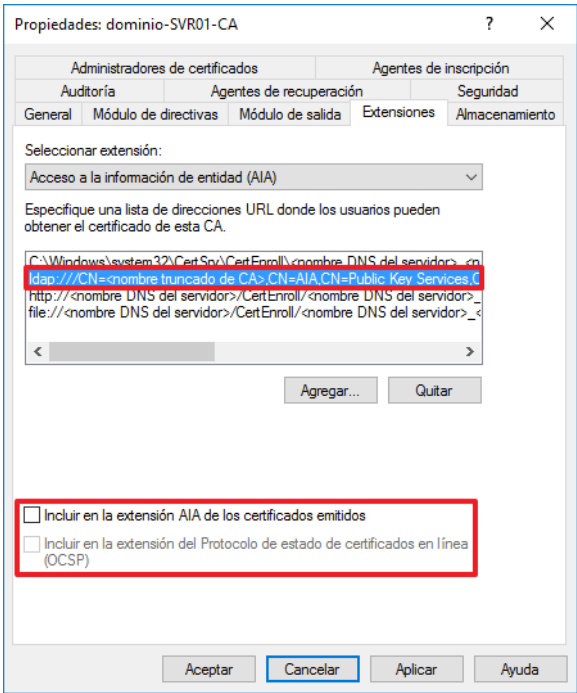
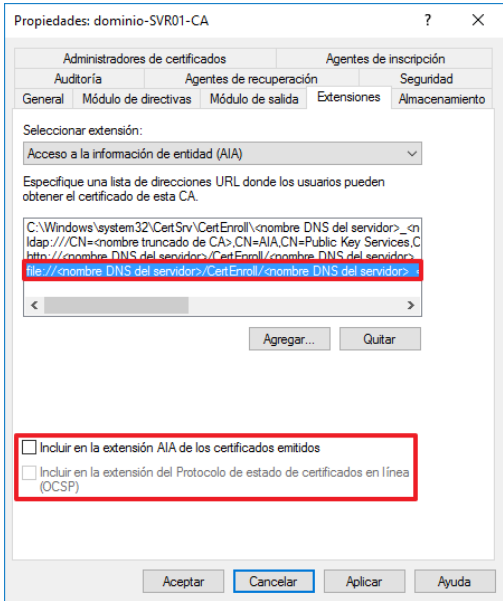
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 74.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\<b>&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</b></p>                   |
| 75.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, deshabilite la publicación de CRLs mediante ldap seleccionando <b>“<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor&gt;,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>”</b> y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>  |

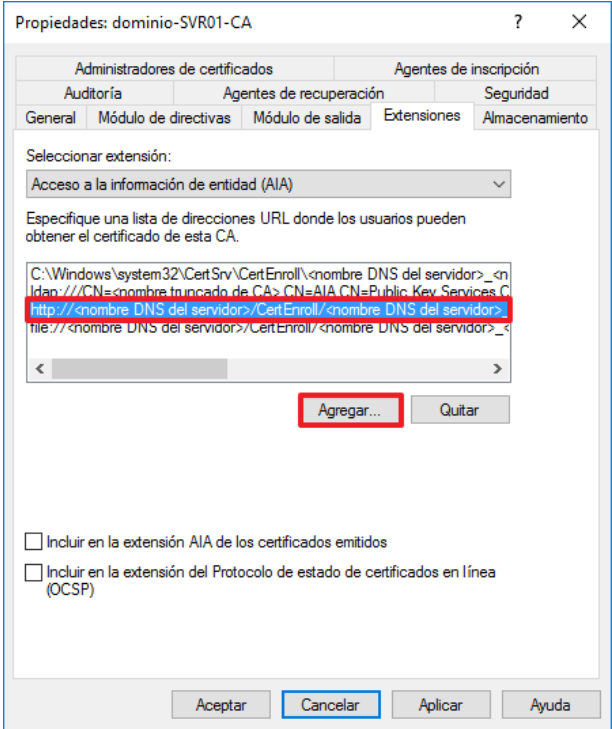
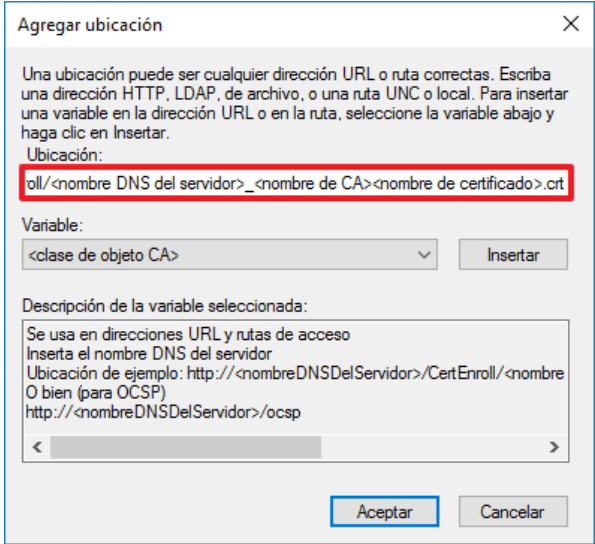
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 76.  | <p>De nuevo en “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> asegúrese que tiene todas las opciones desmarcadas tal y como aparece en la siguiente figura.</p>  |
| 77.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt;sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y copie el elemento mediante la combinación de teclas “Control + C”.</p>                                                                                                |
| 78.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                                                                                                                                                                                              |

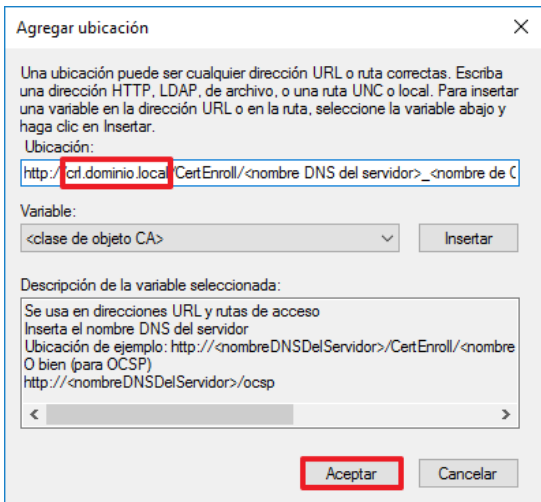
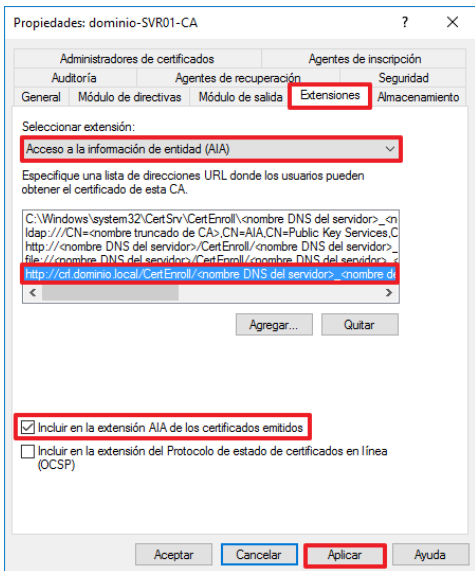
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 79.  | <p>En “Agregar ubicación” coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                                                                              |
| 80.  | <p>En dicha ventana, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

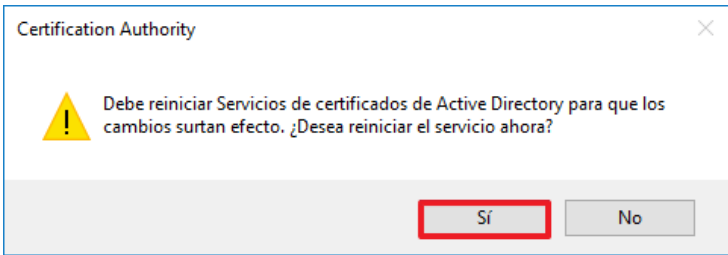
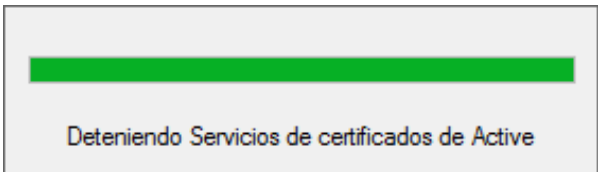
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 81.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul> <p>Pulse “Aplicar” para guardar los cambios</p>  |
| 82.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 83.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 84.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>                                                                       |
| 85.  | <p>Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt” todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 86.  | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> están desmarcadas todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>  |
| 87.  | <p>Seleccione <b>"file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt"</b> y asegúrese que todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>                                                      |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88.  | Seleccione ahora <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b> .                                          |
| 89.  | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                              |
| 90.  | <p>En <b>“Agregar ubicación”</b> coloque el cursor sobre el campo vacío bajo <b>“Ubicación:”</b> y pulse la combinación de teclas <b>“Control + V”</b> para pegar el contenido recién copiado.</p>  |

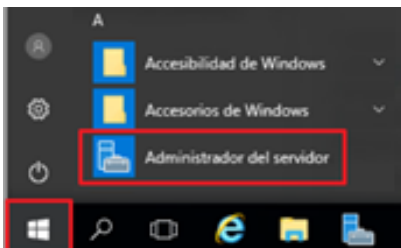
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 91.  | <p>En “Agregar ubicación” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente (B.2. de la presente guía) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |
| 92.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada “http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>                         |

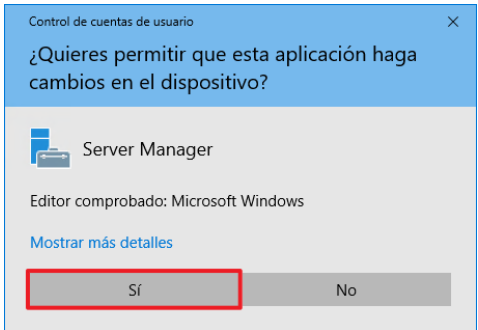
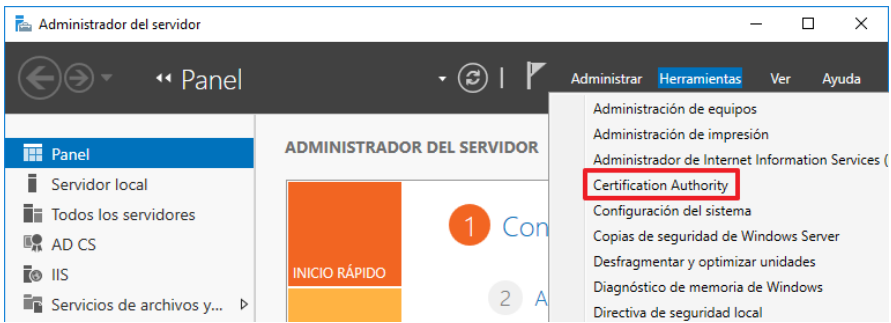
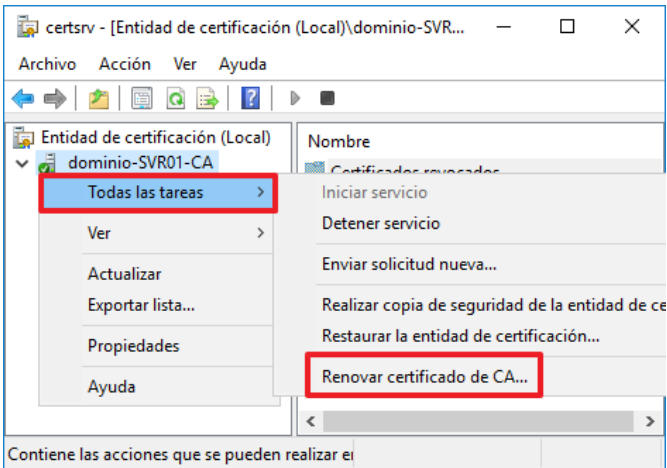
| Paso | Descripción                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>  |
| 94.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                |
| 95.  | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                     |

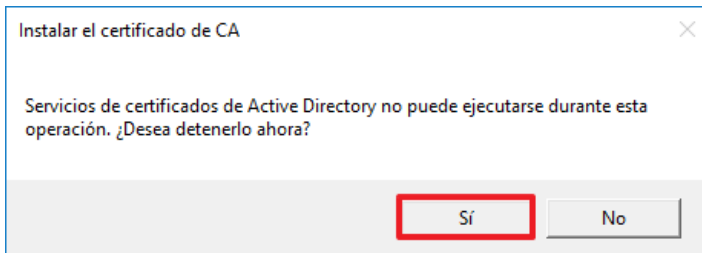
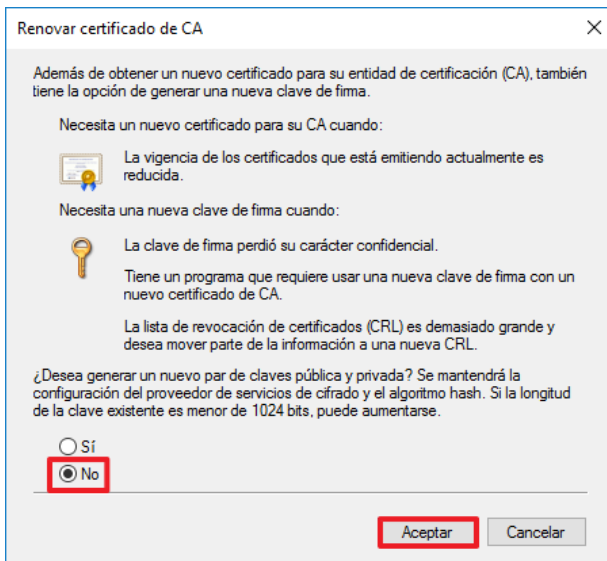
### 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA

Será necesario volver a generar el certificado de la Entidad de Certificación tras hacer modificaciones en las propiedades.

Los pasos que se definen a continuación comprenden la renovación de una Entidad de Certificación raíz de empresa.

| Paso | Descripción                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Inicie sesión en el equipo Entidad de Certificación raíz.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p>            |
| 97.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 98.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                                                                                                                              |
| 99.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                                                         |
| 100. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificados y con el botón derecho del ratón selecciónela y pulse sobre “Todas las tareas → Renovar certificado de CA...”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 101. | <p>Pulse “Sí” en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 102. | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Si la entidad raíz es de empresa, no será necesario establecer ningún paso adicional, en caso de ser una Entidad de Certificación independiente del dominio, además de haber tenido que encenderla para realizar el proceso, será necesario extraer el fichero “.CRT” que se ha generado en la ruta “%SYSTEMROOT%\System32\CertSrv\CertEnroll” y pegarlas en la misma ruta, pero en la Entidad de Certificación subordinada de empresa.</p> |

## ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad para entidad de certificación sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.2.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS”

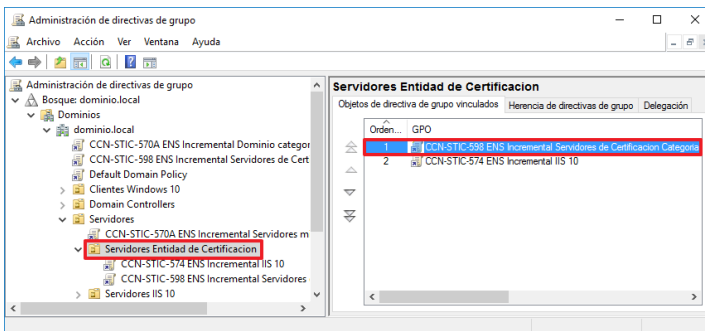
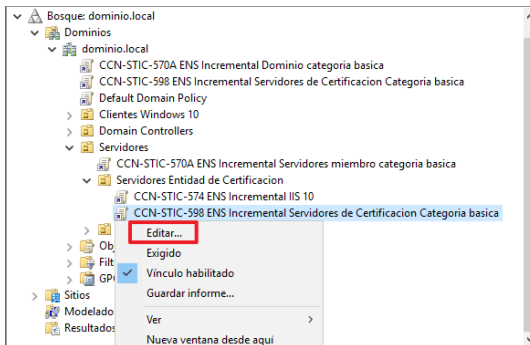
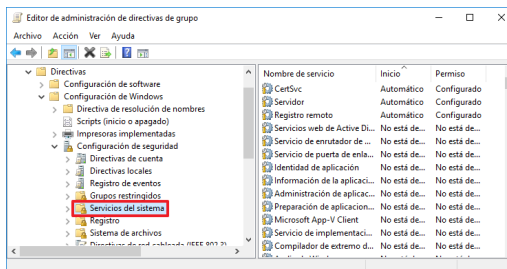
### 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

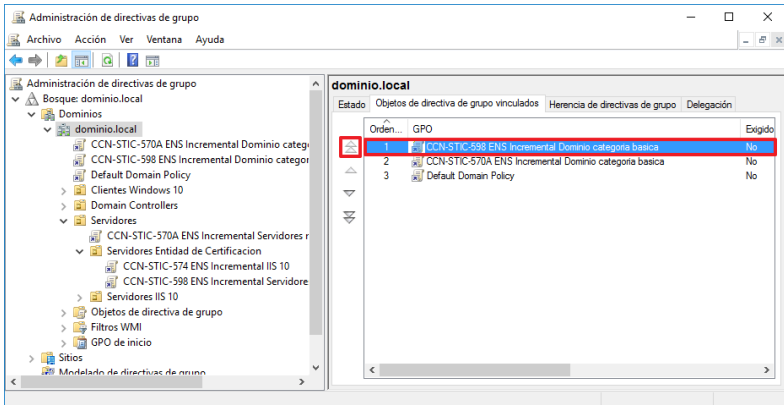
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

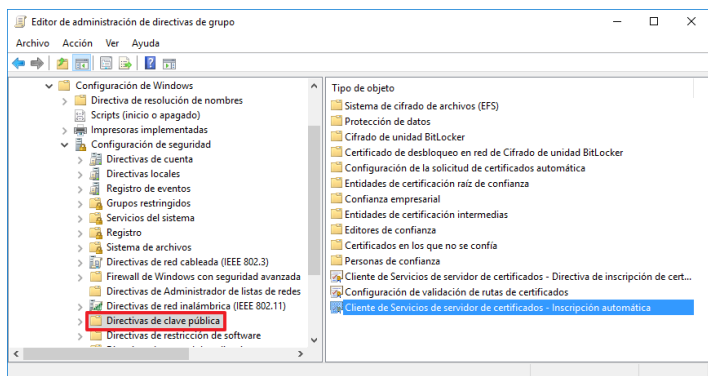
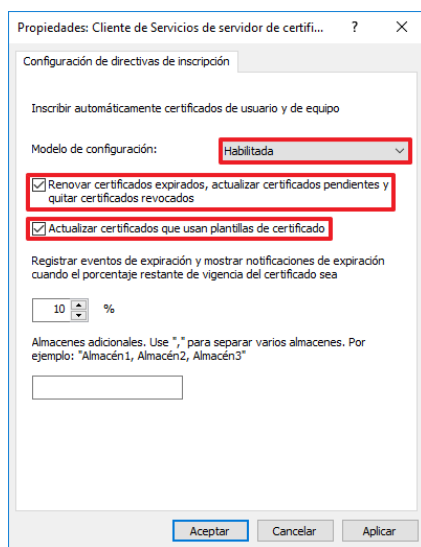
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

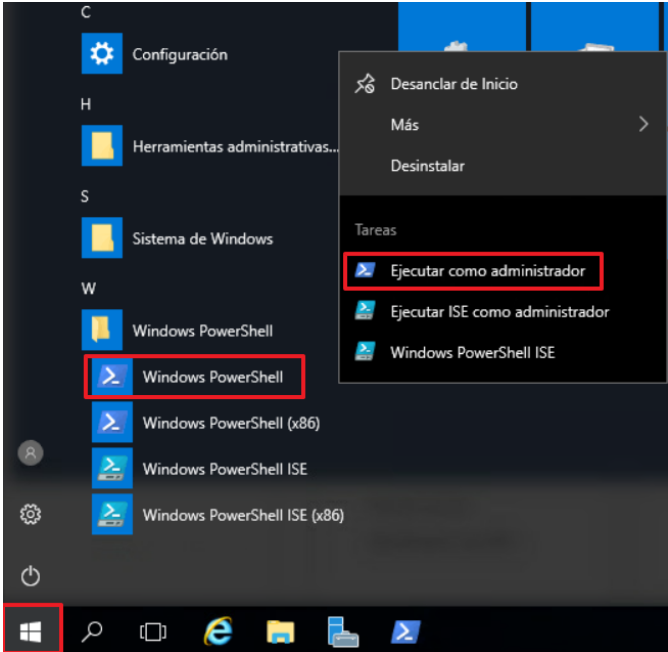
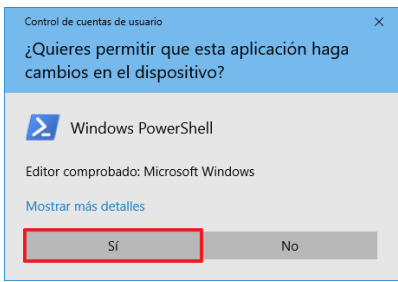
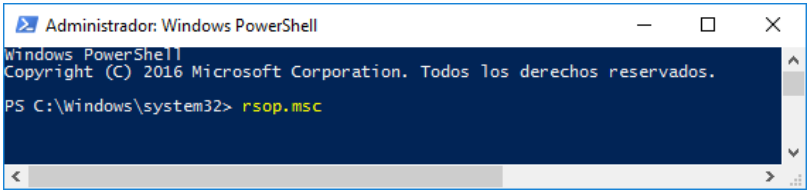
**Nota:** La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

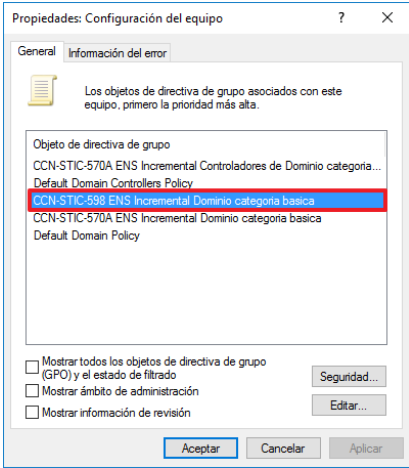
| Comprobación                                   | OK/NOK | Cómo hacerlo                                                                                                              |
|------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------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

| Comprobación                                                                                                                        | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica”.              |        | <p>Ejecute el “Administrador de directivas de grupo” mediante la siguiente ruta:<br/> <b>“Inicio → Herramientas administrativas → Administración de directivas de grupo”</b></p> <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores Entidad de Certificación”. Verifique que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica” está creada y vinculada en el primer lugar de orden de vínculo.</p>                                                                                                                                                                                                                            |
| 3. Verifique los servicios del sistema de la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica”. |        | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”.</p>  <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:<br/> <b>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</b></p>  <p><b>Nota:</b> Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</p> |

| Comprobación                                                                                       | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |             |        |
|----------------------------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| Servicio (Nombre largo)                                                                            | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                      | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Configurado |        |
| Servidor                                                                                           | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Configurado |        |
| Registro Remoto                                                                                    | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Configurado |        |
| 4. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Dominio categoria basica". |                         | <p>Ejecute el "Administrador de directivas de grupo" a través de la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b><br/> Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política "CCN-STIC-598 ENS Incremental Dominio categoria basica" está creada y vinculada en el primer lugar de orden de vínculo.</p>  |             |        |

| Comprobación                                                                                                                                    | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 5. Verifique la configuración de inscripción automática de certificados en la política “CCN-STIC-598 ENS Incremental Dominio categoria basica”. |        | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”. Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:</p> <p><b>Directiva CCN-STIC-598 ENS Incremental Dominio categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  <p>Haga doble clic sobre el objeto “Cliente de Servicios de servidor de certificados – Inscripción automática” y compruebe los valores correspondientes a la inscripción automática.</p>  |        |
| Configuración                                                                                                                                   |        | Estado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | OK/NOK |
| Modelo de configuración                                                                                                                         |        | Habilitada                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |        |
| Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados                                              |        | Habilitada (marcada)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |        |
| Actualizar certificados que usan plantillas de certificado                                                                                      |        | Habilitada (marcada)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |        |

| Comprobación                                                                                                                             | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6. Verifique la correcta aplicación de la política "CCN-STIC-598 Incremental Dominio categoría básica" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                              |
|--------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>A continuación, haga clic derecho sobre “Configuración de equipo”, seleccione “Propiedades” y, en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría básica” aparece en la lista como muestra la imagen.</p>  |

## 2. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN

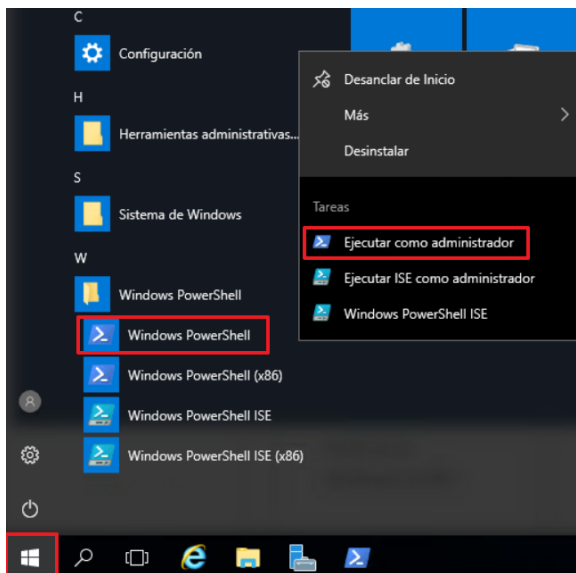
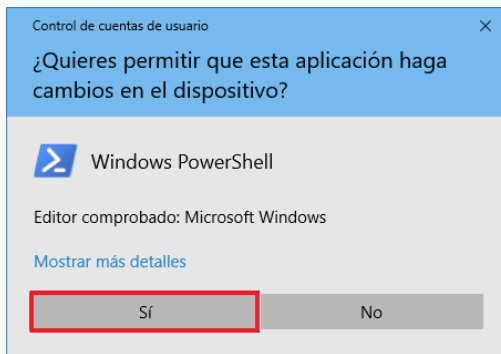
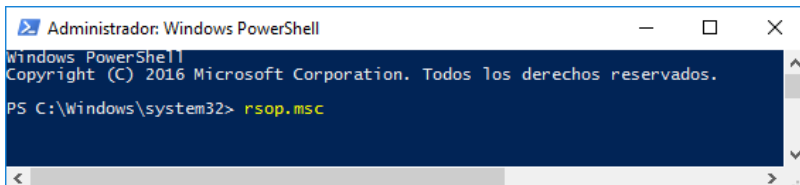
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

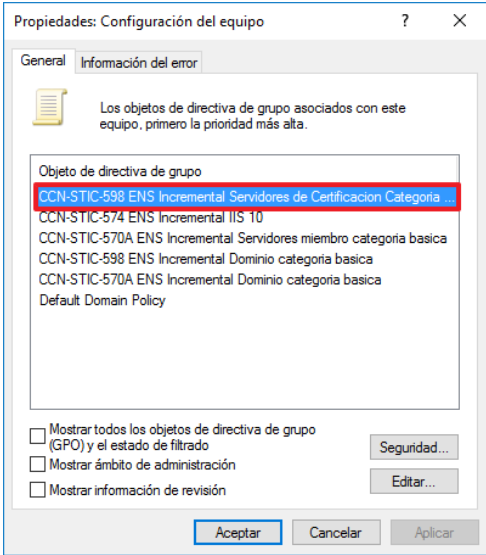
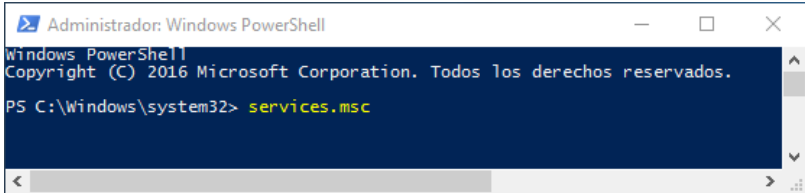
Para realizar las comprobaciones pertinentes en los servidores miembros se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

Las consolas y herramientas que se utilizarán son las siguientes:

- a) Conjunto resultante de directivas (rsop.msc).
- b) Servicios (services.msc).

| Comprobación                                                              | OK/NOK | Cómo hacerlo                                                                                                                               |
|---------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación raíz de empresa. |        | En el servidor Entidad de Certificación raíz de empresa, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |

| Comprobación                                                                                                                                                     | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Verifique la correcta aplicación de la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee "rsop.msc" en la consola de comandos que se ha abierto:</p>  |

| Comprobación                                                                                                                                                                | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                          |             |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                             |                         | <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica” aparece en la lista como muestra la imagen.</p>  |             |        |
| 3. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                   |             |        |
| Servicio (Nombre largo)                                                                                                                                                     | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                               | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                            | Configurado |        |
| Servidor                                                                                                                                                                    | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                            | Configurado |        |
| Registro Remoto                                                                                                                                                             | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                            | Configurado |        |

### ANEXO A.2.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Windows Server 2016 independientes con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

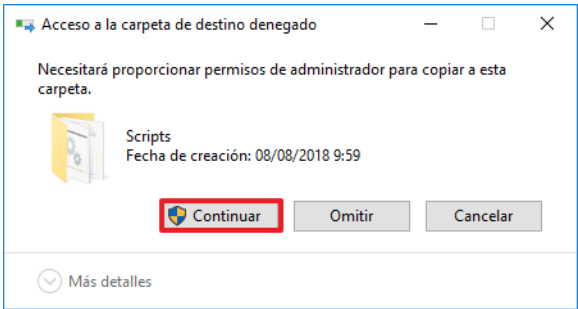
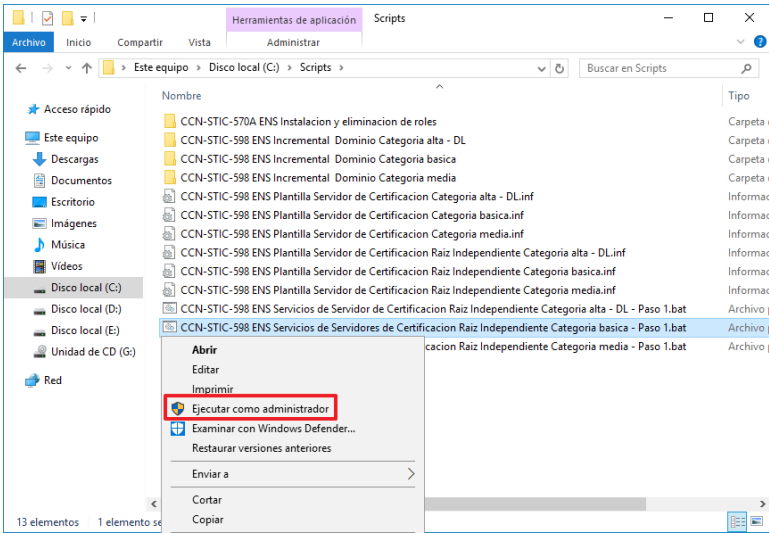
Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

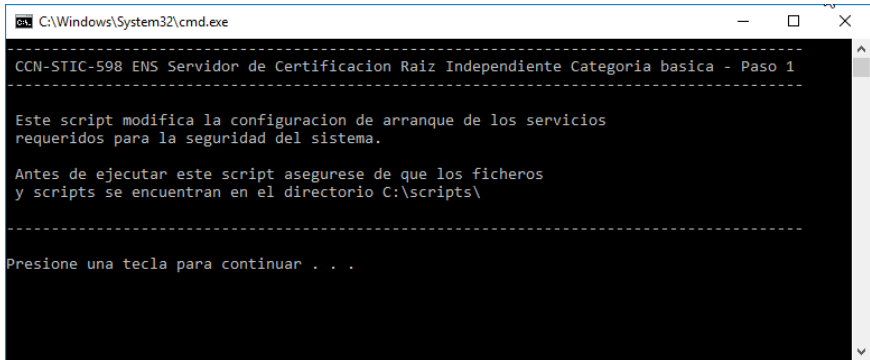
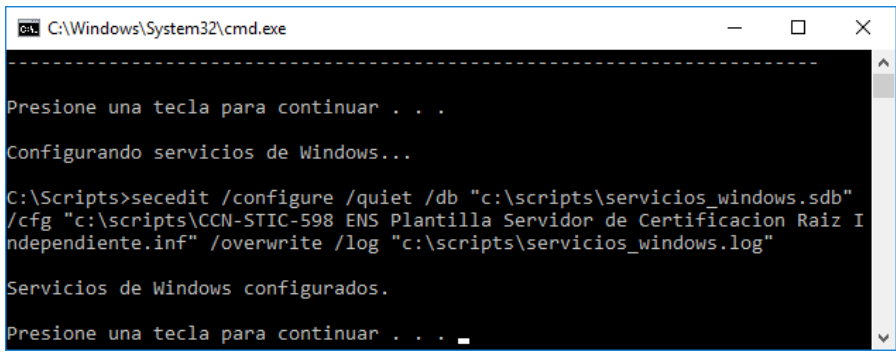
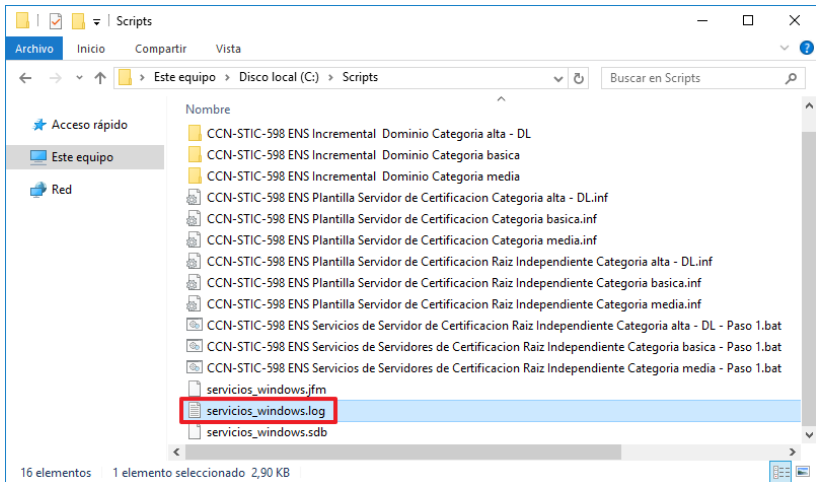
- Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad básica.
- Un servidor independiente del dominio preparado siguiendo la guía CCN-STIC-570B Anexo A con una categorización de seguridad básica.
- Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad básica.

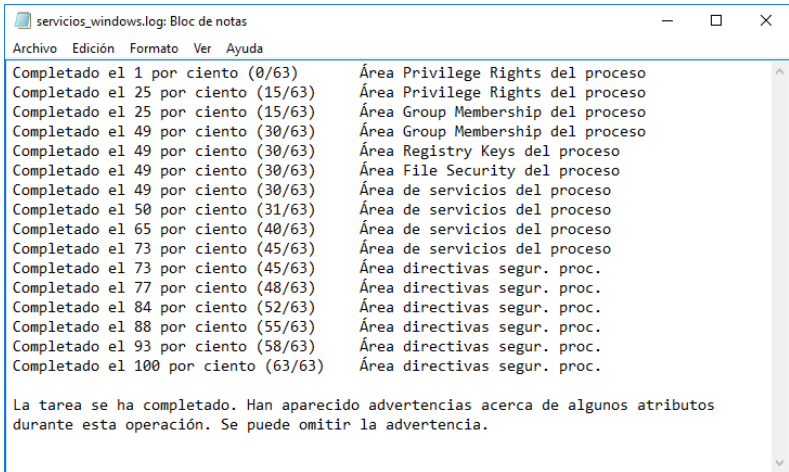
## 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DEL DOMINIO

Los pasos que se describen a continuación se realizarán en todos aquellos servidores con el rol de Entidad de Certificación raíz independiente del dominio sobre Microsoft Windows Server 2016, que implementen servicios o información de categoría básica y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

| Paso | Descripción                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor independiente donde se va a aplicar seguridad según criterios de ENS.</p>  |
| 2.   | Cree el directorio "Scripts" en la unidad C:\.                                                                                                                                                |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.   | <p>Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.</p>  <p><b>Nota:</b> Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Haga clic en el botón “Continuar” e introduzca las credenciales.</p>                                                                                                                                                                                                                                                                                                                                                                  |
| 4.   | <p>A continuación, diríjase a la carpeta “C:\Scripts” y ejecute con permisos de administrador el script “CCN-STIC ENS Servicios de Certificación Raíz Independiente Categoría básica – Paso 1.bat”. Este script aplica al sistema la plantilla de servicios para la seguridad del sistema.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.   | <p>Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría básica del ENS.</p>                                                                                                                                                                                                                                                                                                                                              |
| 6.   | <p>Una vez completado el proceso, deberá pulsar una tecla para continuar.</p>  |
| 7.   | <p>Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta "C:\Scripts" con el nombre de "servicios_windows.log".</p>                                                                                                                                                                                                                                                                                                                    |

| Paso | Descripción                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.   | <p>Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.</p>  |

## 2. CONFIGURACIONES DE SEGURIDAD SOBRE EL DOMINIO

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría básica.

No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

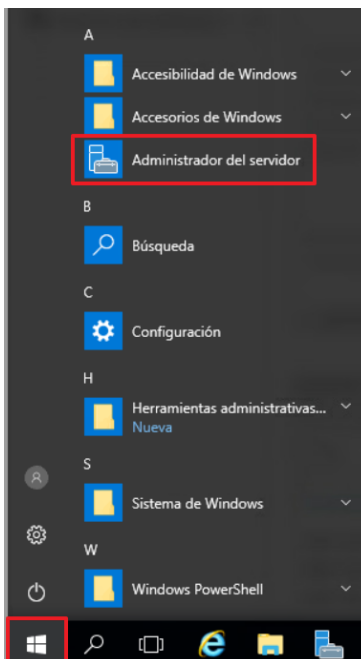
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

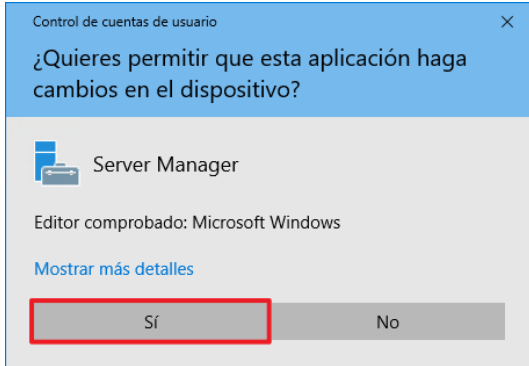
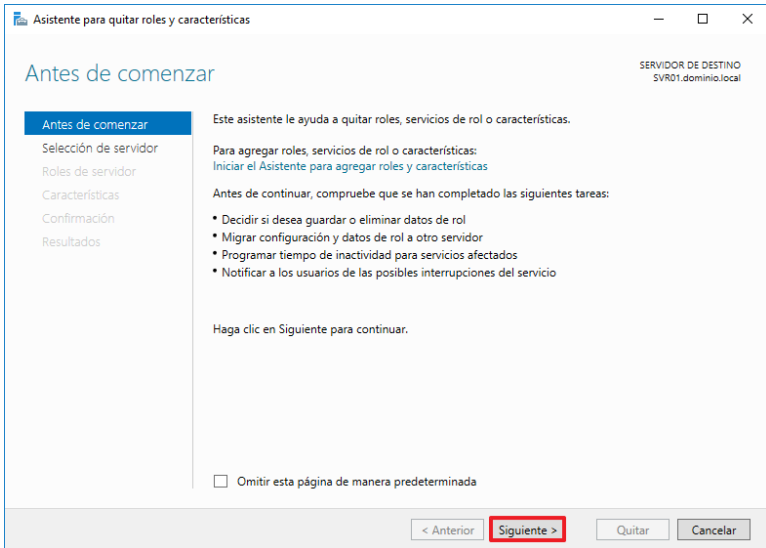
### 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

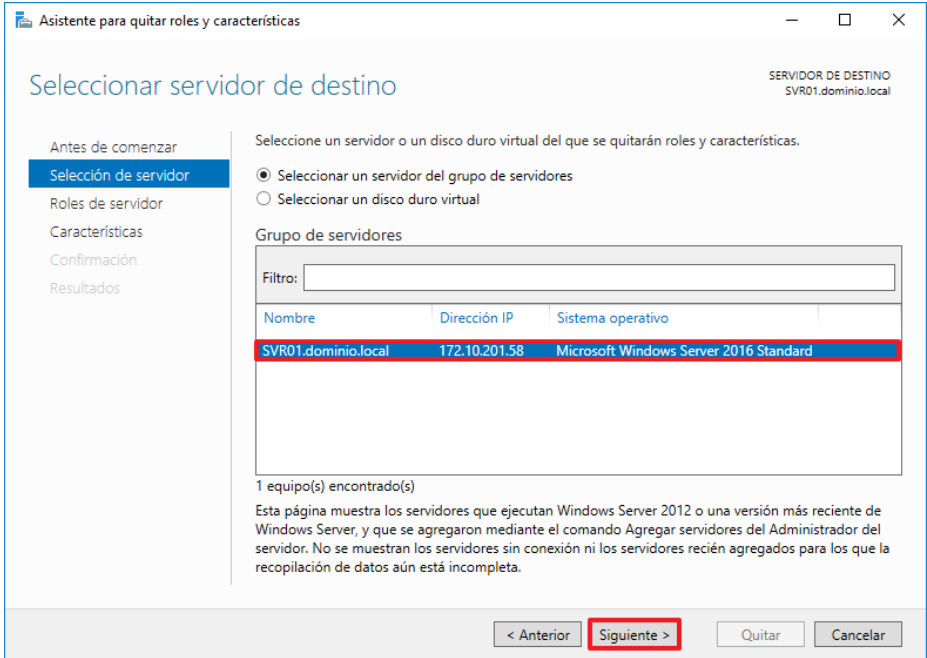
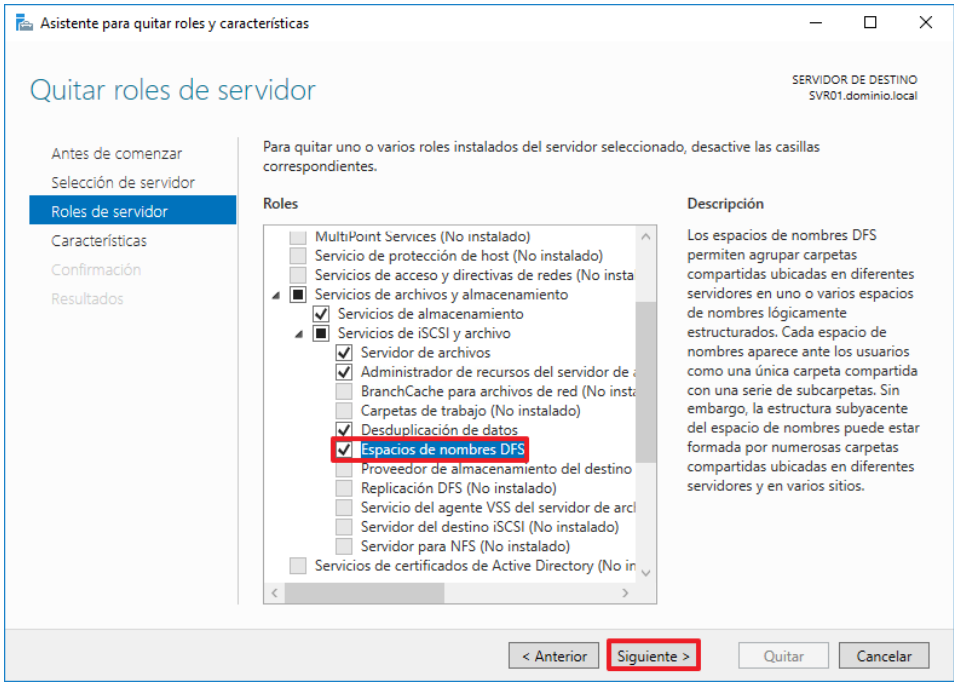
Uno de los aspectos que marca el ENS, desde su requisito de la categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

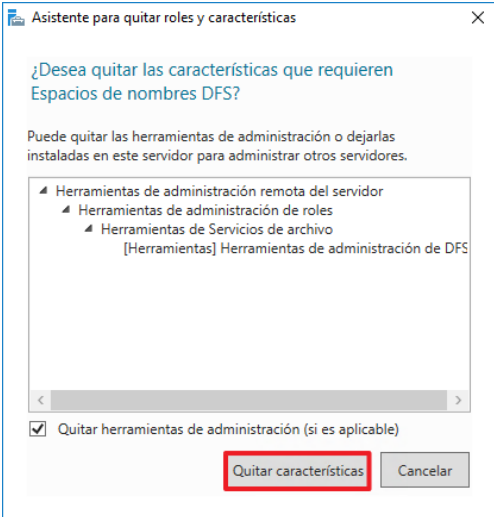
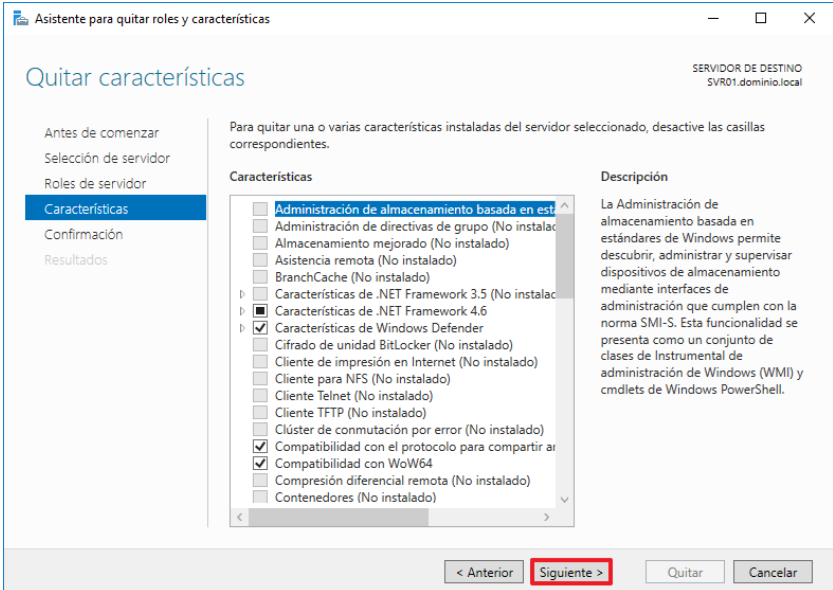
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de Entidad de Certificación.

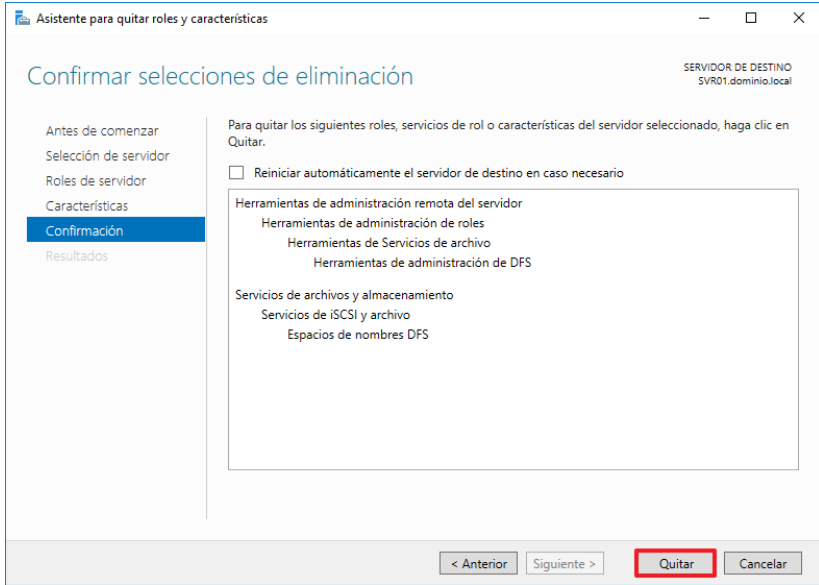
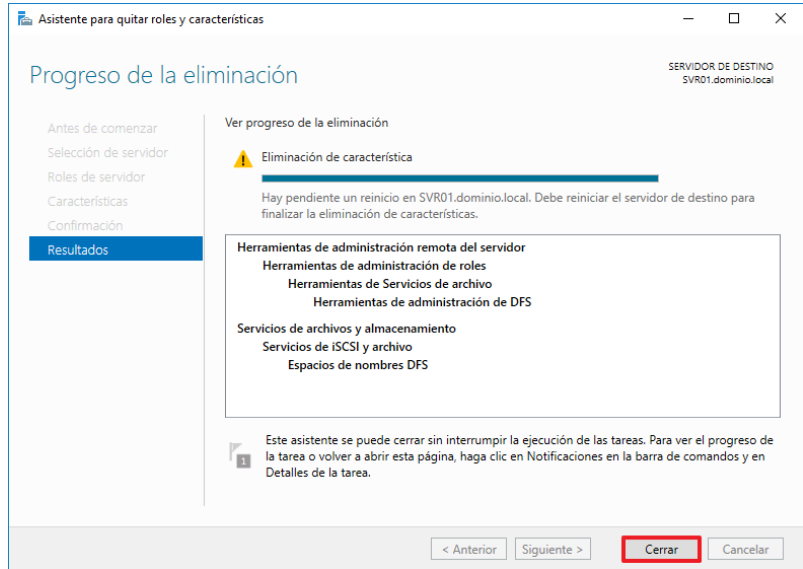
**Nota:** Para continuar con el siguiente paso a paso deberá realizar previamente el “ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR MIEMBRO O CONTROLADOR DE DOMINIO QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA O ALTA DEL ENS” de la guía “CCN-STIC-570A - Implementación del ENS en Microsoft Windows Server 2016” y una vez finalizado deberá desvincular y/o eliminar la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” creada en dicho anexo.

| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.   | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor Entidad de Certificación .</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 10.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                |

| Paso | Descripción                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>             |
| 12.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>               |
| 13.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>  |

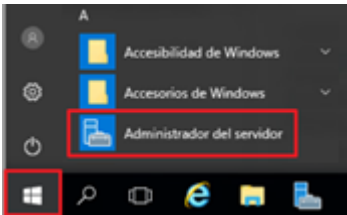
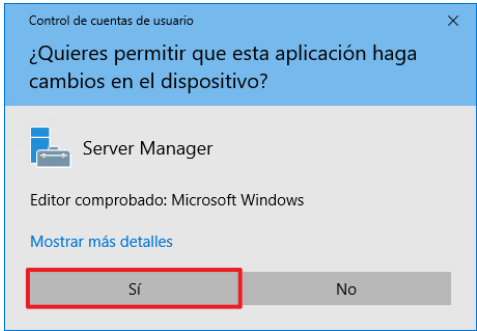
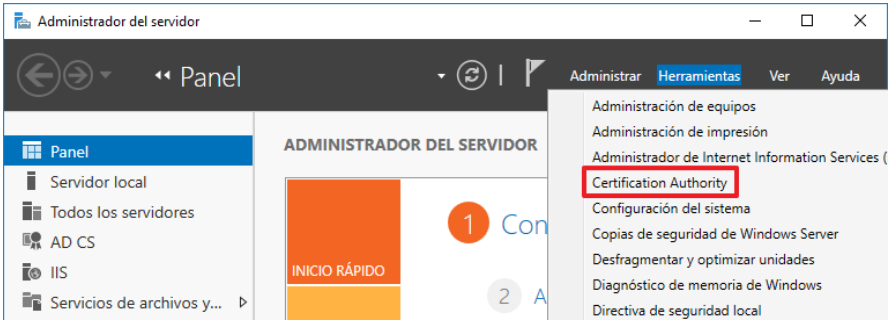
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p>                                                      |
| 15.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |

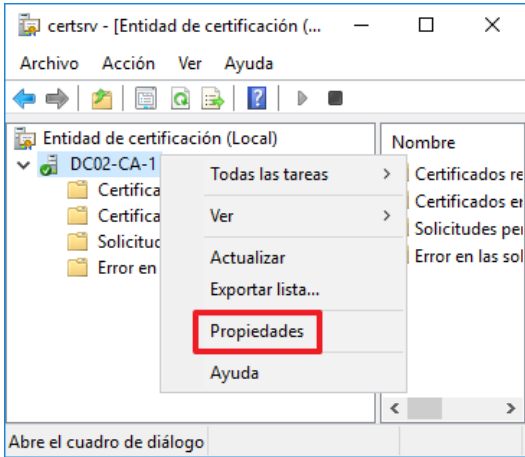
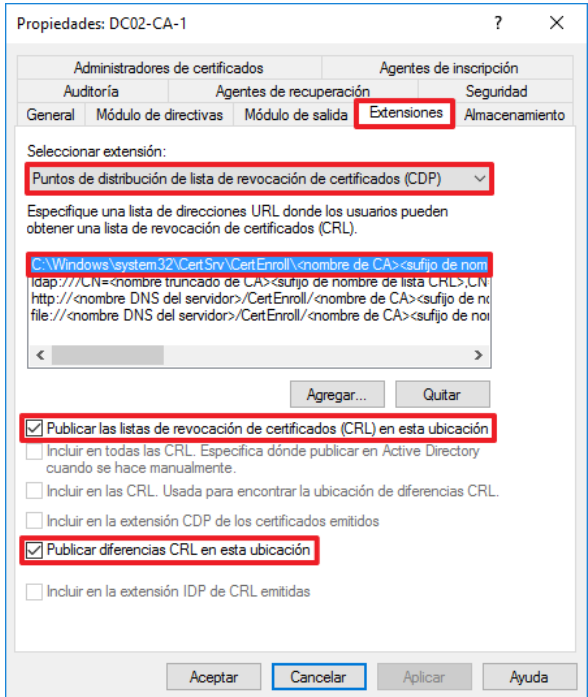
| Paso | Descripción                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.  | <p>En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p> |
| 17.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>                                                                                                      |

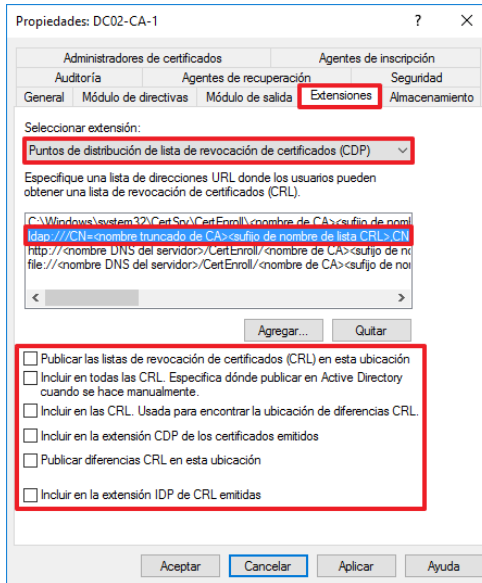
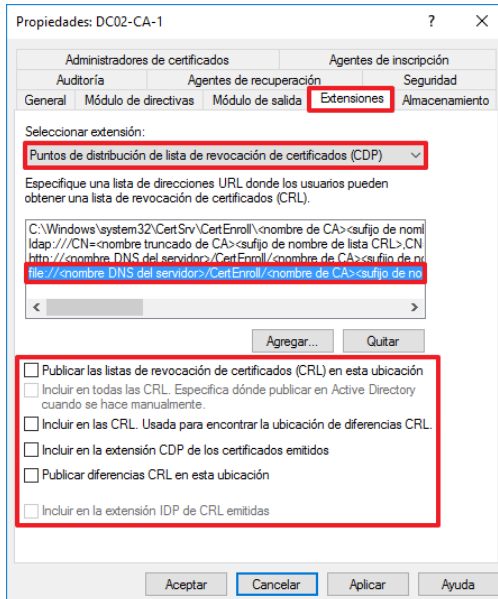
| Paso | Descripción                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                     |
| 19.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 20.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                    |

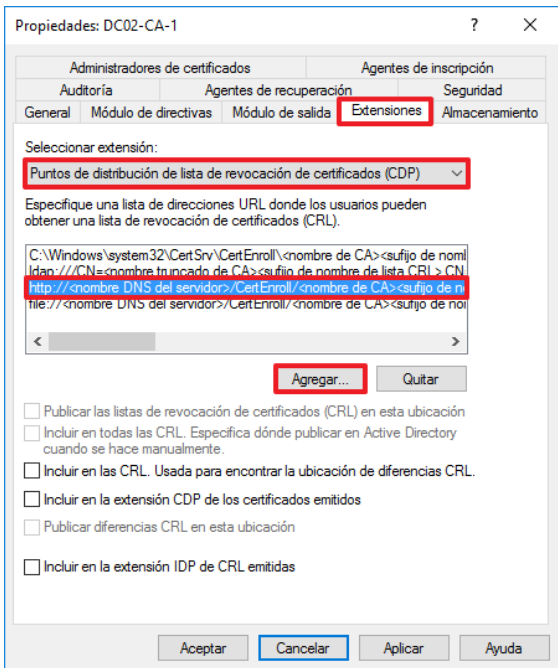
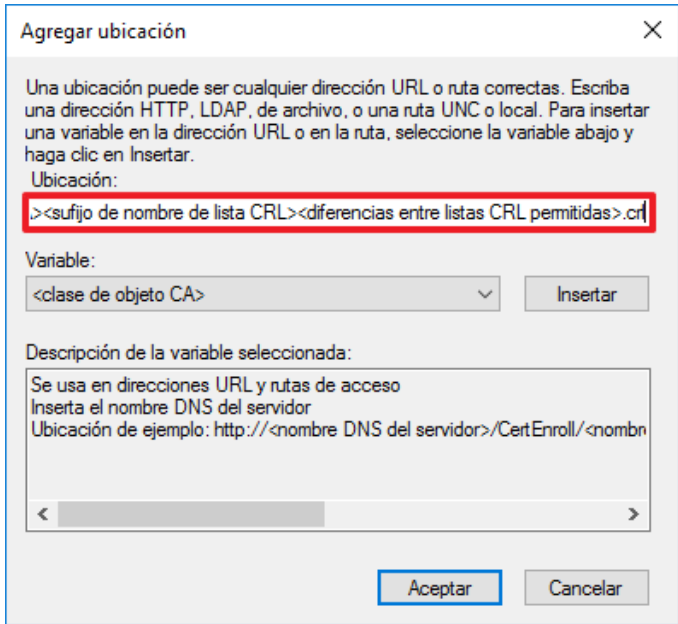
## 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL)

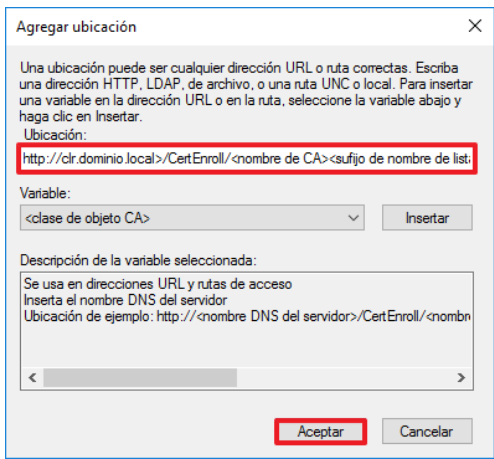
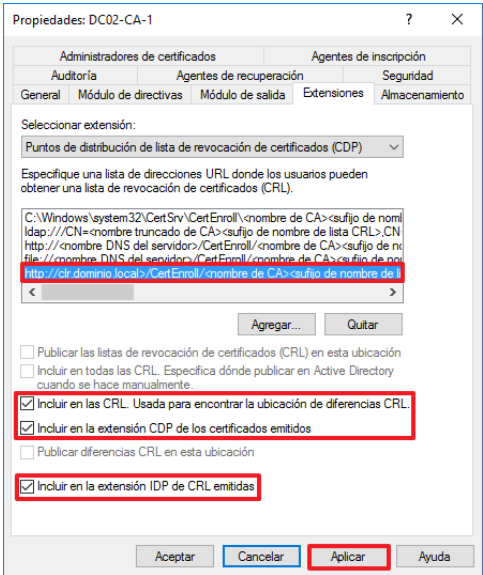
Los pasos que se describen a continuación se realizarán sobre el servidor Entidad de Certificación independiente del dominio.

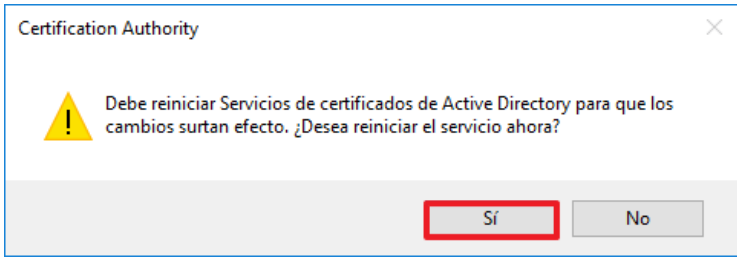
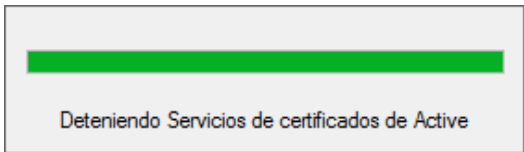
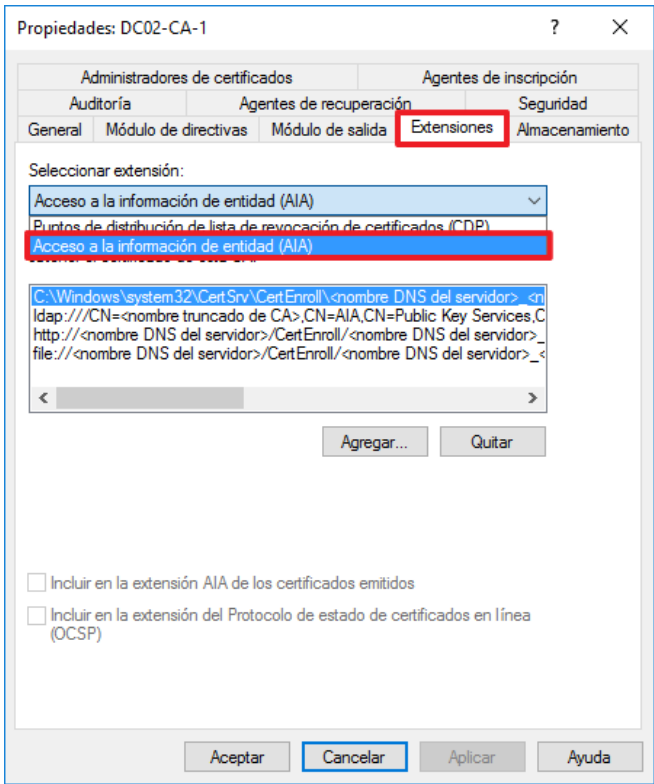
| Paso | Descripción                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21.  | Si no lo ha hecho anteriormente, inicie sesión en el equipo donde se va a instalar el servidor independiente Entidad de Certificación raíz.<br><br><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de administrador local. |
| 22.  | Acceda al “administrador del servidor” mediante el icono de la barra de tareas.<br><br>                                                                 |
| 23.  | El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.<br><br>                                      |
| 24.  | En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.<br><br>                      |

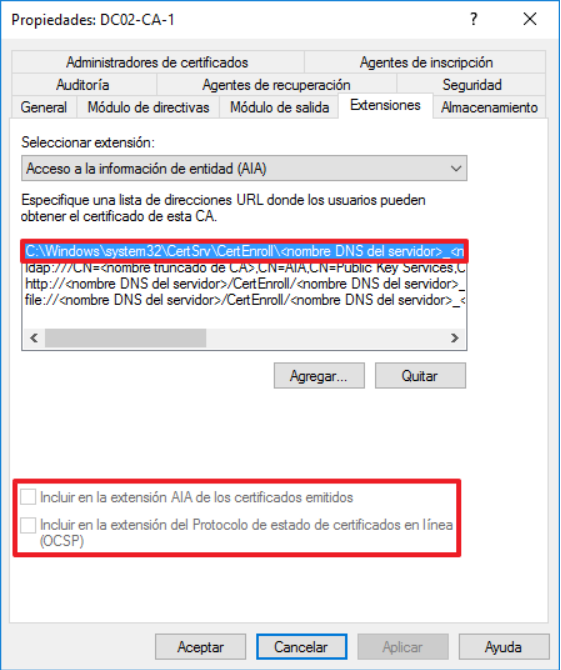
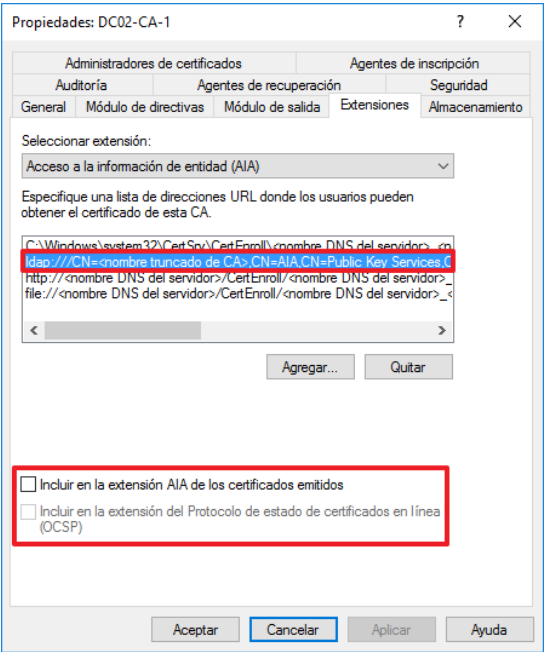
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente, con el botón derecho del ratón selecciónelo y pulse sobre “Propiedades”.</p>                                                                                                                                                                                                                                                                                                                                |
| 26.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</p>  |

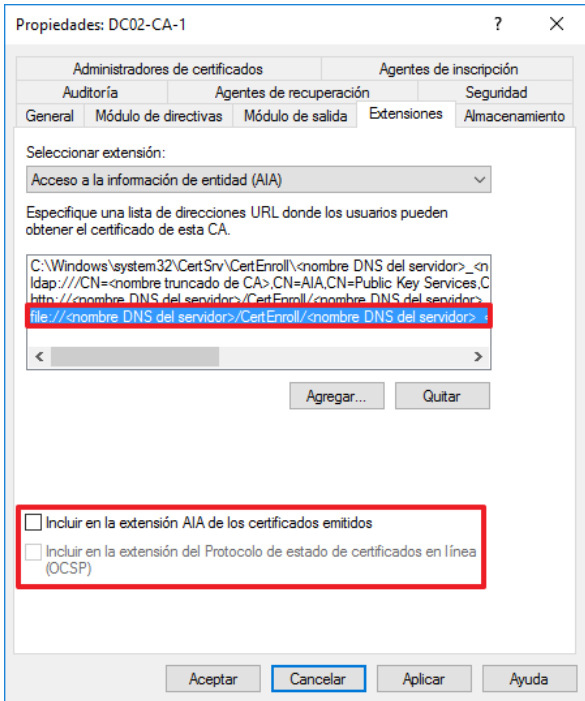
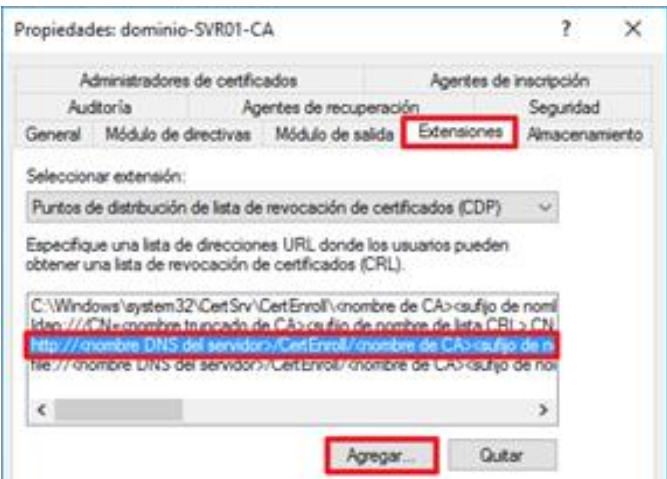
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando “<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>” y desmarque todas las opciones.</p> <p>Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>  |
| 28.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “<b>file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y desmarque todas las opciones como muestra la siguiente figura:</p>                                                                                                                                                                    |

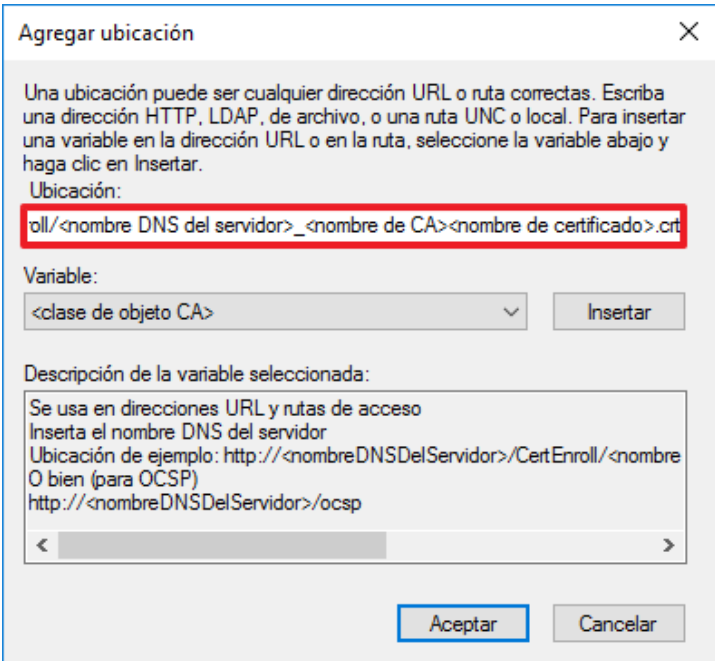
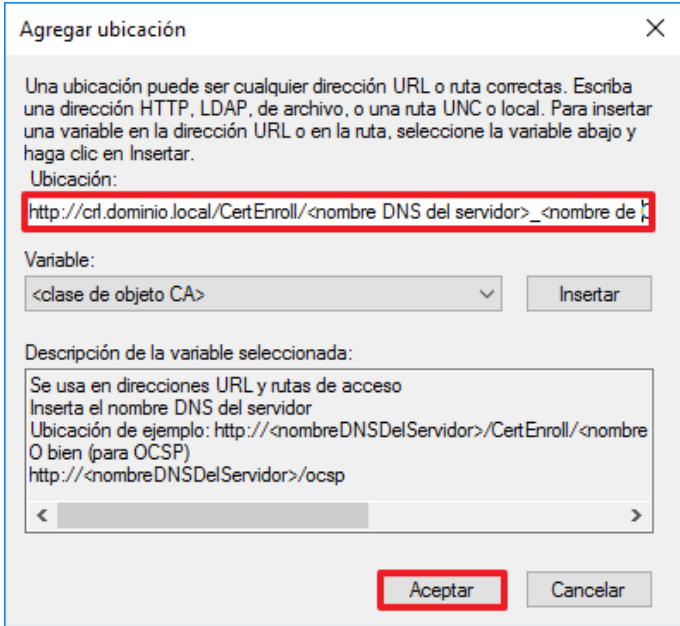
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29.  | De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto. |
| 30.  | Pulse el botón “Agregar”.<br>                                                                                                                                                                                                                                                                      |
| 31.  | Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.<br>                                                                                                                                               |

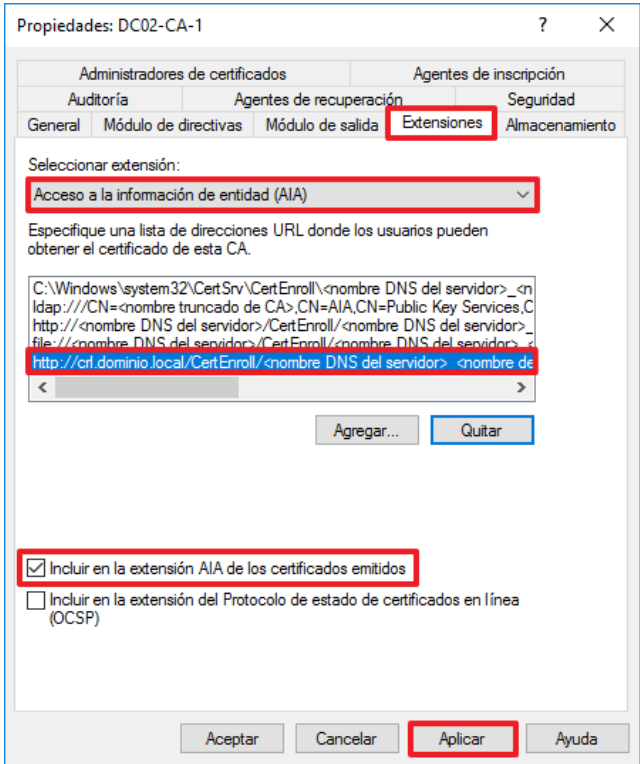
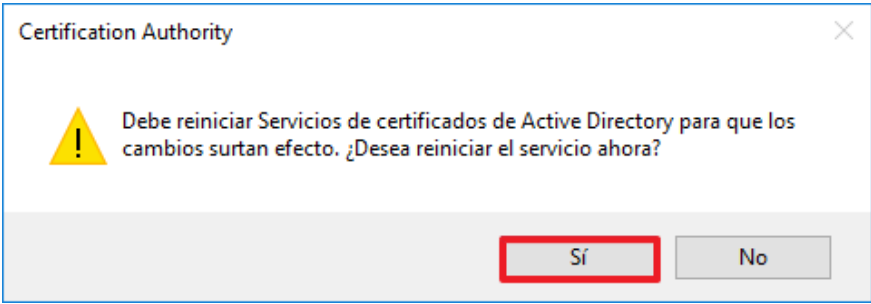
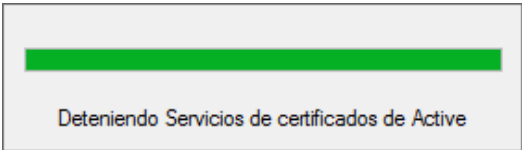
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 32.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                                             |
| 33.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

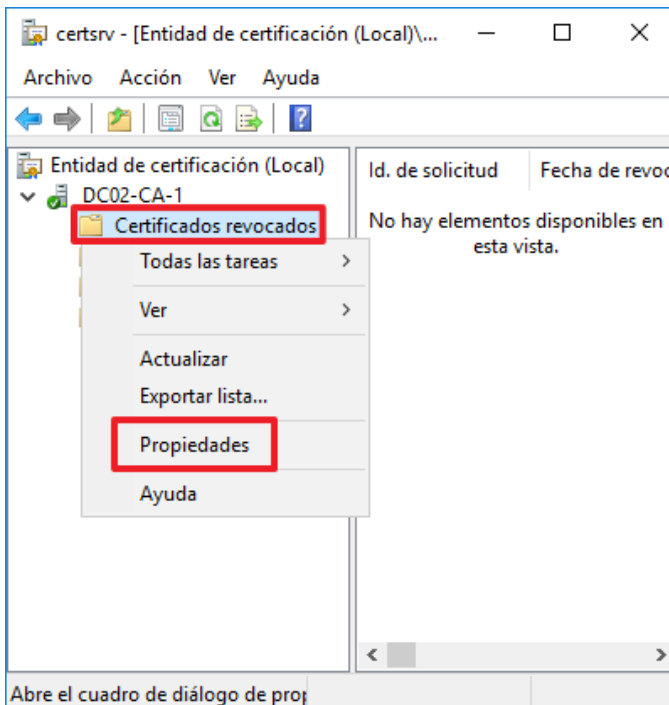
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 35.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 36.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

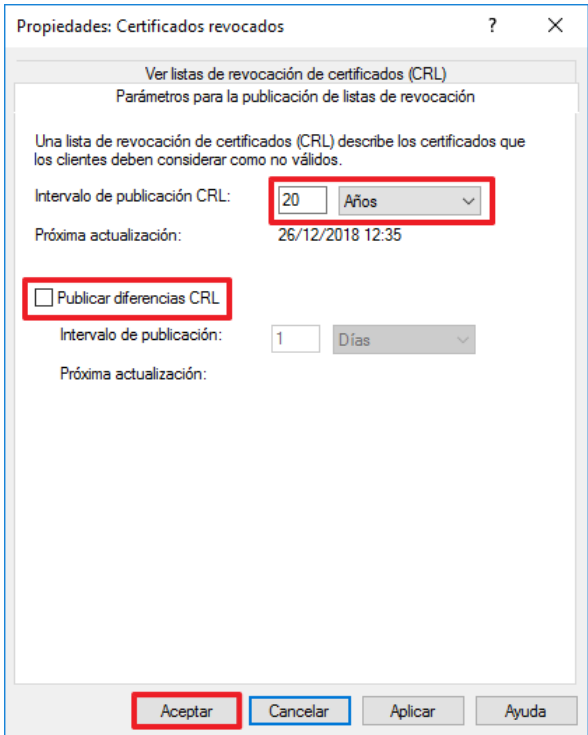
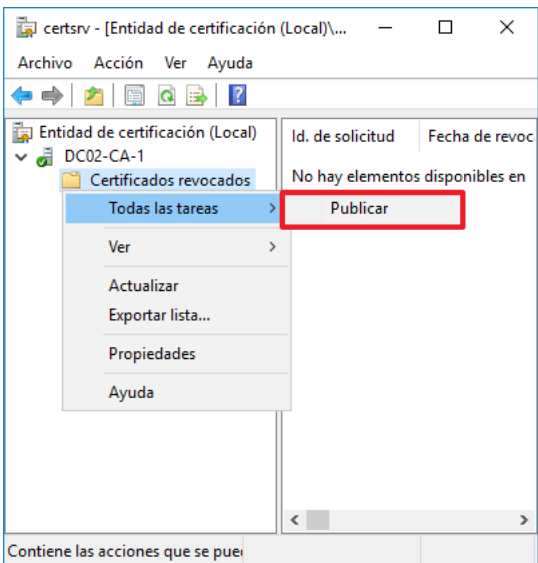
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 37.  | <p>Compruebe que en el objeto <b>"C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt"</b> todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.</p>                     |
| 38.  | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |

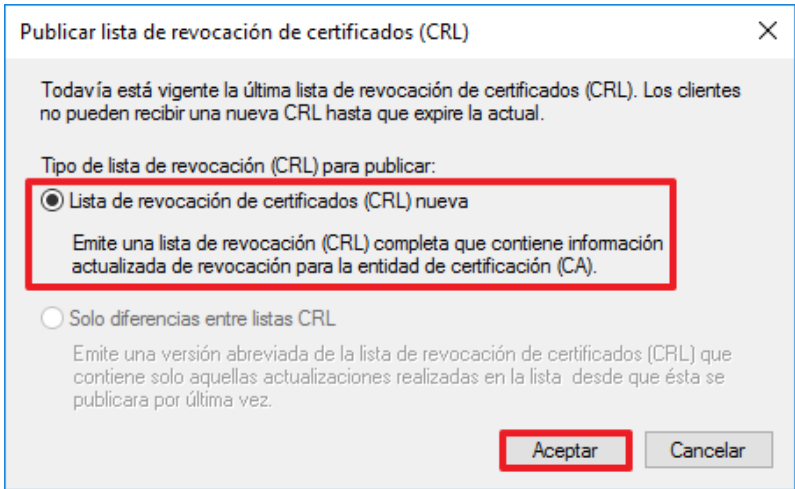
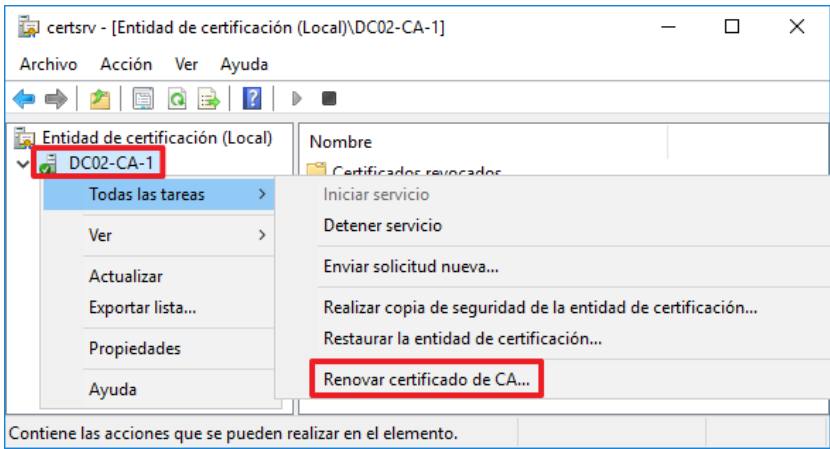
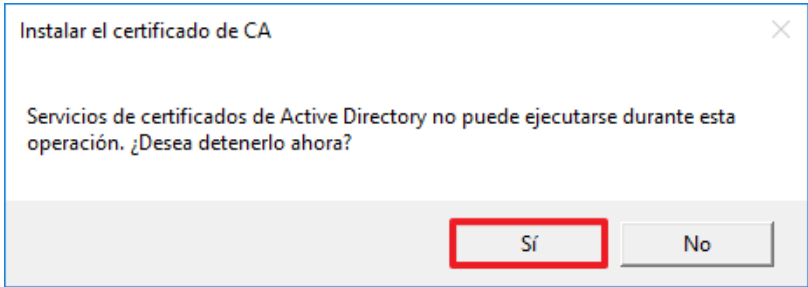
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 39.  | <p>Seleccione ahora <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y desmarque la opción <b>“Incluir en la extensión AIA de los certificados emitidos”</b>.</p>  |
| 40.  | <p>Seleccione ahora <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b>.</p>                                                                                                  |
| 41.  | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                                                                                           |

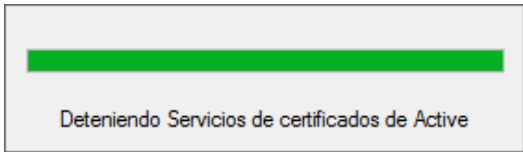
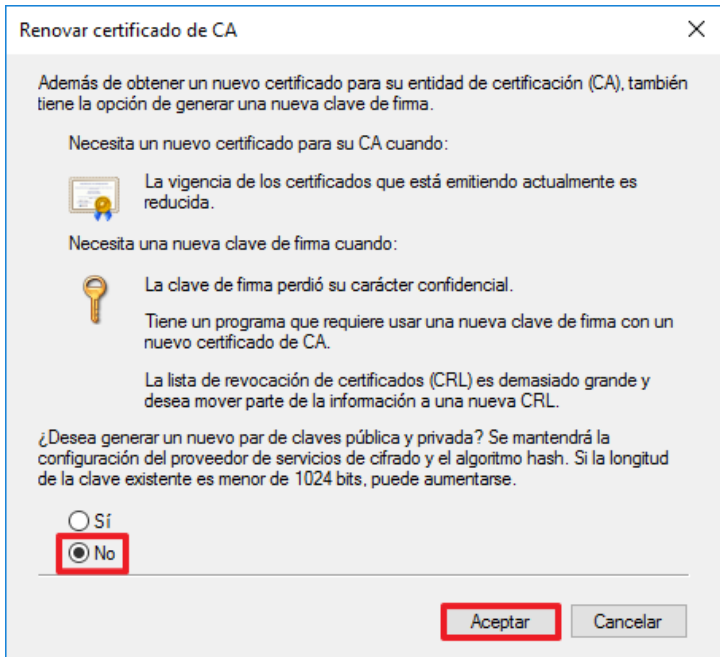
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 42.  | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                                                                                                                                    |
| 43.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 44.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt</b>” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”.</p> <p>Pulse “Aplicar” para guardar los cambios.</p>  |
| 45.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                          |
| 46.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                        |
| 47.  | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 48.  | El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL, al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.                                                                                                                                                                                                                                                                                                                                                         |
| 49.  | <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:</p> <p><b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b></p> <p>Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>  |

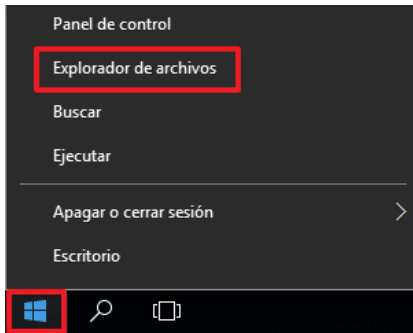
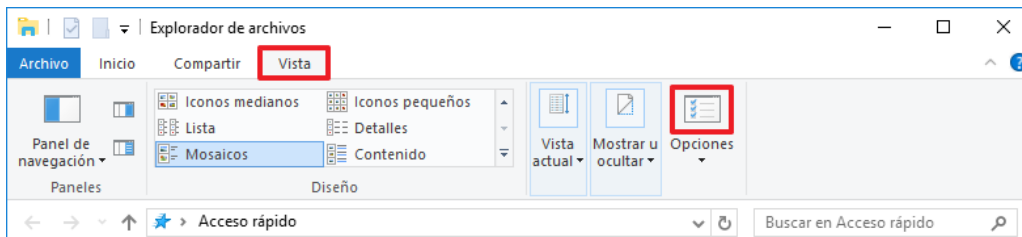
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 50.  | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p>  <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p> |
| 51.  | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                                                                                                                                                                                                                                                                                           |

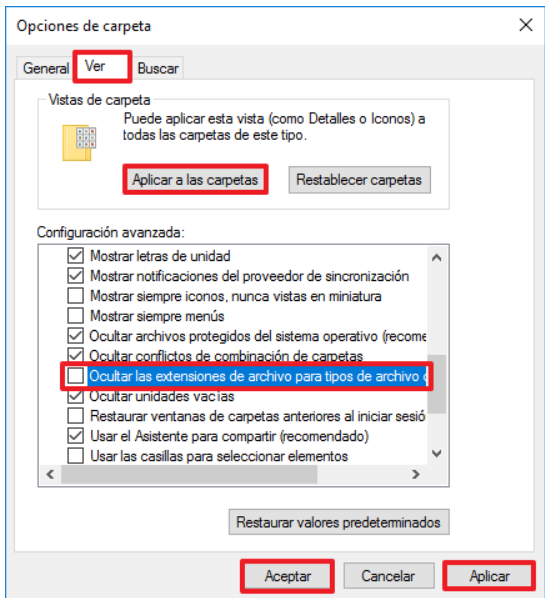
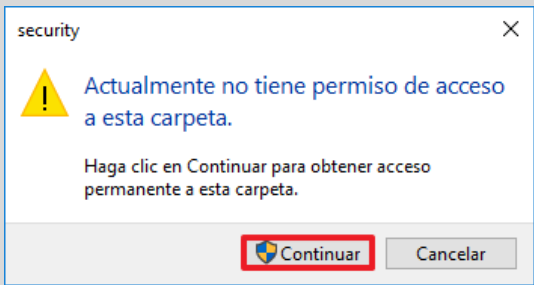
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52.  | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>                                                                                                                                                                                  |
| 53.  | <p>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 “<b>Todas las tareas → Renovar certificado de CA...</b>”.</p>  |
| 54.  | <p>Pulse “Sí” en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                          |

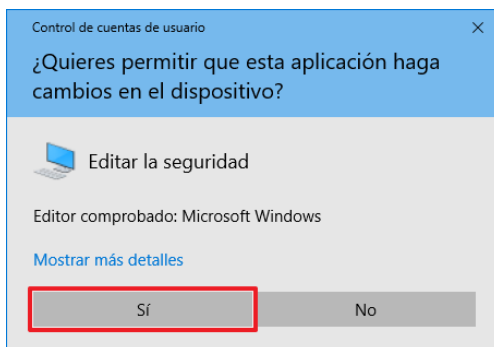
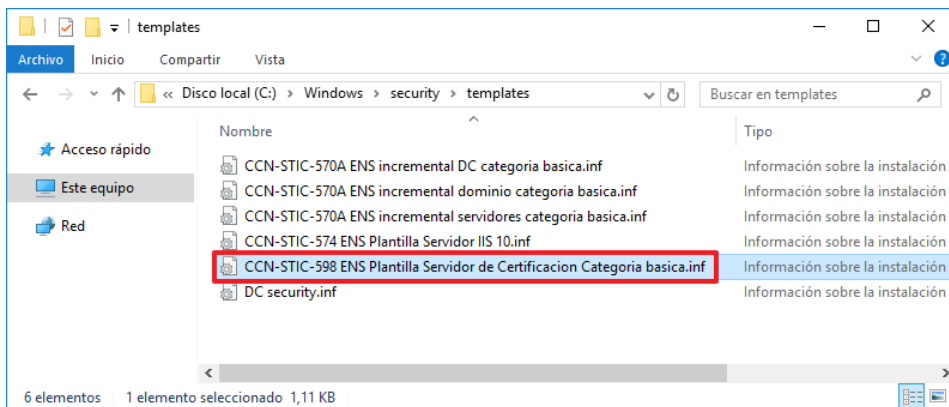
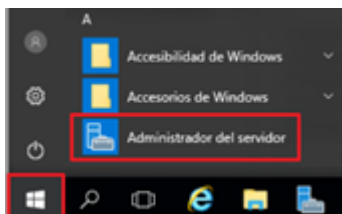
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 55.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                       |
| 56.  | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Este proceso comienza en segundo plano y puede tardar unos minutos. No debe cerrar la ventana hasta que finalice el proceso.</p> |

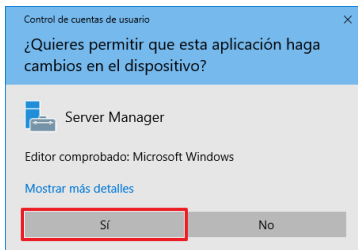
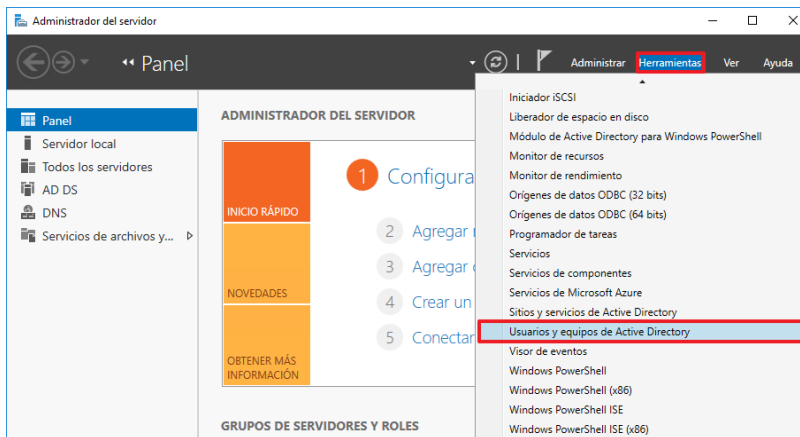
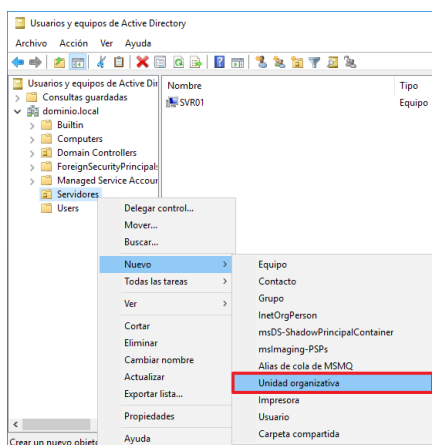
## 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO

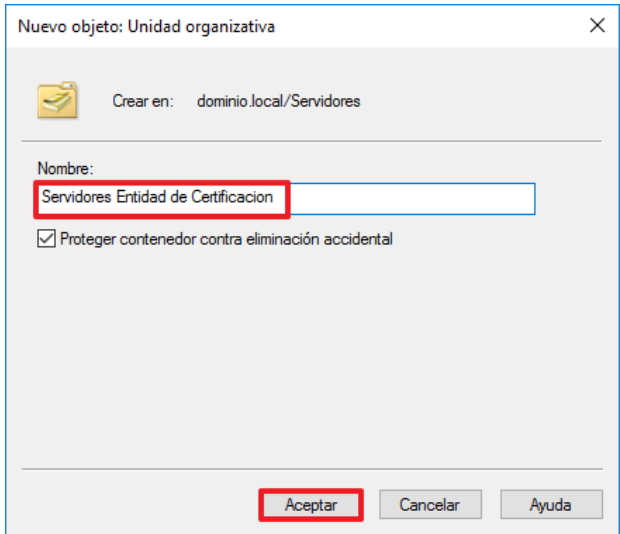
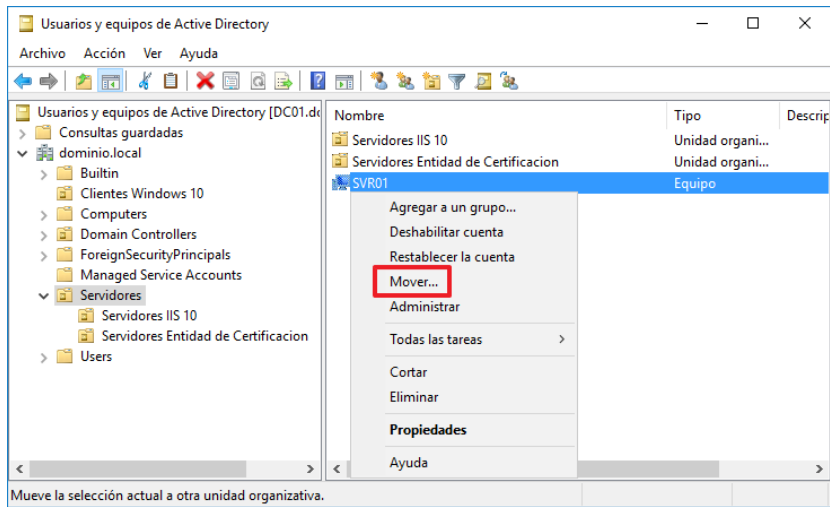
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor de Entidad de Certificación.

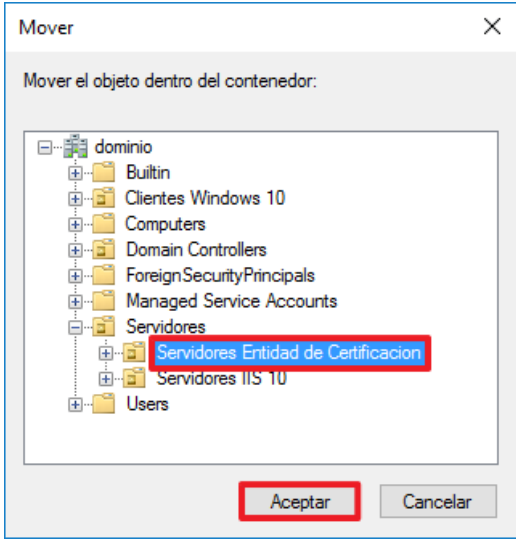
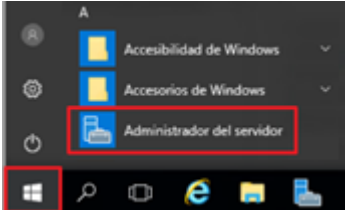
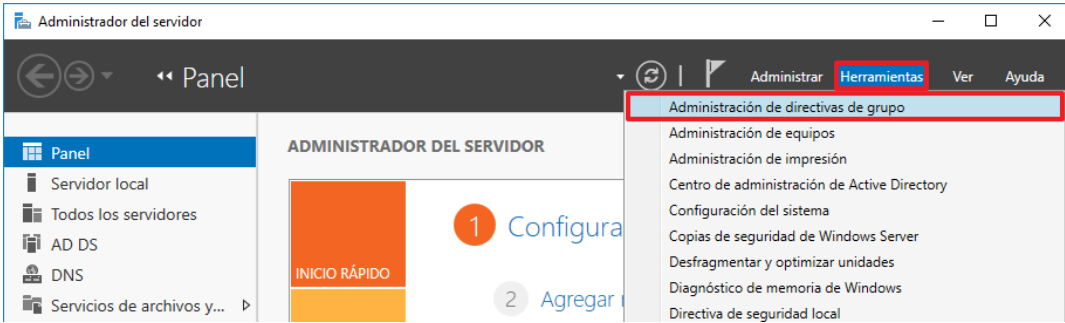
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p>                                                                                                                                           |
| 58.  | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                                                                                                                                                                    |
| 59.  | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                                                                                                                                                                                                                    |
| 60.  | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>  |
| 61.  | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                     |

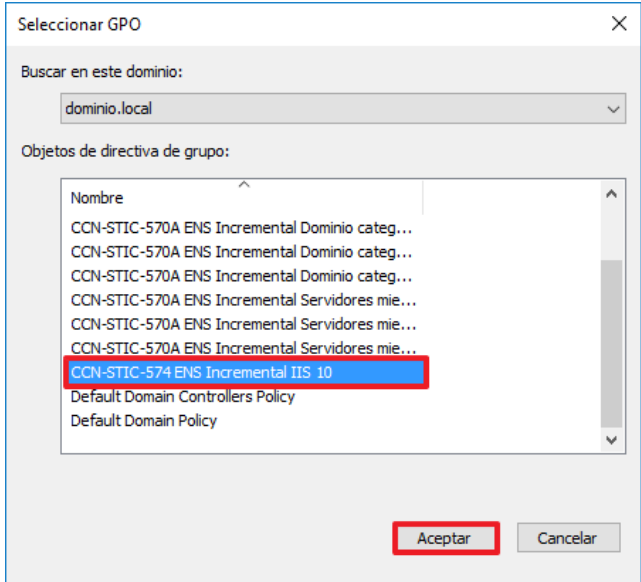
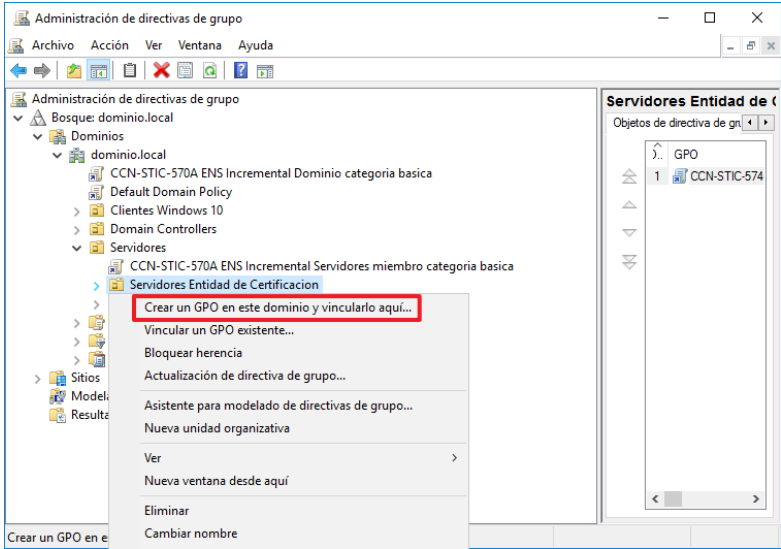
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 62.  | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |
| 63.  | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                            |

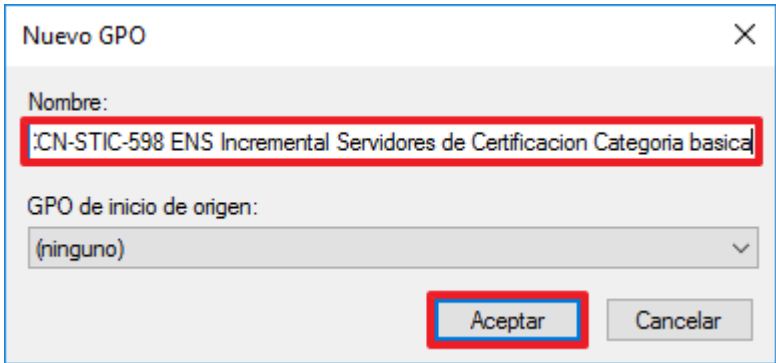
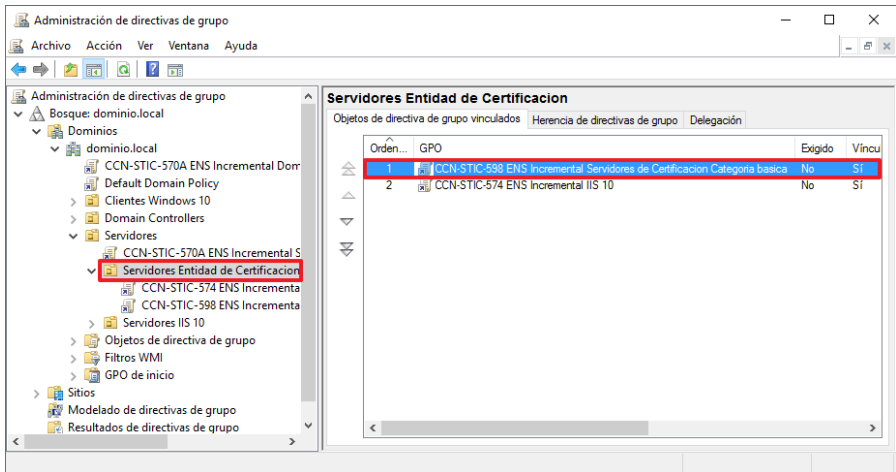
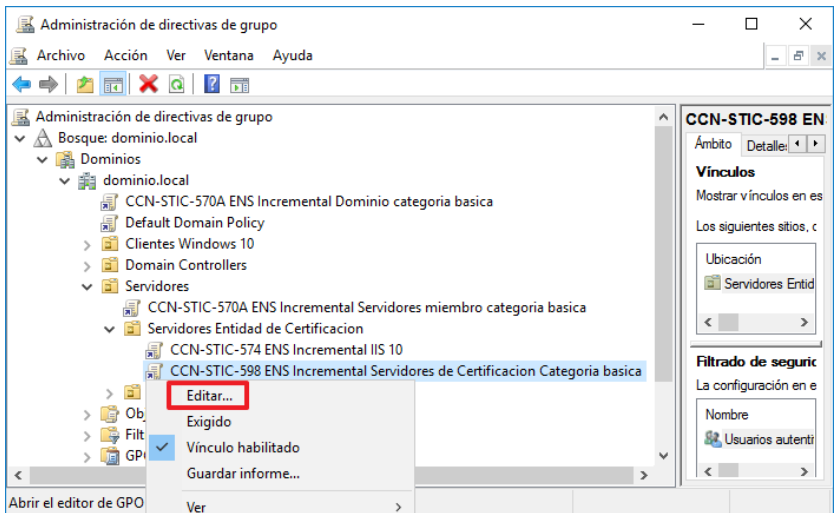
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64.  | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |
| 65.  | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría básica.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>                                                                                                                                                                                                                                                                                                                                                                                   |
| 66.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |

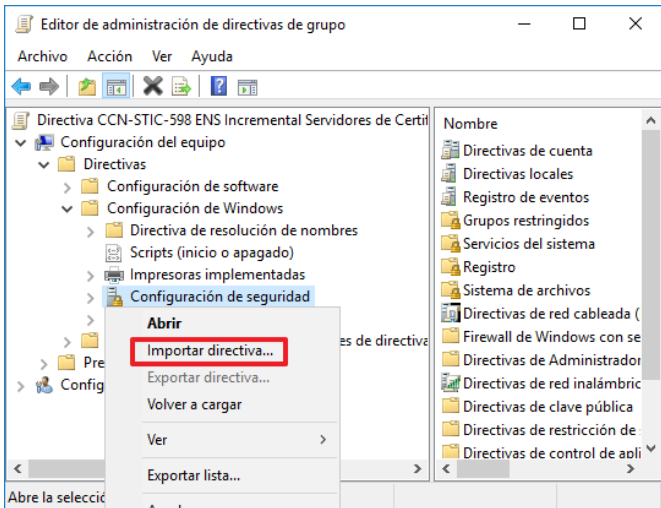
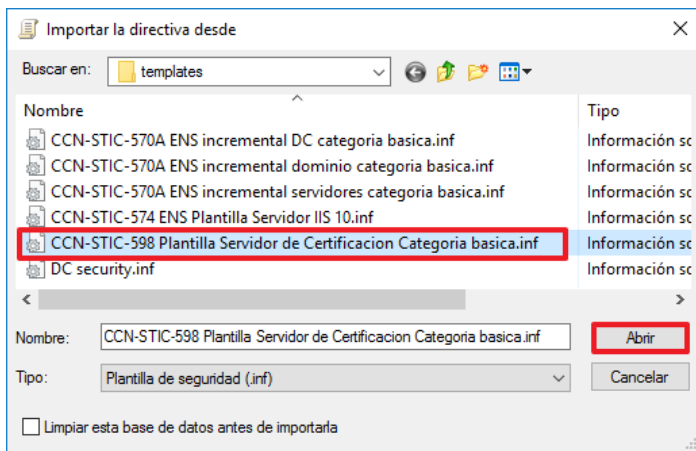
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 67.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 68.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione “Herramientas → Usuarios y equipos de Active Directory”.</p>                                                                                                                                                                                                                                                                                                                           |
| 69.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo “&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local → Servidores”.</p> |

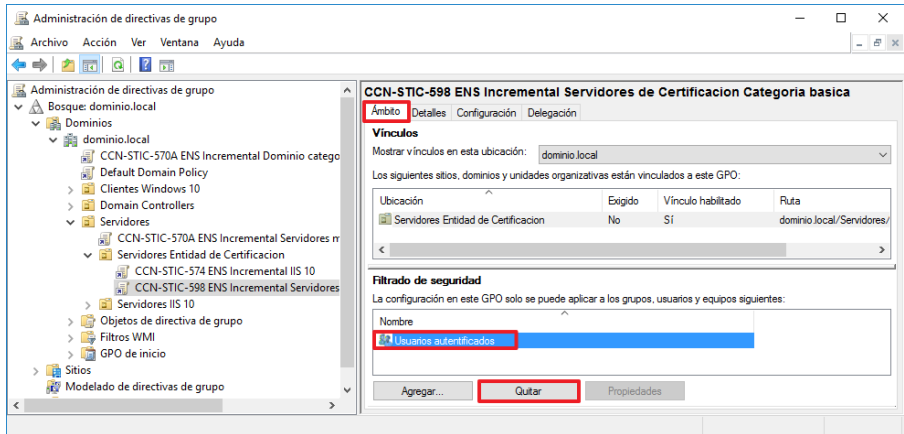
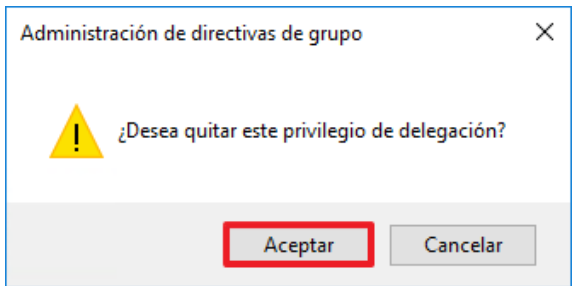
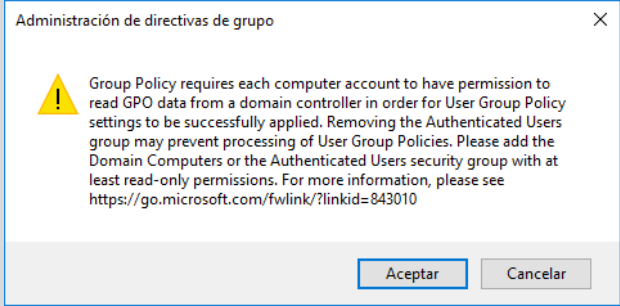
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 70.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                       |
| 71.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores entidad de certificación a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |

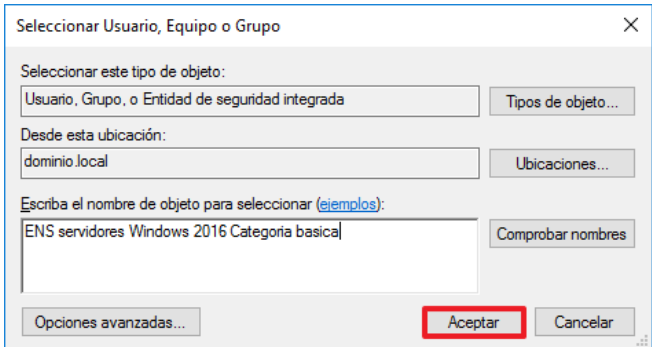
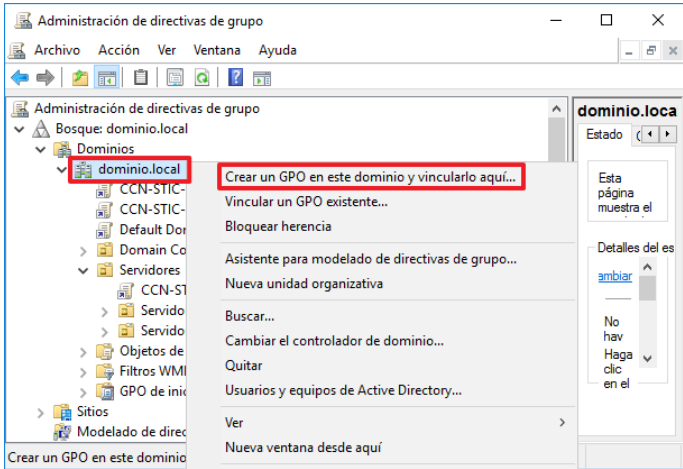
| Paso | Descripción                                                                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 72.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>                                                                                                                    |
| 73.  | <p>Cierre la herramienta de “Usuarios y equipos de Active Directory”.</p>                                                                                                                                                                                                                                                    |
| 74.  | <p>A continuación, abra el “Administrador del servidor”.</p>                                                                                                                                                                             |
| 75.  | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón “Herramientas → Administración de directivas de grupo”.</p>                                                                                 |
| 76.  | <p>A continuación, despliegue el nodo “Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p> |

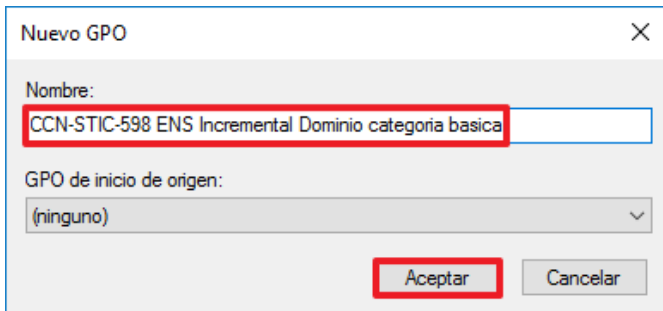
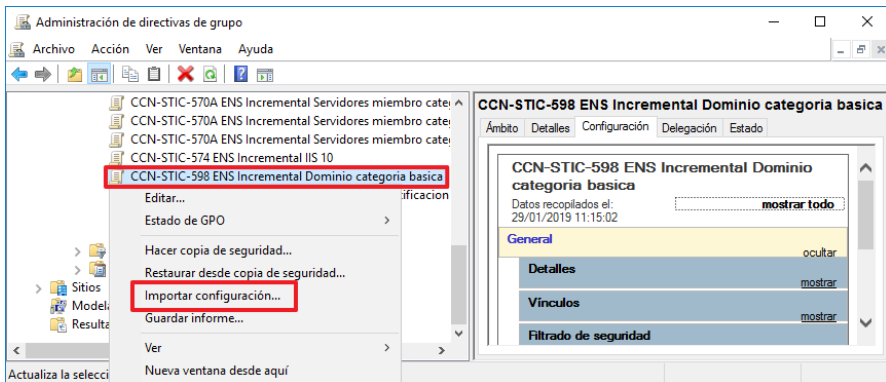
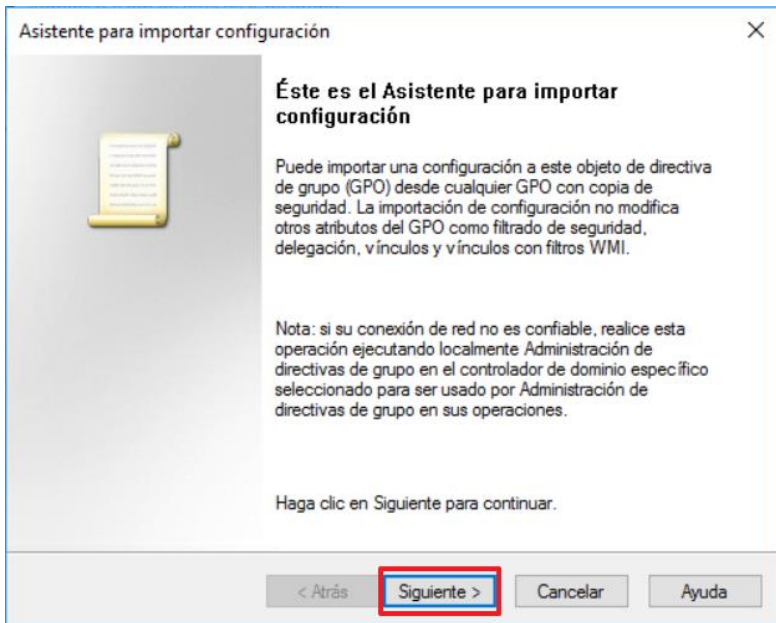
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 77.  | <p>Seleccione “Vincular un GPO existente...” y vincule el objeto de directiva de grupo “CCN-STIC-574 ENS Incremental IIS 10” a la nueva unidad organizativa “Servidores Entidad de Certificación”, haciendo clic con el botón derecho sobre ella.</p>                  |
| 78.  | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>  |

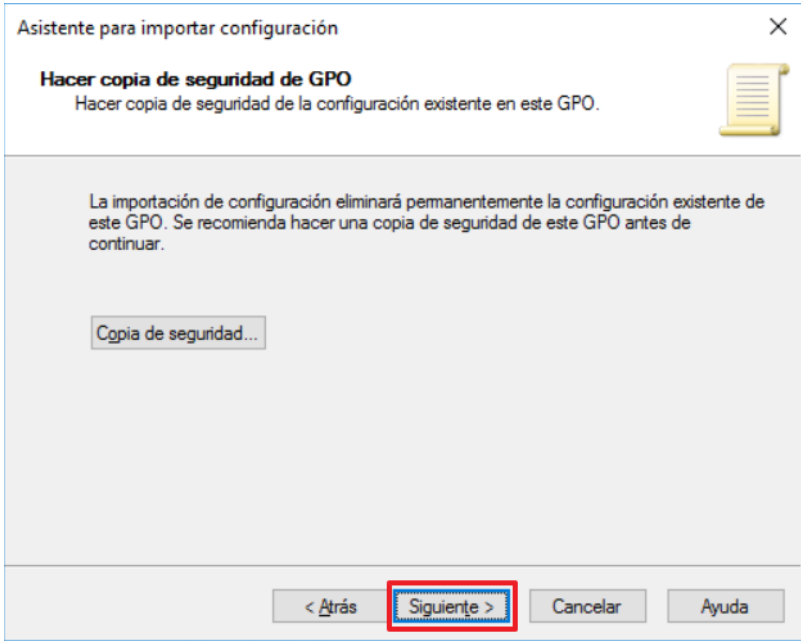
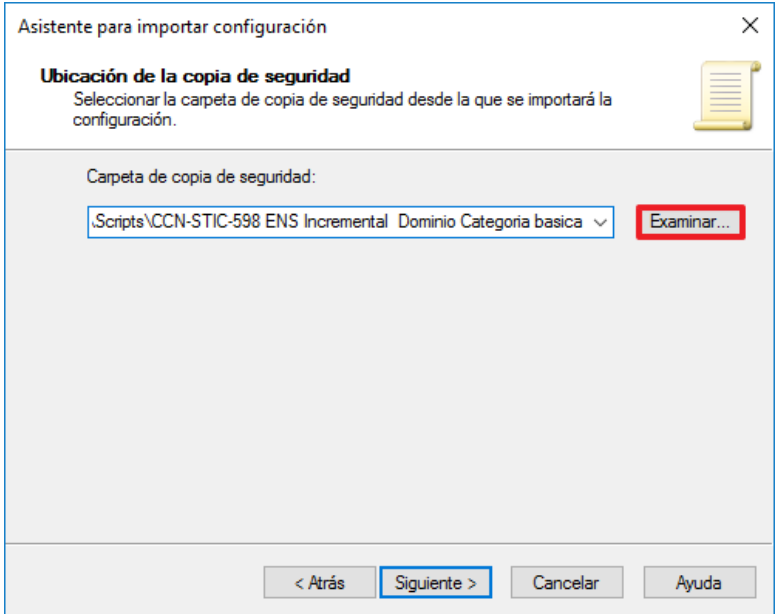
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 79.  | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica” y haga clic en el botón “Aceptar”.</p>                                                                                                                        |
| 80.  | <p>Seleccione la unidad organizativa “<b>Servidores Entidad de Certificación</b>”. En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  |
| 81.  | <p>De esta forma, se garantiza que la directiva se aplica correctamente.</p>                                                                                                                                                                                                                                                                               |
| 82.  | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción “Editar”.</p>                                                                                                                             |

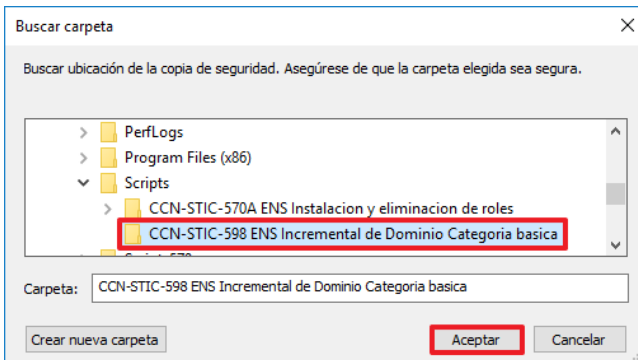
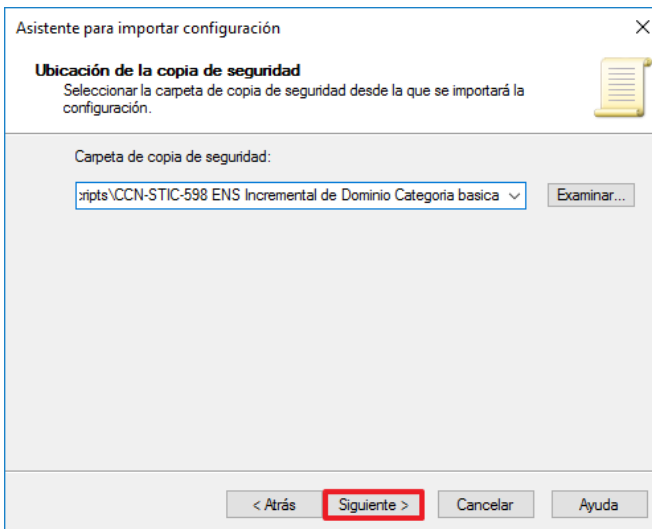
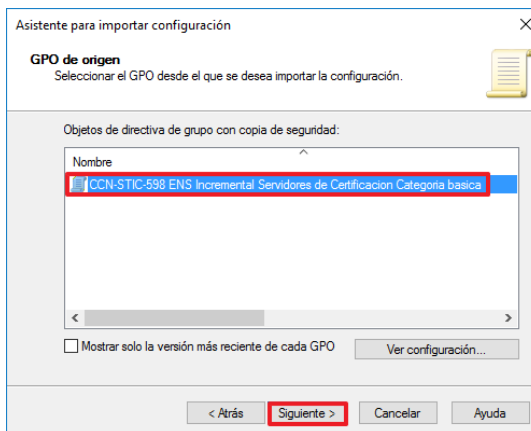
| Paso | Descripción                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 83.  | Expanda el nodo <b>“Configuración del equipo → Directivas→ Configuración de Windows → Configuración de seguridad”</b> .                                                                                                                                                 |
| 84.  | <p>Pulse con el botón derecho sobre <b>“Configuración de seguridad”</b> y seleccione la opción <b>“Importar directiva...”</b>.</p>                                                    |
| 85.  | <p>Seleccione la plantilla <b>“C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría básica.inf”</b>. Haga clic en el botón <b>“Abrir”</b>.</p>  |
| 86.  | Cierre el <b>“Editor de administración de directivas de grupo”</b> .                                                                                                                                                                                                    |

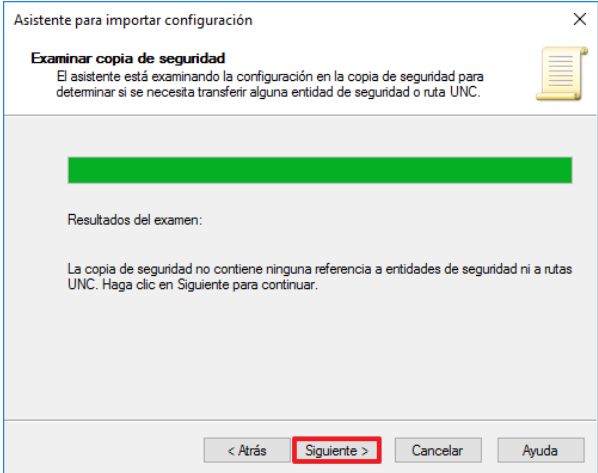
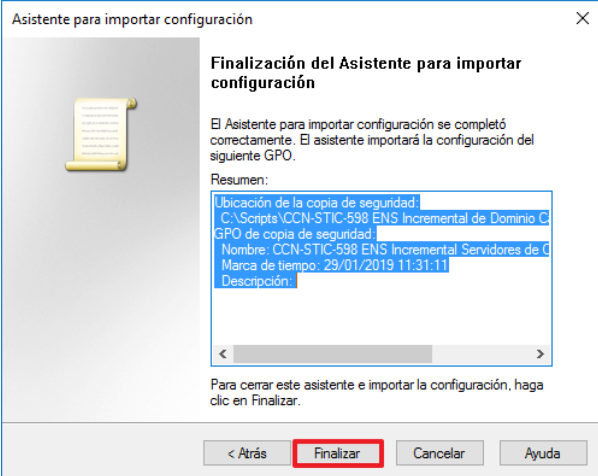
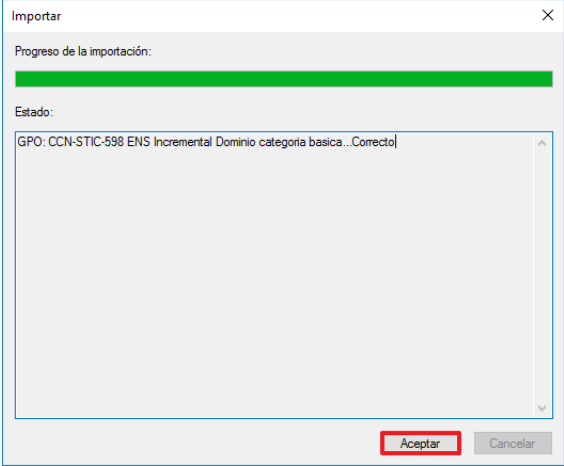
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.  | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>                                                           |
| 88.  | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 89.  | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidores Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoría básica” que contiene el servidor con el rol “Servidores Entidad de Certificación”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 90.  | Cierre la ventana “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 91.  | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 92.  | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

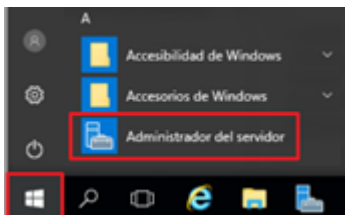
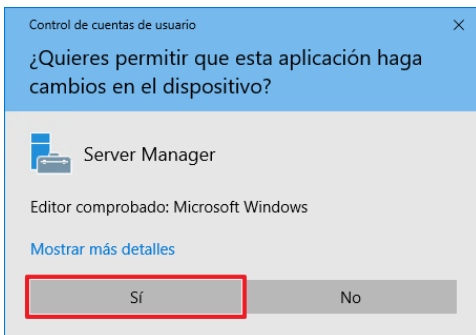
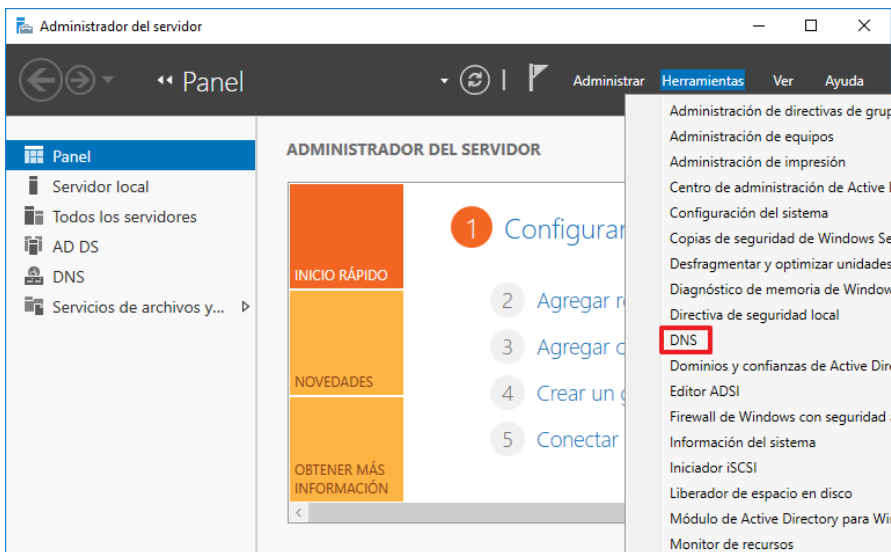
| Paso | Descripción                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93.  | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 Incremental Dominio categoria basica” y pulse el botón “Aceptar”.</p>                                                                                          |
| 94.  | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>  |
| 95.  | <p>Haga clic en “Siguiente &gt;” en el “Asistente para importar configuración”.</p>                                                                                                                                      |

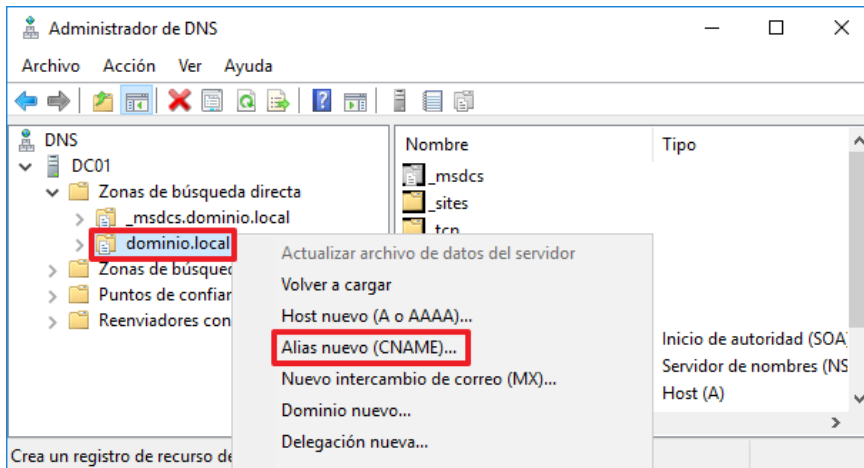
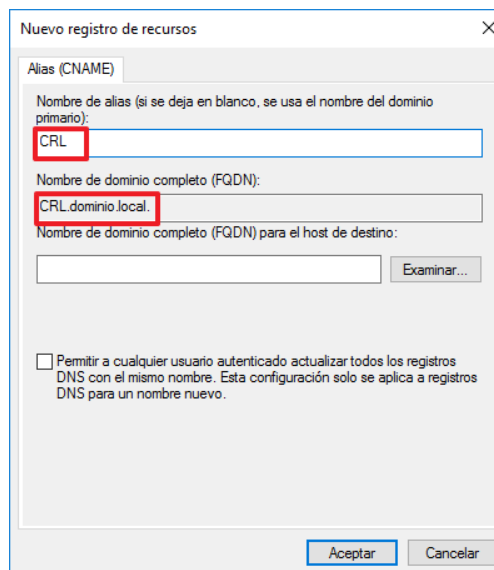
| Paso | Descripción                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Haga clic en “Siguiente”.</p>      |
| 97.  | <p>Haga clic en “Examinar...”.</p>  |

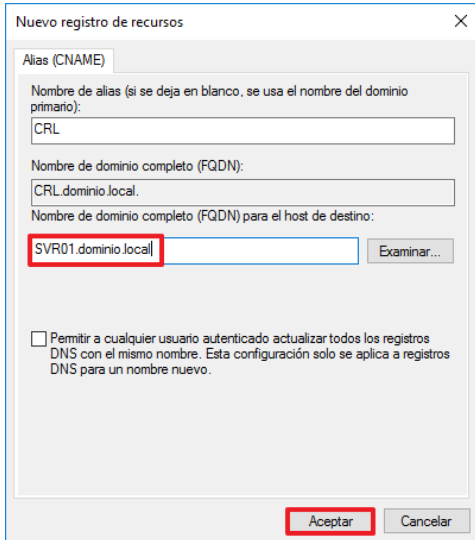
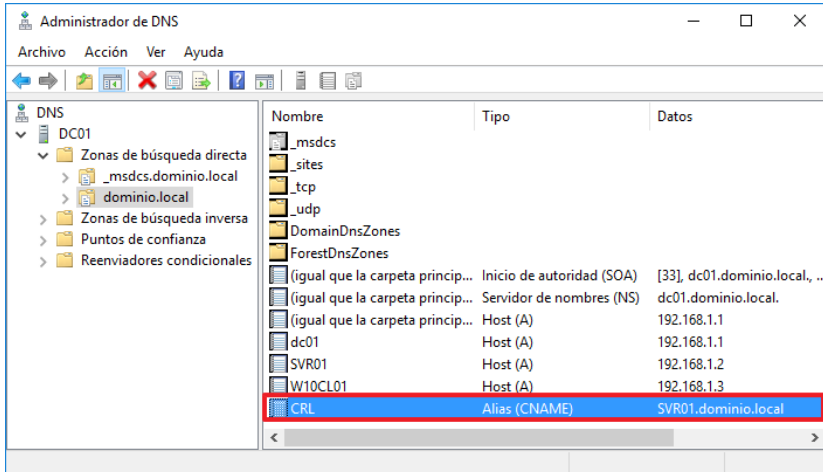
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 98.  | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoría basica” y pulse “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                   |
| 99.  | <p>Pulse “Siguiente &gt;” para continuar con la importación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 100. | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio Categoría basica” y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 101. | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>                                                                                                 |
| 102. | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                                                                                                                   |
| 103. | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>  |
| 104. | <p>Cierre la ventana “Administración de directivas de grupo”.</p>                                                                                                                                                                                                   |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

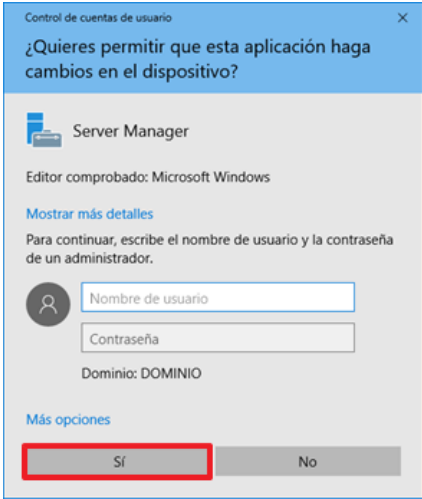
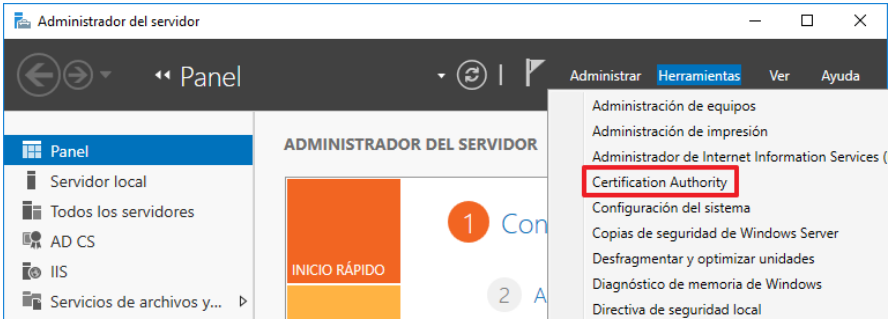
| Paso | Descripción                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 105. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p>Nota: Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>         |
| 106. | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 107. | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                   |
| 108. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>  |

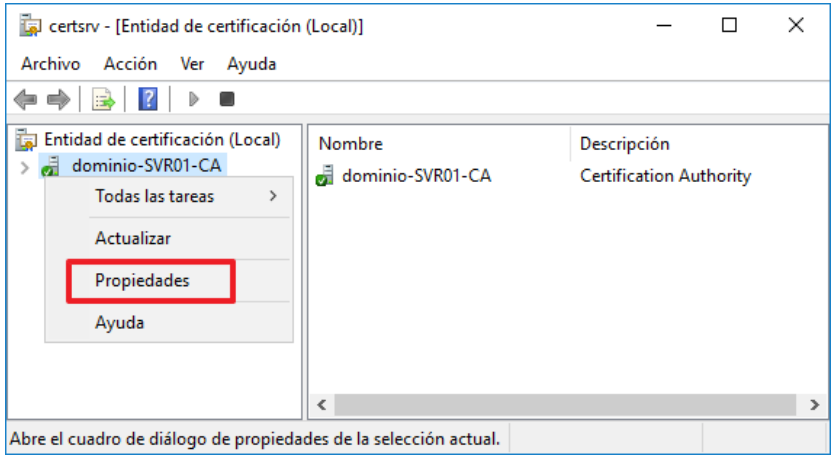
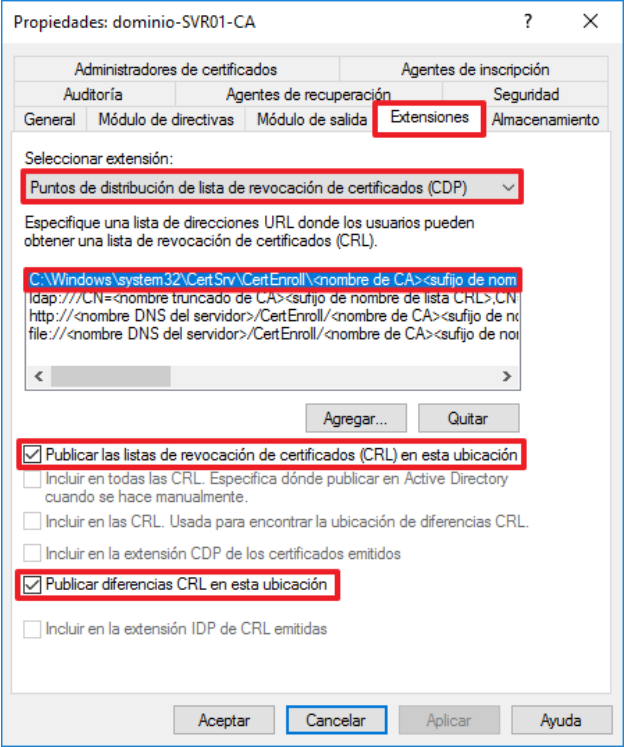
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 109. | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: “&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”.</p> <p>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>                                                         |
| 110. | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |

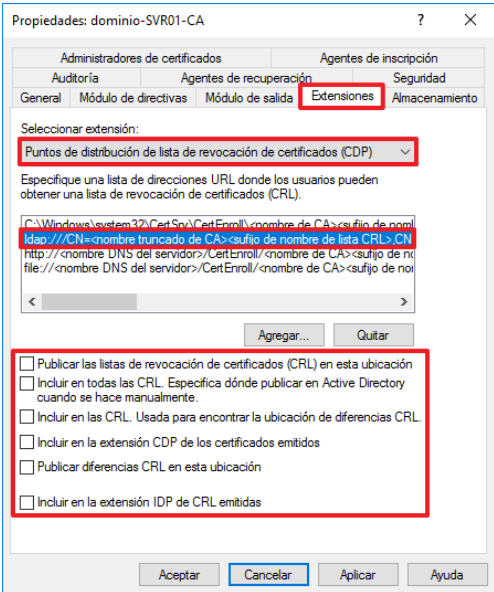
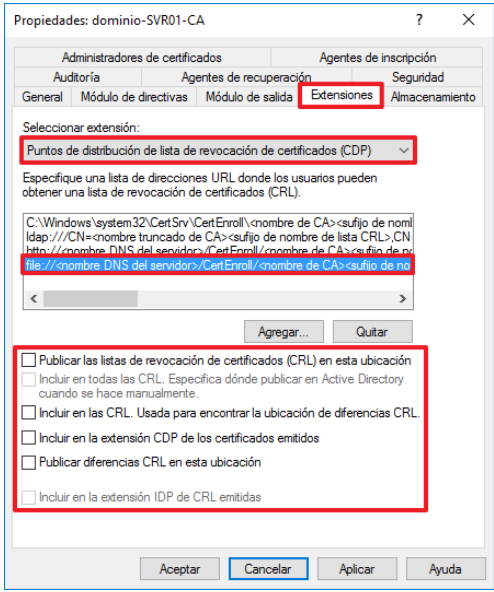
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 111. | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación subordinada de empresa y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p> |
| 112. | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>                                                                                                                                                                                                  |

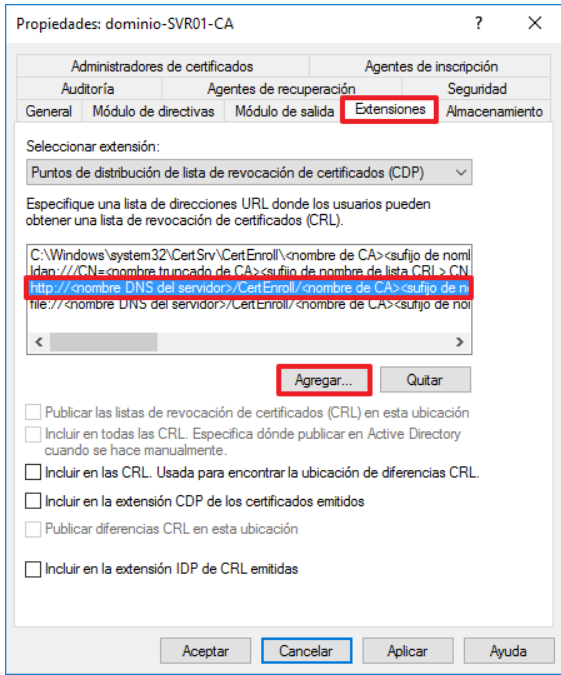
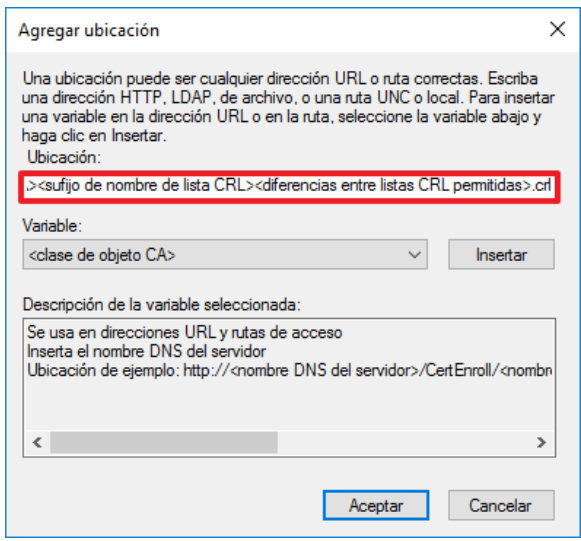
## 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.

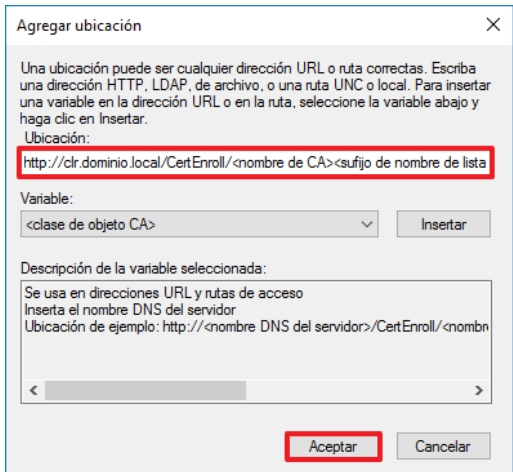
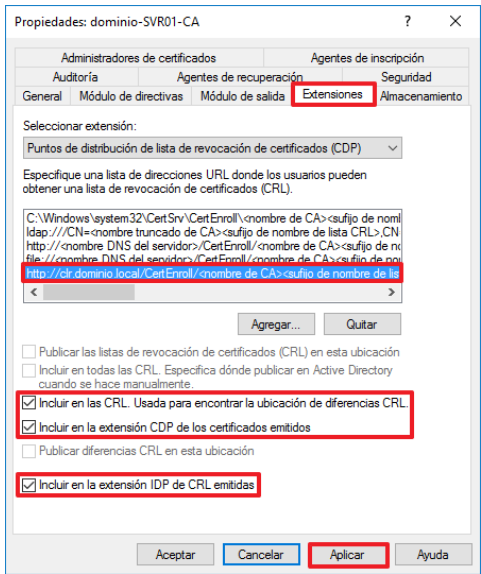
Los pasos que se describen a continuación se realizarán sobre el servidor miembro de Entidad de Certificación subordinada del dominio.

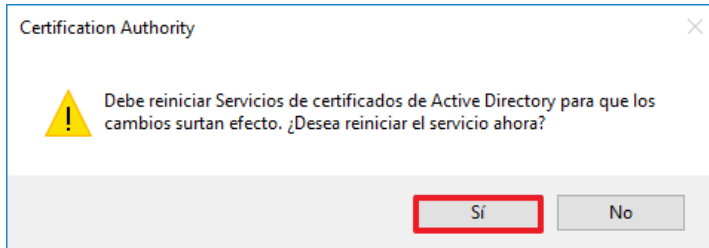
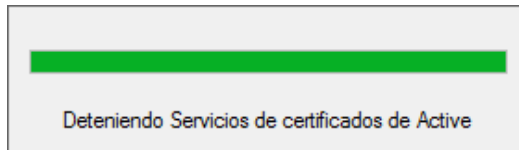
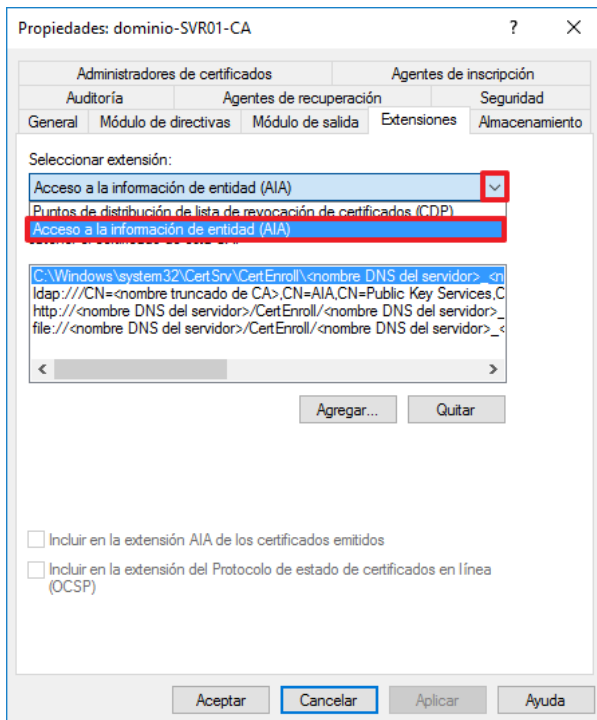
| Paso | Descripción                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 113. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>                                                        |
| 114. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                                    |
| 115. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí”.</p>  |
| 116. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                    |

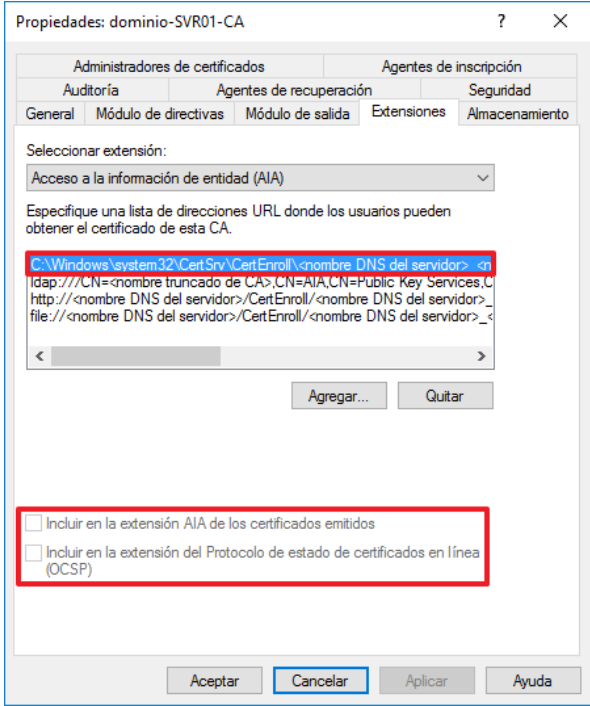
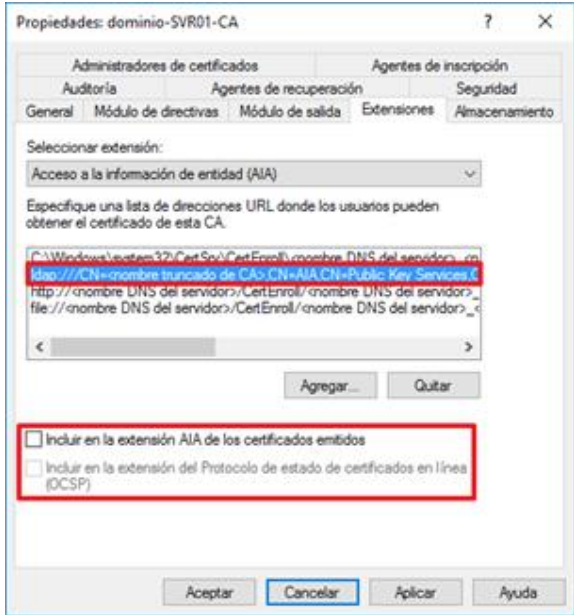
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 117. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente y con el botón derecho del ratón seleccione “Propiedades”.</p>                                                                                                                                                                                                                                                                                                                                               |
| 118. | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</p>  |

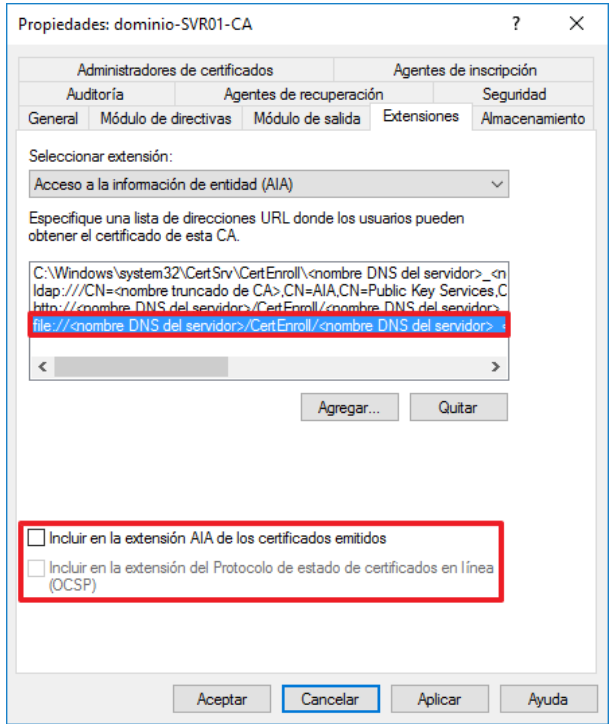
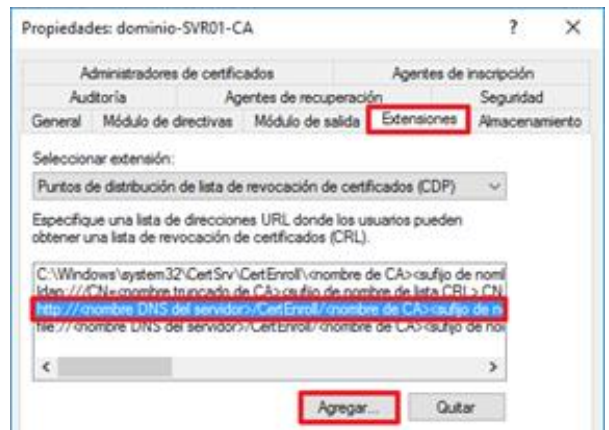
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 119. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando “<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>” y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>  |
| 120. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “<b>file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y desmarque todas las opciones como muestra la siguiente figura:</p>                                                                                                                                                               |

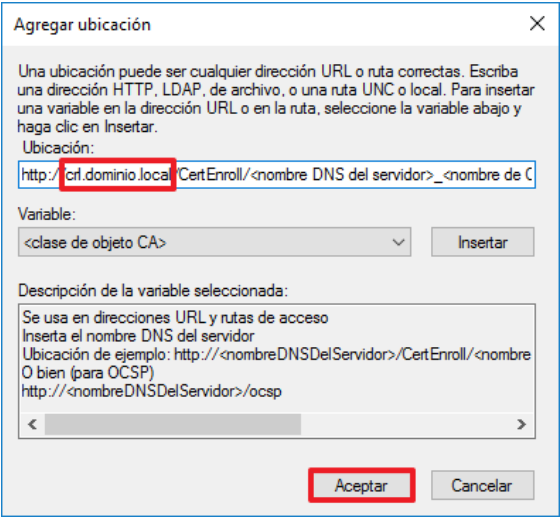
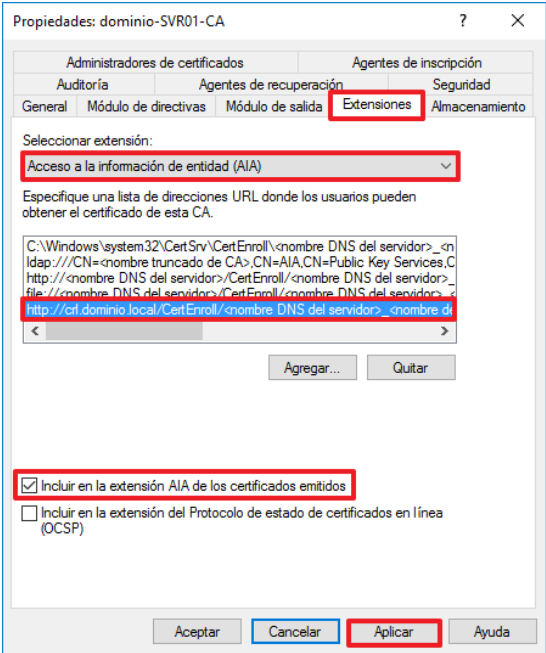
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 121. | De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto. |
| 122. | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                                                                   |
| 123. | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                            |

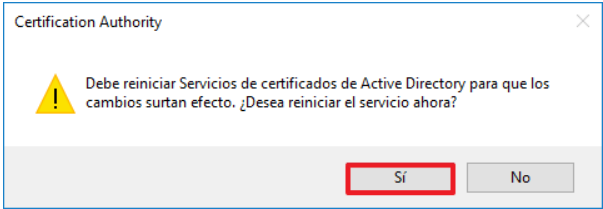
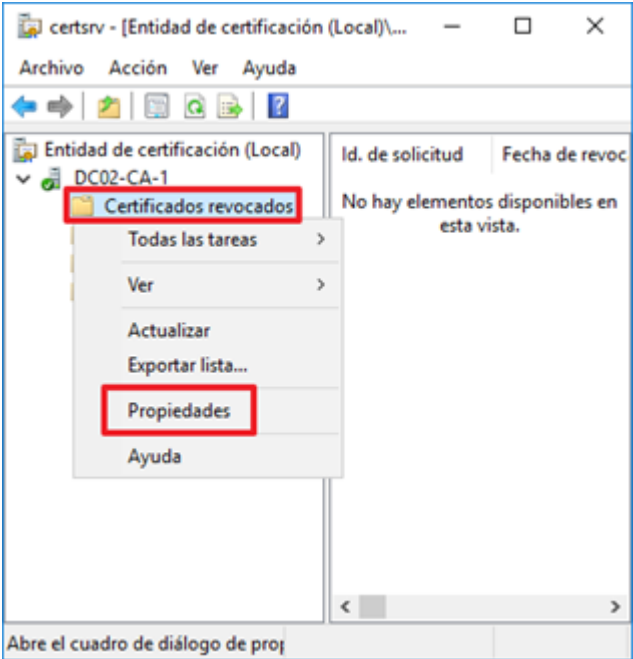
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 124. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creó anteriormente (Punto 2.3 PREPARACIÓN DEL DIRECTORIO ACTIVO) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                                 |
| 125. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos</li> <li>– Incluir en la extensión IDP de CRL emitidas</li> </ul> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

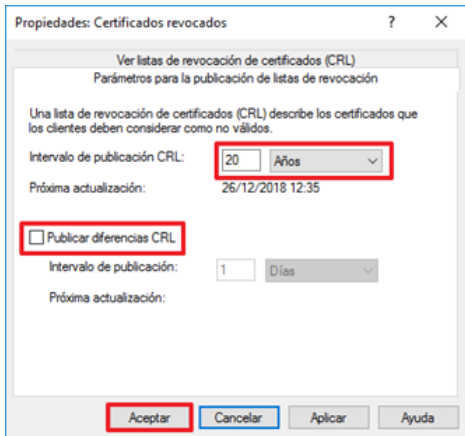
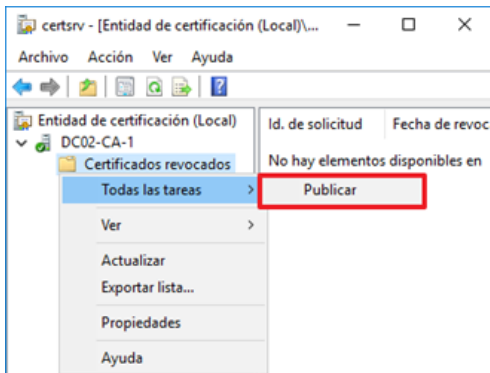
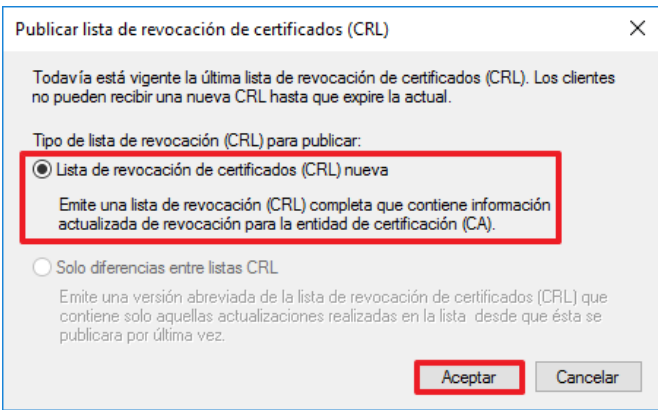
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 126. | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 127. | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 128. | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 129. | <p>Compruebe que en el objeto <b>"C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt"</b> todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura:</p>                     |
| 130. | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura:</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 131. | <p>Seleccione ahora <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y desmarque la opción <b>“Incluir en la extensión AIA de los certificados emitidos”</b>.</p>  |
| 132. | <p>Seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b>.</p>                                                                                                        |
| 133. | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                                                                                           |
| 134. | <p>Coloque el cursor sobre el campo vacío bajo <b>“Ubicación:”</b> y pulse la combinación de teclas <b>“Control + V”</b> para pegar el contenido recién copiado.</p>                                                                                                                                                                                  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 135. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios:</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                              |
| 136. | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 137. | <p>El sistema le solicitará reiniciar los “Servicios de certificados”. Para ello, pulse “Sí, en el siguiente mensaje de advertencia</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 138. | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 139. | <p>El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL y al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.</p> <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:</p> <p><b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b></p> <p>Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 140. | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p>  <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p> |
| 141. | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                                                                                                                                                                                                                                                                                          |
| 142. | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |

## ANEXO A.2.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.2.3 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS”.

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de Entidad de Certificación sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría básica del ENS.

### 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ

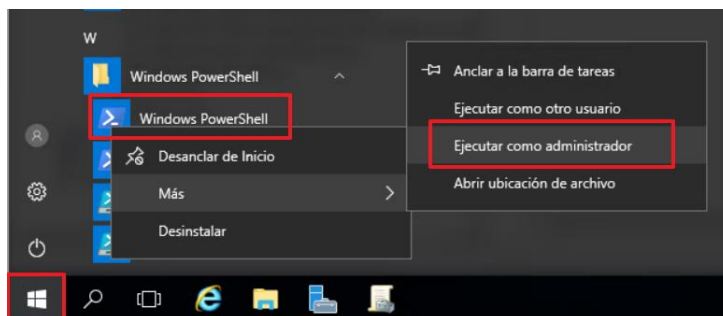
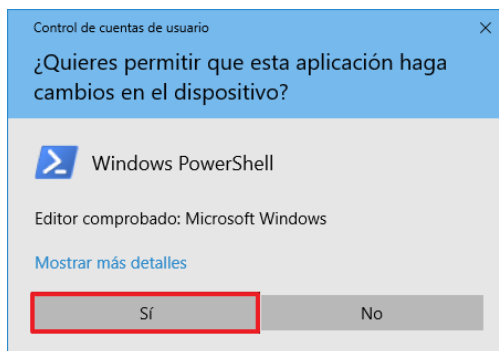
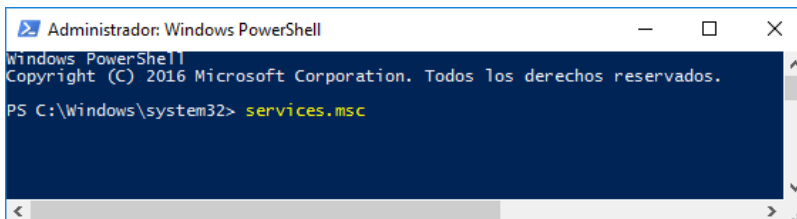
Para realizar esta lista de comprobación primero deberá iniciar sesión en el servidor independiente con una cuenta de usuario que tenga privilegios de administración.

Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

- a) Servicios (services.msc).

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

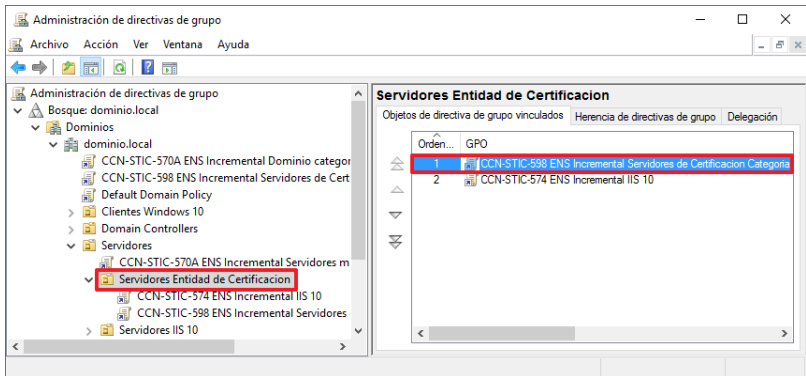
| Comprobación                                                            | OK/NOK | Cómo hacerlo                                                                                                                      |
|-------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor independiente Entidad de Certific. raíz |        | En el servidor independiente Entidad de Certificación raíz, inicie sesión con una cuenta que tenga privilegios de administración. |

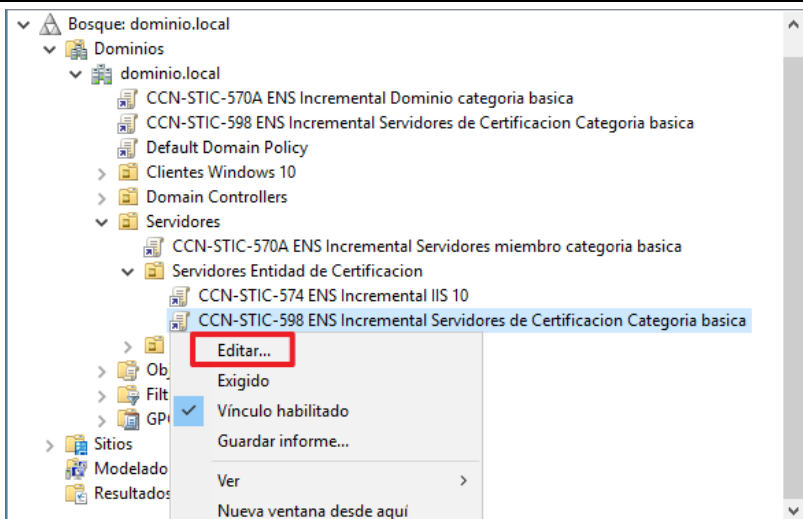
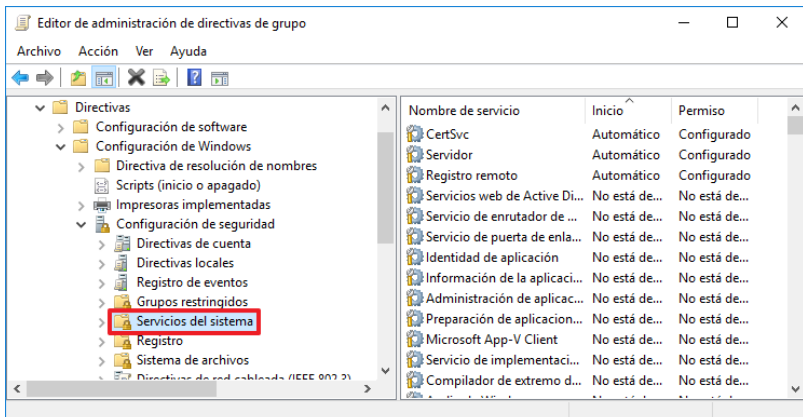
| Comprobación                                                                       | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |             |        |
|------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| 2. Verifique la correcta aplicación de la configuración de servicios del sistema". |                         | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic en <b>"Inicio de Windows → Windows PowerShell"</b> clic con el botón derecho sobre el icono de PowerShell, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse <b>"Sí"</b> en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee <b>"rsop.msc"</b> en la consola de comandos que se ha abierto:</p>  <p>En la consola de "Servicios", compruebe los siguientes valores.</p> |             |        |
| Servicio (Nombre largo)                                                            | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                      | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Configurado |        |

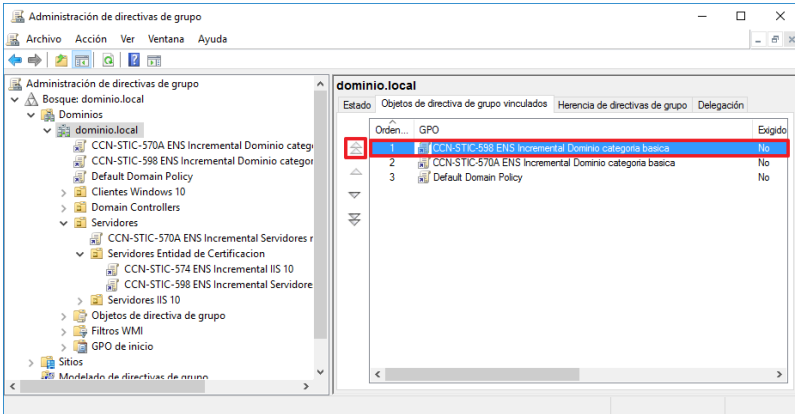
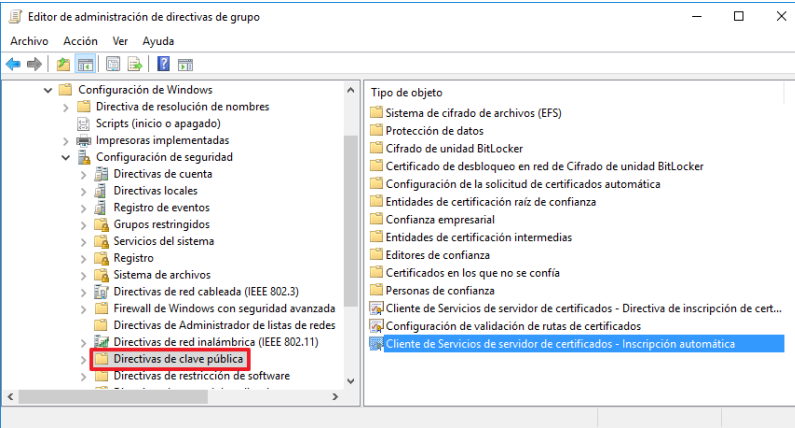
## 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO

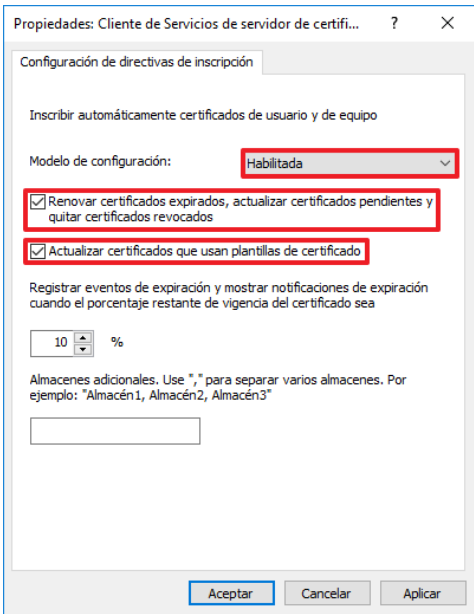
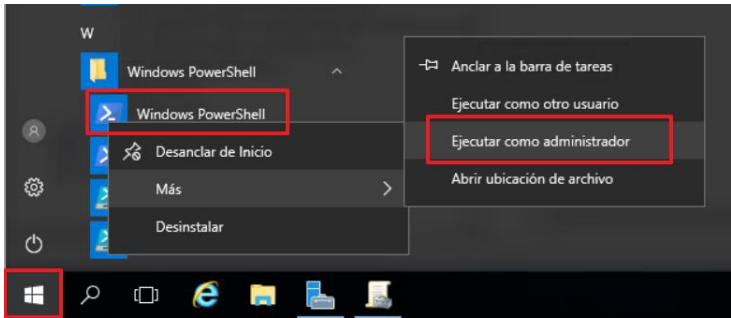
Las consolas y herramientas que se utilizarán son las siguientes:

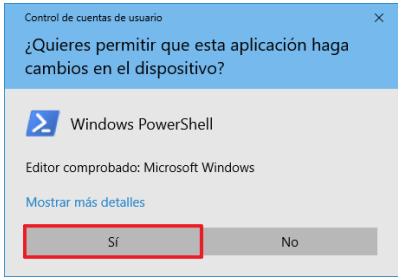
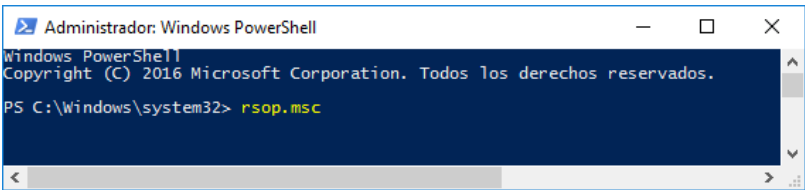
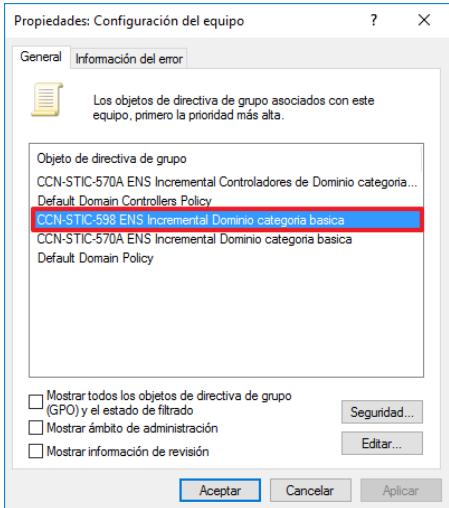
- Administrador de directivas de grupo (gpmc.msc).
- Usuarios y equipos de Active Directory (dsa.msc).
- Conjunto resultante de directivas (rsop.msc).

| Comprobación                                                                                                                        | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en un controlador de dominio.                                                                                      |        | En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 2. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica".              |        | <p>Ejecute el "Administrador de directivas de grupo" mediante la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b></p> <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa "Servidores Entidad de Certificación". Verifique que la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica" está creada y vinculada en el primer lugar de orden de vínculo.</p>  |
| 3. Verifique los servicios del sistema de la directiva "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica". |        | Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo".                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Comprobación                                  | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |             |        |
|-----------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                               |                         | <div></div> <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:<br/><b>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</b></p> <div></div> <p><b>Nota:</b> Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</p> |             |        |
| Servicio (Nombre largo)                       | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Configurado |        |
| Servidor                                      | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Configurado |        |
| Registro Remoto                               | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Configurado |        |

| Comprobación                                                                                                                                    | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Dominio categoria basica”.                                              |        | <p>Ejecute el “Administrador de directivas de grupo” a través de la siguiente ruta:<br/> <b>“Inicio → Herramientas administrativas → Administración de directivas de grupo”</b><br/> Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política “CCN-STIC-598 ENS Incremental Dominio categoria básica” está creada y vinculada en el primer lugar de orden de vínculo.</p>                                                      |
| 5. Verifique la configuración de inscripción automática de certificados en la política “CCN-STIC-598 ENS Incremental Dominio categoria basica”. |        | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”. Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:<br/> <b>Directiva CCN-STIC-598 ENS Incremental Dominio categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  |

| Comprobación                                                                                                                             | OK/NOK               | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------|--------|-------------------------|------------|--|----------------------------------------------------------------------------------------------------|----------------------|--|------------------------------------------------------------|----------------------|--|
|                                                                                                                                          |                      | <p>Haga doble clic sobre el objeto “Cliente de Servicios de servidor de certificados – Inscripción automática” y compruebe los valores correspondientes a la inscripción automática.</p>                                                                                                                                                                                                         |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|                                                                                                                                          |                      | <table border="1"> <thead> <tr> <th>Configuración</th><th>Estado</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Modelo de configuración</td><td>Habilitada</td><td></td></tr> <tr> <td>Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados</td><td>Habilitada (marcada)</td><td></td></tr> <tr> <td>Actualizar certificados que usan plantillas de certificado</td><td>Habilitada (marcada)</td><td></td></tr> </tbody> </table> | Configuración | Estado | OK/NOK | Modelo de configuración | Habilitada |  | Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados | Habilitada (marcada) |  | Actualizar certificados que usan plantillas de certificado | Habilitada (marcada) |  |
| Configuración                                                                                                                            | Estado               | OK/NOK                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Modelo de configuración                                                                                                                  | Habilitada           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados                                       | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Actualizar certificados que usan plantillas de certificado                                                                               | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| 6. Verifique la correcta aplicación de la política “CCN-STIC-598 Incremental Dominio categoría básica” en un equipo miembro del dominio. |                      | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic en “Inicio de Windows → Windows PowerShell” clic con el botón derecho sobre el icono de PowerShell, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>                                                                |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse “Sí” en la ventana de “Control de cuentas de usuario”.</p>  <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  <p>A continuación, haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría básica” aparece en la lista como muestra la imagen.</p>  |

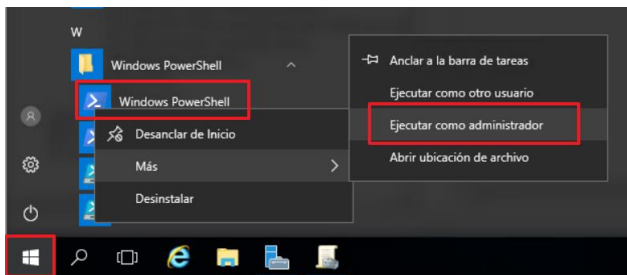
### 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA

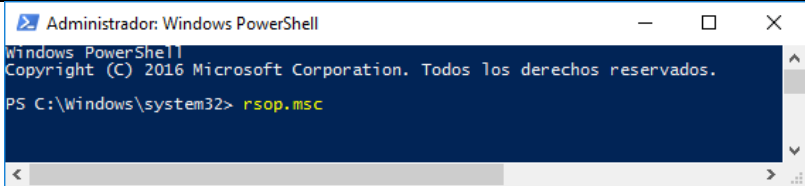
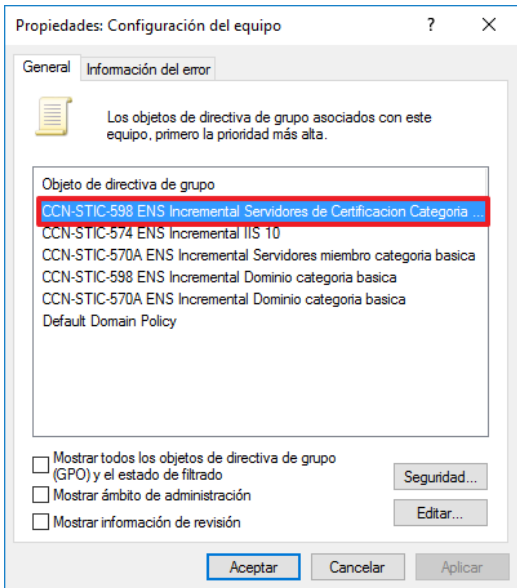
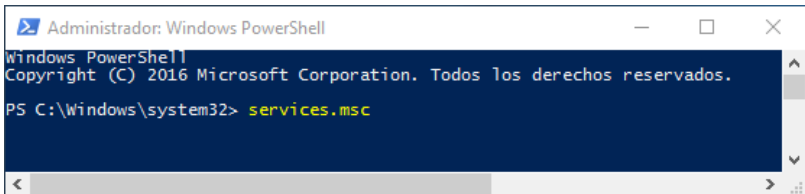
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

Para realizar las comprobaciones pertinentes en los servidores miembros se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

Las consolas y herramientas que se utilizarán son las siguientes:

- a) Conjunto resultante de directivas (rsop.msc).
- b) Servicios (services.msc).

| Comprobación                                                                                                                                                     | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación raíz de empresa.                                                                                        |        | En el servidor Entidad de Certificación raíz de empresa, inicie sesión con una cuenta que tenga privilegios de administración del dominio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2. Verifique la correcta aplicación de la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic en <b>"Inicio de Windows → Windows PowerShell"</b> clic con el botón derecho sobre el icono de PowerShell, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario". Teclee "rsop.msc" en la consola de comandos que se ha abierto:</p> |

| Comprobación                                                                                                                                                                | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                   |             |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                             |                         | <div></div> <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica” aparece en la lista como muestra la imagen.</p> <div></div> |             |        |
| 3. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría básica”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p> <div></div> <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                                                                                                                 |             |        |
| Servicio (Nombre largo)                                                                                                                                                     | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                               | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |
| Servidor                                                                                                                                                                    | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |
| Registro Remoto                                                                                                                                                             | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |

## ANEXO A.3. CATEGORÍA MEDIA

### ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

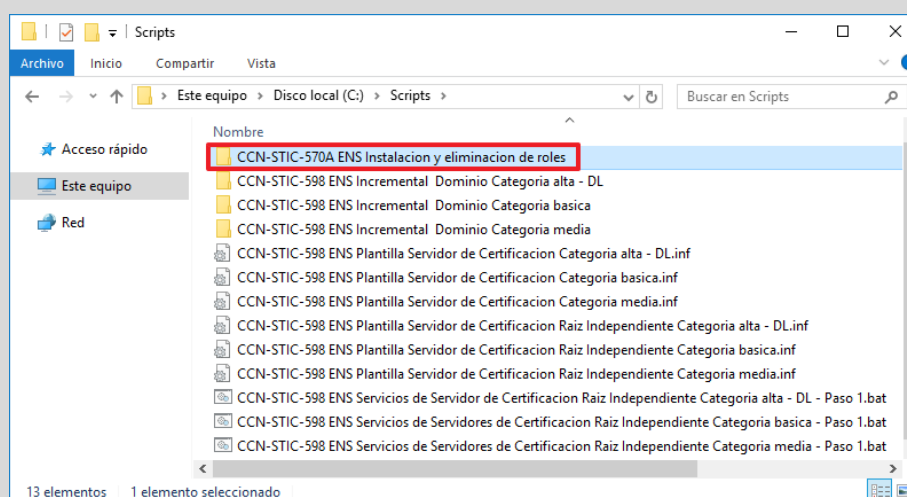
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Microsoft Windows Server 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

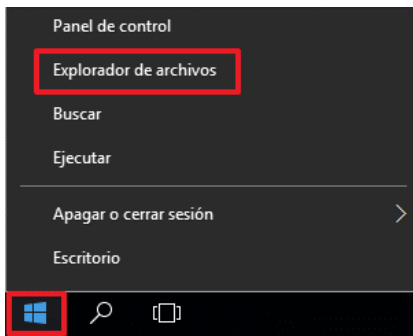
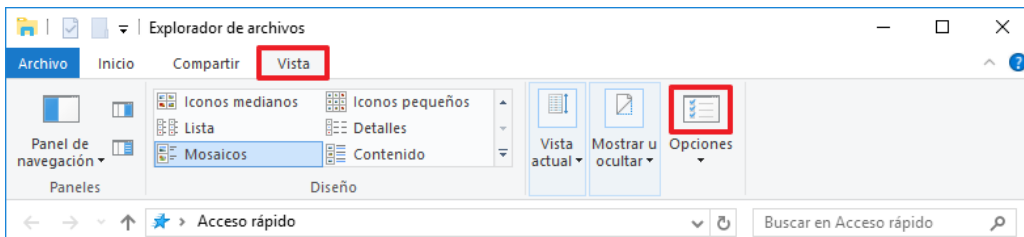
- Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad media.
- Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad media.

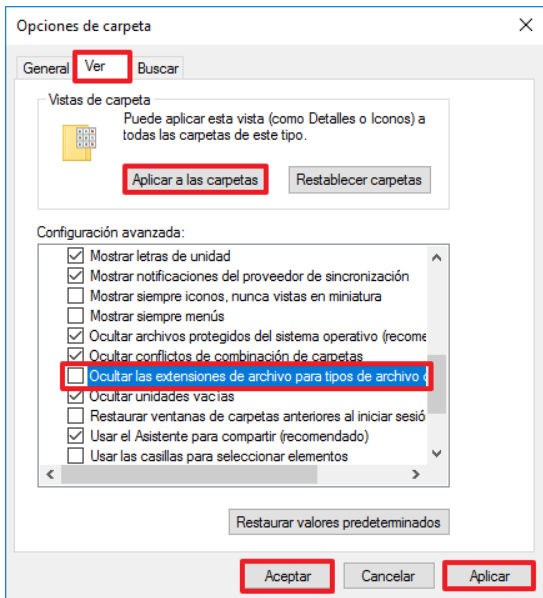
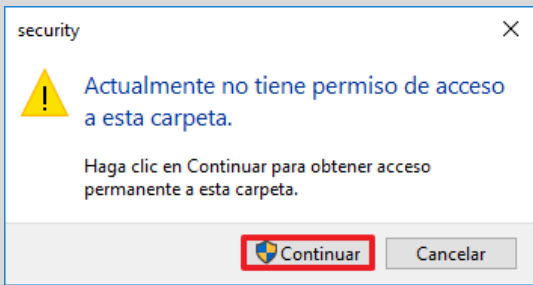
**Nota:** Si instala un Servidor de Entidad de Certificación por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO. En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía “CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016” encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta “Scripts” adjunta a la presente guía.

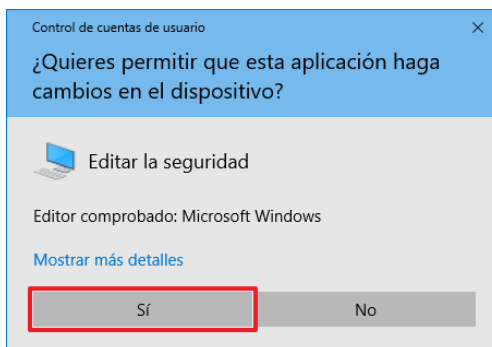
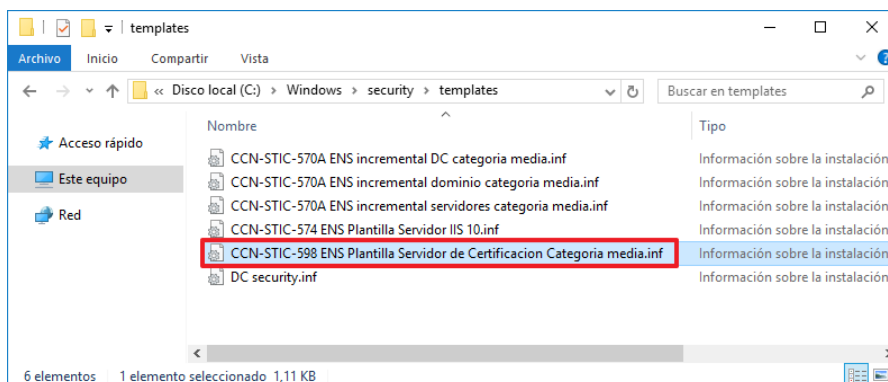
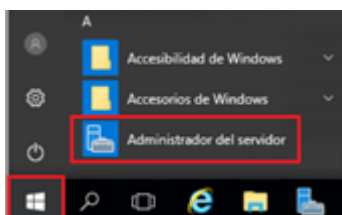


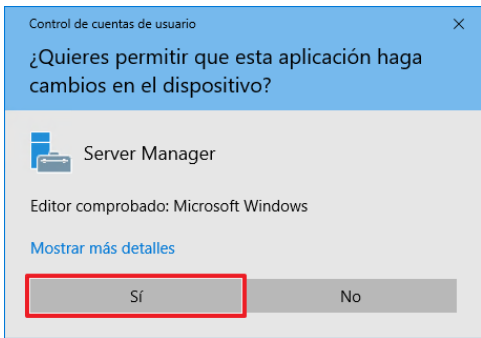
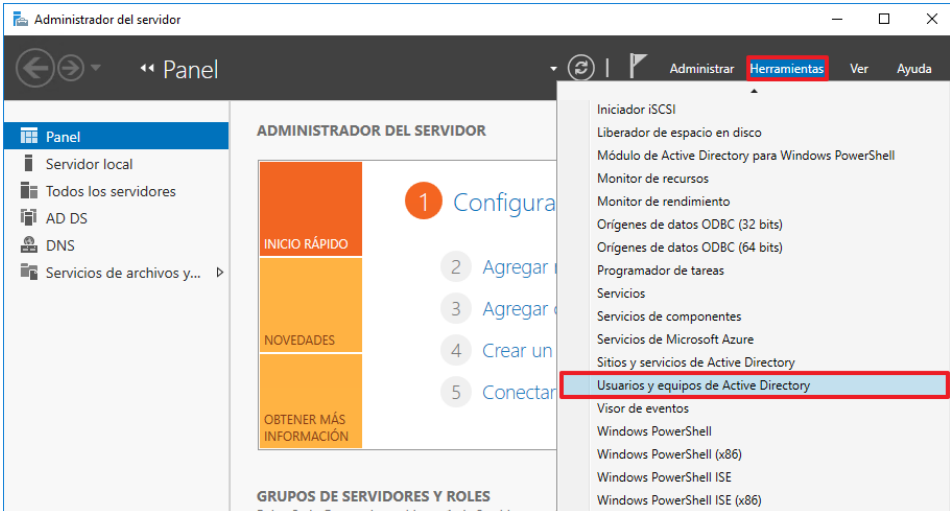
## 1. PREPARACIÓN DEL DOMINIO

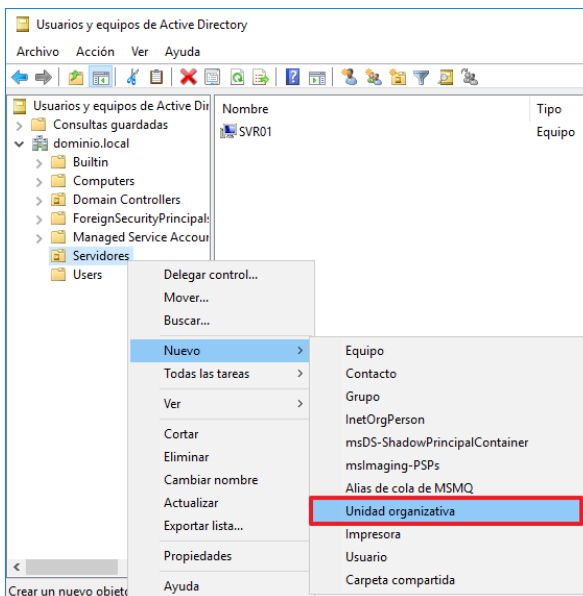
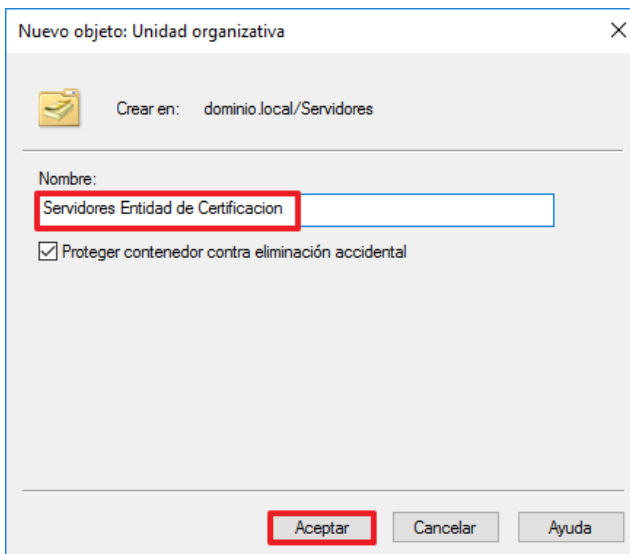
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor de Entidad de Certificación.

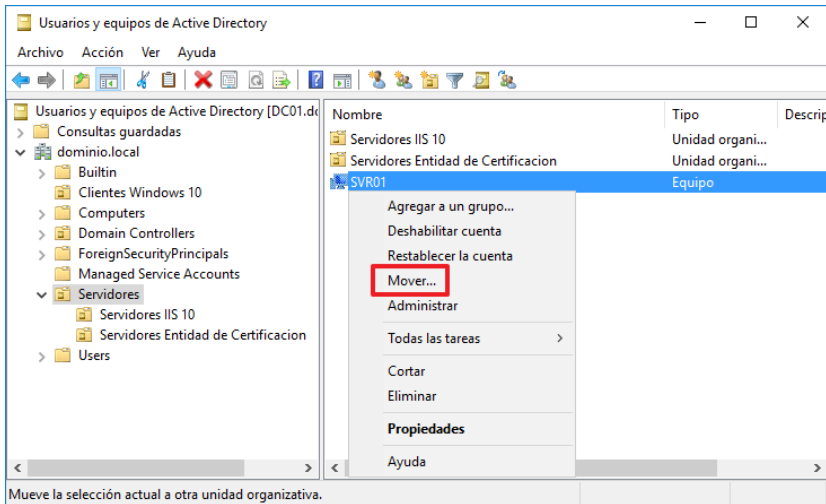
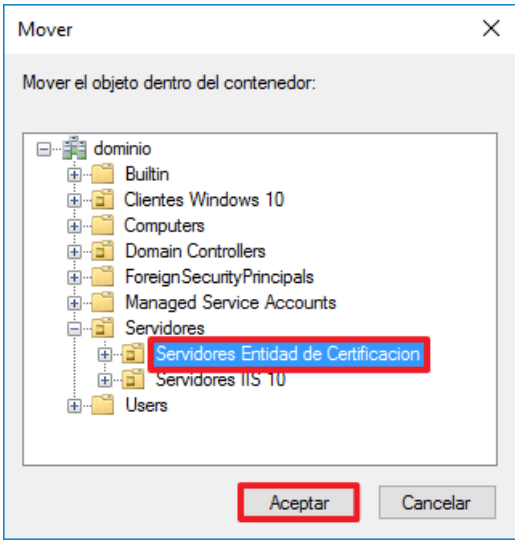
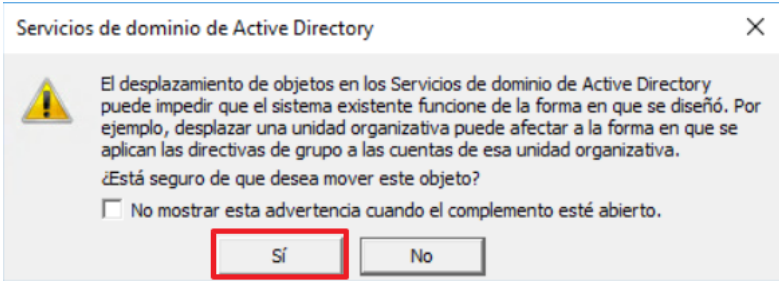
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p>                                                                                                                                           |
| 2.   | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                                                                                                                                                                    |
| 3.   | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                                                                                                                                                                                                                    |
| 4.   | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>  |
| 5.   | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                     |

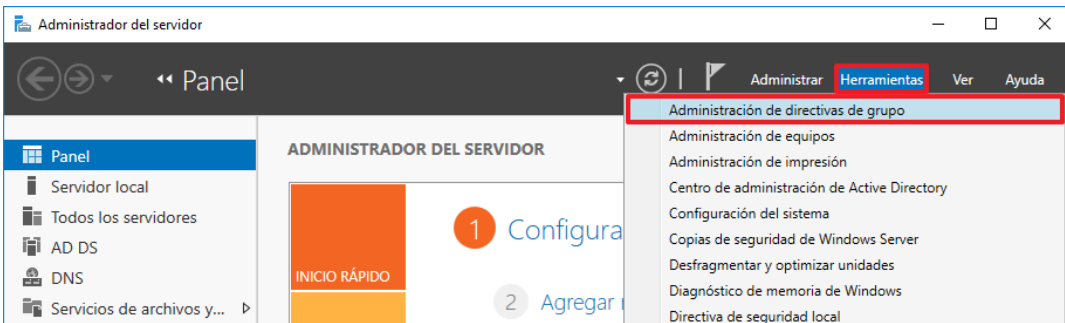
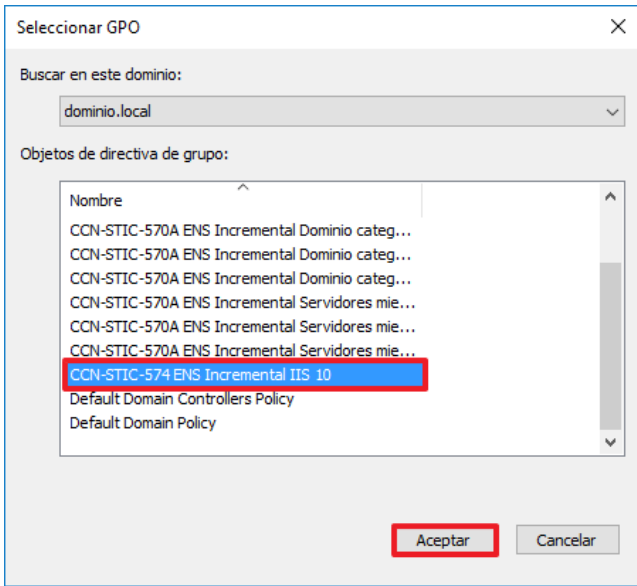
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |
| 7.   | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                            |

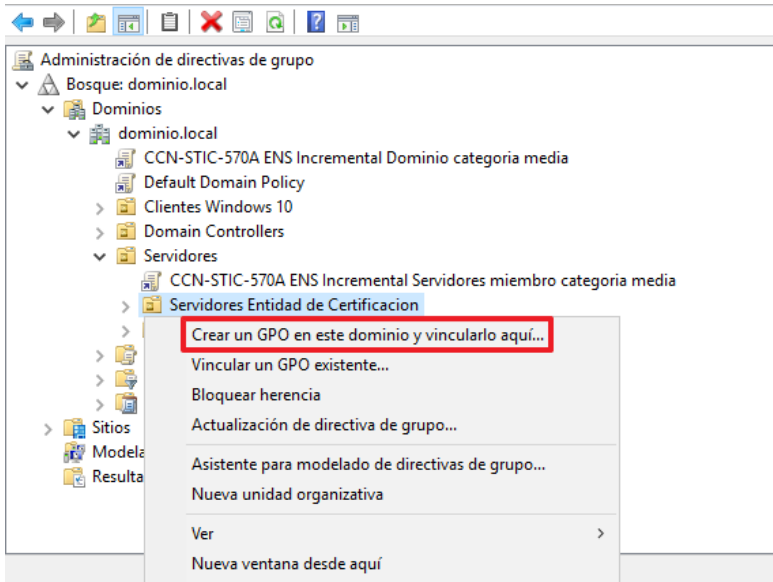
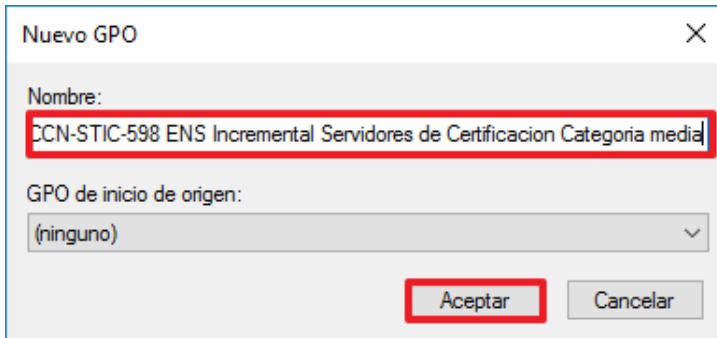
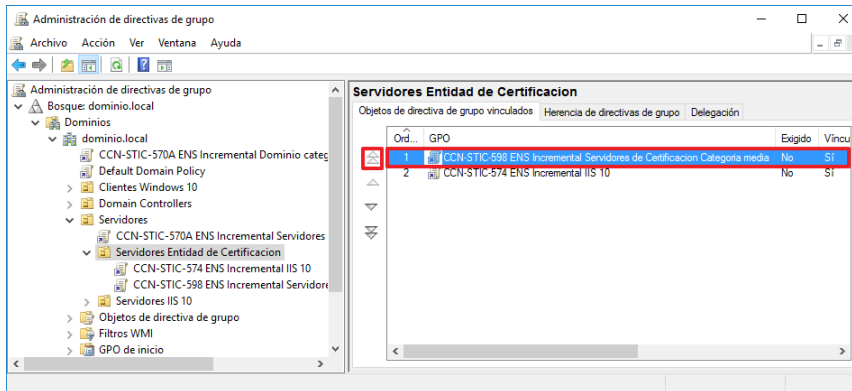
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.   | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |
| 9.   | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría media.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| 10.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |

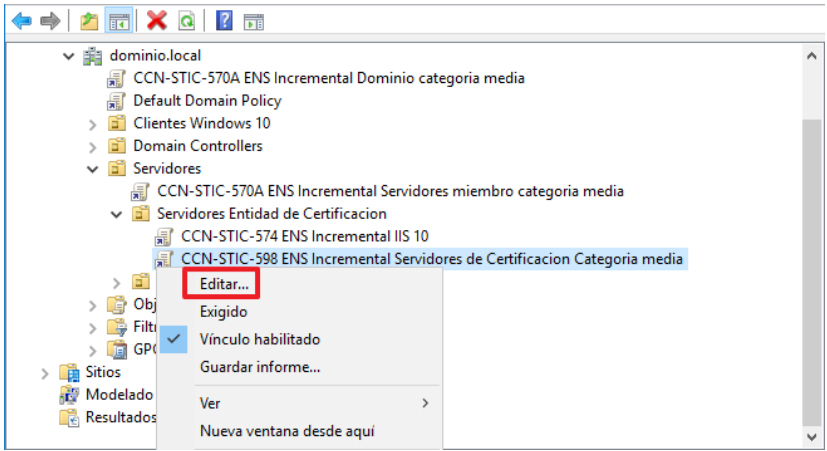
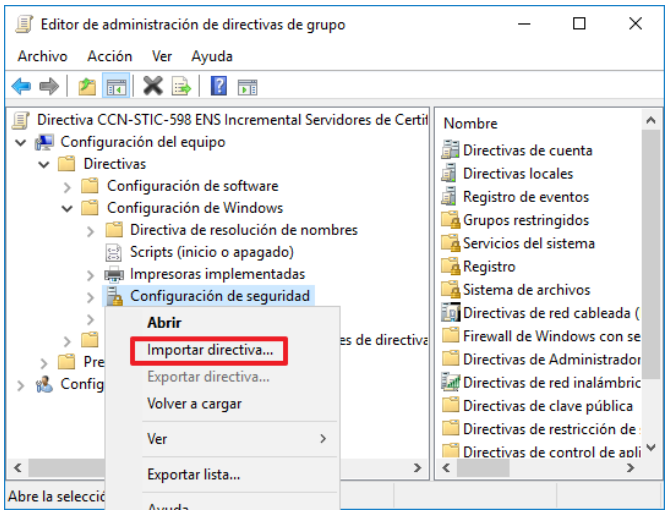
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                             |
| 12.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione “Herramientas → Usuarios y equipos de Active Directory”.</p>  |

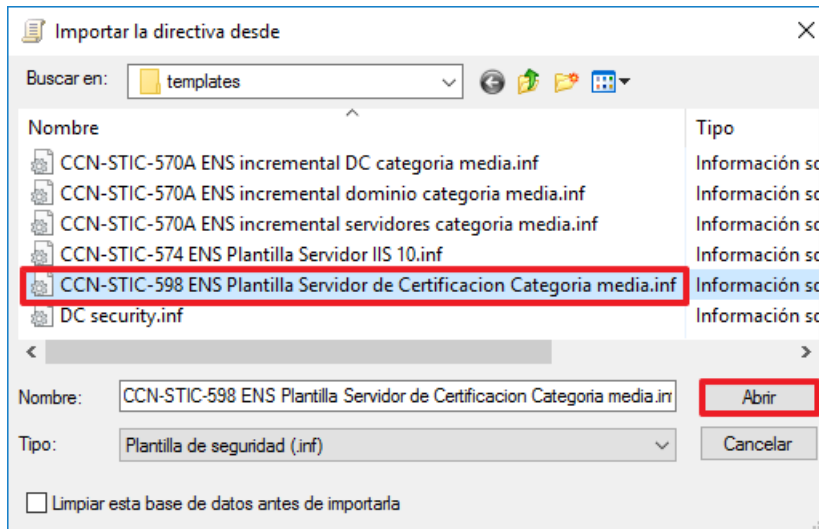
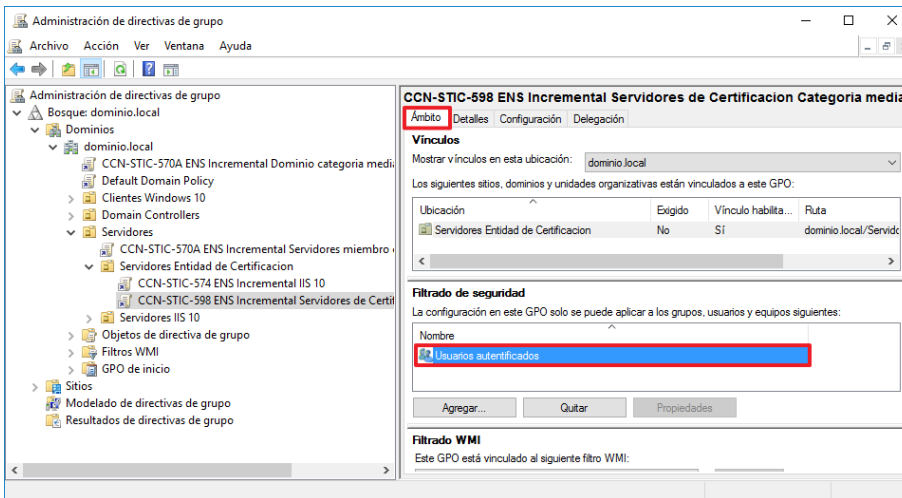
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo “&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local → Servidores”.</p> |
| 14.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

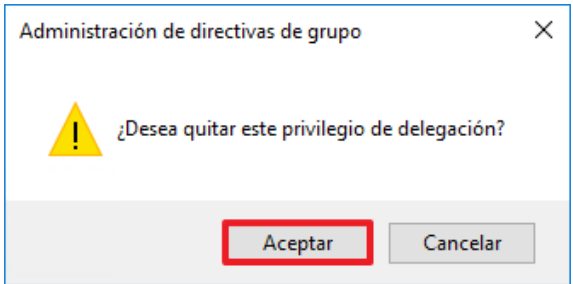
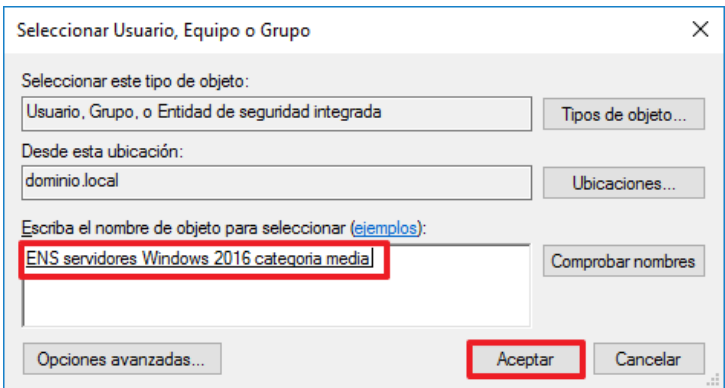
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores entidad de certificación a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |
| 16.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                         |
| 17.  | <p>Acepte el mensaje de advertencia</p>                                                                                                                                                                                                                                                                                                         |
| 18.  | <p>Cierre la herramienta de “Usuarios y equipos de Active Directory”.</p>                                                                                                                                                                                                                                                                                                                                                           |

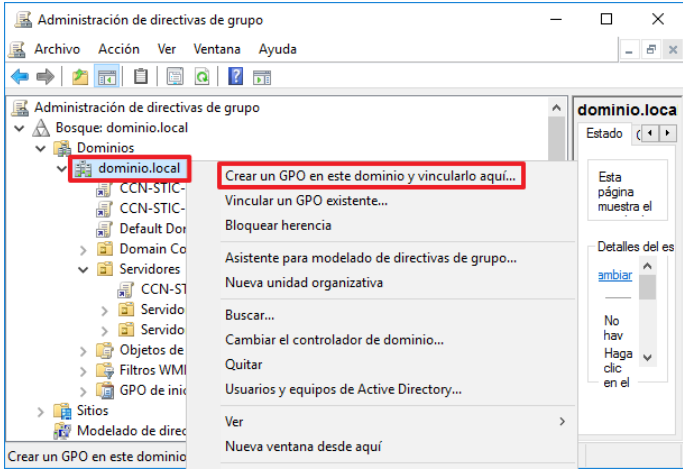
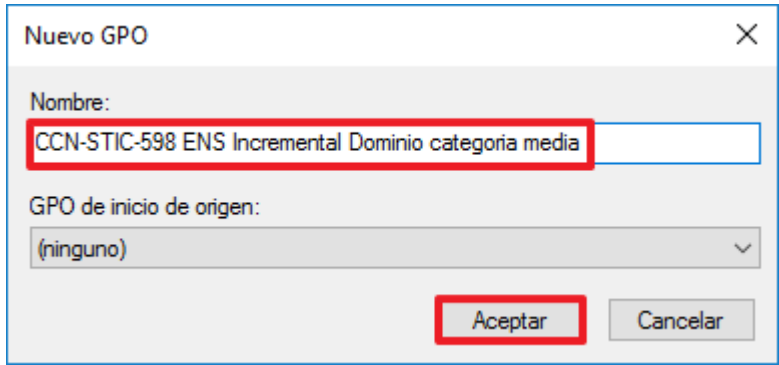
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.  | A continuación, abra el “Administrador del servidor”.                                                                                                                                                                                                                                                                                      |
| 20.  | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón <b>“Herramientas → Administración de directivas de grupo”</b>.</p>                                                                                          |
| 21.  | <p>A continuación, despliegue el nodo <b>“Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”</b>.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p>        |
| 22.  | <p>Seleccione “Vincular un GPO existente...” y vincule el objeto de directiva de grupo “CCN-STIC-574 ENS Incremental IIS 10” a la nueva unidad organizativa “Servidores Entidad de Certificación”, haciendo clic con el botón derecho sobre ella.</p>  |

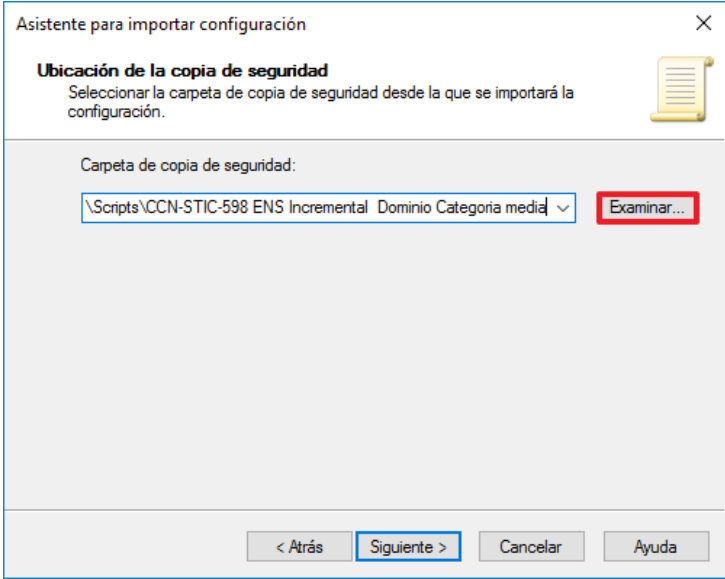
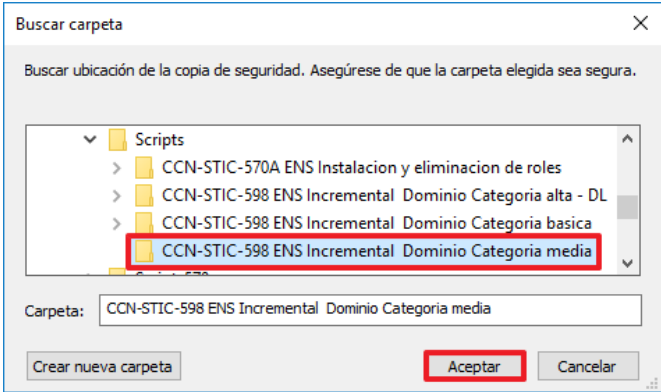
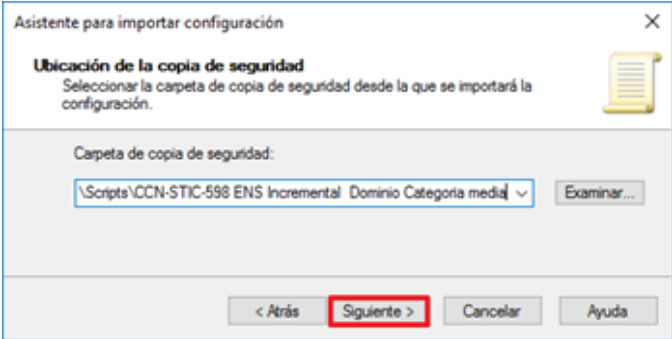
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23.  | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>       |
| 24.  | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” y haga clic en el botón “Aceptar”.</p>                                                                                                                        |
| 25.  | <p>Seleccione la unidad organizativa “<b>Servidores Entidad de Certificación</b>”. En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  |
| 26.  | <p>De esta forma, se garantiza que la directiva se aplica correctamente.</p>                                                                                                                                                                                                                                                                                |

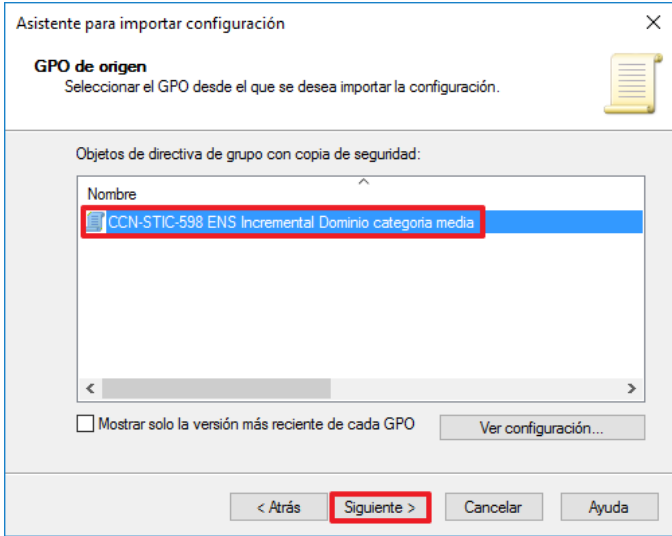
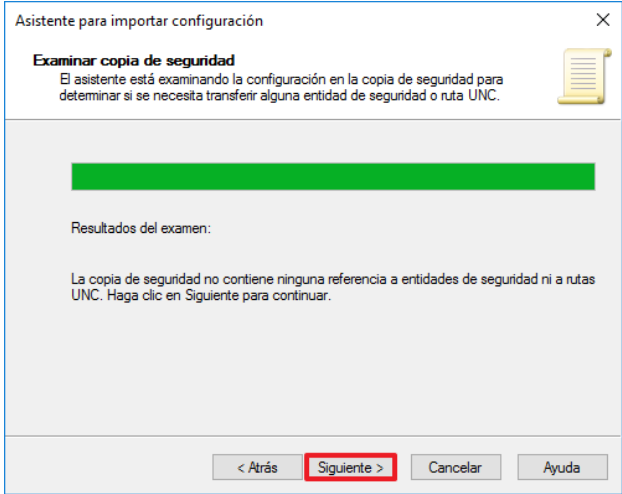
| Paso | Descripción                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27.  | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción “Editar”.</p>  |
| 28.  | <p>Expanda el nodo “Configuración del equipo → Directivas→ Configuración de Windows → Configuración de seguridad”.</p>                                                                                                        |
| 29.  | <p>Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.</p>                      |

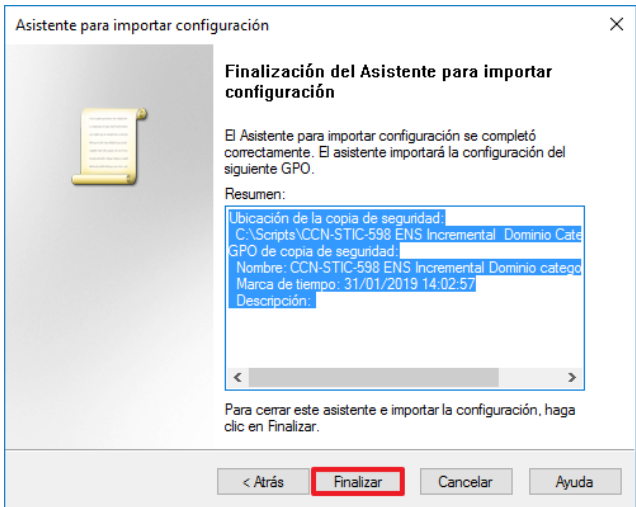
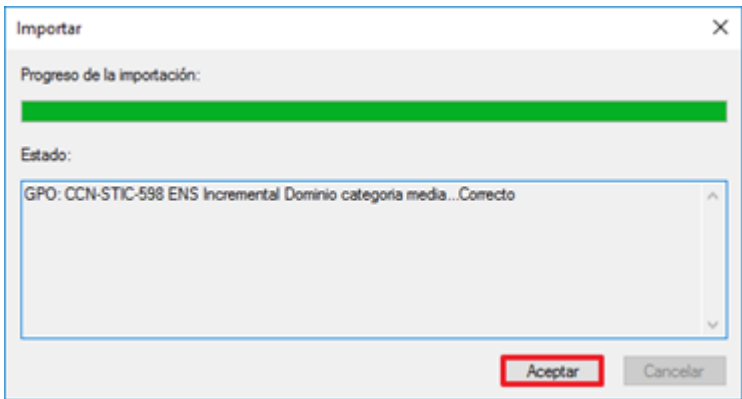
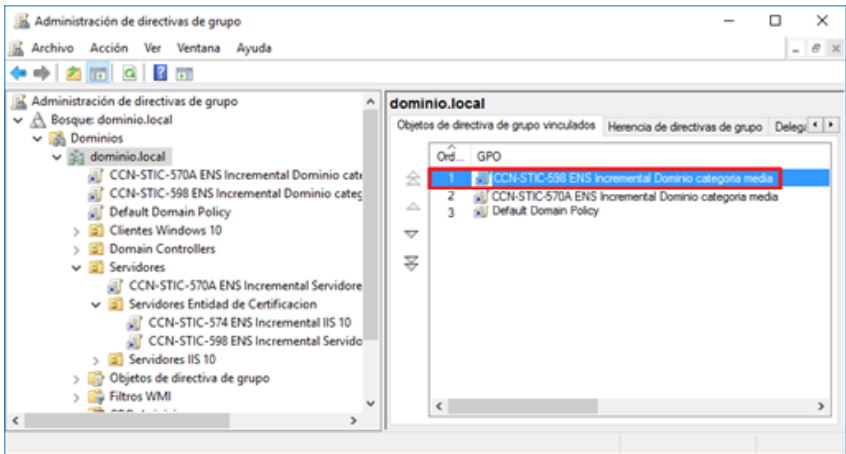
| Paso | Descripción                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30.  | <p>Seleccione la plantilla “C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría media.inf”. Haga clic en el botón “Abrir”.</p>                                                     |
| 31.  | <p>Cierre el “Editor de administración de directivas de grupo”.</p>                                                                                                                                                                                                                                       |
| 32.  | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33.  | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>                                                              |
| 34.  | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidores Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoría media” que contiene el servidor con el rol “Servidores Entidad de Certificación”.</p> |
| 35.  | <p>Cierre la ventana “Editor de administración de directivas de grupo”.</p>                                                                                                                                                                                                                                                                                                                                                |

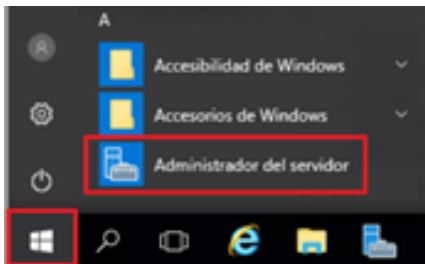
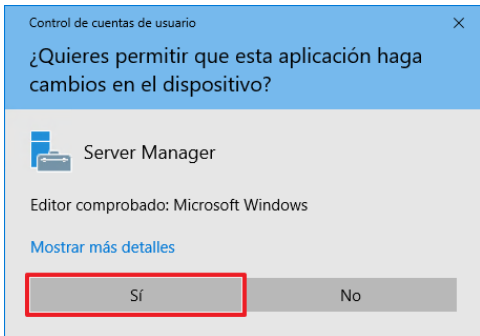
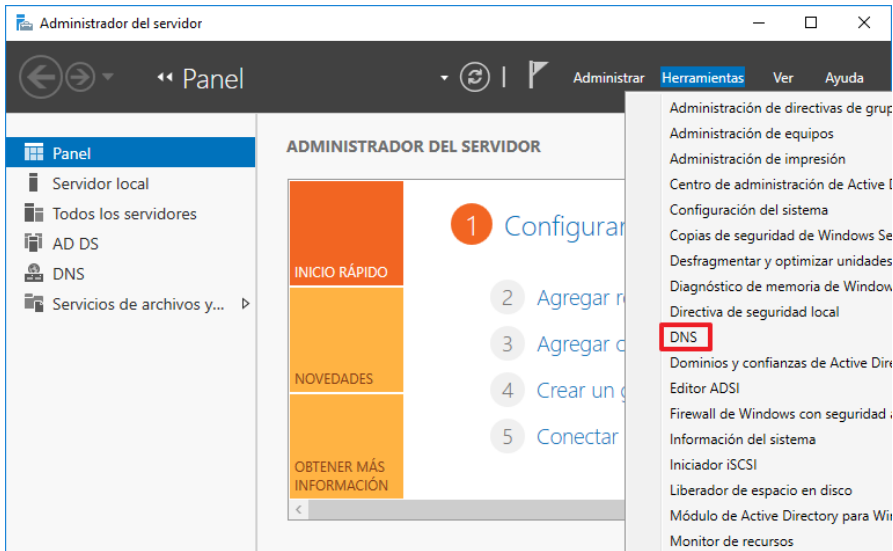
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 36.  | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 37.  | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 38.  | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 Incremental Dominio categoria media” y pulse el botón “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 39.  | Haga clic en “Siguiente >” en el “Asistente para importar configuración”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

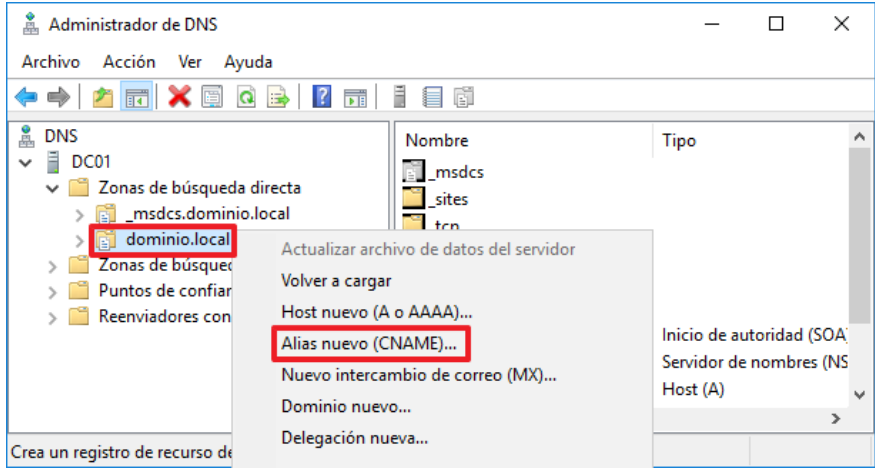
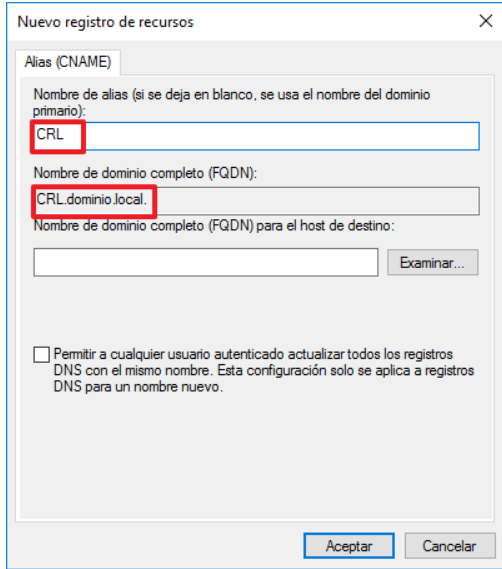
| Paso | Descripción                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 40.  | <p>Haga clic en “Examinar...”.</p>                                                                                                                                         |
| 41.  | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoria media” y pulse “Aceptar”.</p>  |
| 42.  | <p>Pulse “Siguiete &gt;” para continuar con la importación.</p>                                                                                                          |

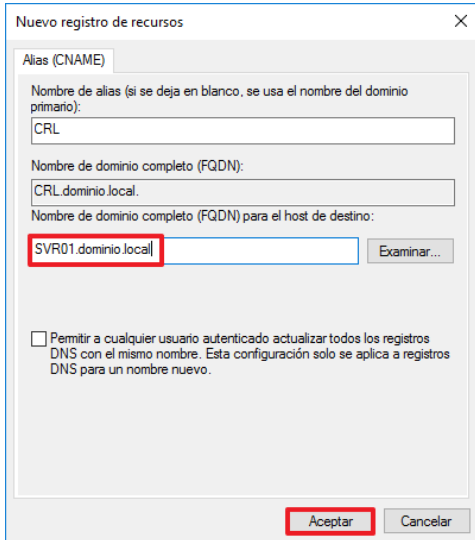
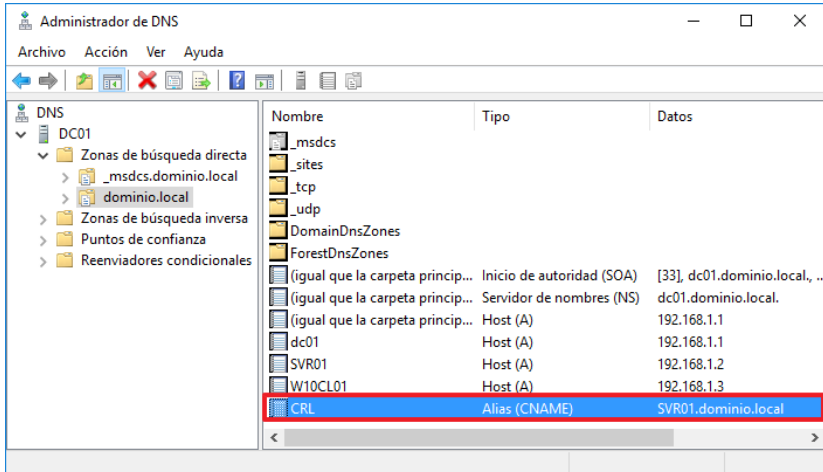
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 43.  | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio categoria media” y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |
| 44.  | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Paso | Descripción                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45.  | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                                                                                                                                                              |
| 46.  | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>                                             |
| 47.  | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>  |
| 48.  | <p>Cierre la ventana “Administración de directivas de grupo”.</p>                                                                                                                                                                                                                                             |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

| Paso | Descripción                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 49.  | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>  |
| 50.  | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 51.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                  |
| 52.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 53.  | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: “&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”.</p> <p>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>                                                         |
| 54.  | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 55.  | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación subordinada de empresa y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p> |
| 56.  | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>                                                                                                                                                                                                  |

## 2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría media.

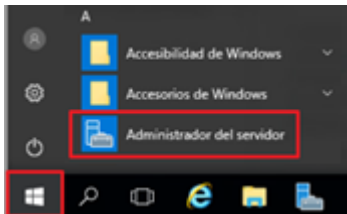
No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

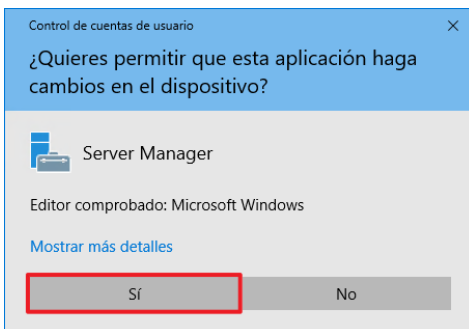
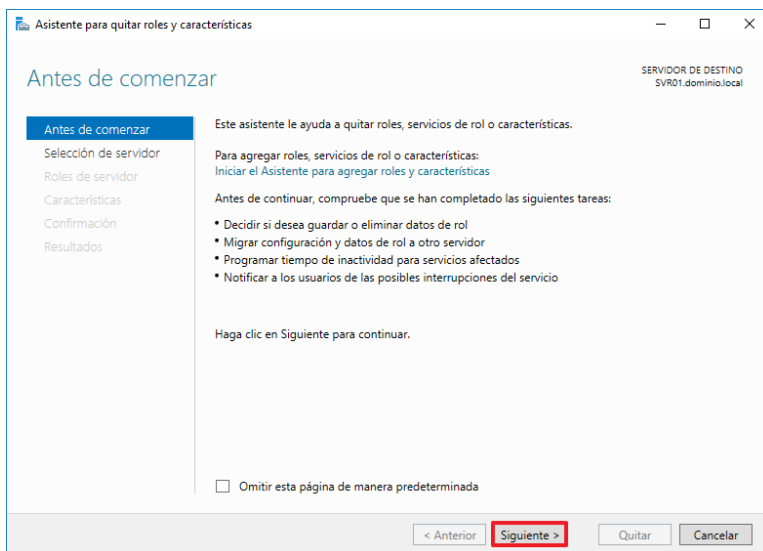
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

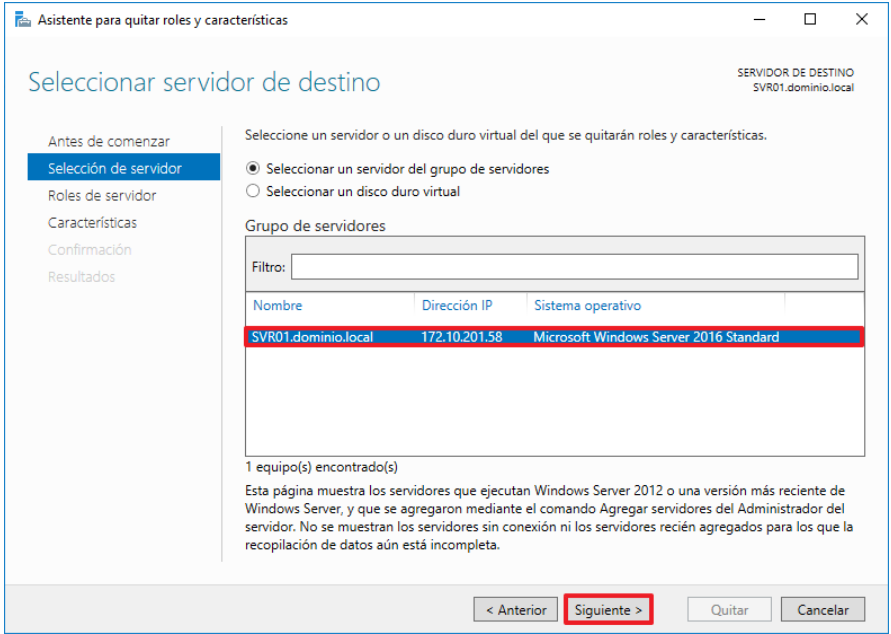
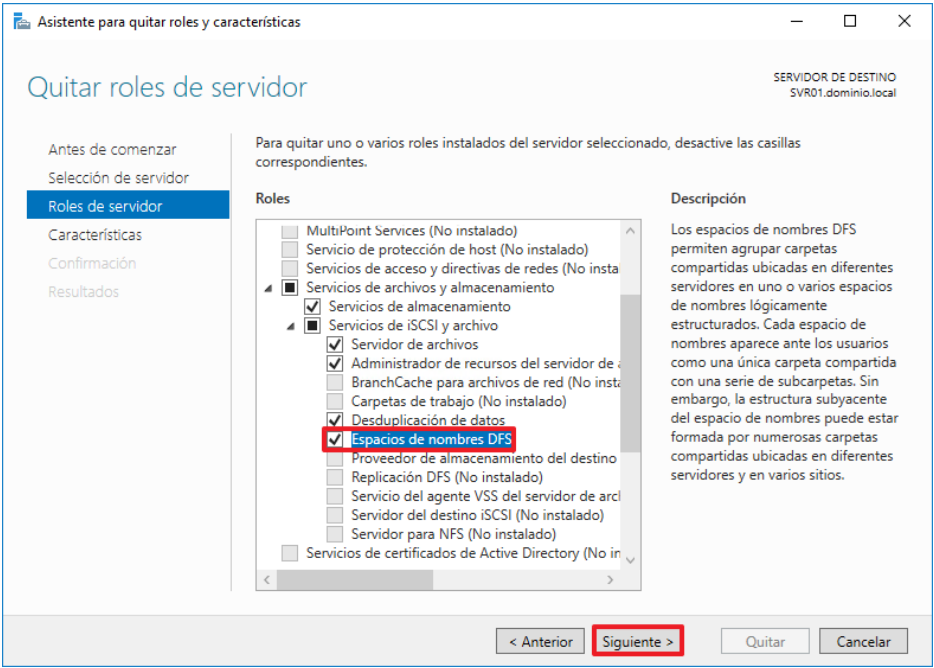
## 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

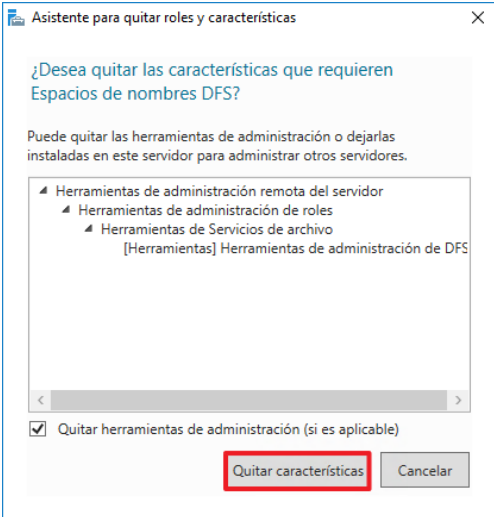
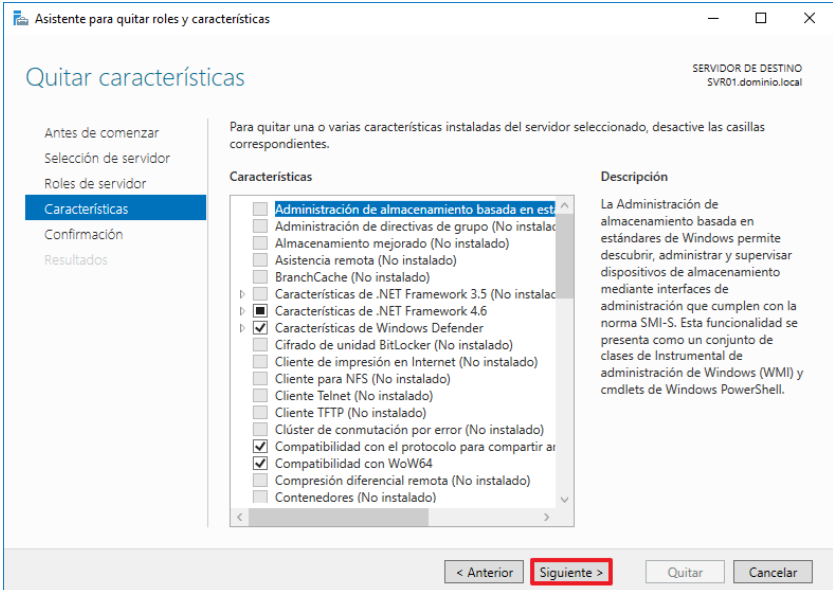
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

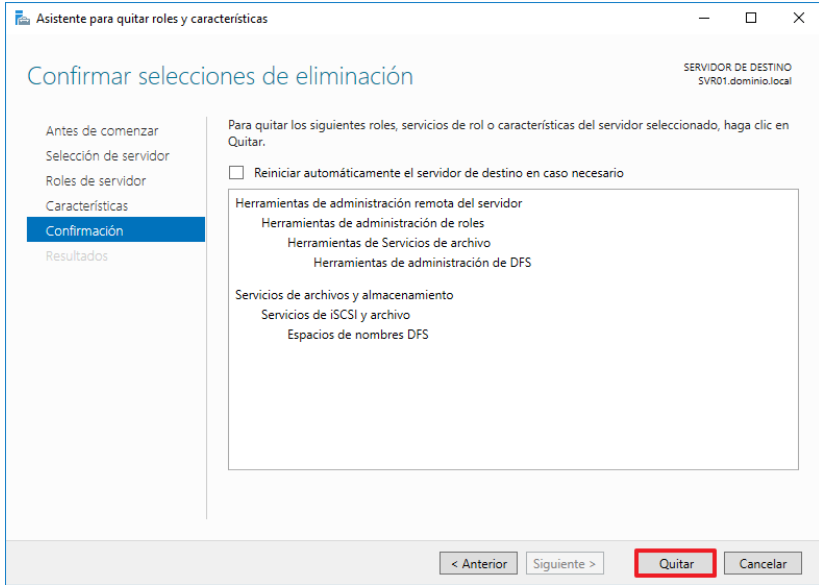
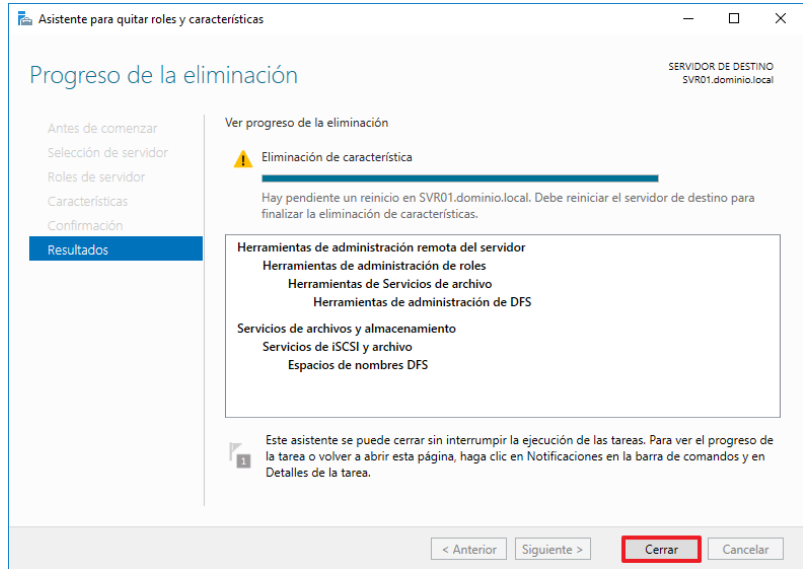
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de Certificación.

| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor Entidad de Certificación.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 58.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                               |

| Paso | Descripción                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 59.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>             |
| 60.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>               |
| 61.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 62.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p>                                                      |
| 63.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |

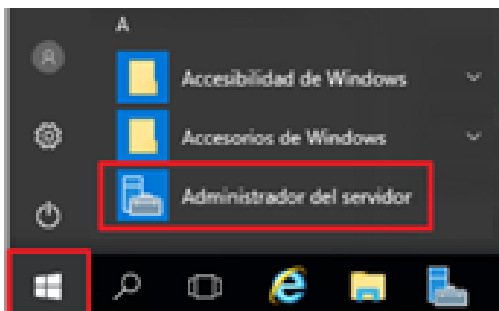
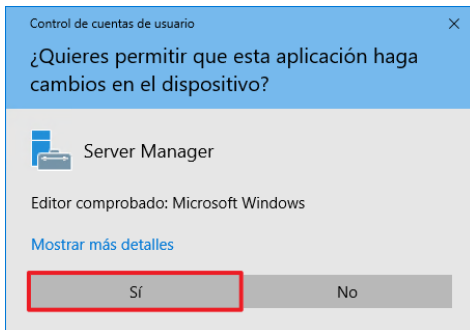
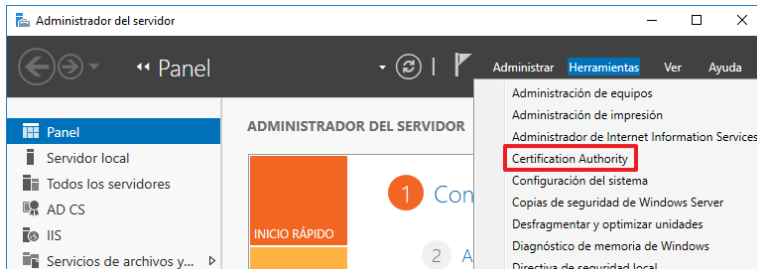
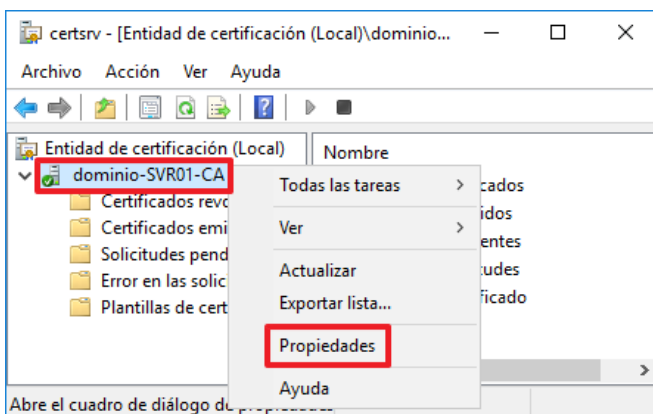
| Paso | Descripción                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64.  | <p>En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p> |
| 65.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>                                                                                                      |

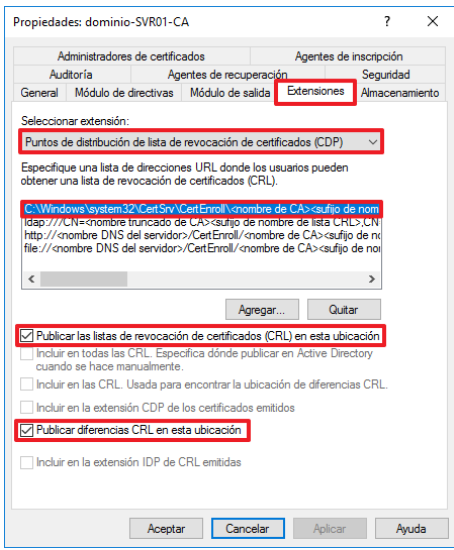
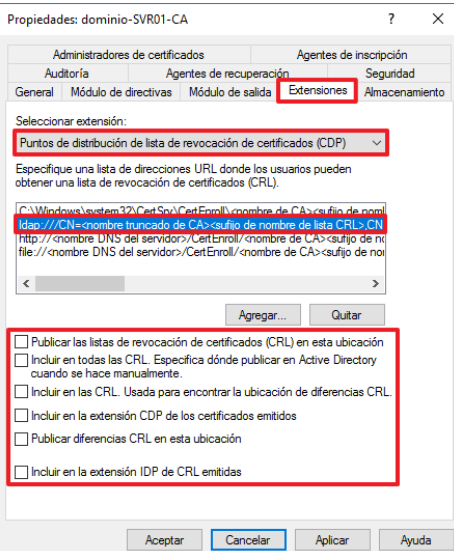
| Paso | Descripción                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 66.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                     |
| 67.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 68.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                    |

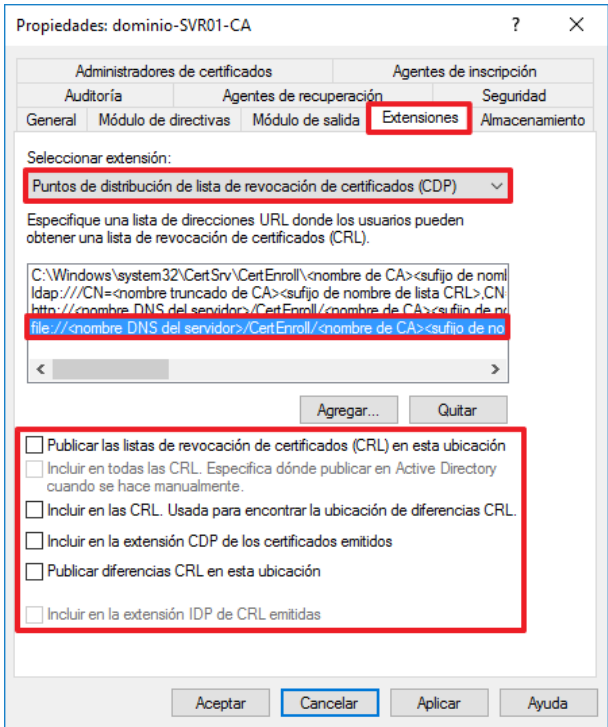
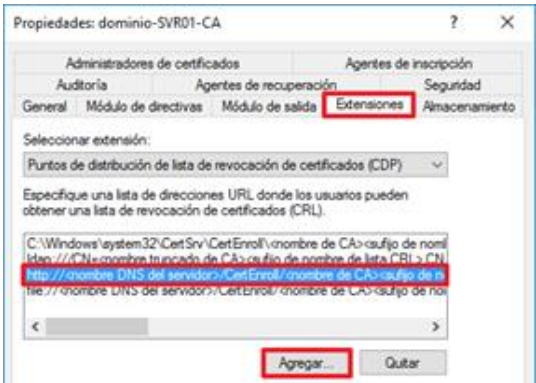
## 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA

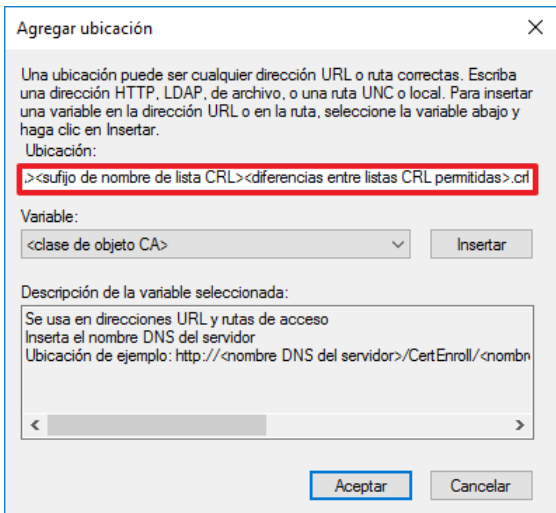
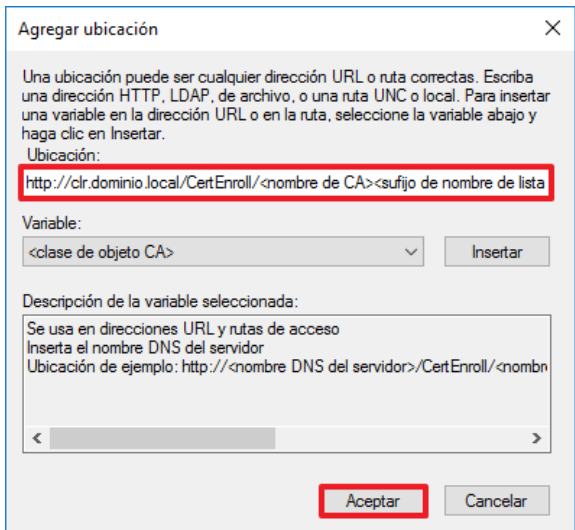
En este apartado, se establecerá la configuración que permite que un sitio web mantenga las CRLs de modo que sean accesibles por todos los clientes de la Entidad de Certificación.

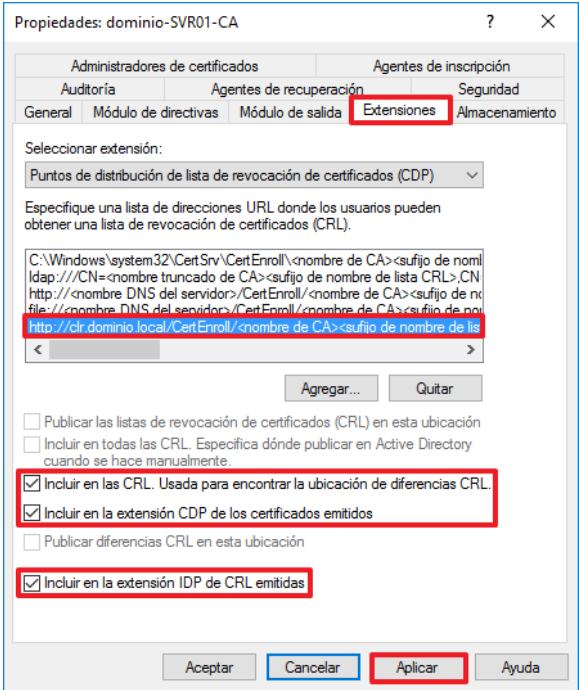
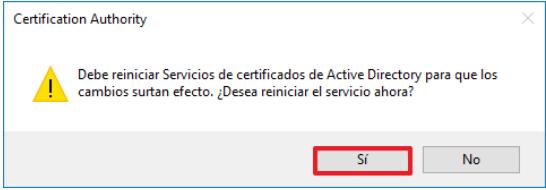
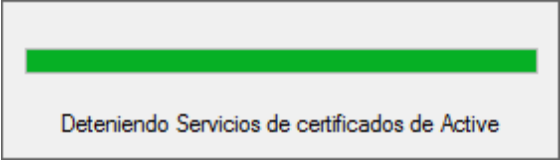
| Paso | Descripción                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 69.  | <p>Inicie sesión en el equipo que posea la Entidad de Certificación raíz de empresa.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p> |

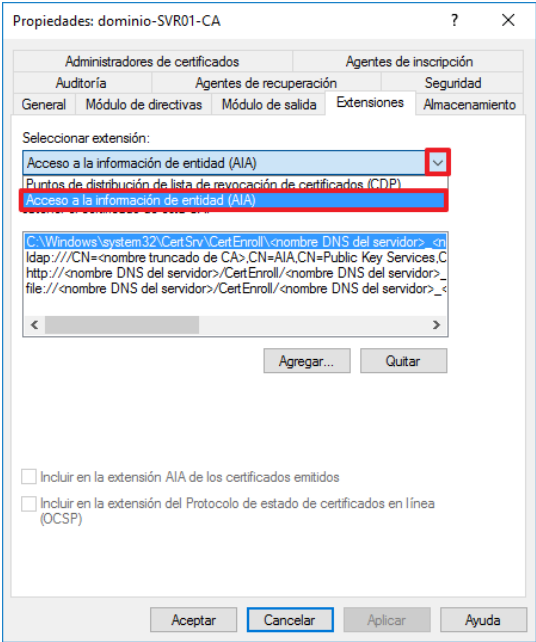
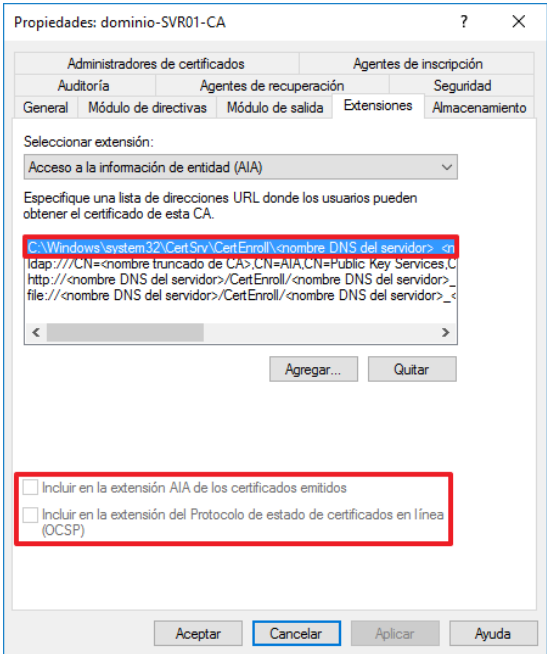
| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 70.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>                                                                                                                                         |
| 71.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                   |
| 72.  | <p>En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                                                                  |
| 73.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado de la Entidad de Certificación configurada recientemente y, con el botón derecho del ratón selecciónela, y pulse la opción “Propiedades”.</p>  |

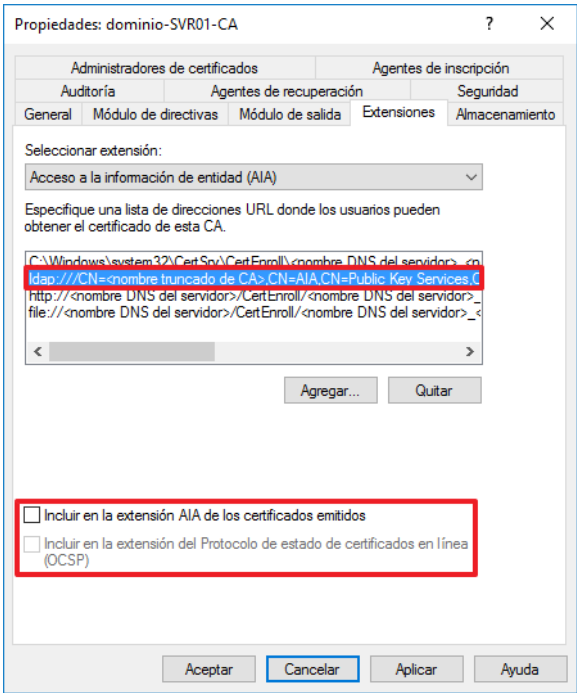
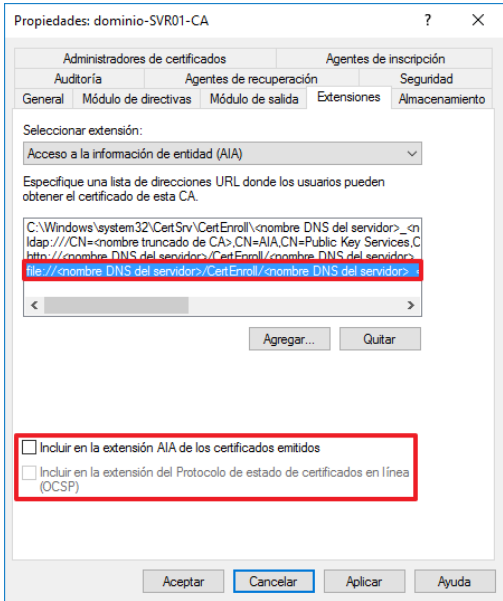
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 74.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\<nombre b="" ca&gt;&lt;="" crl="" crl&gt;&lt;diferencias="" de="" entre="" lista="" listas="" nombre="" permitidas&gt;.crl”<="" sufijo=""> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</nombre></b></p>  |
| 75.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, deshabilite la publicación de CRLs mediante ldap seleccionando <b>“ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;”</b> y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>                          |

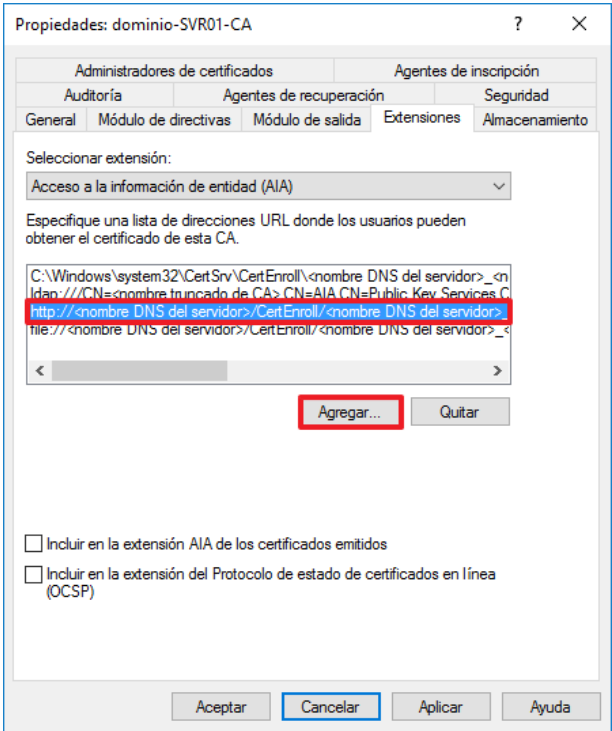
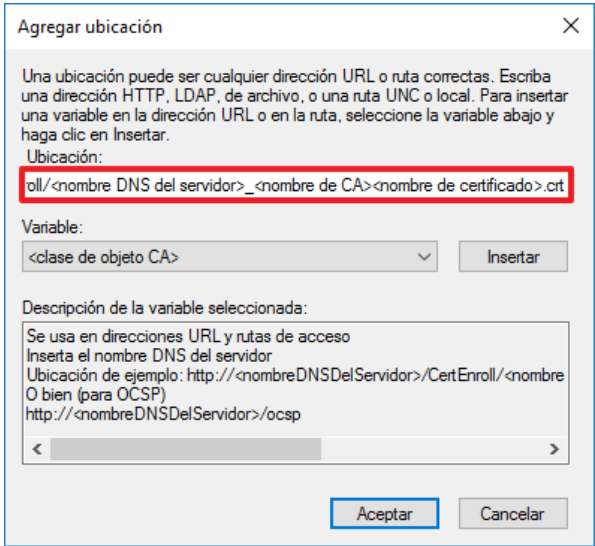
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 76.  | <p>De nuevo en “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> asegúrese que tiene todas las opciones desmarcadas tal y como aparece en la siguiente figura.</p>  |
| 77.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt;sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y copie el elemento mediante la combinación de teclas “Control + C”.</p>                                                                                                |
| 78.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                                                                                                                                                                                              |

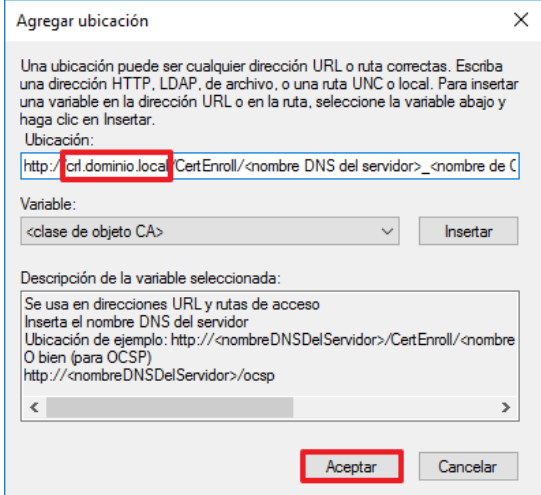
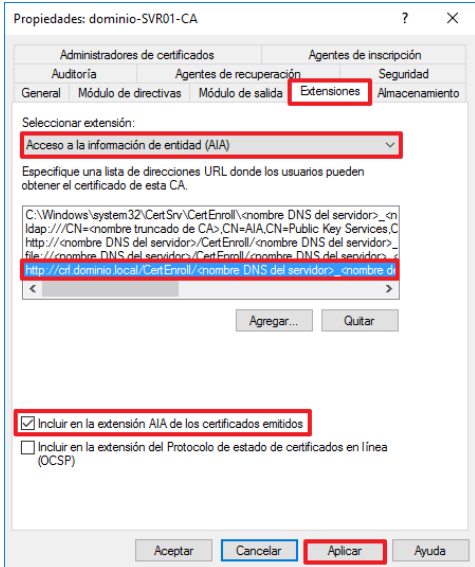
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 79.  | <p>En “Agregar ubicación” coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                                                                              |
| 80.  | <p>En dicha ventana, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

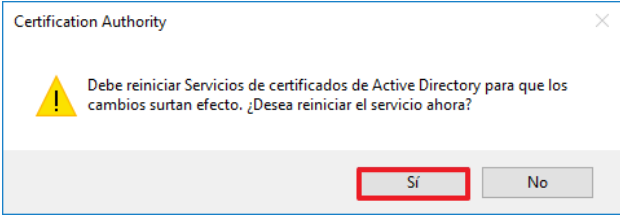
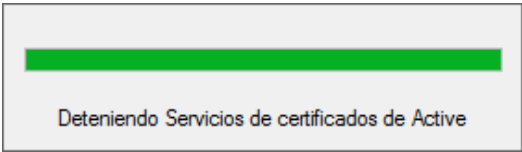
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 81.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul> <p>Pulse “Aplicar” para guardar los cambios</p>  |
| 82.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 83.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 84.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>                                                                       |
| 85.  | <p>Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt” todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 86.  | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> están desmarcadas todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>  |
| 87.  | <p>Seleccione <b>"file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt"</b> y asegúrese que todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>                                                      |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88.  | Seleccione ahora <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b> .                                          |
| 89.  | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                              |
| 90.  | <p>En <b>“Agregar ubicación”</b> coloque el cursor sobre el campo vacío bajo <b>“Ubicación:”</b> y pulse la combinación de teclas <b>“Control + V”</b> para pegar el contenido recién copiado.</p>  |

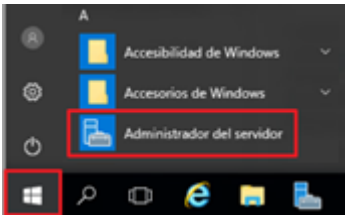
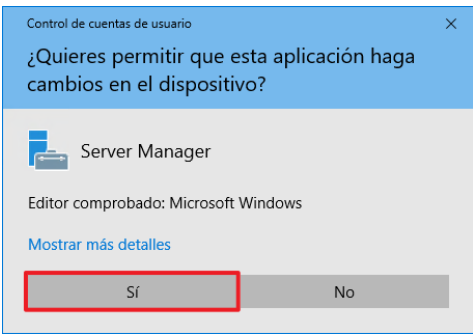
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 91.  | <p>En “Agregar ubicación” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente (B.2. de la presente guía) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |
| 92.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada “http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>                         |

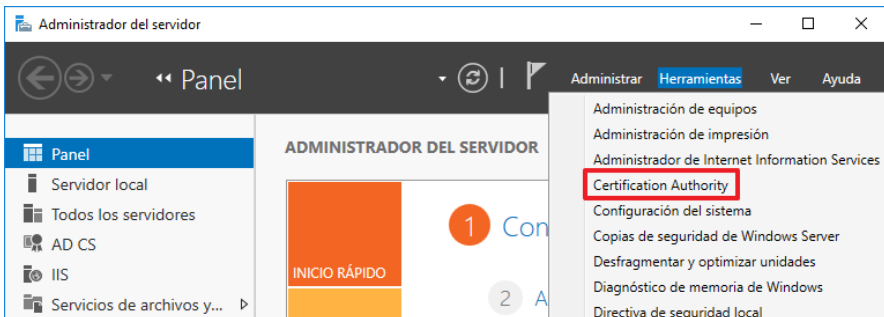
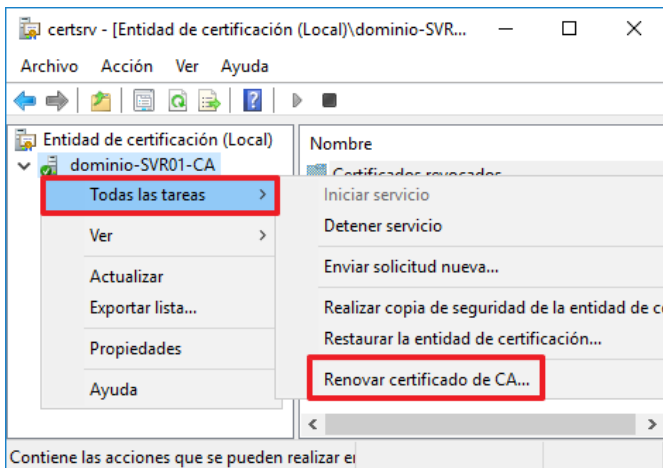
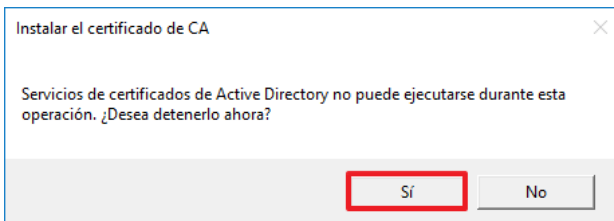
| Paso | Descripción                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>  |
| 94.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                |
| 95.  | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                     |

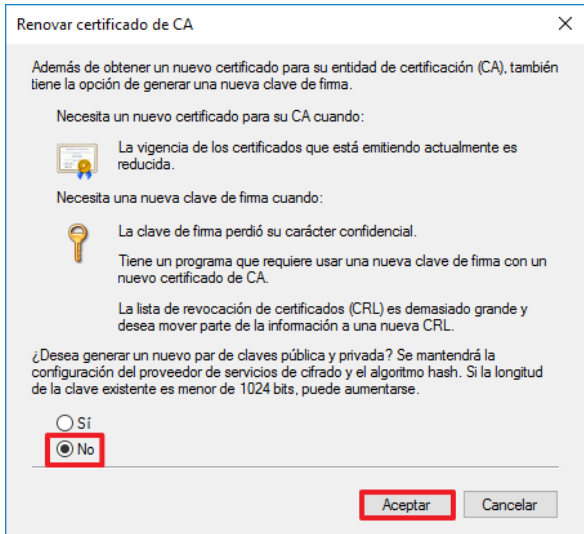
### 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA

Será necesario volver a generar el certificado de la Entidad de Certificación tras hacer modificaciones en las propiedades.

Los pasos que se definen a continuación comprenden la renovación de una Entidad de Certificación raíz de empresa.

| Paso | Descripción                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Inicie sesión en el equipo Entidad de Certificación raíz.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p>                                 |
| 97.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>                       |
| 98.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>  |

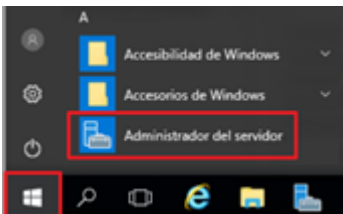
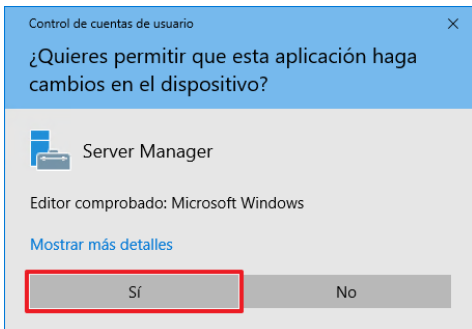
| Paso | Descripción                                                                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 99.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                                                         |
| 100. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificados y con el botón derecho del ratón selecciónela y pulse sobre “Todas las tareas → Renovar certificado de CA...”.</p>  |
| 101. | <p>Pulse “Sí” en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                         |

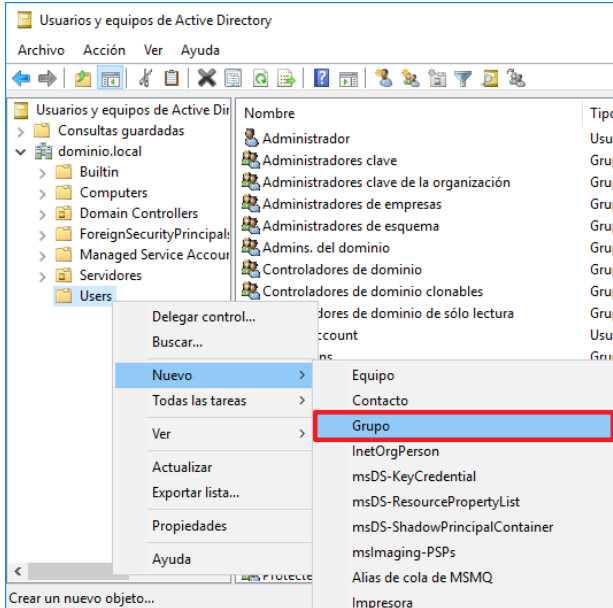
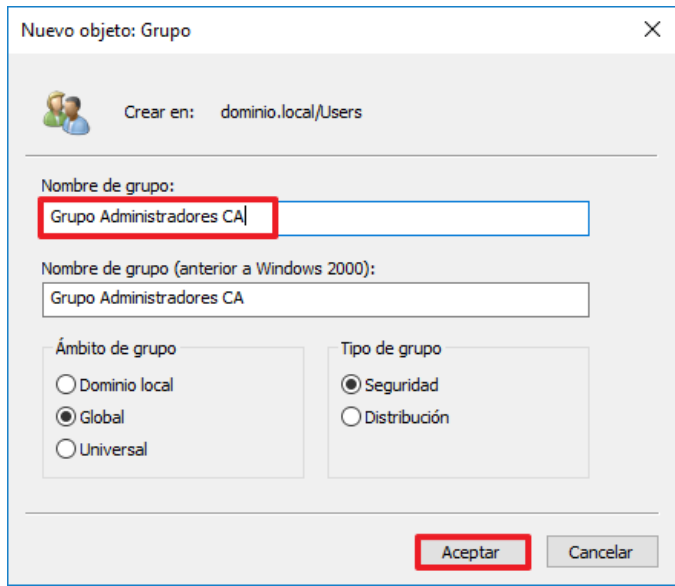
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 102. | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Si la entidad raíz es de empresa, no será necesario establecer ningún paso adicional, en caso de ser una Entidad de Certificación independiente del dominio, además de haber tenido que encenderla para realizar el proceso, será necesario extraer el fichero “.CRT” que se ha generado en la ruta “%SYSTEMROOT%\System32\CertSrv\CertEnroll” y pegarlas en la misma ruta, pero en la Entidad de Certificación subordinada de empresa.</p> |

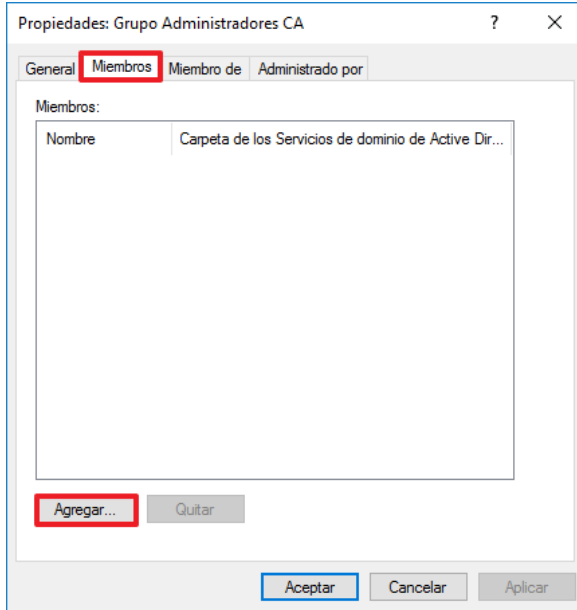
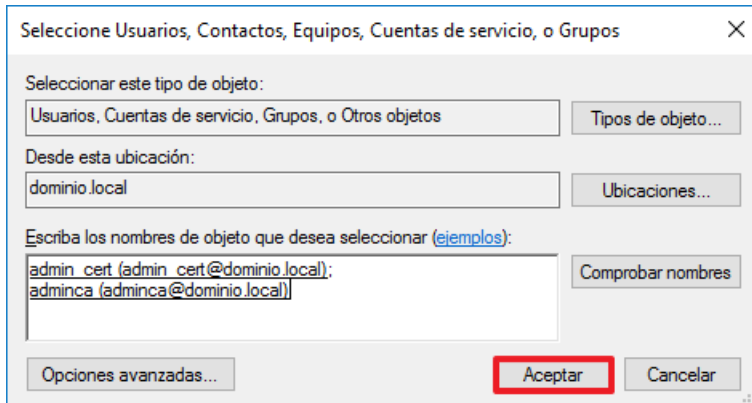
## 2.4. SEGREGACIÓN DE ROLES

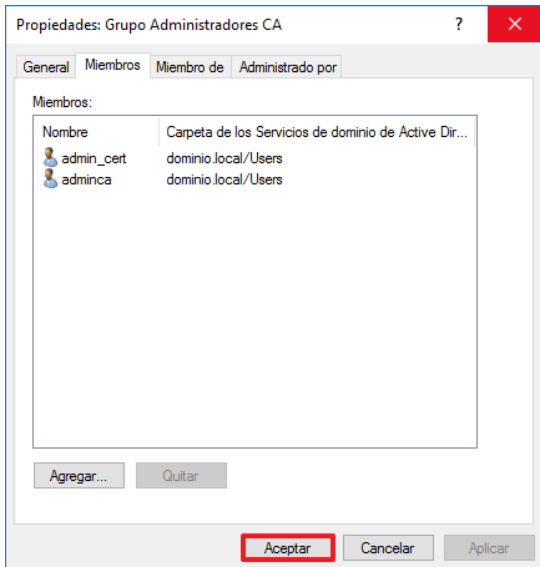
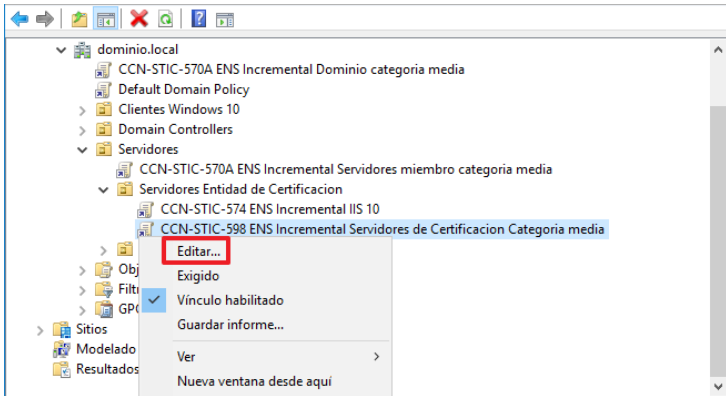
Con la aplicación del ENS para la categoría media sobre una Entidad de Certificación será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar una Entidad de Certificación.

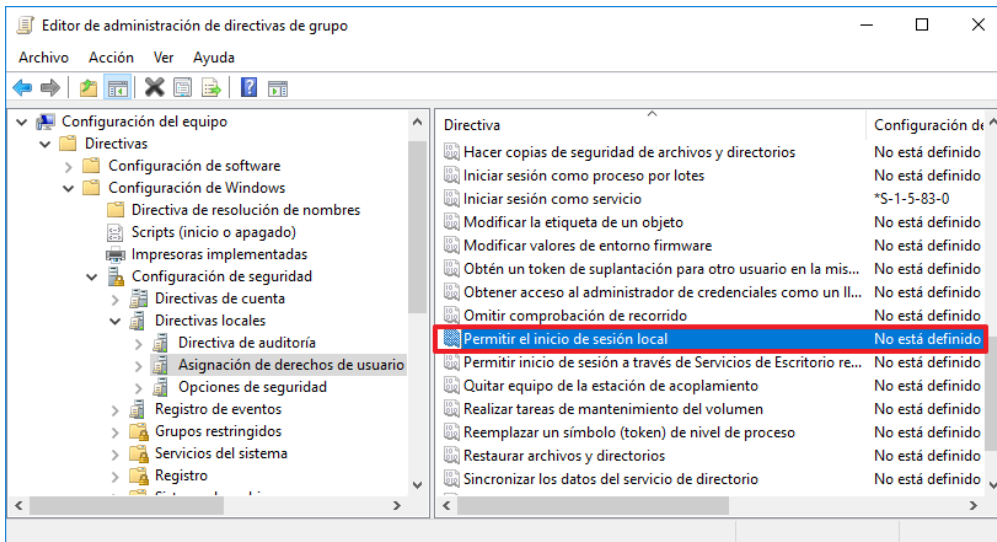
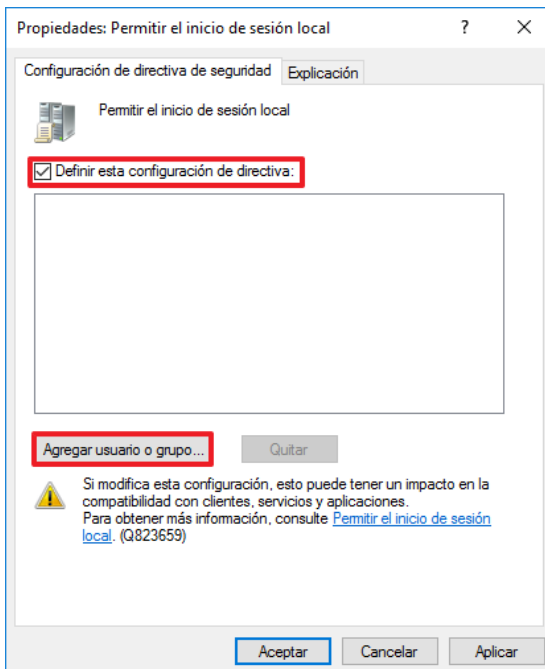
| Paso | Descripción                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 103. | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |

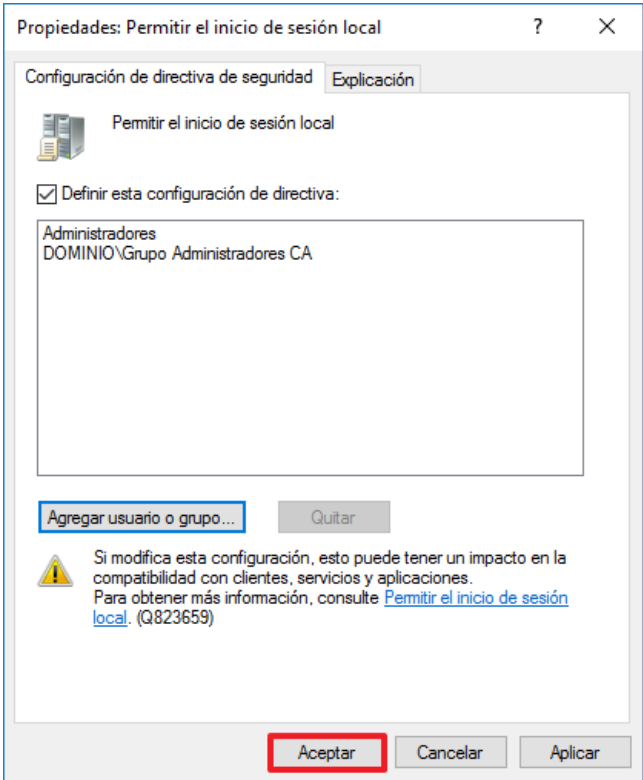
| Paso | Descripción                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 104. | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>  |
| 105. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>    |
| 106. | <p>Acceda al apartado “Herramientas” y seleccione “Usuarios y Equipos de Active Directory”.</p>                   |

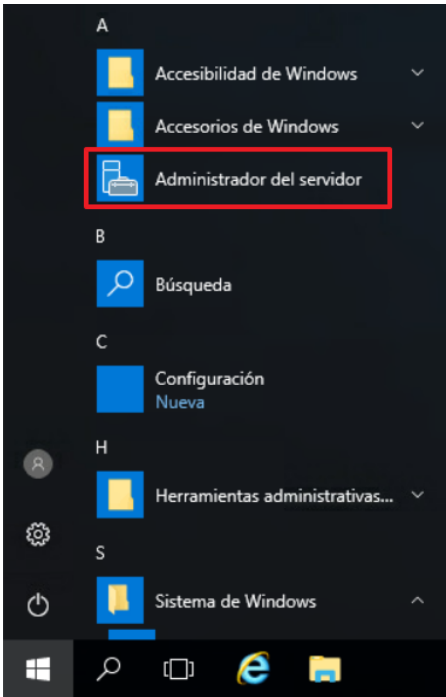
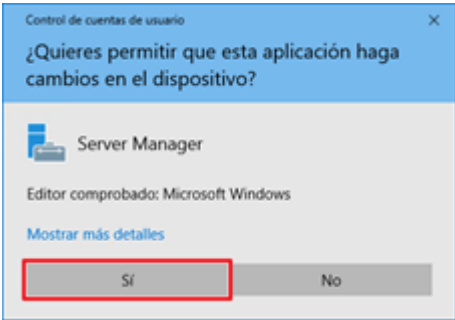
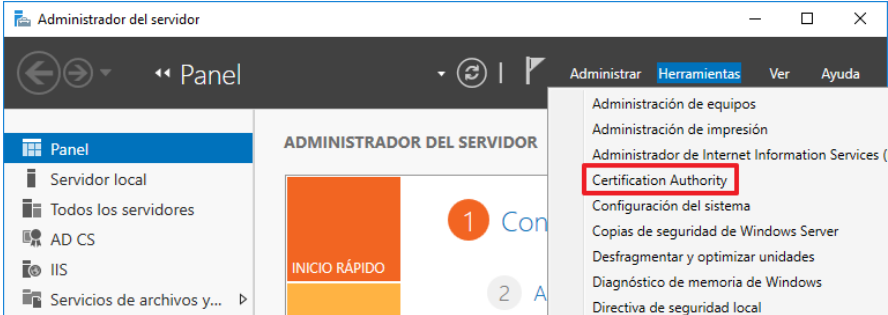
| Paso | Descripción                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 107. | <p>Despliegue el nodo “&lt;su dominio&gt; → Users”. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual “Nuevo → Grupo”.</p>                |
| 108. | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |

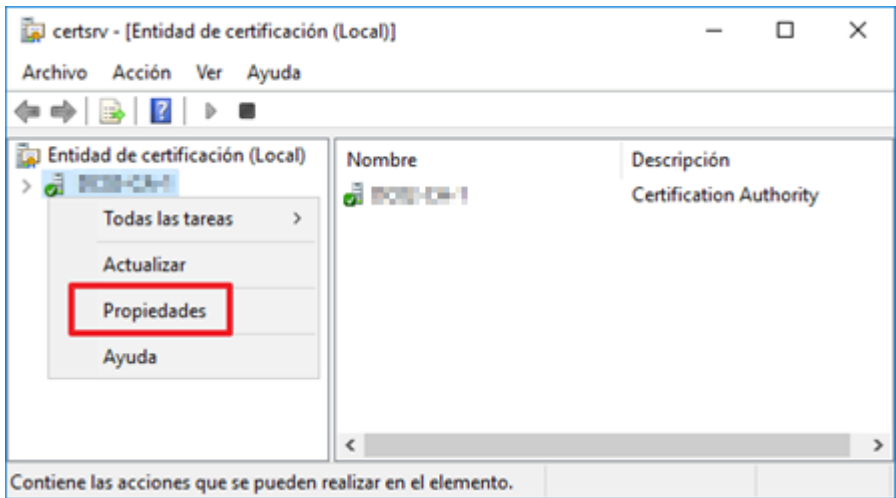
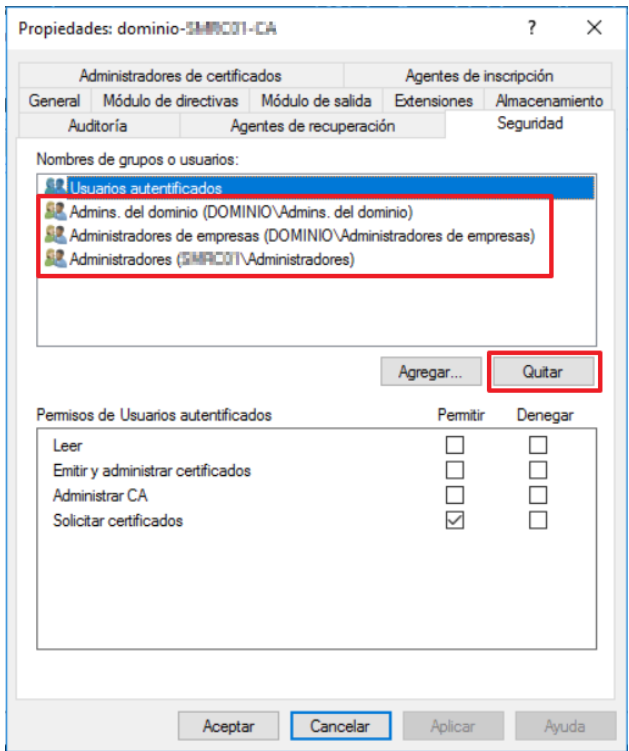
| Paso | Descripción                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 109. | <p>Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>                                              |
| 110. | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la generación de esta guía.”</p> |

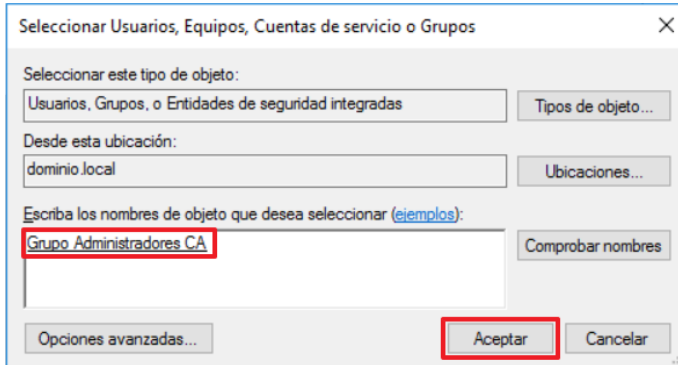
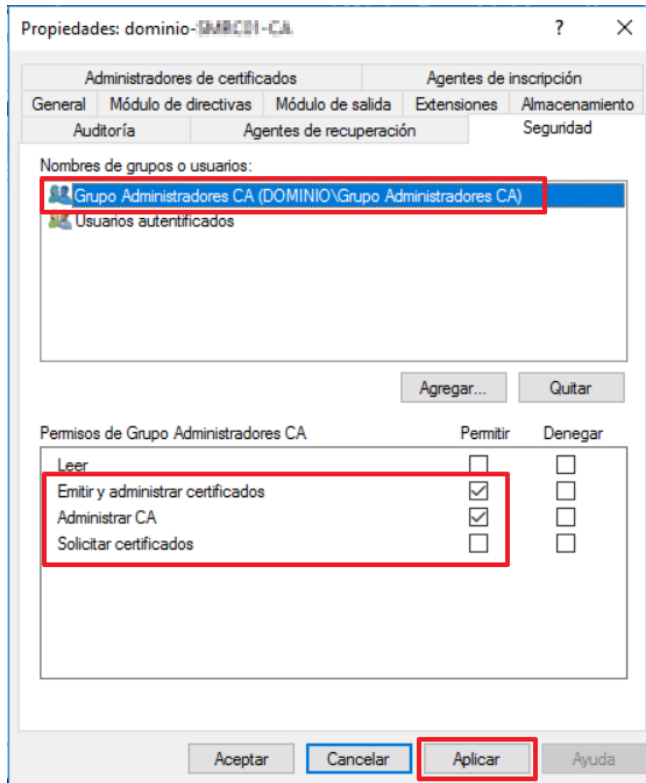
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 111. | <p>Pulse “Aceptar” cuando haya finalizado.</p>                                                                                                                                                                                                                                                                                                      |
| 112. | <p>A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione <b>“Herramientas → Administración de directivas de grupo”</b>.</p>                                                            |
| 113. | <p>Expanda el árbol <b>“Bosque:&lt;nombre de su bosque&gt; → Dominios → &lt;nombre de su dominio&gt;” → “Servidores” → “Entidad certificadora”</b> y pulse con el botón derecho el objeto GPO denominado <b>“CCN-STIC-598 Incremental Servidor Entidad de Certificación”</b>, y seleccione la opción del menú contextual <b>“Editar...”</b>.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 114. | <p>Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta.<br/> <b>“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</b>.</p> <p>Haga doble clic en el panel derecho sobre la directiva <b>“Permitir el inicio de sesión local”</b>.</p>  |
| 115. | <p>Marque la casilla <b>“Definir esta configuración de directiva:”</b> y pulse sobre <b>“Agregar usuario o grupo...”</b>.</p>                                                                                                                                                                                                                                     |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 116. | <p>Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor de Entidad de Certificación. Pulse “Aceptar” cuando haya finalizado.</p>  <p><b>Nota:</b> En este ejemplo se hace uso del grupo denominado “Grupo Administración CA”. Deberá adaptar esta configuración a las necesidades de su organización.</p> |
| 117. | <p>A continuación, inicie sesión en el servidor miembro del dominio donde se va a aplicar seguridad para el Servidor de Entidad de Certificación.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador del dominio.</p>                                                                                                                        |

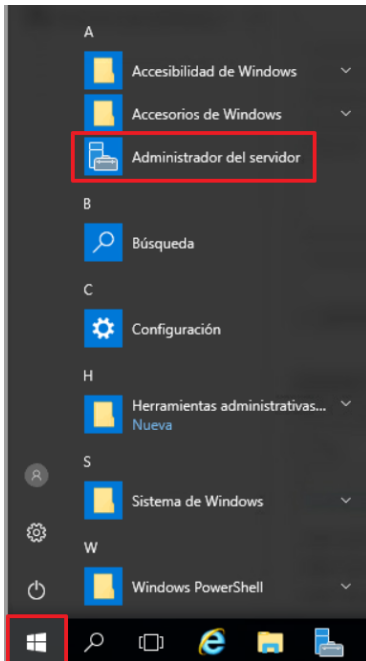
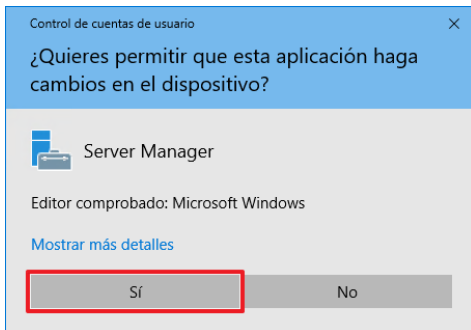
| Paso | Descripción                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 118. | <p>A continuación, ejecute la consola administrativa “Certification Authority”. Para ello, clic en <b>“Inicio de Windows → Administrador del servidor”</b>.</p>                |
| 119. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>  |
| 120. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                           |

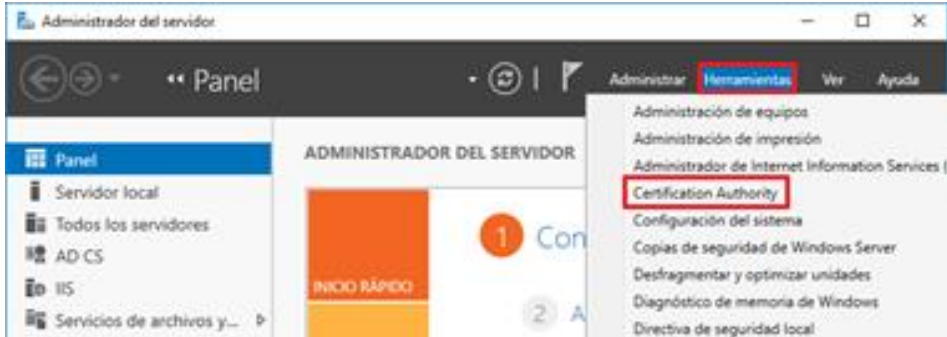
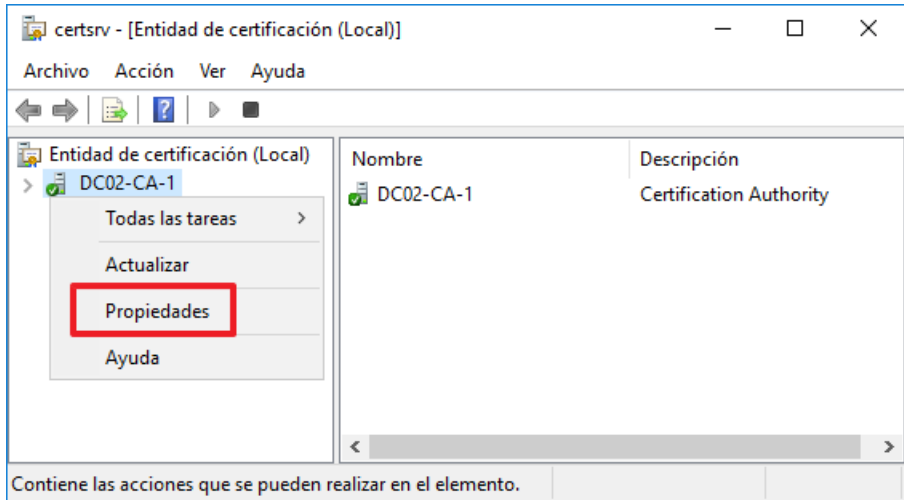
| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 121. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>                                                                                             |
| 122. | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque uno a uno los grupos Administradores (del dominio, de empresa y locales) y, pulse “Quitar” para eliminar los grupos.</p>  |

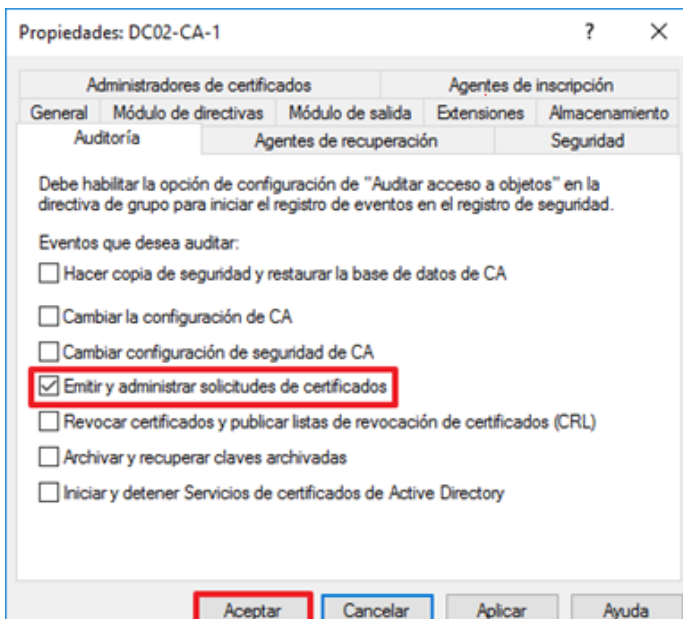
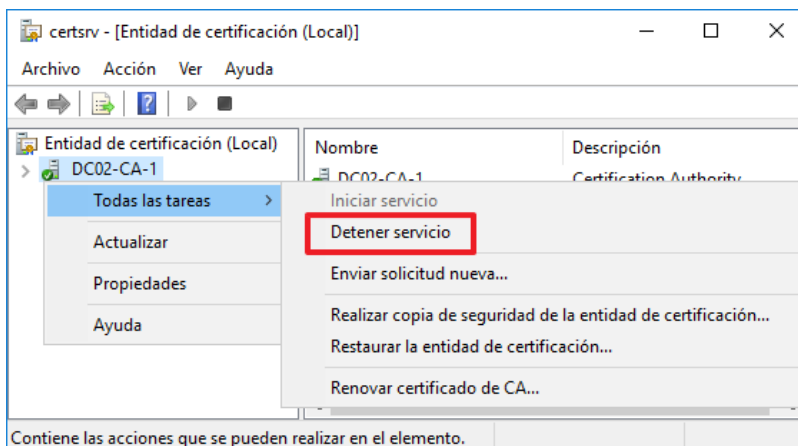
| Paso | Descripción                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 123. | <p>A continuación, añada el grupo “Grupo Administradores CA” y pulse “Aceptar”.</p>                                                                                                                                  |
| 124. | <p>Seleccione el grupo recién añadido, otórguele los permisos “Emitir y administrar certificados” y “Administrar CA” y desmarque la opción “Solicitar certificados”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 125. | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                                                                 |

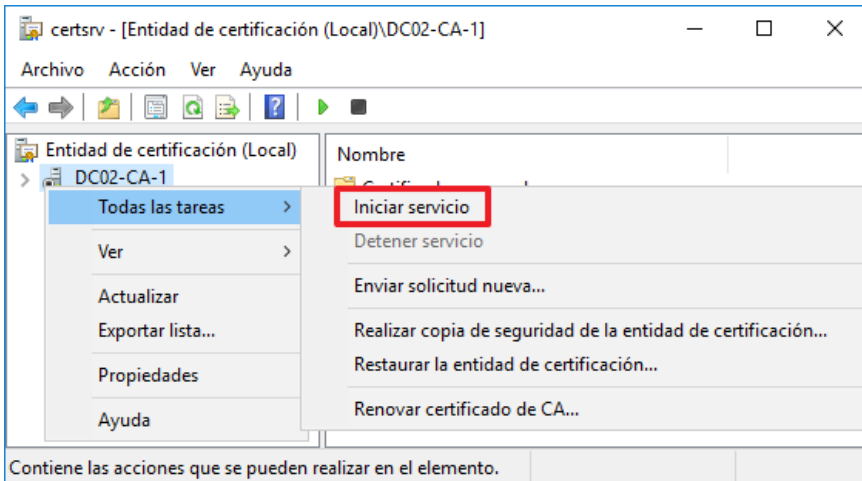
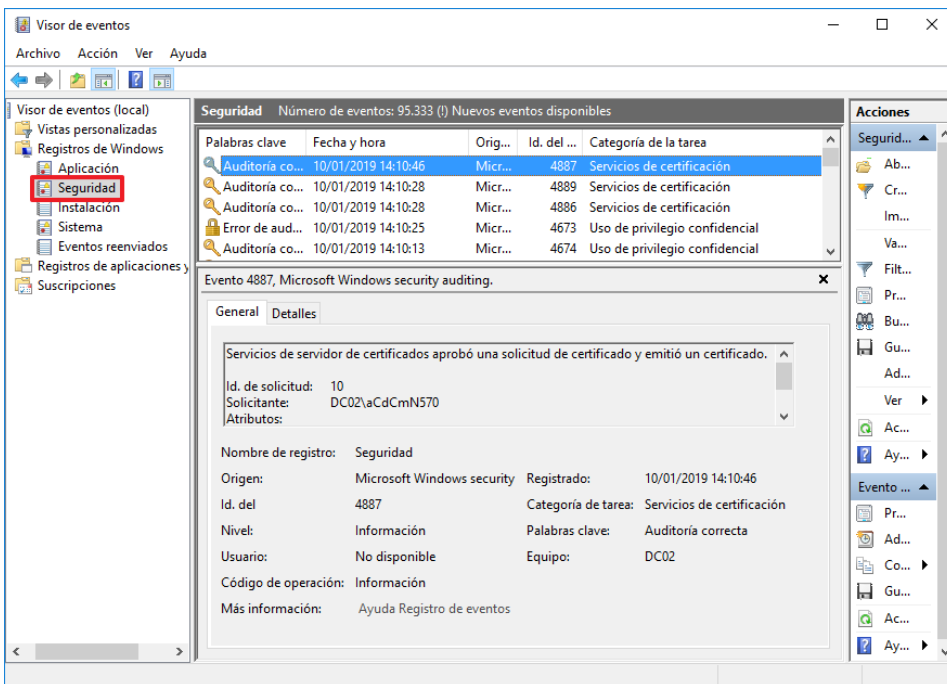
## 2.5. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

Existe la posibilidad de auditar el control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoría de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación.

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 126. | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 127. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  <p>The screenshot shows the Windows Start menu search results. The search bar at the top contains the text 'Administrador del servidor'. Below the search bar, a list of results is displayed. The first result, 'Administrador del servidor', is highlighted with a red rectangular box. The search results are organized into sections: 'A' (Accesibilidad de Windows, Accesorios de Windows), 'B' (Búsqueda), 'C' (Configuración), 'H' (Herramientas administrativas... Nueva), 'S' (Sistema de Windows), and 'W' (Windows PowerShell). The Windows logo is also visible in the bottom left corner of the Start menu.</p> |
| 128. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>  <p>The screenshot shows a Windows User Account Control (UAC) dialog box titled 'Control de cuentas de usuario'. The main text asks: '¿Quieres permitir que esta aplicación haga cambios en el dispositivo?'. Below the text, there is a section for the application, showing the 'Server Manager' icon and the text 'Editor comprobado: Microsoft Windows'. There is a link 'Mostrar más detalles'. At the bottom, there are two buttons: 'Sí' and 'No'. The 'Sí' button is highlighted with a red rectangular box.</p>                                                                                                                                           |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 129. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                   |
| 130. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 131. | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: “<b>Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales</b>”.</p> |
| 132. | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú “<b>Todas las tareas → Detener servicio</b>”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 133. | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú “<b>Acción → Todas las tareas → Iniciar servicio</b>” para iniciarlo de nuevo.</p>                                                                                                                                                                                                                                                                                                                         |
| 134. | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: “<b>Inicio → Herramientas administrativas → Visor de eventos</b>”. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: “<b>Visor de eventos (local) → Registro de Windows → Seguridad</b>”.</p> |

## ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad para entidad de certificación sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.3.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS”

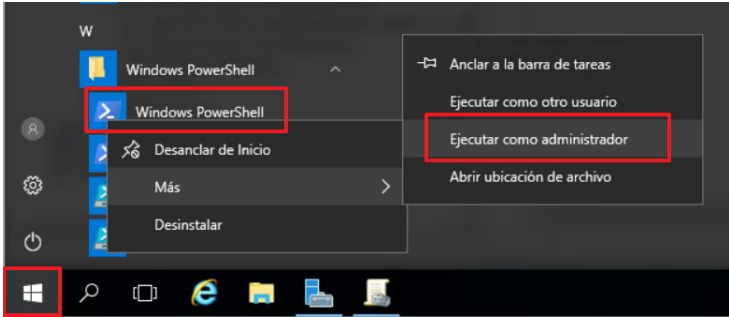
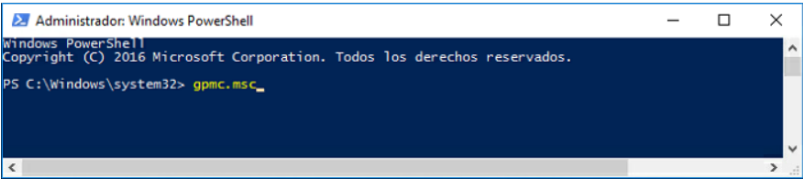
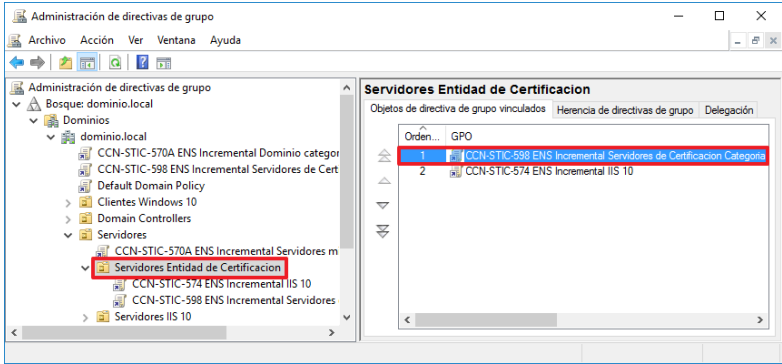
### 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

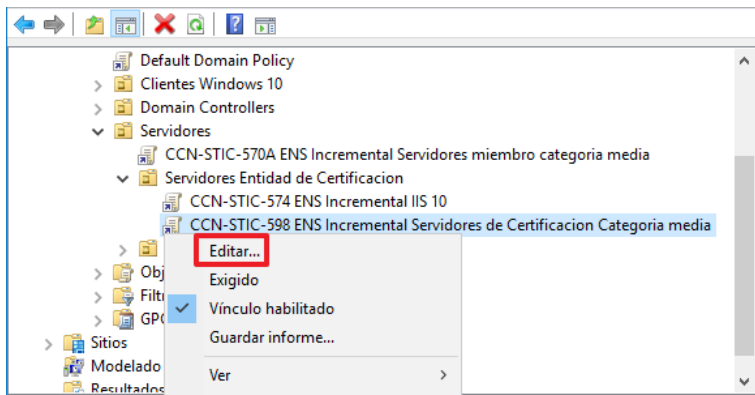
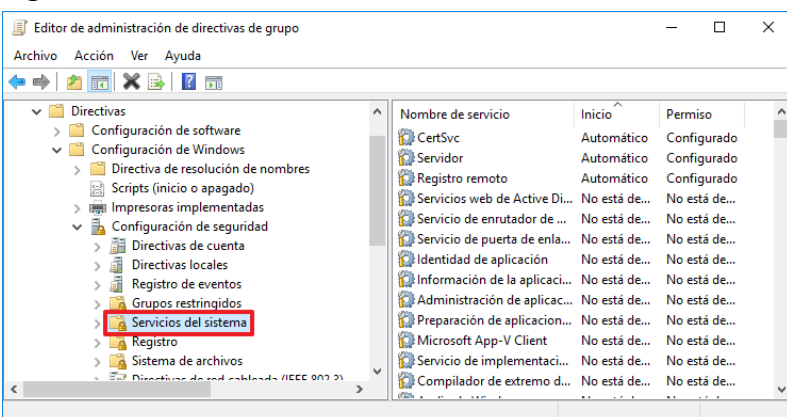
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

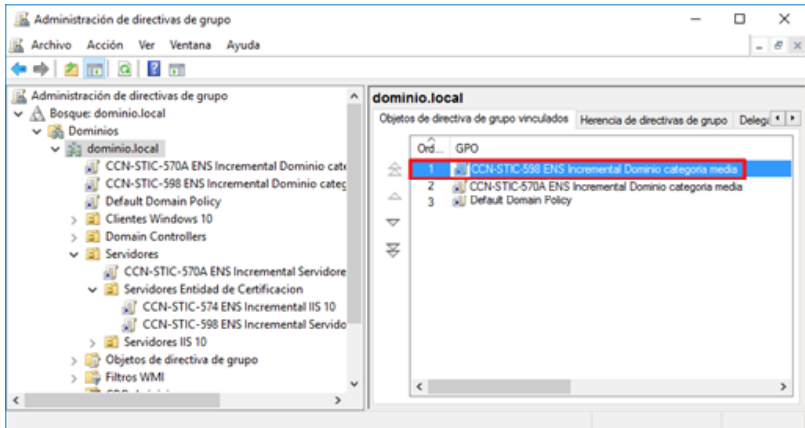
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

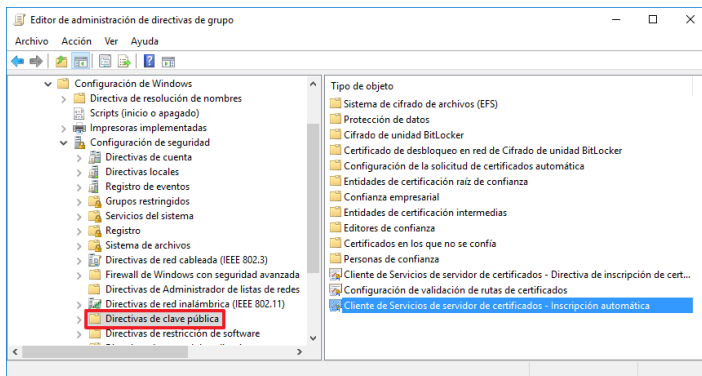
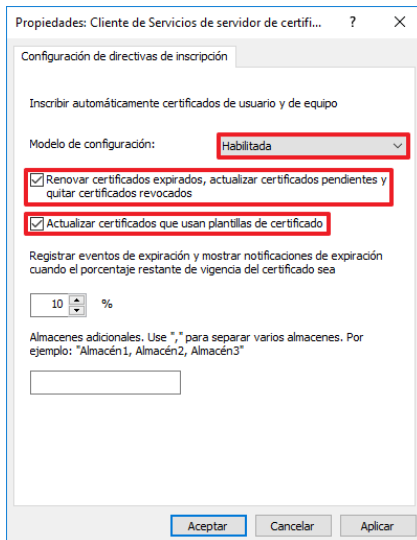
**Nota:** La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

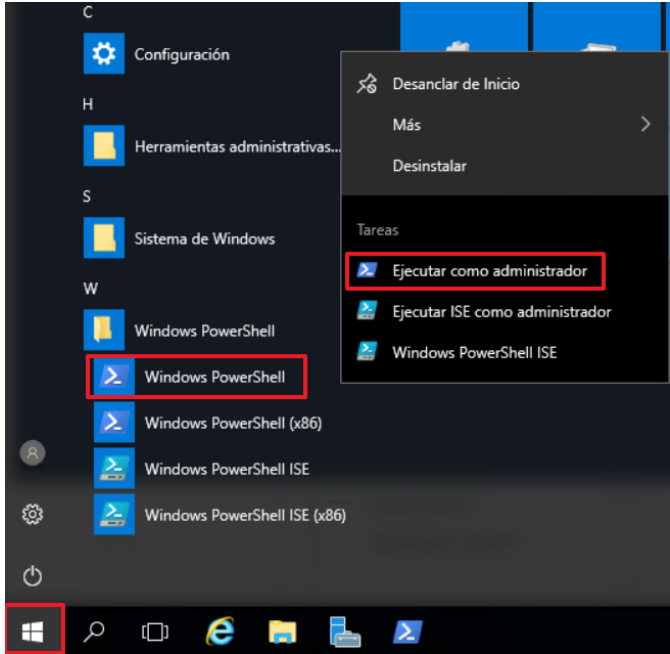
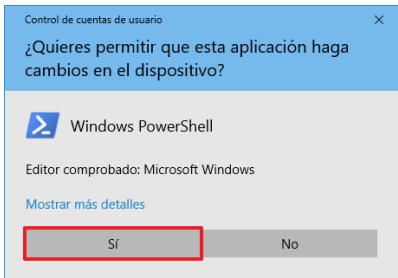
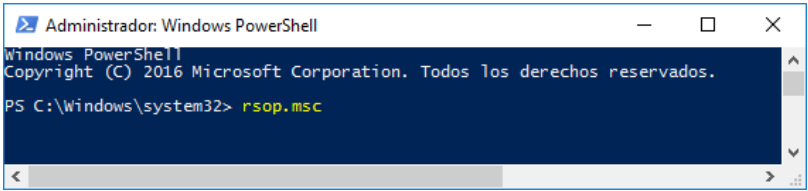
| Comprobación                                   | OK/NOK | Cómo hacerlo                                                                                                              |
|------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------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

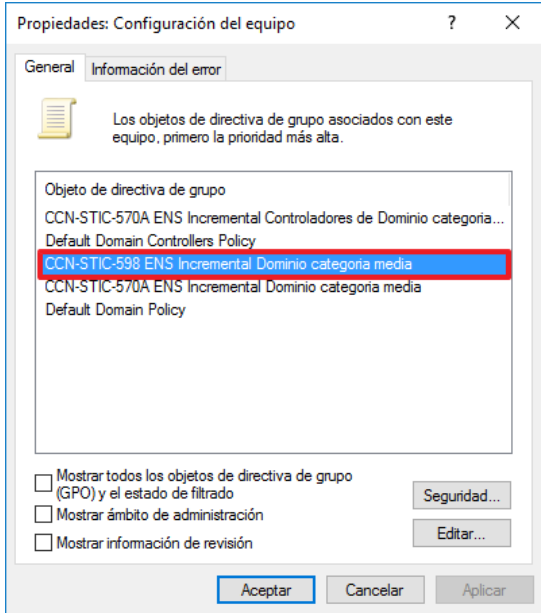
| Comprobación                                                                                                          | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Abra el administrador de directivas de grupo                                                                       |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic en “Inicio de Windows” y, con el botón derecho sobre el icono de PowerShell de la lista de programas, y, en el menú contextual que aparecerá, marque la opción "Ejecutar como administrador":</p>  <p>El control de cuentas de usuario le solicitará confirmación de ejecución, para ello, haga clic en “Sí”.</p> <p>Teclee “gpmc.msc” en la consola de comandos que se ha abierto:</p>  |
| 3. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”. |        | <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores Entidad de Certificación”. Verifique que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” está creada y vinculada en el primer lugar de orden de vínculo.</p>                                                                                                                                                                                                                                                                  |

| Comprobación                                                                                                                       | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |             |        |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| 4. Verifique los servicios del sistema de la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”. |                         | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”.</p>  <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:<br/><b>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</b></p>  <p><b>Nota:</b> Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</p> |             |        |
| Servicio (Nombre largo)                                                                                                            | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                      | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Configurado |        |
| Servidor                                                                                                                           | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Configurado |        |
| Registro Remoto                                                                                                                    | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Configurado |        |

| Comprobación                                                                                      | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Dominio categoria media". |        | <p>Ejecute el "Administrador de directivas de grupo" a través de la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b></p> <p>Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política "CCN-STIC-598 ENS Incremental Dominio categoria media" está creada y vinculada en el primer lugar de orden de vínculo.</p>  |

| Comprobación                                                                                                                                   | OK/NOK               | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------|--------|-------------------------|------------|--|----------------------------------------------------------------------------------------------------|----------------------|--|------------------------------------------------------------|----------------------|--|
| 6. Verifique la configuración de inscripción automática de certificados en la política "CCN-STIC-598 ENS Incremental Dominio categoria media". |                      | <p>Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo". Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:</p> <p><b>Directiva CCN-STIC-598 ENS Incremental Dominio categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  <p>Haga doble clic sobre el objeto "Cliente de Servicios de servidor de certificados – Inscripción automática" y compruebe los valores correspondientes a la inscripción automática.</p>  <table border="1"> <thead> <tr> <th>Configuración</th><th>Estado</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Modelo de configuración</td><td>Habilitada</td><td></td></tr> <tr> <td>Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados</td><td>Habilitada (marcada)</td><td></td></tr> <tr> <td>Actualizar certificados que usan plantillas de certificado</td><td>Habilitada (marcada)</td><td></td></tr> </tbody> </table> | Configuración | Estado | OK/NOK | Modelo de configuración | Habilitada |  | Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados | Habilitada (marcada) |  | Actualizar certificados que usan plantillas de certificado | Habilitada (marcada) |  |
| Configuración                                                                                                                                  | Estado               | OK/NOK                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Modelo de configuración                                                                                                                        | Habilitada           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados                                             | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Actualizar certificados que usan plantillas de certificado                                                                                     | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |

| Comprobación                                                                                                                            | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. Verifique la correcta aplicación de la política "CCN-STIC-598 Incremental Dominio categoría media" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                 |
|--------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>A continuación, haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría media” aparece en la lista como muestra la imagen.</p>  |

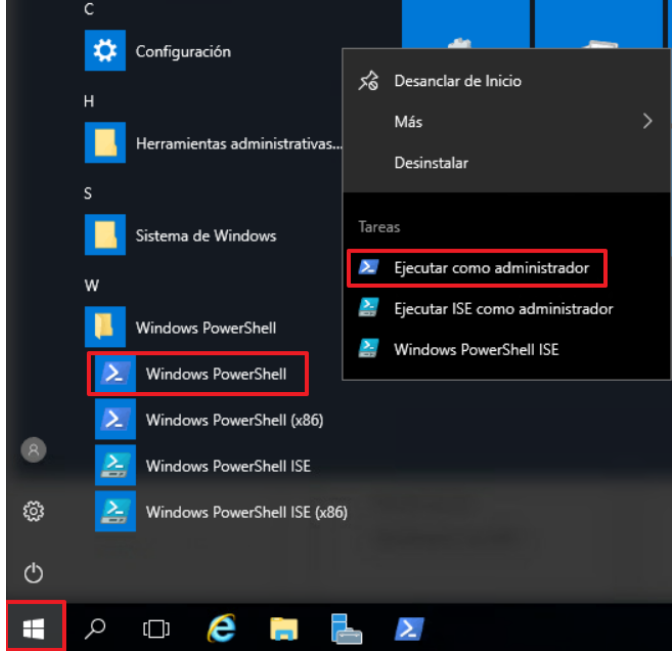
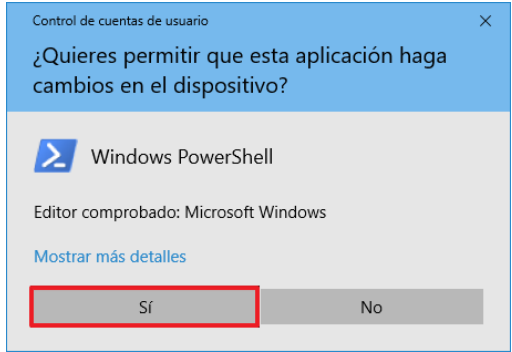
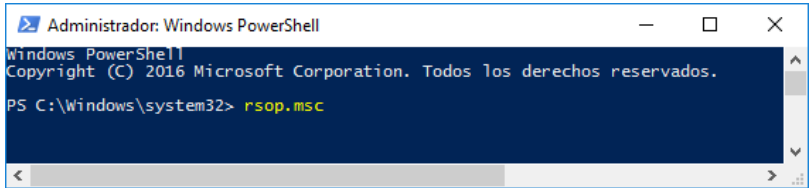
## 2. COMPROBACIONES EN SERVIDOR MIEMBRO

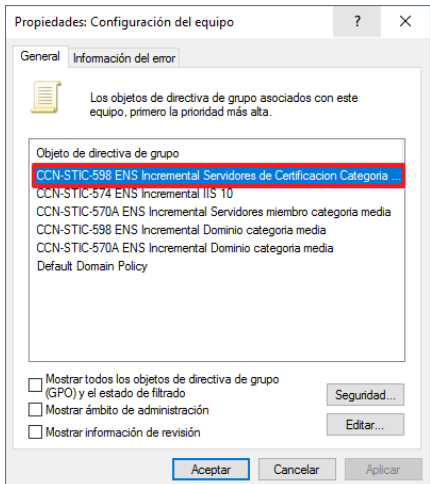
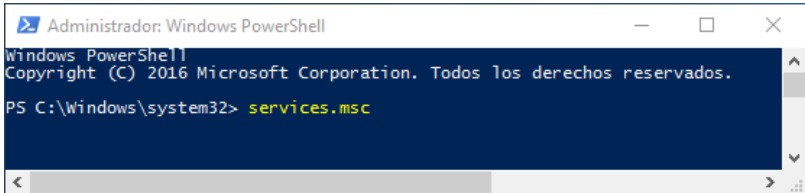
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

Para realizar las comprobaciones pertinentes en los servidores miembros se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

- Conjunto resultante de directivas (rsop.msc)
- Consola de servicios (services.msc)

| Comprobación                                                              | OK/NOK | Cómo hacerlo                                                                                                                               |
|---------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación raíz de empresa. |        | En el servidor Entidad de Certificación raíz de empresa, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |

| Comprobación                                                                                                                                                    | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Verifique la correcta aplicación de la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse “Sí” en la ventana de “Control de cuentas de usuario”.</p>  <p>Teclee “rsop.msc” en la consola de comandos que se ha abierto:</p>  |

| Comprobación                                                                                                                                                               | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                        |             |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                            |                         | <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” aparece en la lista como muestra la imagen.</p>  |             |        |
| 3. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                 |             |        |
| Servicio (Nombre largo)                                                                                                                                                    | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                              | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                              | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Servidor                                                                                                                                                                   | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Registro Remoto                                                                                                                                                            | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                          | Configurado |        |

### ANEXO A.3.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

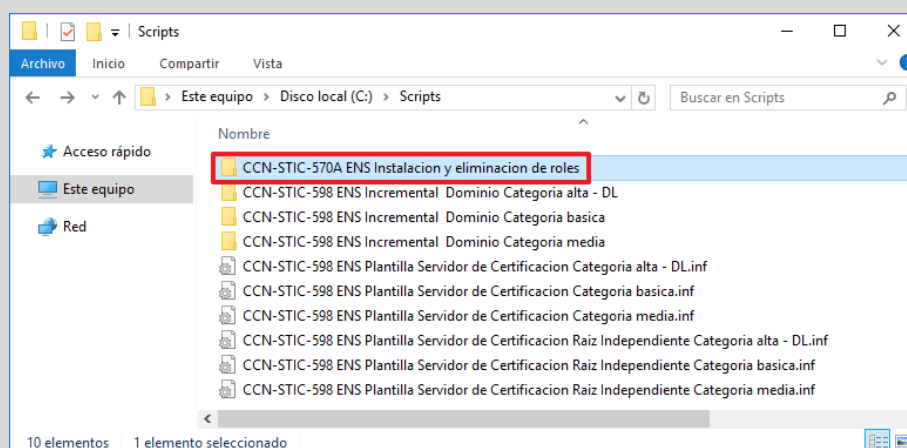
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Microsoft Windows Server 2016 independientes con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

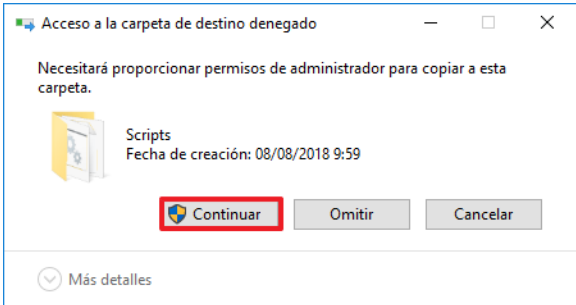
- a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad media.
- b) Un servidor independiente del dominio preparado siguiendo la guía CCN-STIC-570B Anexo A con una categorización de seguridad media.
- c) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad media.

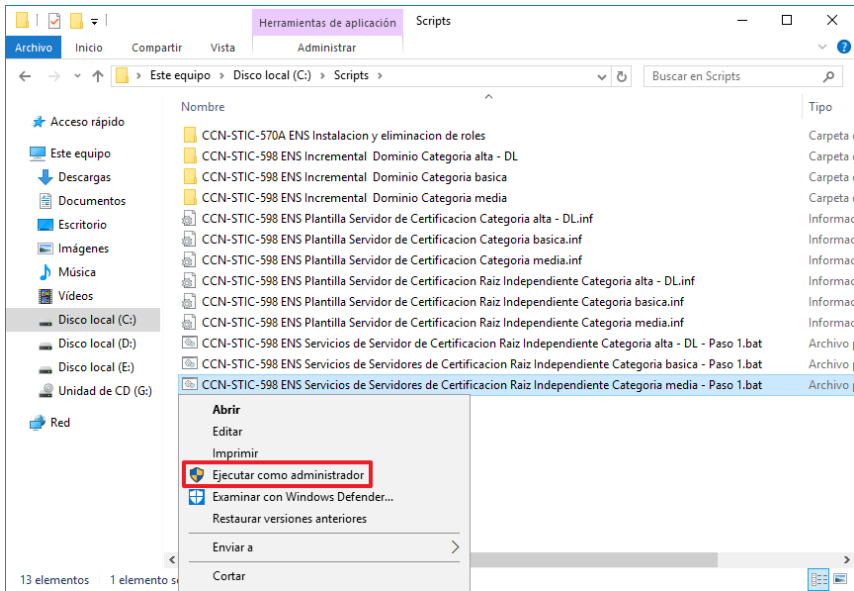
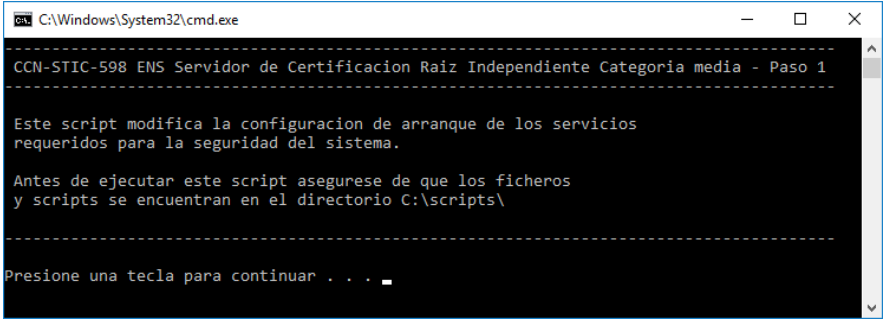
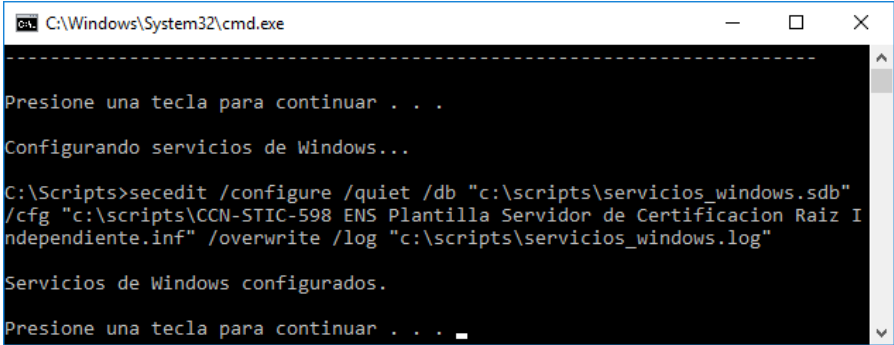
**Nota:** Si instala un Servidor de Entidad de Certificación por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO. En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía “CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016” encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta “Scripts” adjunta a la presente guía.

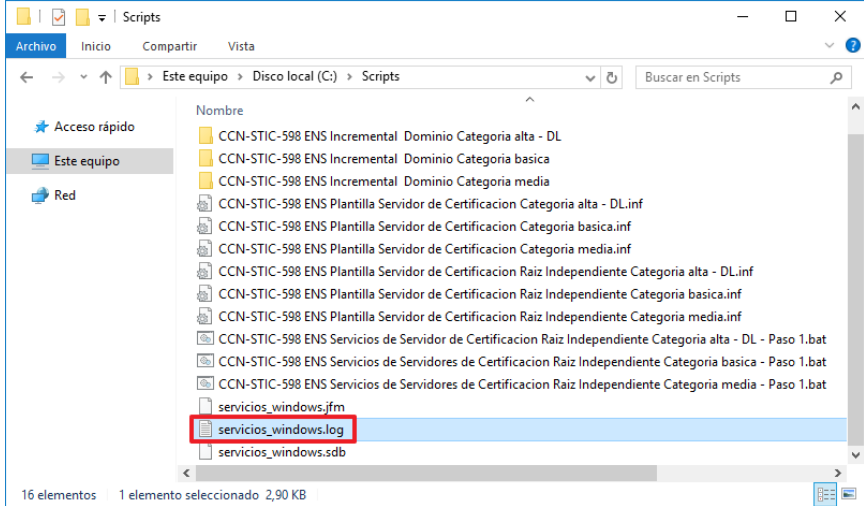
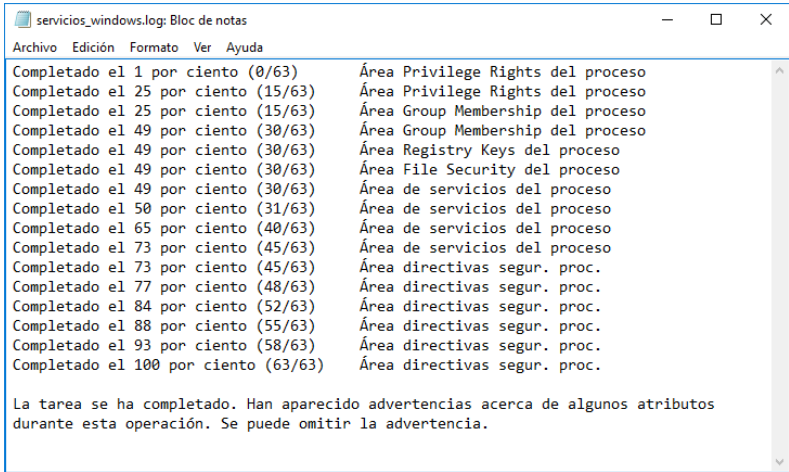


## 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DE DOMINIO

Los pasos que se describen a continuación se realizarán en todos aquellos servidores con el rol de Entidad de Certificación raíz independiente del dominio sobre Microsoft Windows Server 2016, que implementen servicios o información de categoría media y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

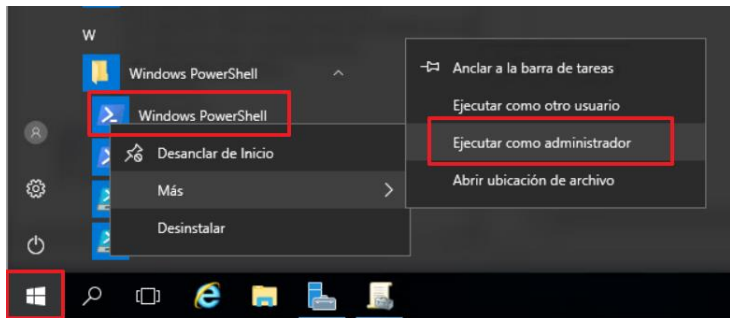
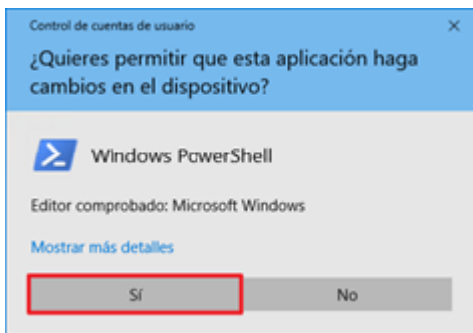
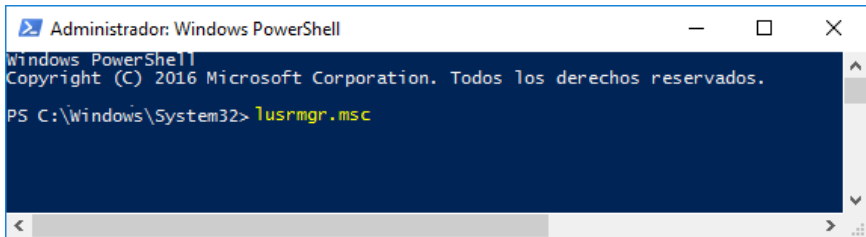
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor independiente donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta con permisos de administrador.</p>                                                                                                                                                |
| 2.   | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                                                                                                                                                            |
| 3.   | <p>Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.</p>  <p><b>Nota:</b> Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Haga clic en el botón “Continuar” e introduzca las credenciales.</p> |

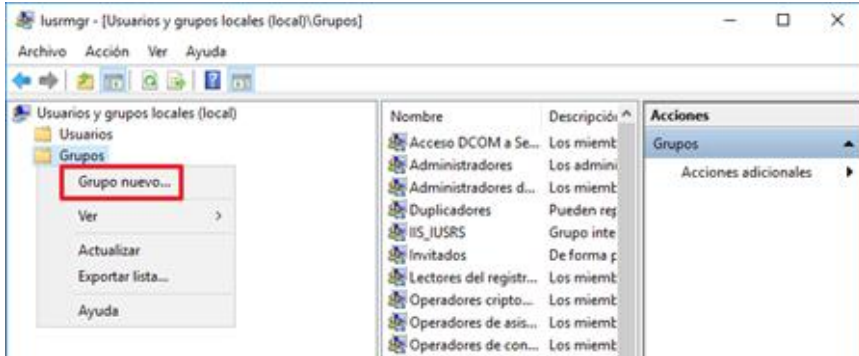
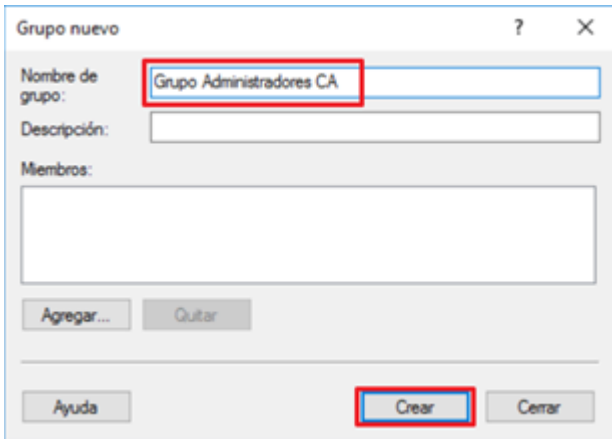
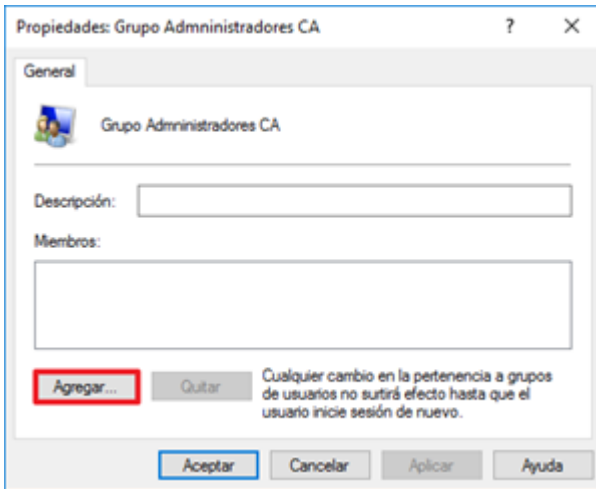
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | <p>A continuación, diríjase a la carpeta “C:\Scripts” y ejecute con permisos de administrador el script “CCN-STIC ENS Servicios de Certificación Raíz Independiente Categoría media – Paso 1.bat”.</p> <p>Este script aplica al sistema la plantilla de servicios para la seguridad del sistema.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.</p> |
| 5.   | <p>Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría media del ENS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 6.   | <p>Una vez completado el proceso, deberá pulsar una tecla para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

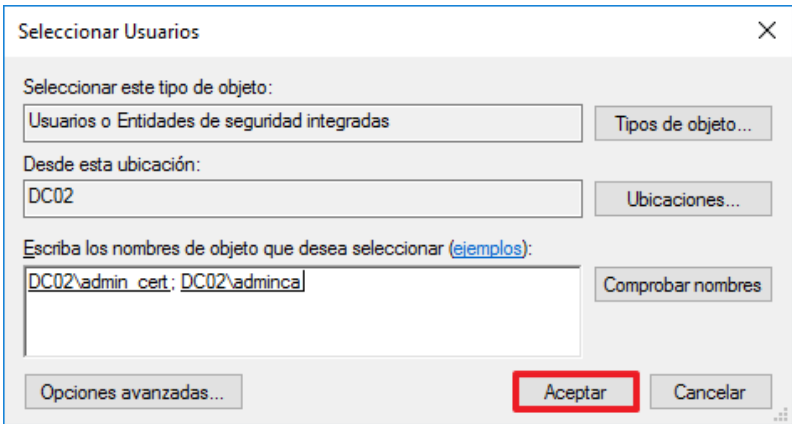
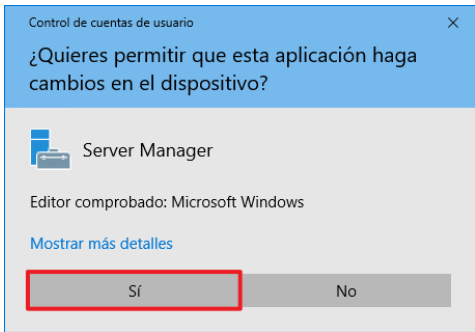
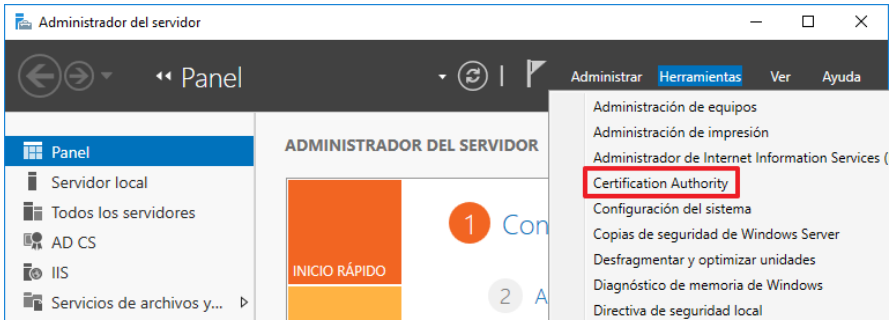
| Paso | Descripción                                                                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.   | <p>Pulse de nuevo otra tecla, para finalizar la ejecución del script.<br/>La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “servicios_windows.log”.</p>  |
| 8.   | <p>Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.</p>  |

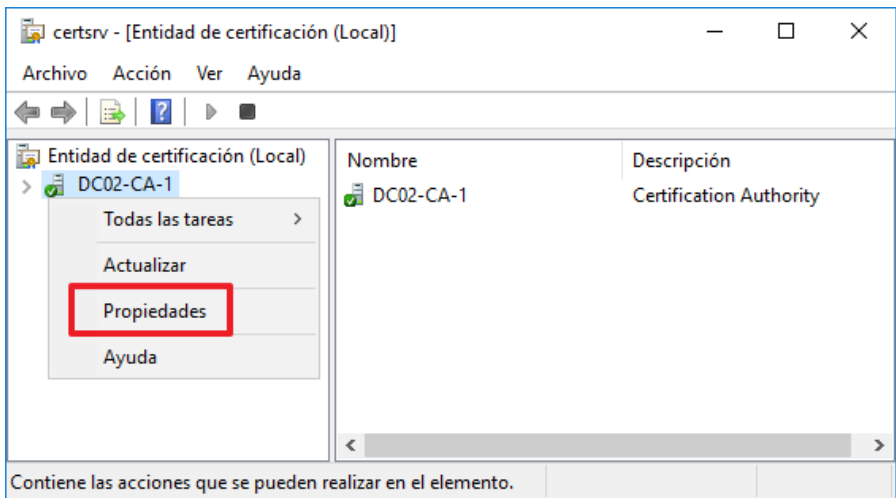
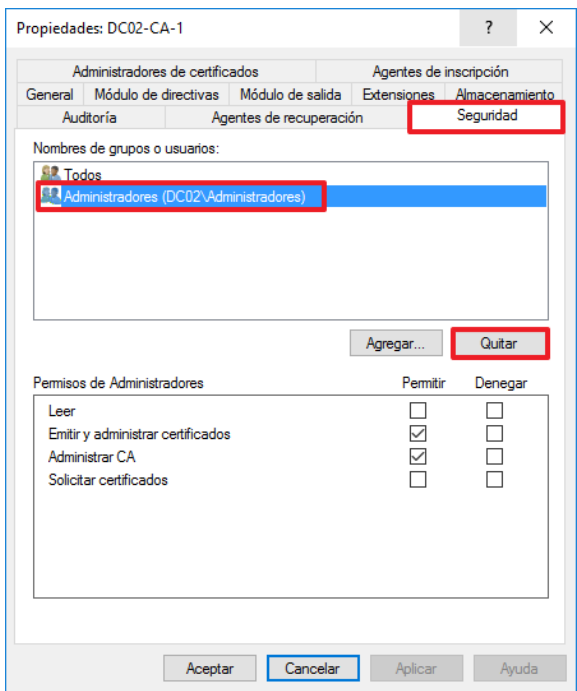
## 1.1. SEGREGACIÓN DE ROLES

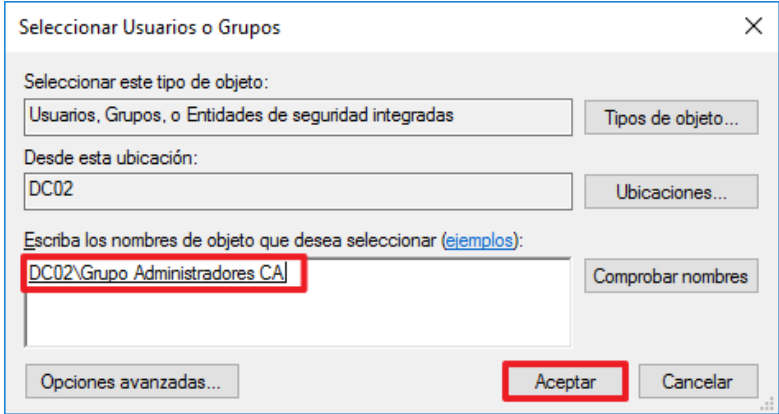
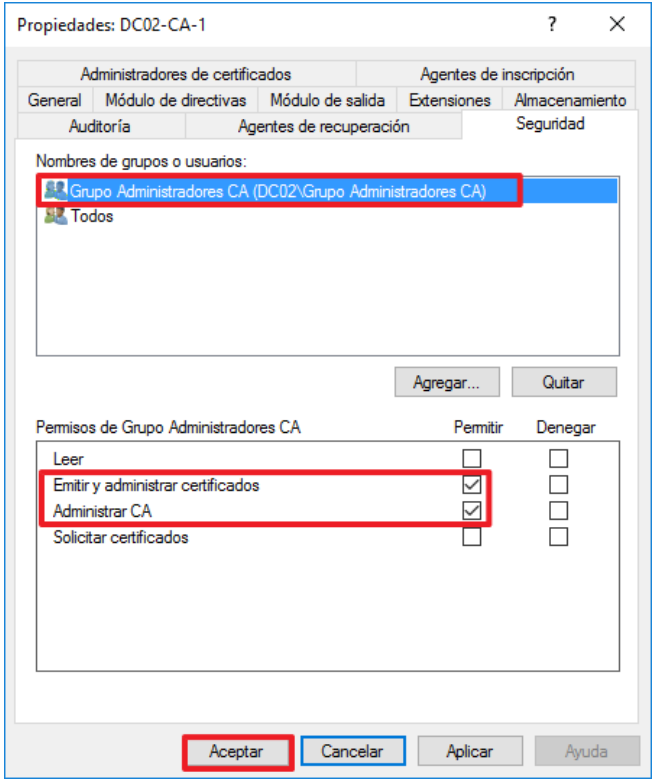
Con la aplicación del ENS para la categoría media sobre una Entidad de Certificación Raíz Independiente, será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar una Entidad de Certificación.

| Paso | Descripción                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.   | <p>Inicie sesión en Servidor de Certificación raíz independiente.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador local.</p>                                                                     |
| 10.  | <p>Ejecute la consola de PowerShell. Para ello pulse sobre “Inicio”, seleccione <b>“Windows Powershell → Windows Powershell”</b> con el botón derecho y pulse sobre la opción “Más → Ejecutar como administrador”.</p>  |
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                        |
| 12.  | <p>Teclee “lsrmgr.msc” en la consola de comandos que se ha abierto.</p>                                                                                                                                                |

| Paso | Descripción                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13.  | <p>Pulse con el botón derecho sobre “Grupos” y seleccione la opción del menú contextual “Grupo nuevo...”.</p>                                                              |
| 14.  | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |
| 15.  | <p>Haga doble clic sobre el grupo recién creado y pulse la pestaña “Agregar agrupo...”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>             |

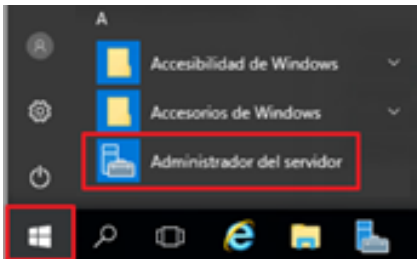
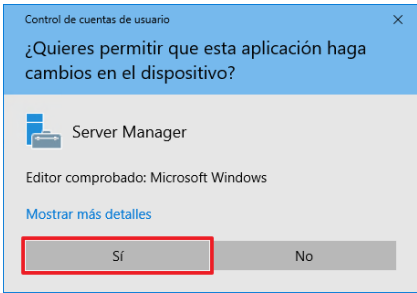
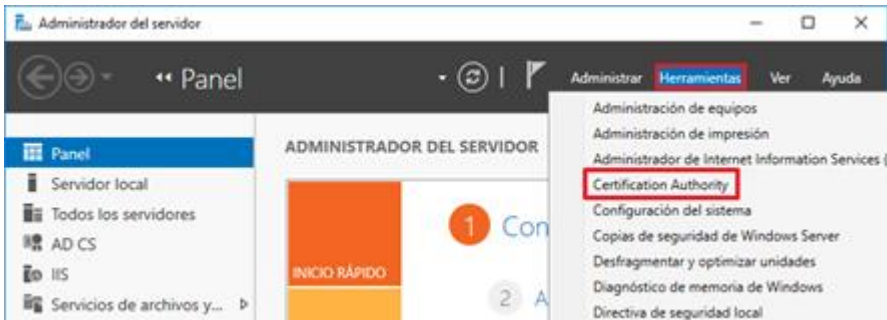
| Paso | Descripción                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.  | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la creación de esta guía.”</p> |
| 17.  | <p>A continuación, ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                          |
| 18.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                               |
| 19.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                           |

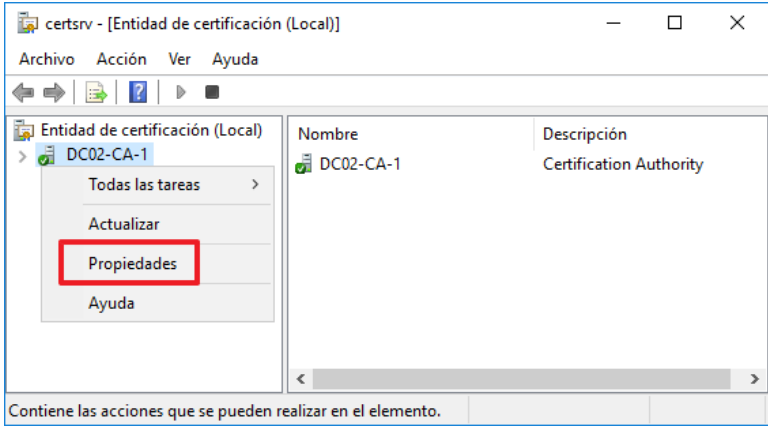
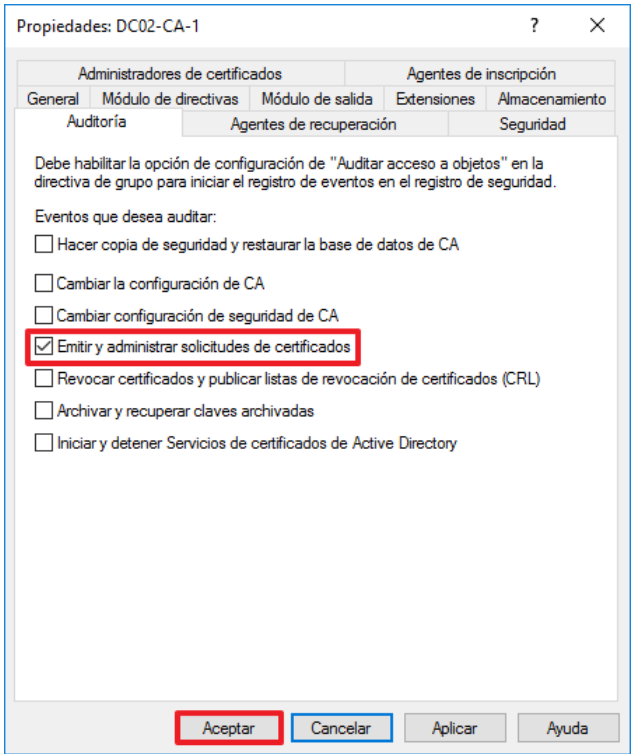
| Paso | Descripción                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.  | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p> |
| 21.  | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque el grupo Administradores. Pulse “Quitar” para eliminar el grupo Administradores.</p>                                     |

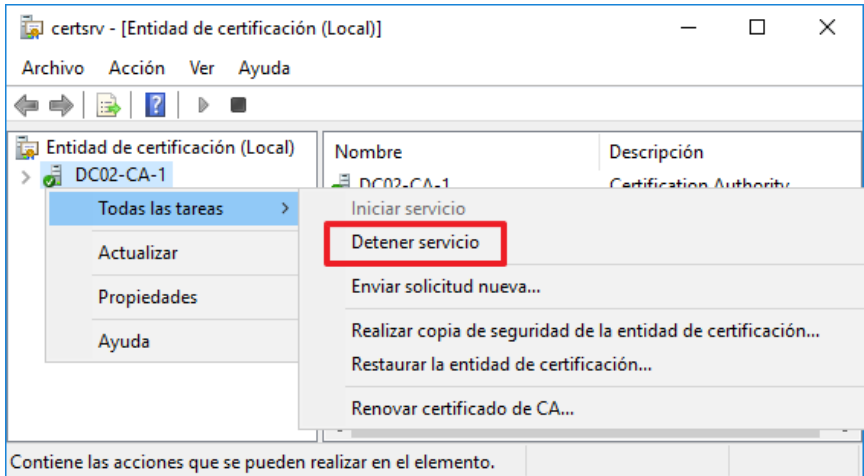
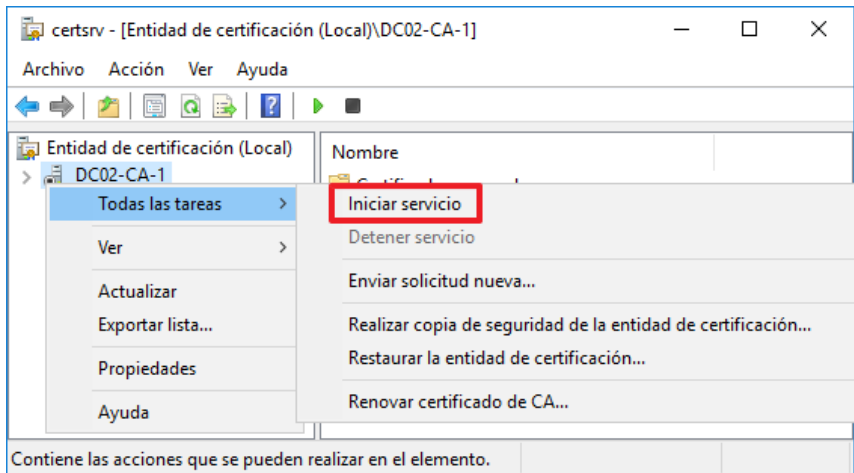
| Paso | Descripción                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22.  | <p>A continuación, añada el grupo recién creado y pulse “Aceptar”.</p>                                                                                                 |
| 23.  | <p>Seleccione el grupo recién añadido y otórguele los permisos “Emitir y administrar certificados” y “Administrar CA”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 24.  | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                   |

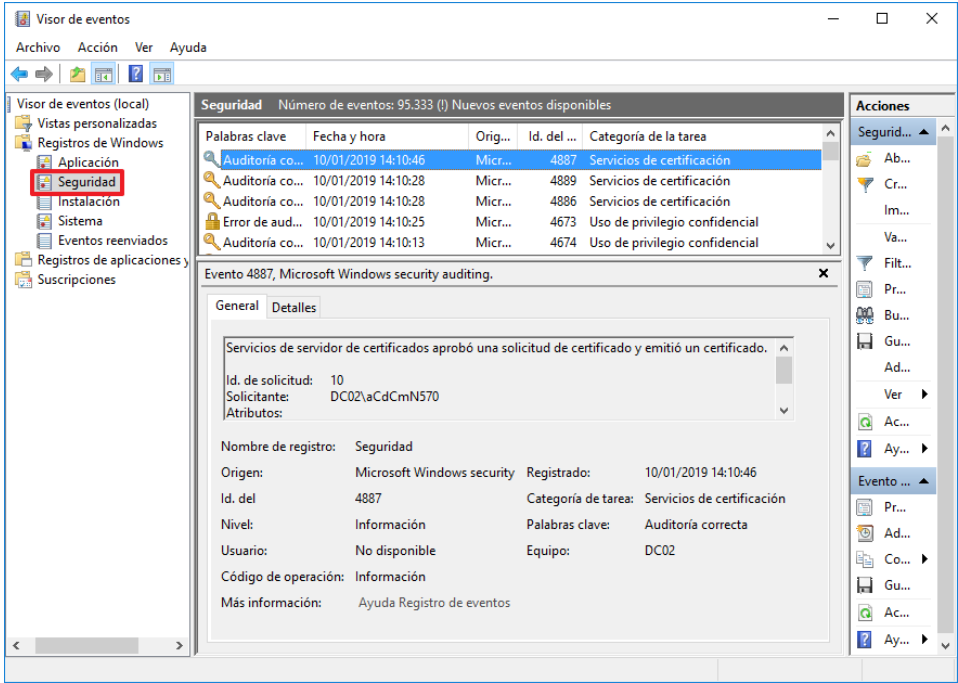
## 1.2. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

Existe la posibilidad de llevar un control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoría de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma.

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25.  | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                            |
| 26.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 27.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                                       |
| 28.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29.  | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 30.  | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31.  | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú <b>“Todas las tareas → Detener servicio”</b>.</p>                                          |
| 32.  | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú <b>“Acción → Todas las tareas → Iniciar servicio”</b> para iniciarlo de nuevo.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33.  | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: <b>“Inicio → Herramientas administrativas → Visor de eventos”</b>. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: <b>“Visor de eventos (local) → Registro de Windows → Seguridad”</b>.</p> |

## 2. CONFIGURACIONES DE SEGURIDAD SOBRE EL DOMINIO

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría básica.

No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

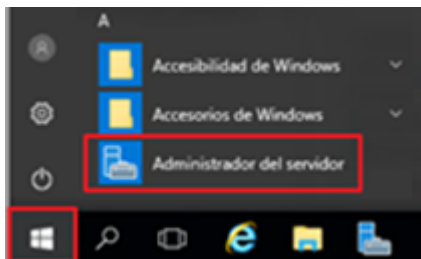
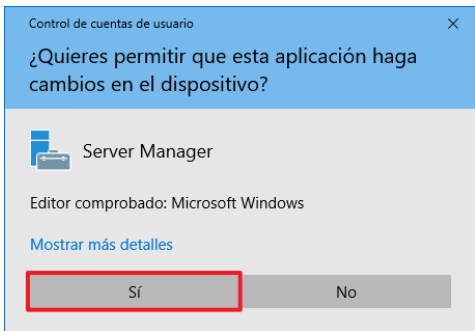
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

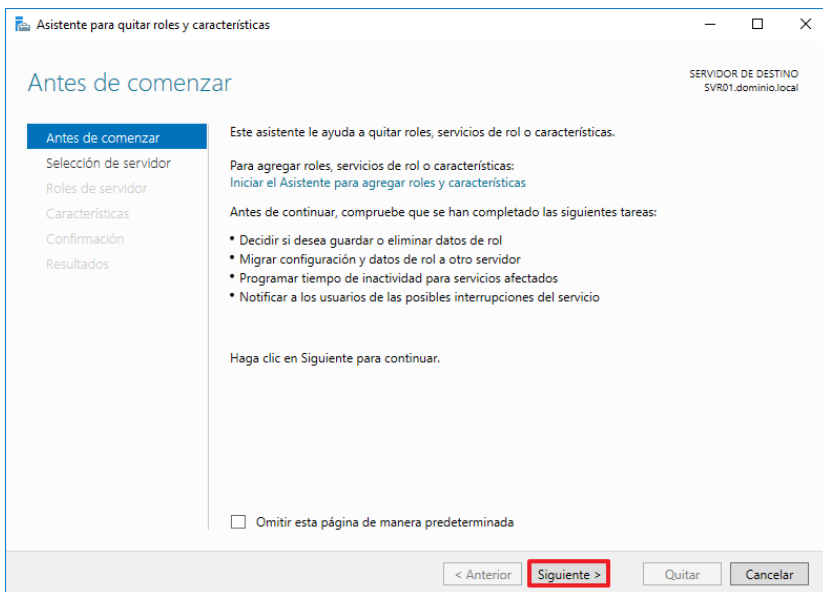
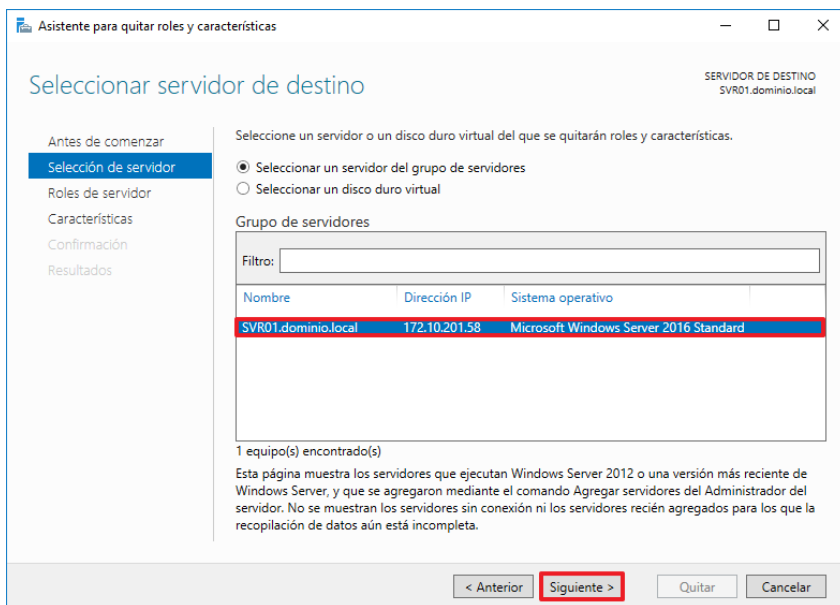
### 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

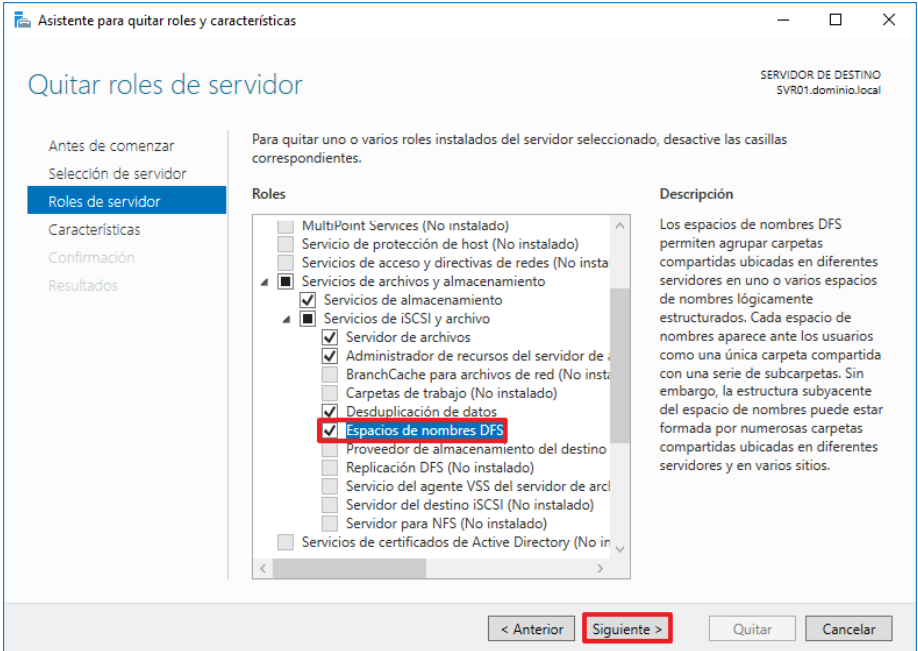
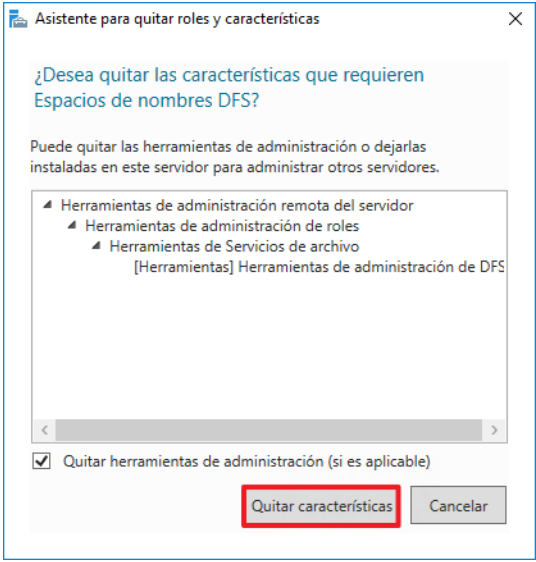
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con

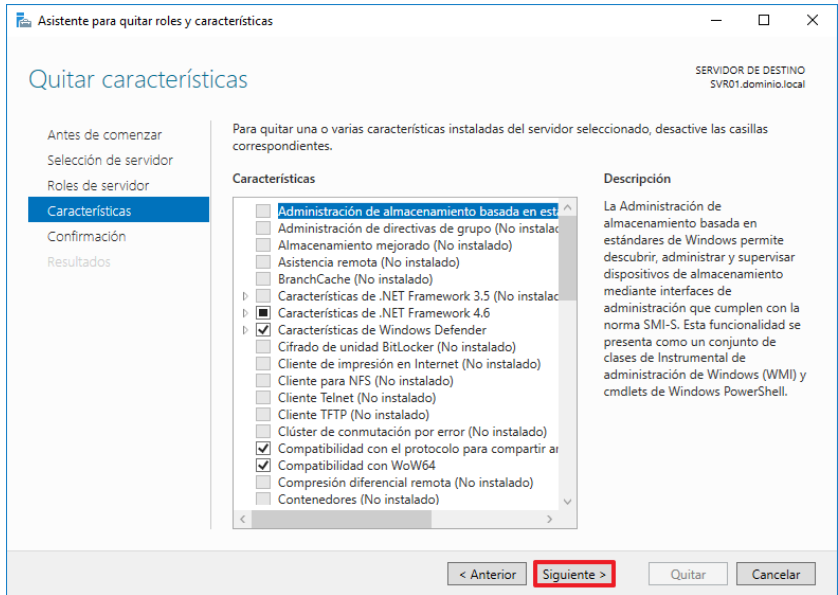
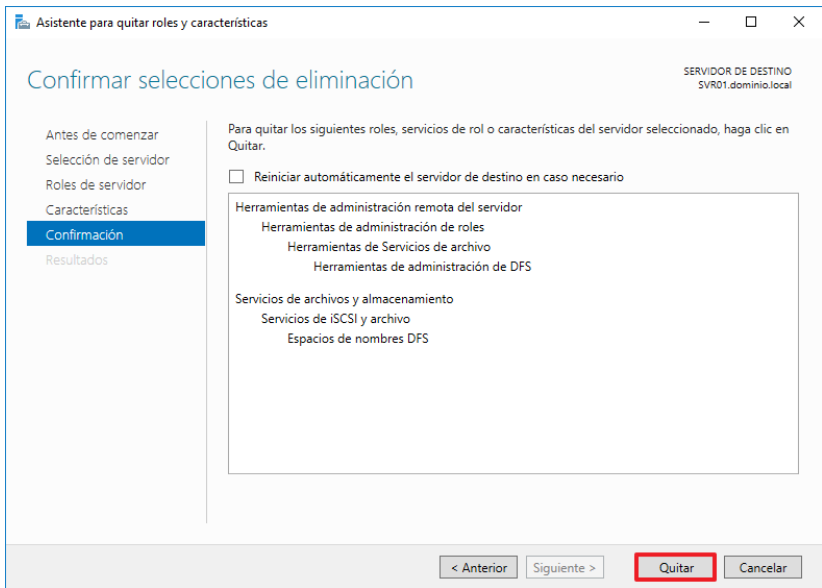
esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

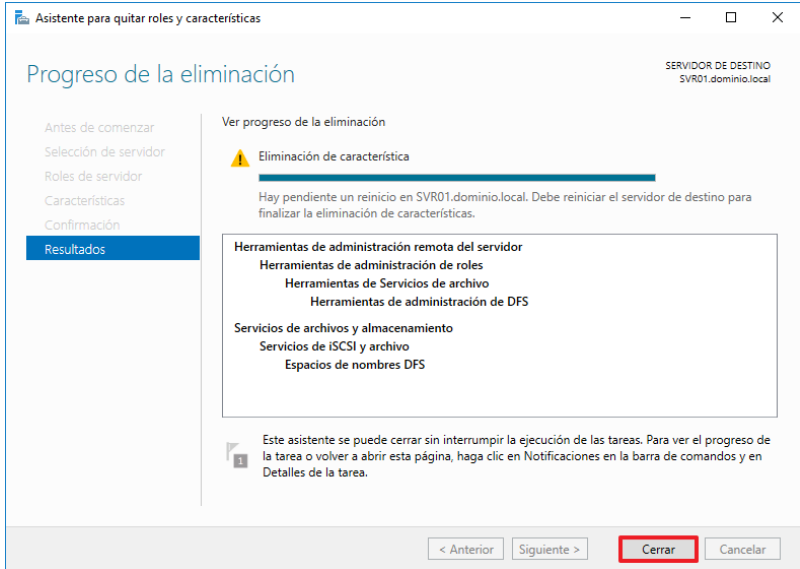
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de Certificación.

| Paso | Descripción                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34.  | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Entidad Certificadora.</p> <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 35.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                 |
| 36.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                  |
| 37.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>                     |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 38.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>                                                                              |
| 39.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p> |

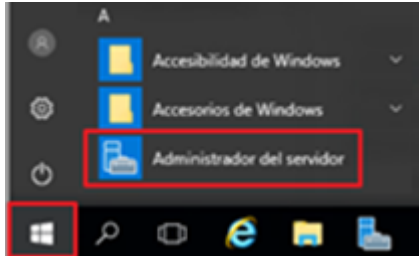
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 40.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |
| 41.  | <p>En el caso de que el rol posea características que dependen de él se lanzará una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p>     |

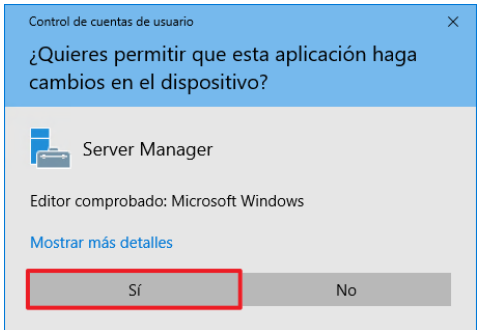
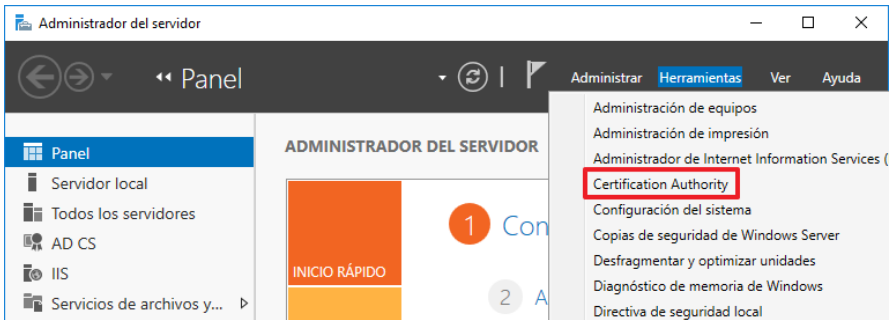
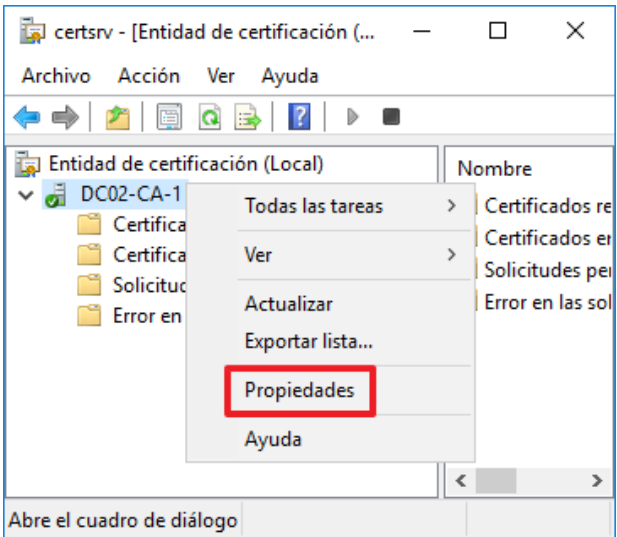
| Paso | Descripción                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 42.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>  |
| 43.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                                                                |

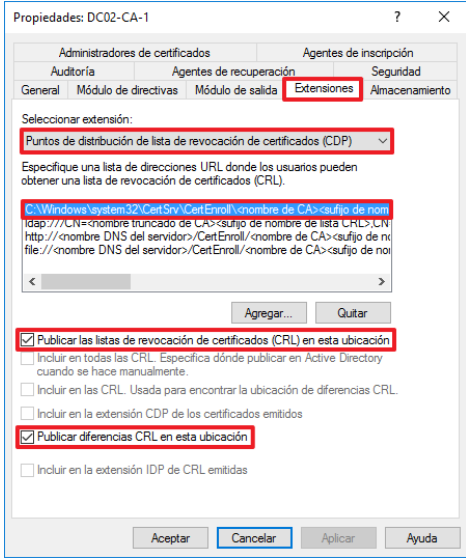
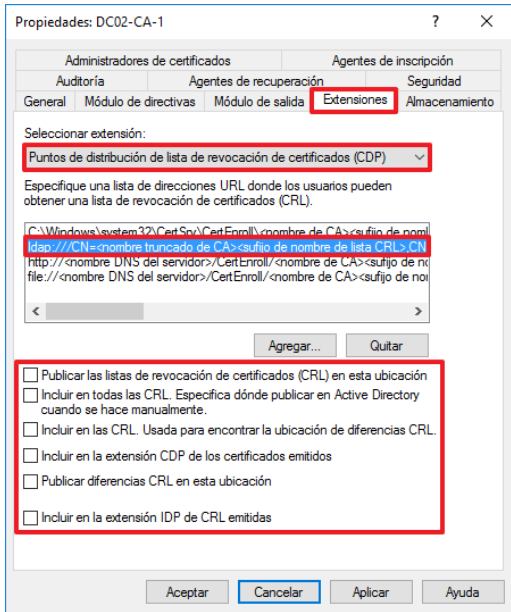
| Paso | Descripción                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 44.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 45.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                  |

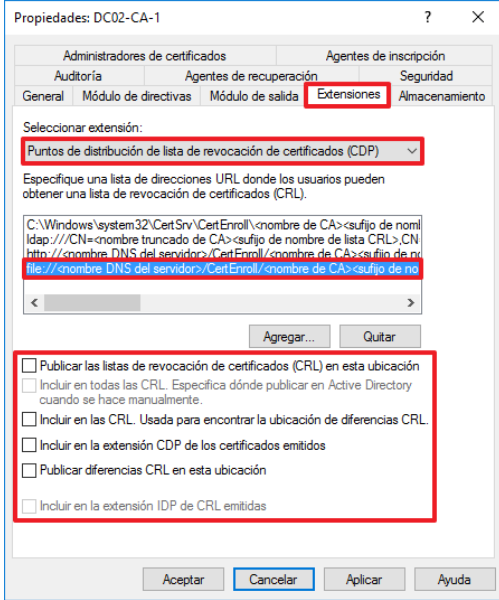
## 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL)

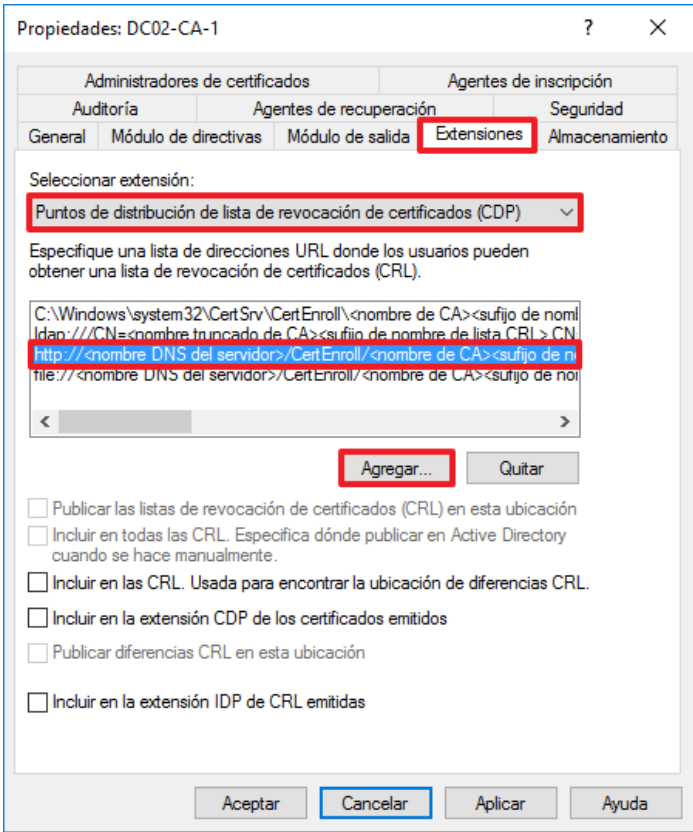
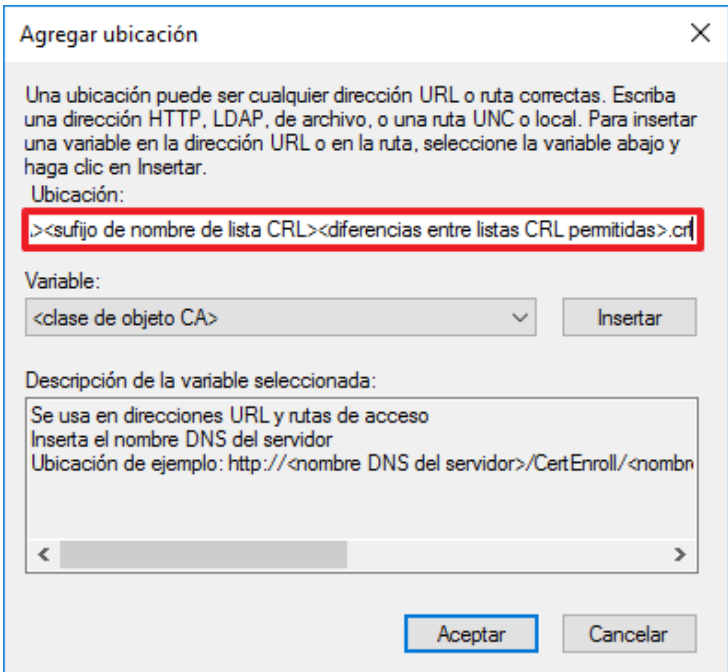
Los pasos que se describen a continuación se realizarán sobre el servidor Entidad de Certificación independiente del dominio.

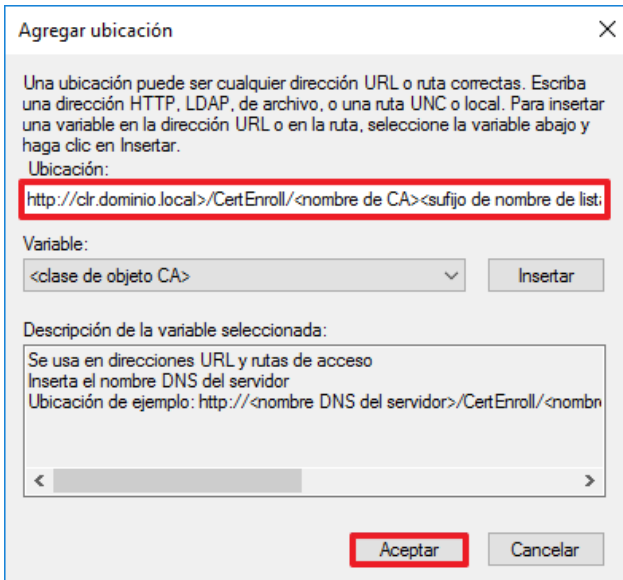
| Paso | Descripción                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46.  | <p>Si no lo ha hecho anteriormente, inicie sesión en el equipo donde se va a instalar el servidor independiente Entidad de Certificación raíz.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de administrador local.</p> |
| 47.  | <p>Acceda al “administrador del servidor” mediante el icono de la barra de tareas.</p>                                                                       |

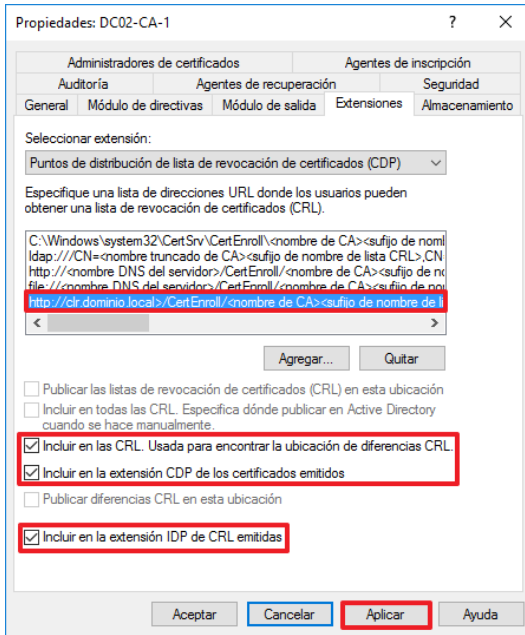
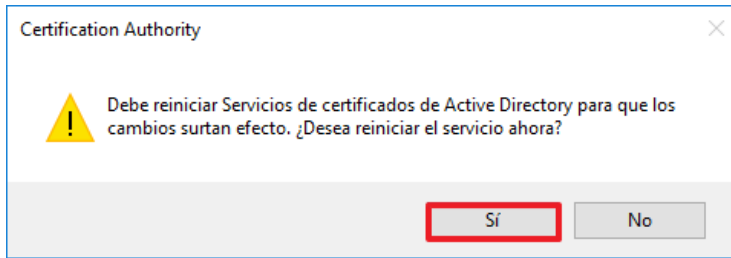
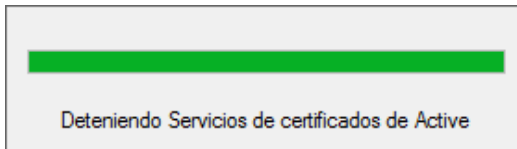
| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 48.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                    |
| 49.  | <p>En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                                                                   |
| 50.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente, con el botón derecho del ratón selecciónelo y pulse sobre “Propiedades”.</p>  |

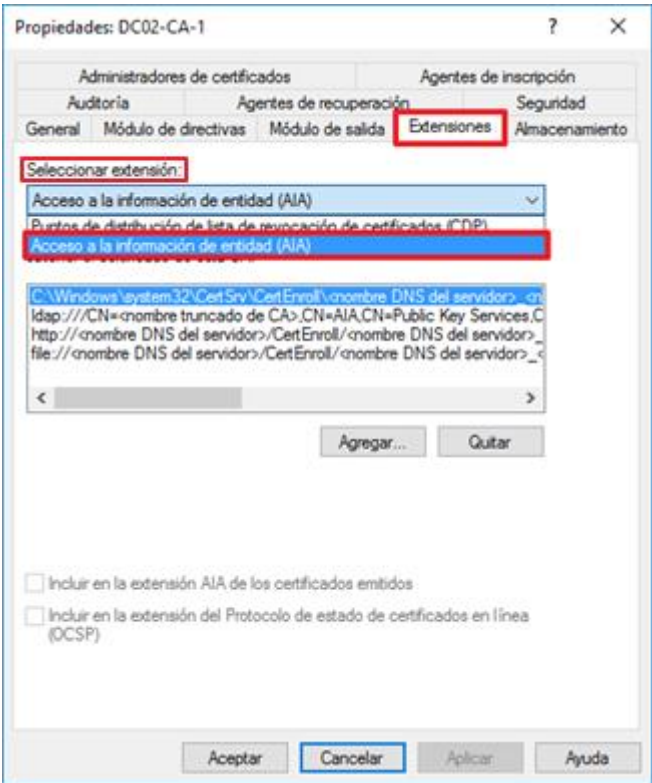
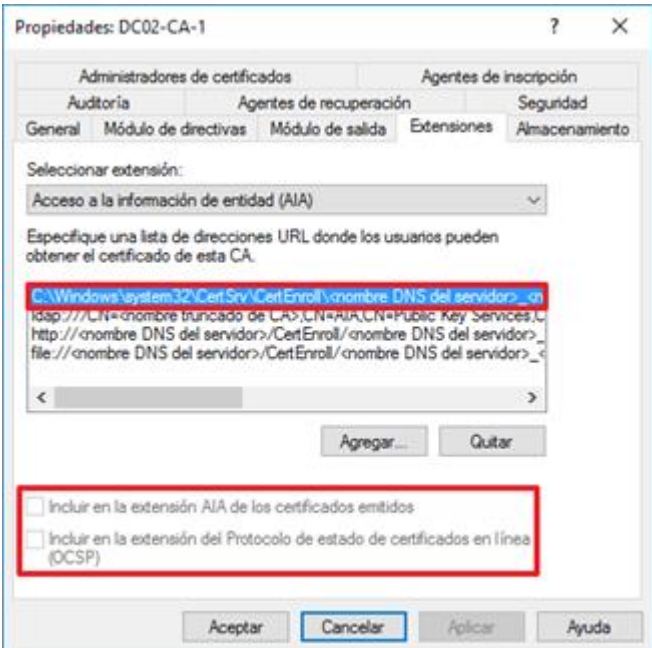
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 51.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\<nombre b="" ca&gt;&lt;="" crl="" crl&gt;&lt;diferencias="" de="" entre="" lista="" listas="" nombre="" permitidas&gt;.crl”<="" sufijo=""> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</nombre></b></p>  |
| 52.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando <b>“ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;”</b> y desmarque todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>                              |

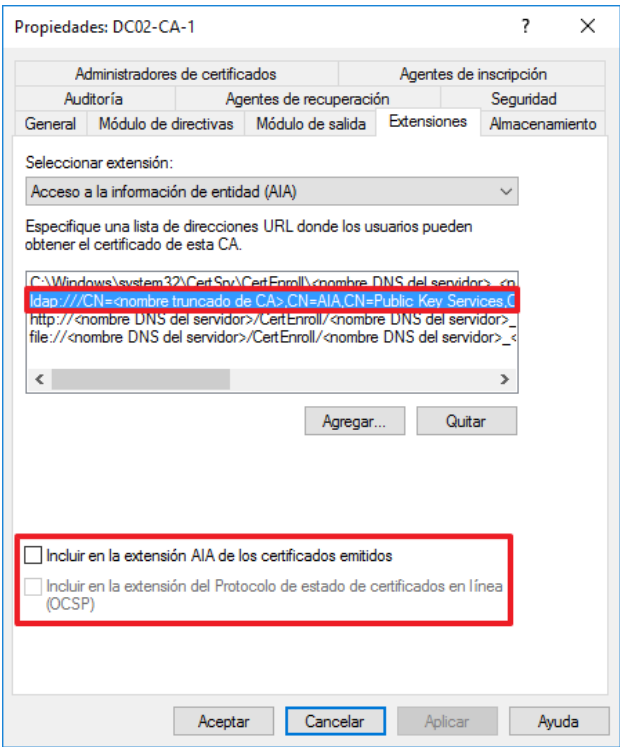
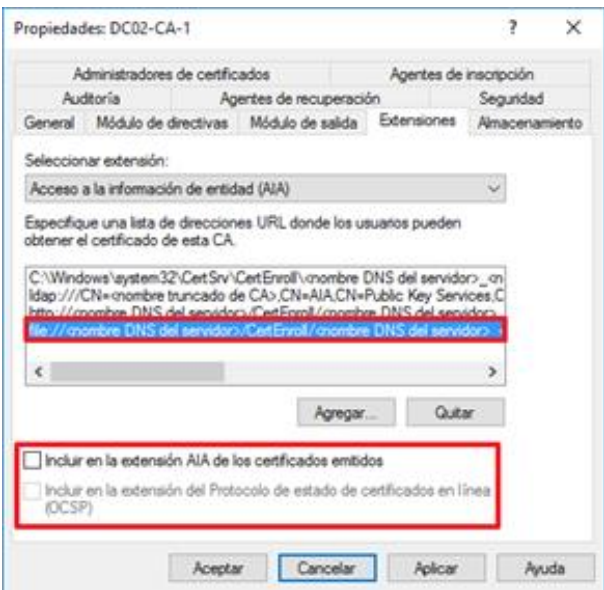
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 53.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y desmarque todas las opciones como muestra la siguiente figura:</p>  |
| 54.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt;sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto.</p>                                                                                                     |

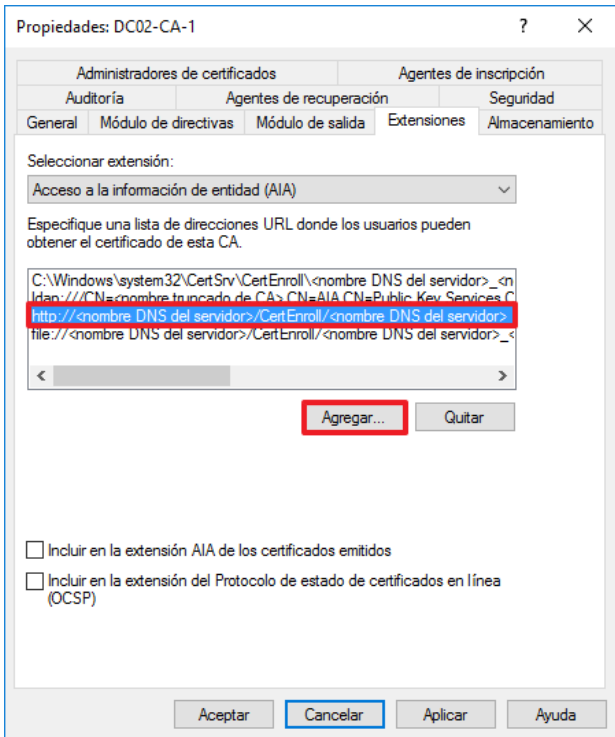
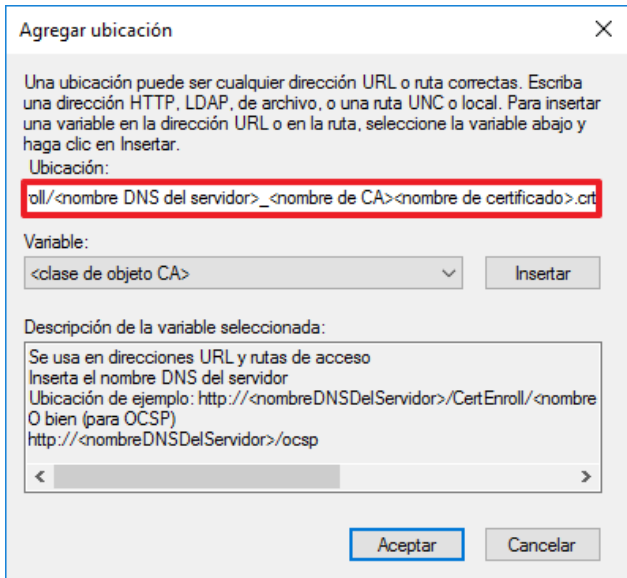
| Paso | Descripción                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 55.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                         |
| 56.  | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>  |

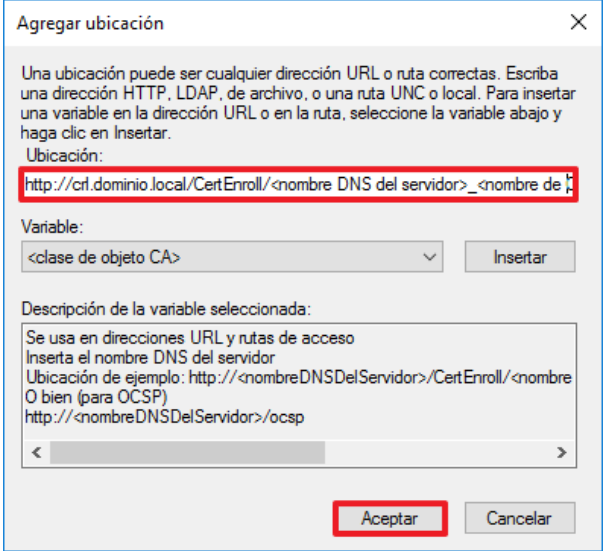
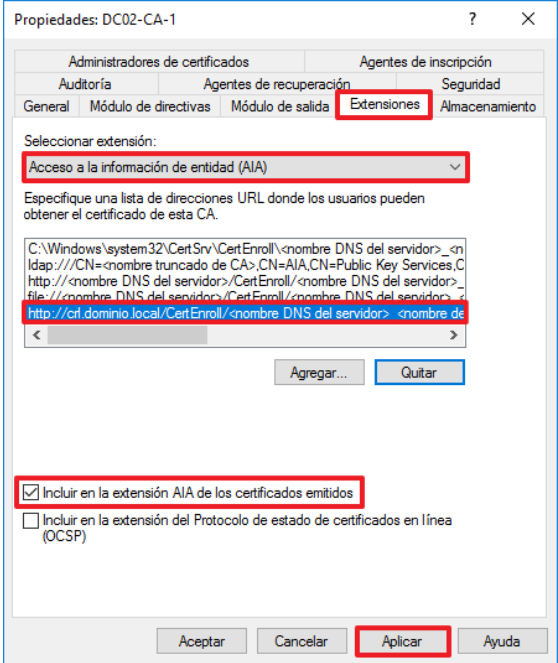
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

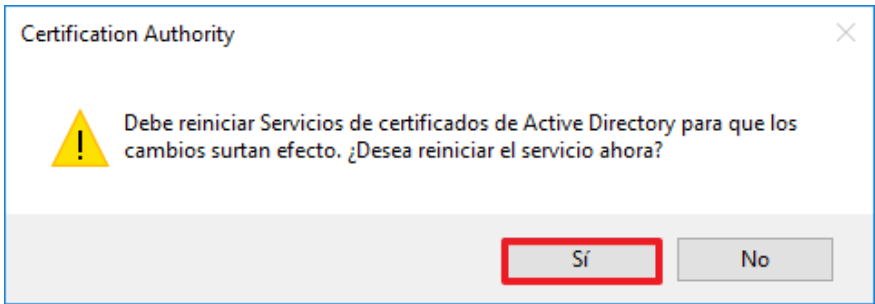
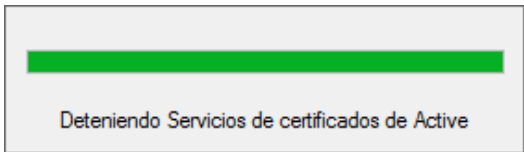
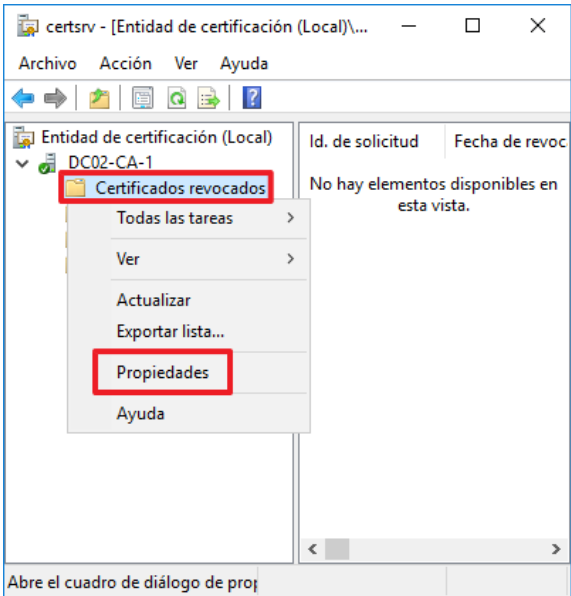
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 58.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y marque los siguientes elementos. Pulse “Aplicar” para guardar los cambios.</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul>  |
| 59.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 60.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

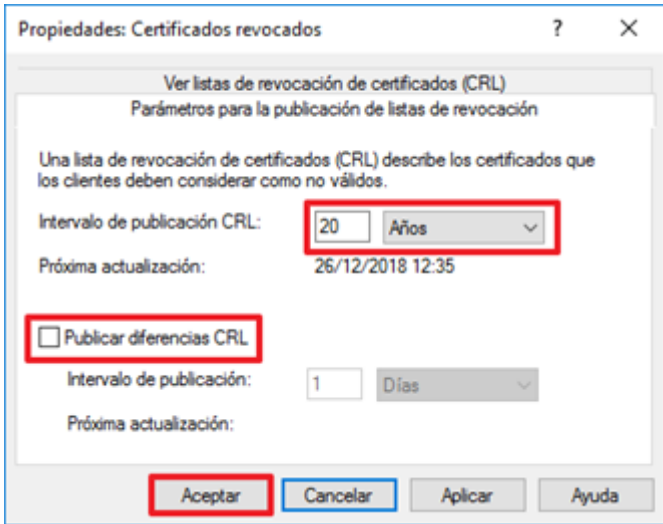
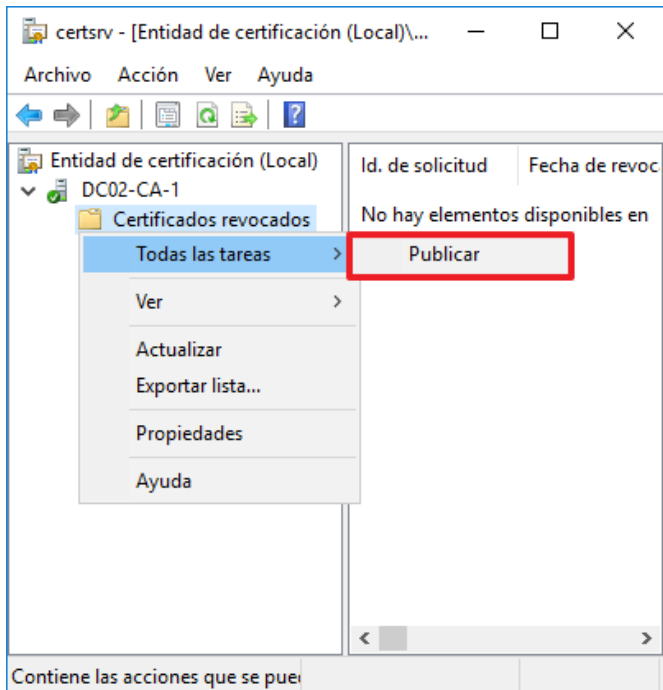
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 61.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>                                                                               |
| 62.  | <p>Compruebe que en el objeto “C:\Windows\System32\CertSrv\CertEnroll\<b>&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt</b>” todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.</p>  |

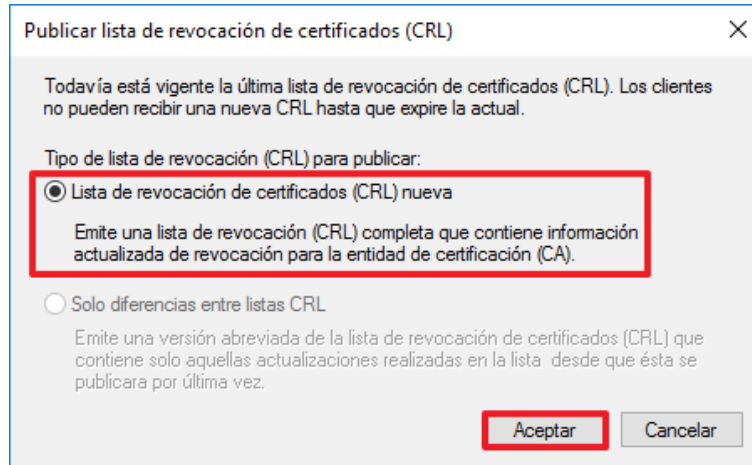
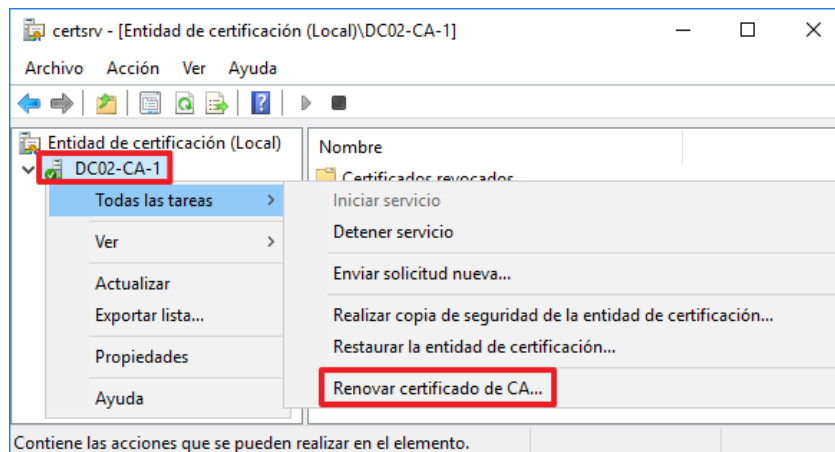
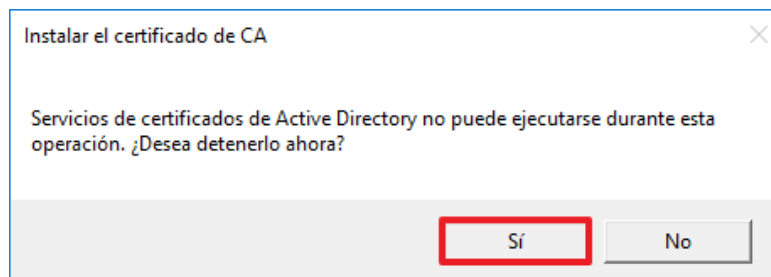
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 63.  | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |
| 64.  | <p>Seleccione ahora <b>"file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt"</b> y desmarque la opción "Incluir en la extensión AIA de los certificados emitidos".</p>                    |
| 65.  | <p>Seleccione ahora <b>"http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt"</b> y copie el elemento mediante la combinación de teclas "Control + C".</p>                                                                                                                     |

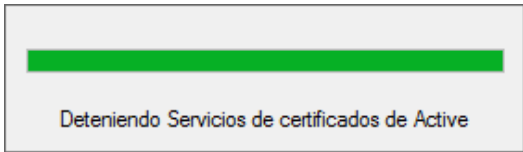
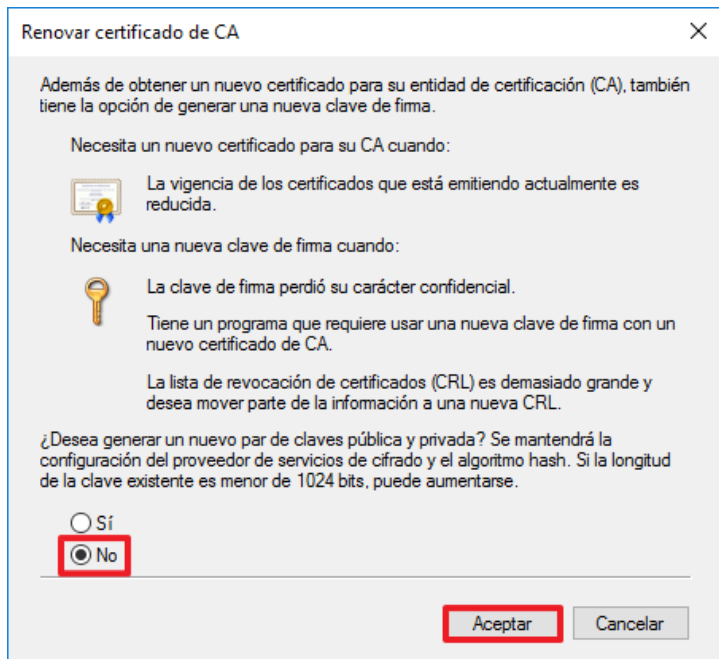
| Paso | Descripción                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 66.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                         |
| 67.  | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 68.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |
| 69.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora “http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>                     |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 70.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 71.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 72.  | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 73.  | <p>El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL, al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.</p>                                                                                                                                                                                                                                                                                                                                               |
| 74.  | <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:<br/> <b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b><br/> Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 75.  | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p>  <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p> |
| 76.  | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                                                                                                                                                                                                                                                                                          |

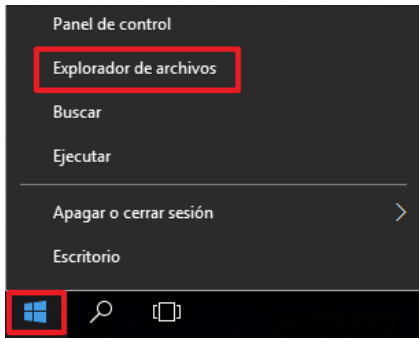
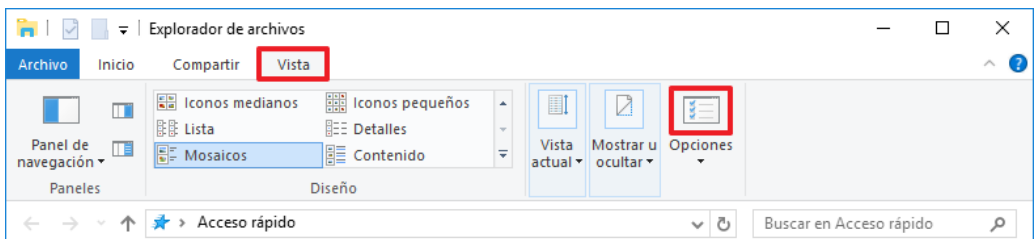
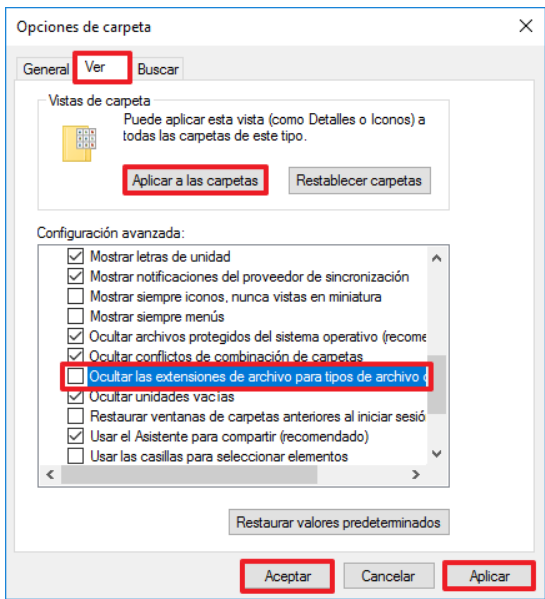
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 77.  | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>                                                                                                                                                                                  |
| 78.  | <p>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 “<b>Todas las tareas → Renovar certificado de CA...</b>”.</p>  |
| 79.  | <p>Pulse “Sí” en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                          |

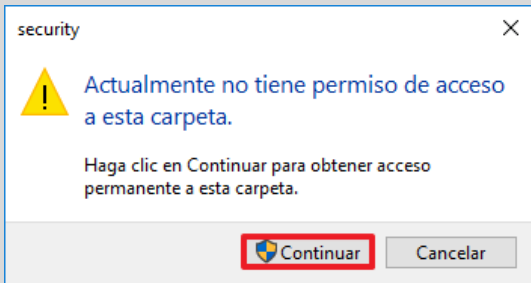
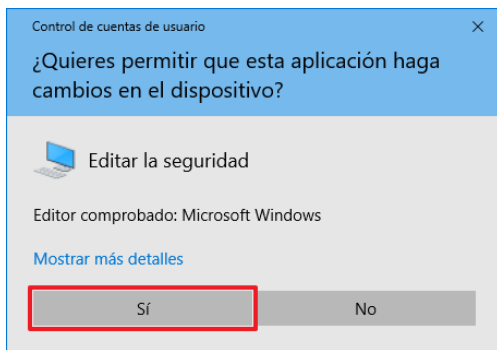
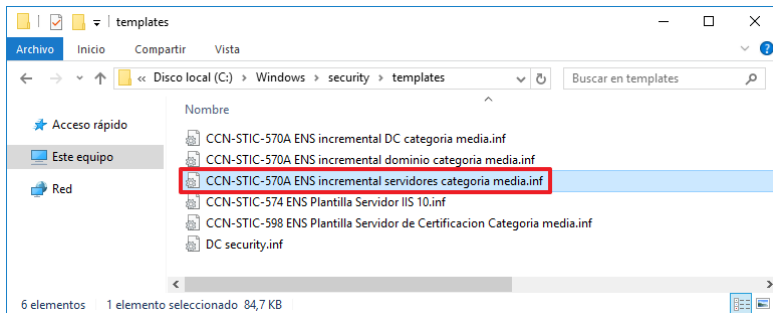
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                       |
| 81.  | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Este proceso comienza en segundo plano y puede tardar unos minutos. No debe cerrar la ventana hasta que finalice el proceso.</p> |

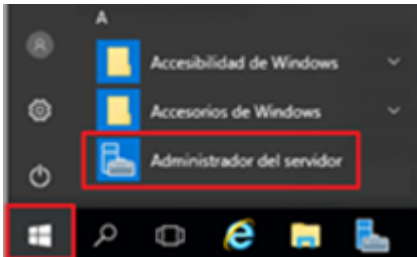
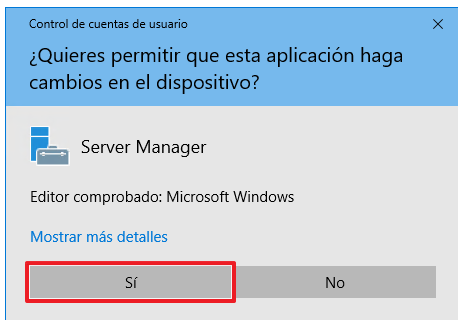
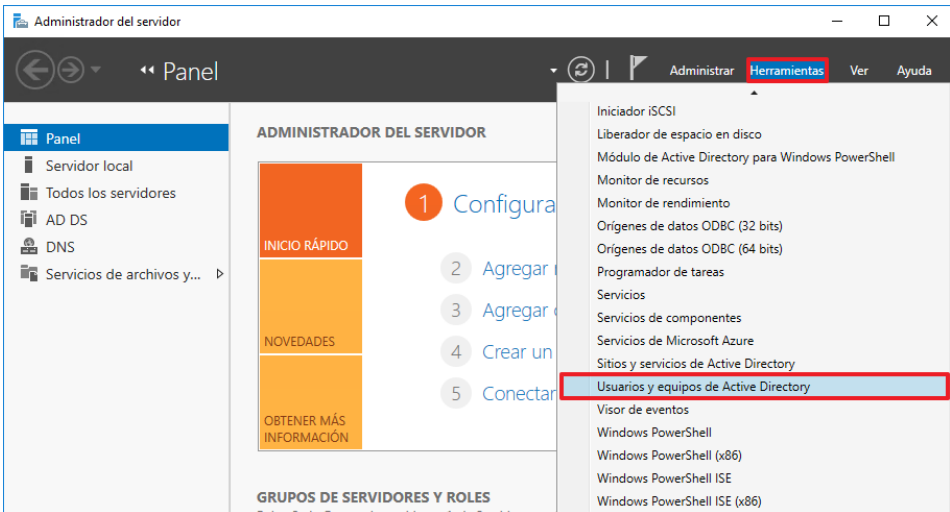
## 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO

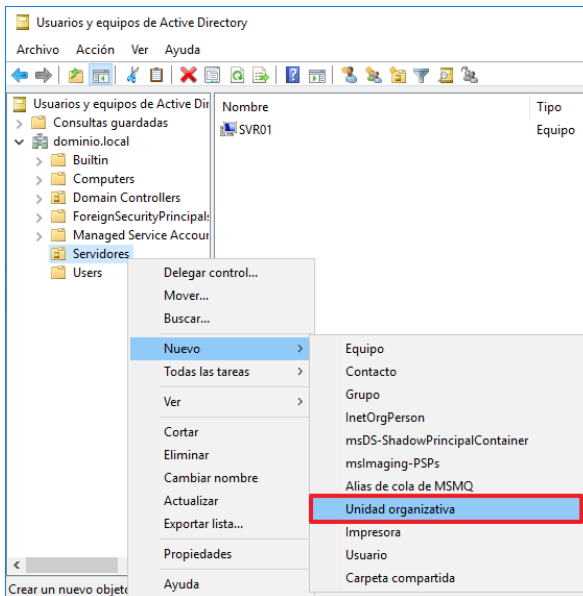
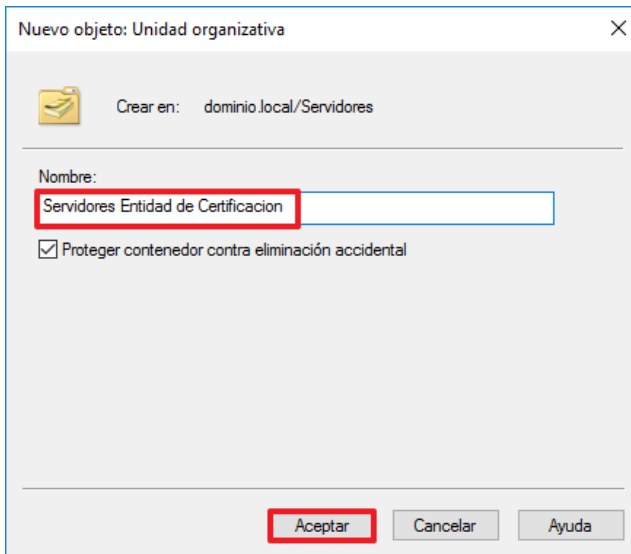
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor Entidad de Certificación subordinada.

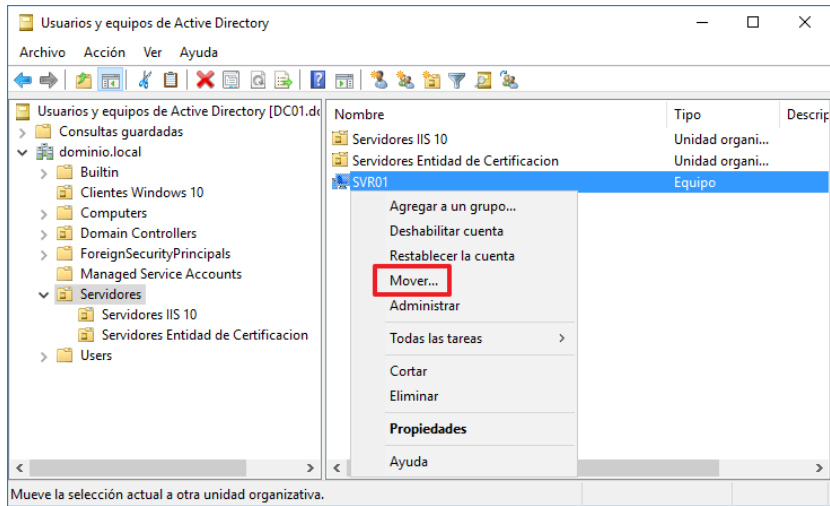
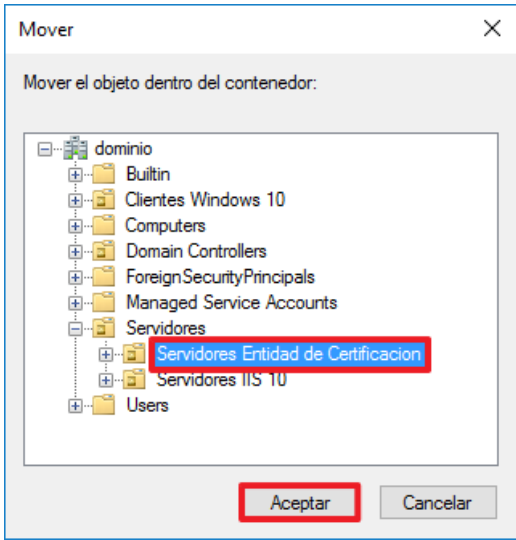
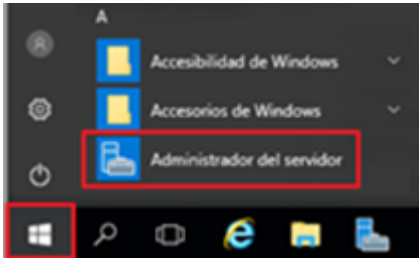
| Paso | Descripción                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 82.  | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para la Entidad de Certificación según criterios de ENS.</p> <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |
| 83.  | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                        |
| 84.  | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                        |

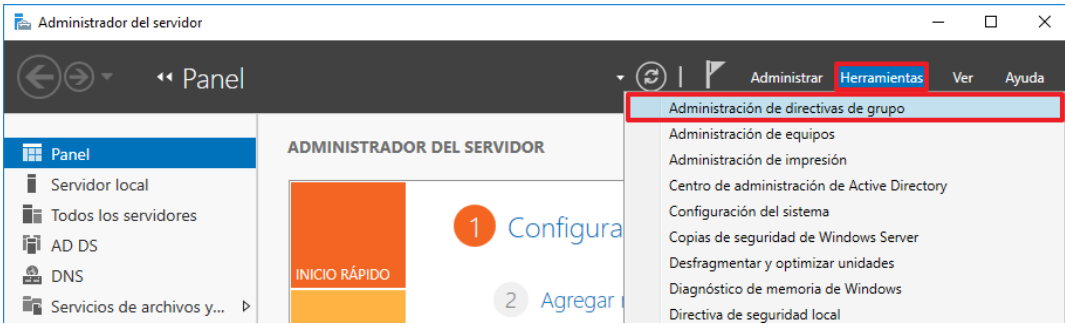
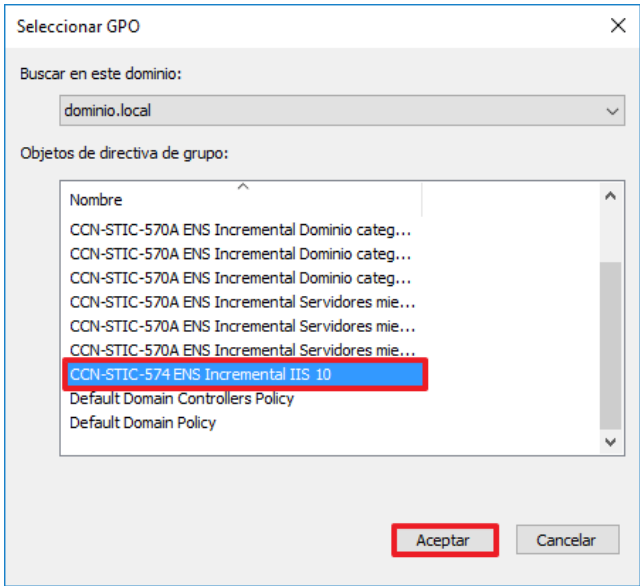
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 85.  | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>                         |
| 86.  | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                                           |
| 87.  | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |

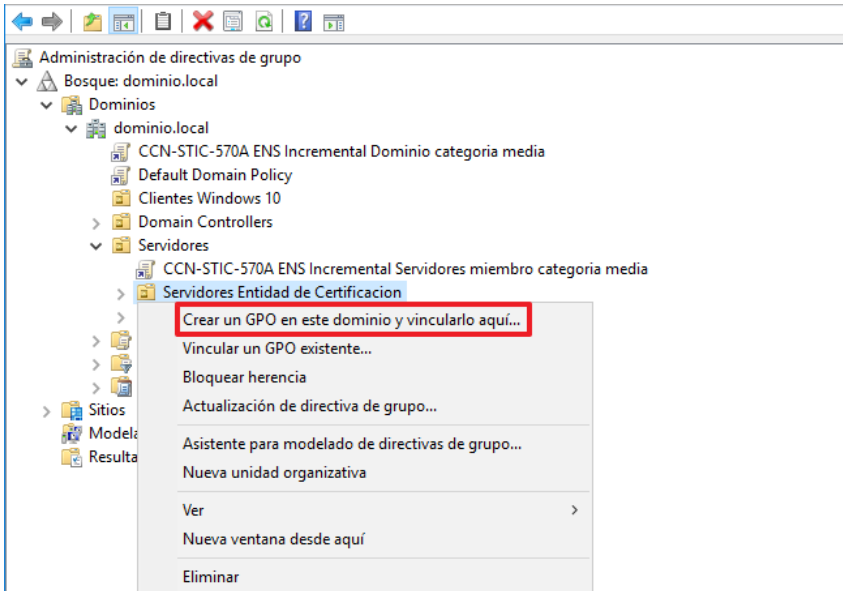
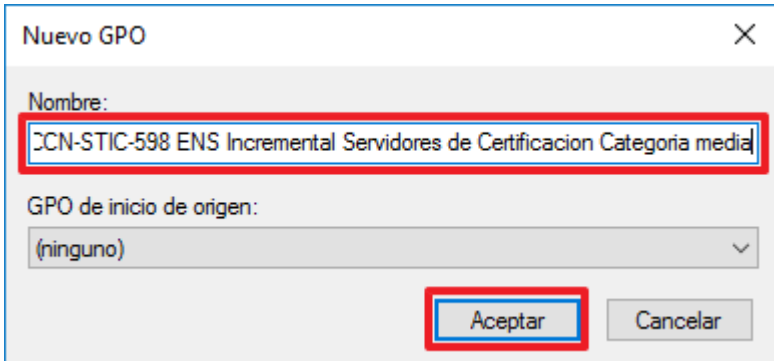
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88.  | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                                                                                                                                                                                                                             |
| 89.  | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |
| 90.  | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría media.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>                                                                                                                                                                                                                                                                                                                                                                                    |

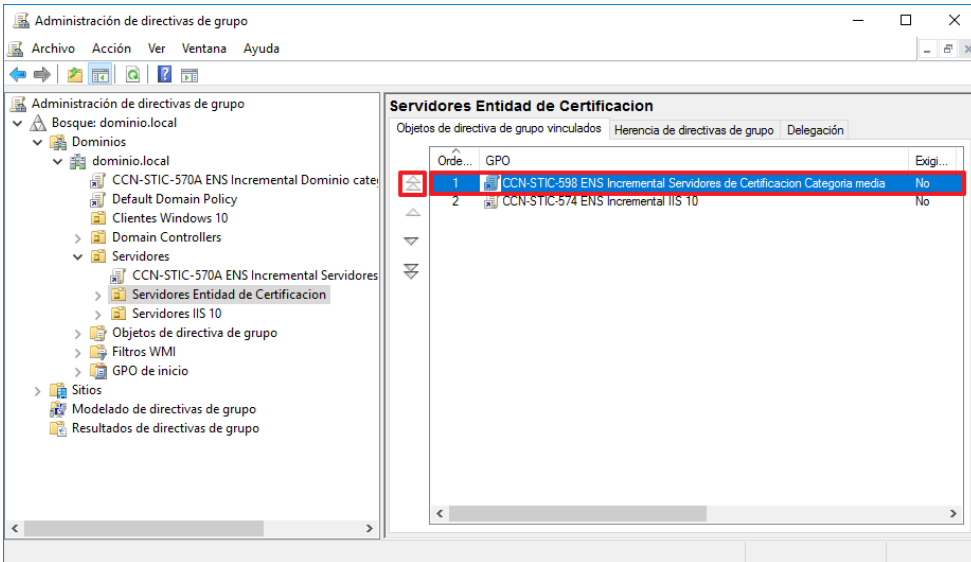
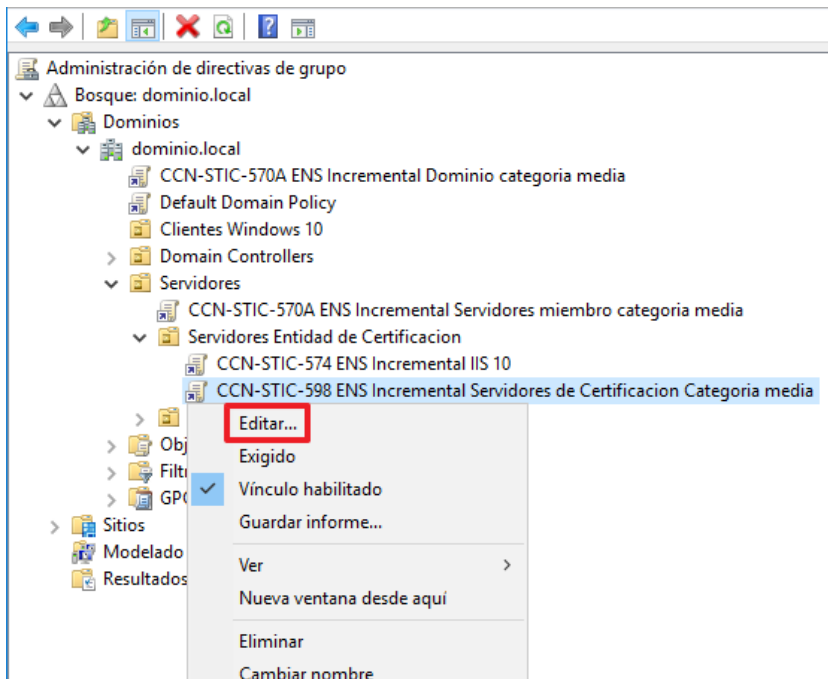
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 91.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                                  |
| 92.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                                    |
| 93.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione <b>“Herramientas → Usuarios y equipos de Active Directory”</b>.</p>  |

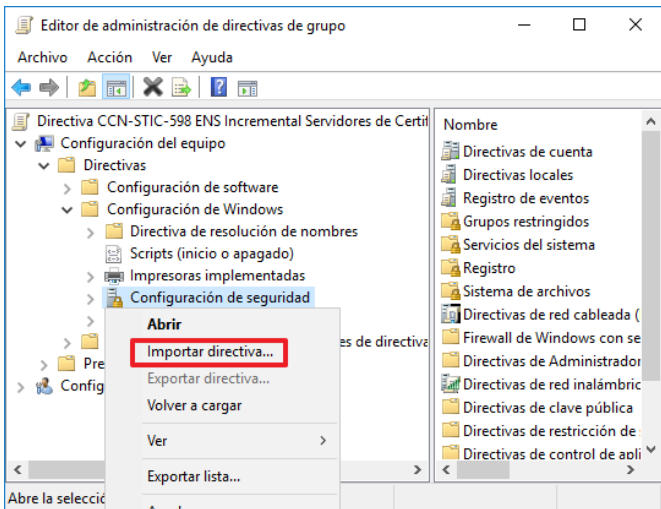
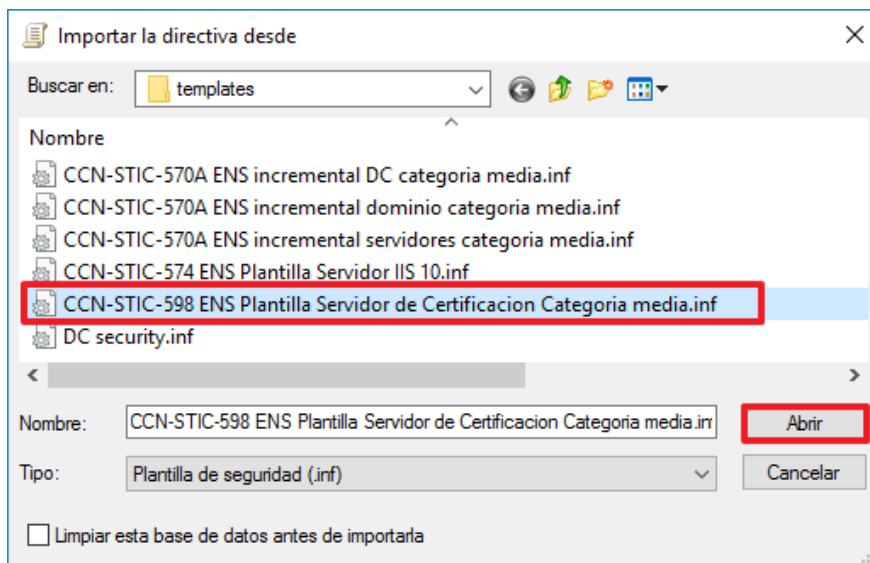
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 94.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo “&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local → Servidores”.</p> |
| 95.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

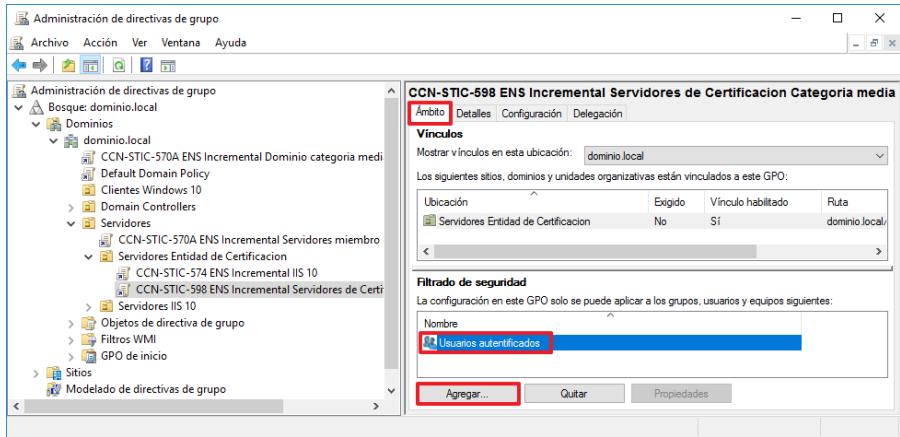
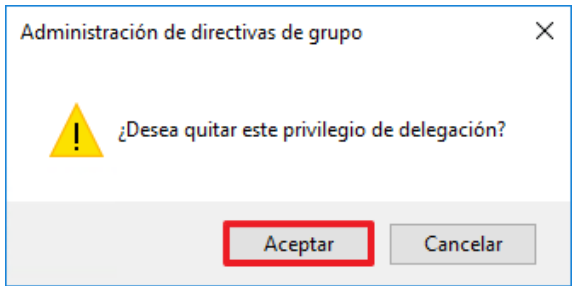
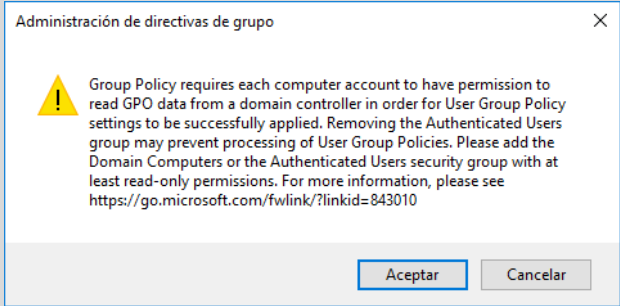
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores entidad de certificación a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |
| 97.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                         |
| 98.  | <p>Cierre la herramienta de “Usuarios y equipos de Active Directory”.</p>                                                                                                                                                                                                                                                                                                                                                           |
| 99.  | <p>A continuación, abra el “Administrador del servidor”.</p>                                                                                                                                                                                                                                                                                    |

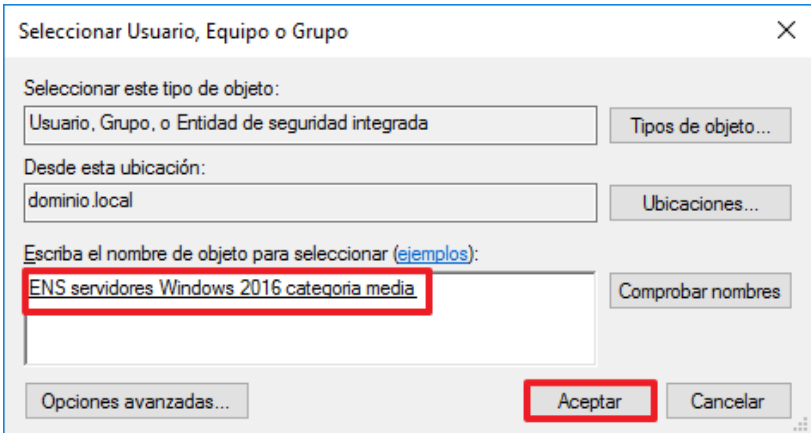
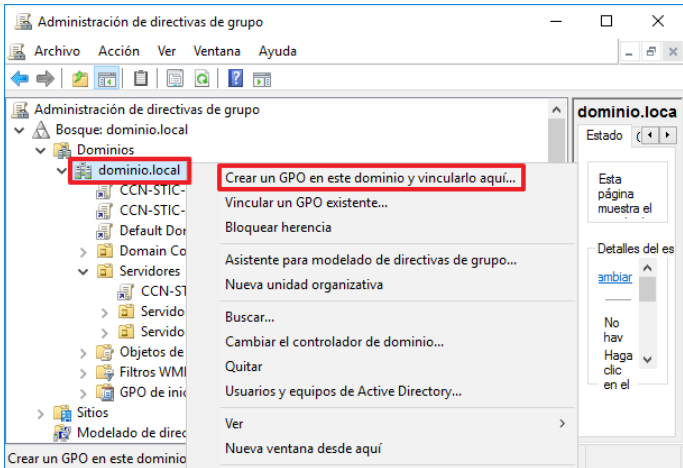
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100. | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón <b>“Herramientas → Administración de directivas de grupo”</b>.</p>                                                                                                               |
| 101. | <p>A continuación, despliegue el nodo <b>“Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”</b>.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p>                             |
| 102. | <p>Seleccione <b>“Vincular un GPO existente...”</b> y vincule el objeto de directiva de grupo <b>“CCN-STIC-574 ENS Incremental IIS 10”</b> a la nueva unidad organizativa <b>“Servidores Entidad de Certificación”</b>, haciendo clic con el botón derecho sobre ella.</p>  |

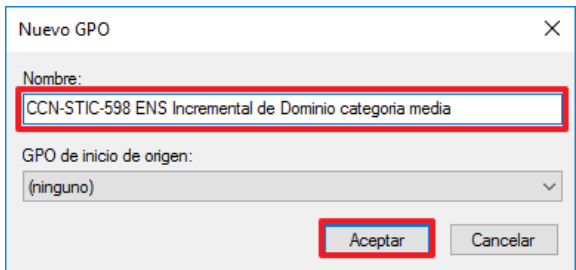
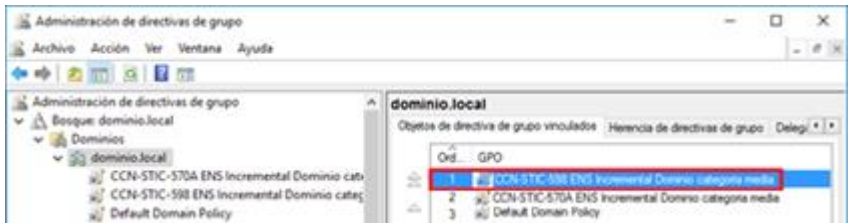
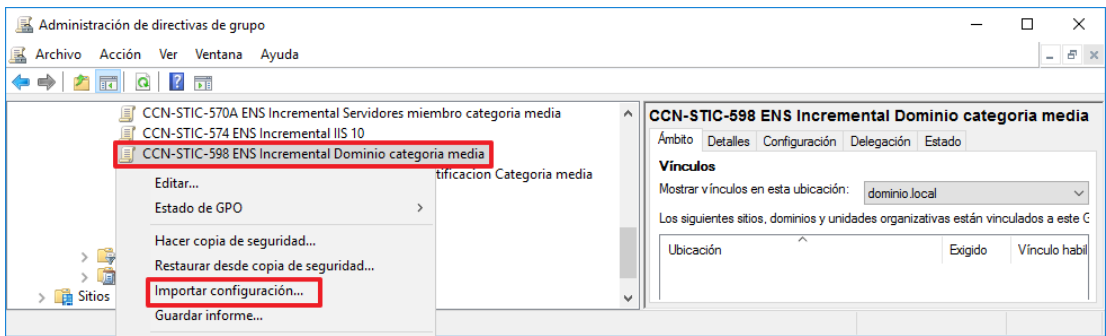
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 103. | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>  |
| 104. | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” y haga clic en el botón “Aceptar”.</p>                                                                                                                   |

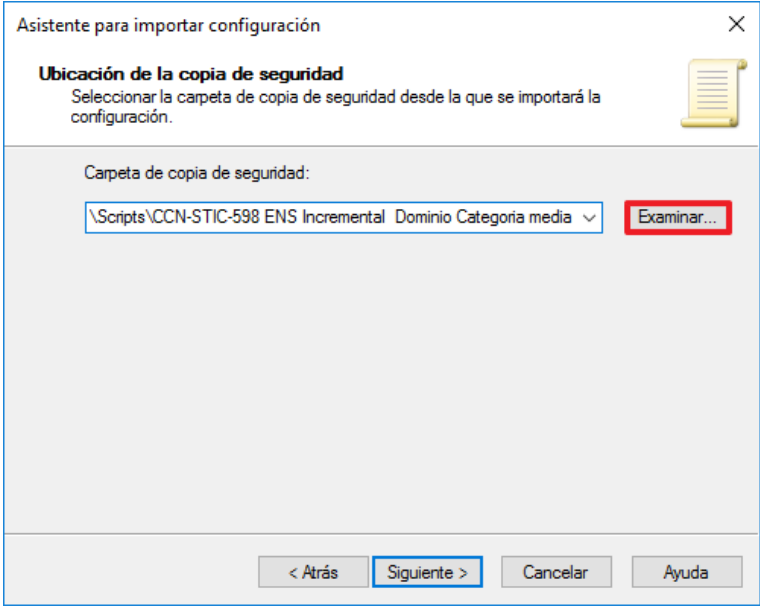
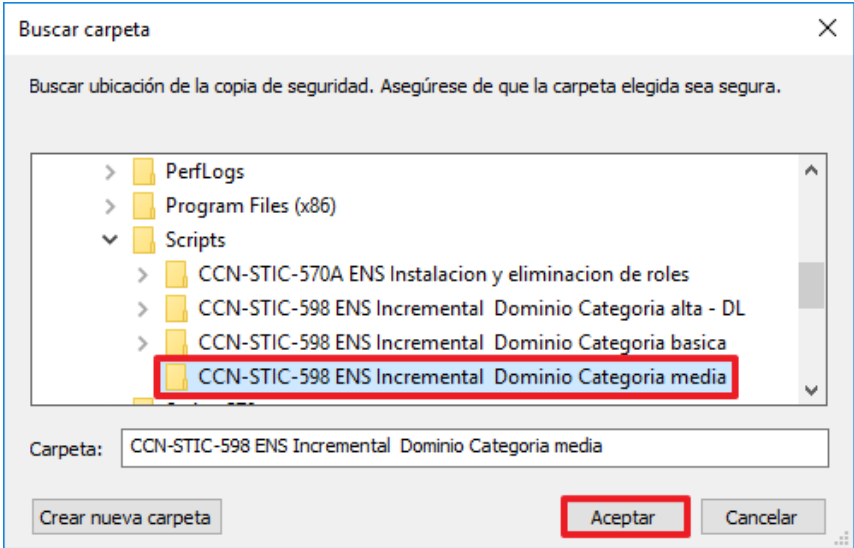
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 105. | <p>Seleccione la unidad organizativa <b>“Servidores Entidad de Certificación”</b>.<br/>En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  |
| 106. | De esta forma, se garantiza que la directiva se aplica correctamente.                                                                                                                                                                                                                                                                                         |
| 107. | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción <b>“Editar”</b>.</p>                                                                                                                         |
| 108. | <p>Expanda el nodo <b>“Configuración del equipo → Directivas→ Configuración de Windows → Configuración de seguridad”</b>.</p>                                                                                                                                                                                                                                 |

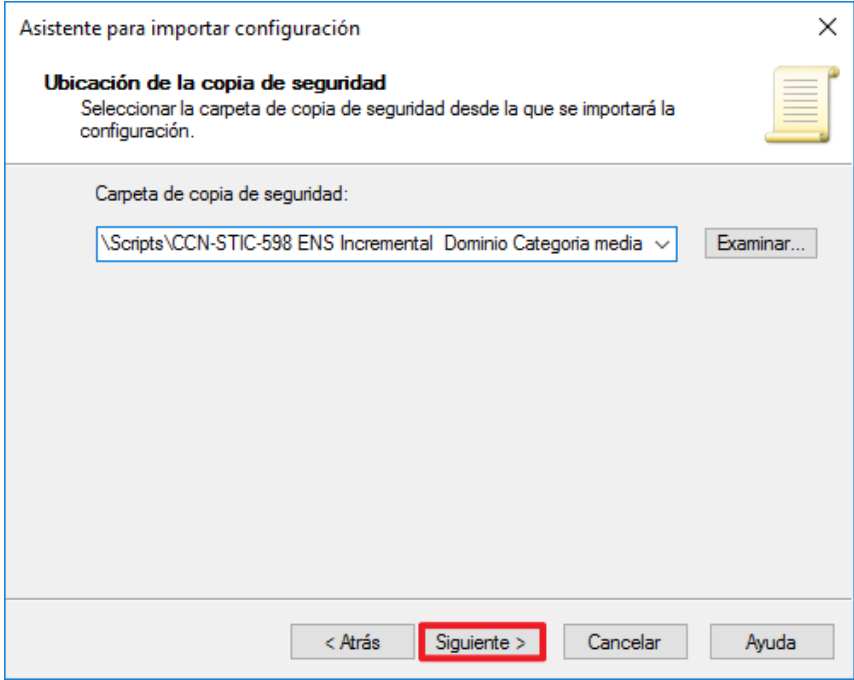
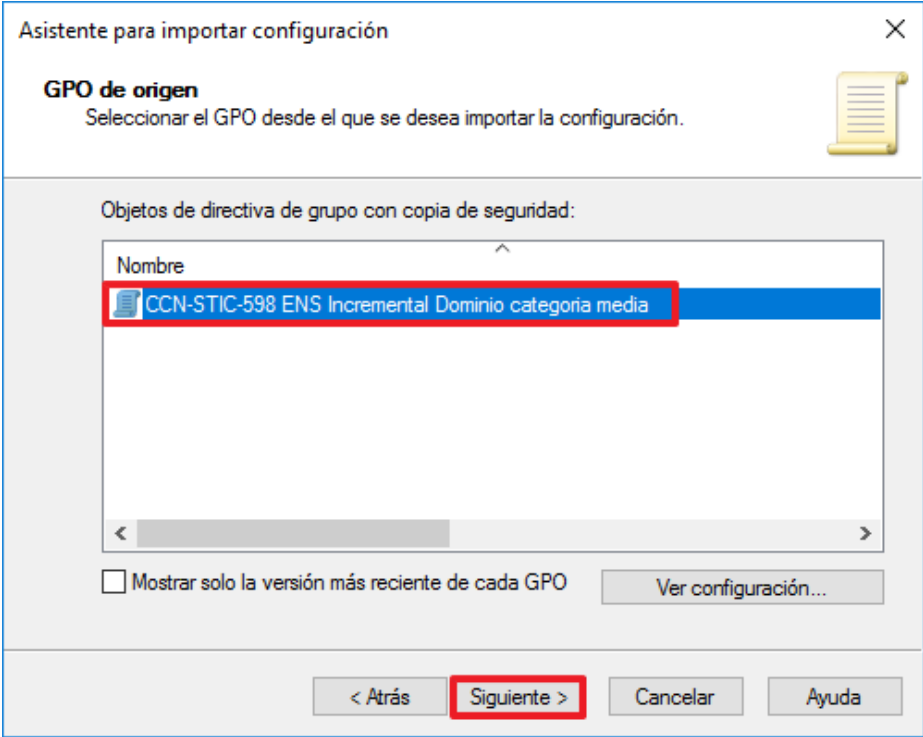
| Paso | Descripción                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 109. | <p>Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.</p>                                                  |
| 110. | <p>Seleccione la plantilla “C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría media.inf”. Haga clic en el botón “Abrir”.</p>  |
| 111. | <p>Cierre el “Editor de administración de directivas de grupo”.</p>                                                                                                                                                                                     |

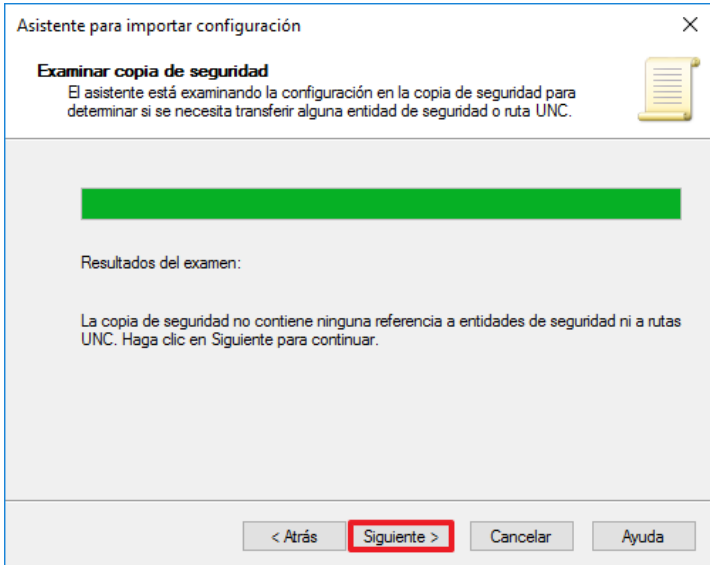
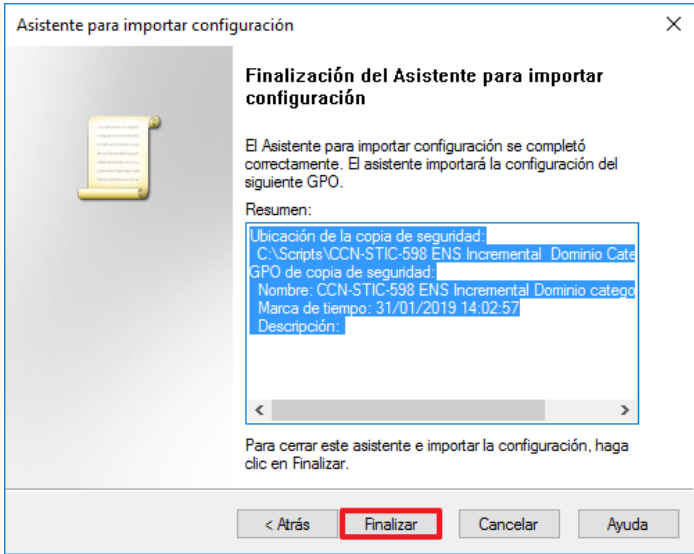
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 112. | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>                                                           |
| 113. | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>  |

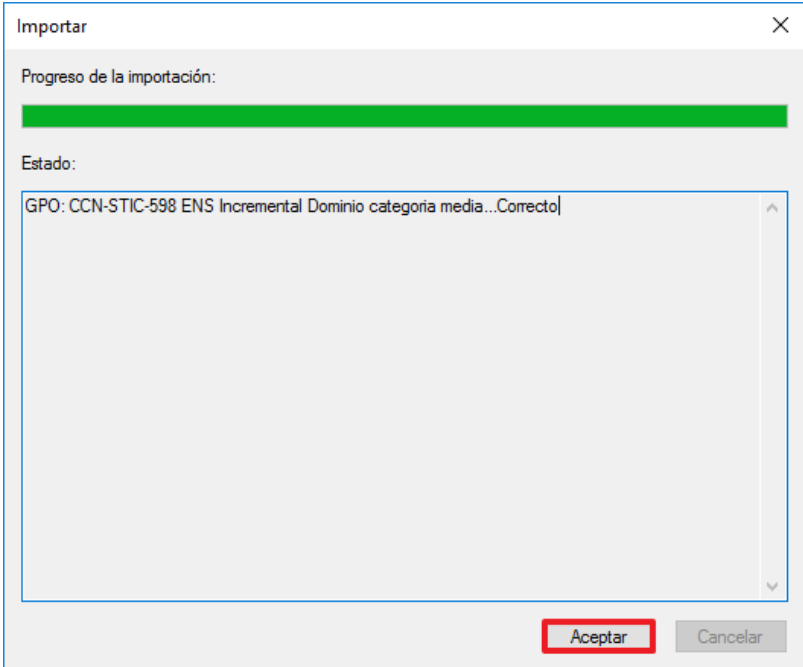
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 114. | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidores Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria media” que contiene el servidor con el rol “Servidores Entidad de Certificación”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 115. | Cierre la ventana “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 116. | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 117. | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Paso | Descripción                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 118. | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 ENS Incremental Dominio categoría media” y pulse el botón “Aceptar”.</p>                                                                                       |
| 119. | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>  |
| 120. | <p>Despliegue el contenedor “Objetos de directiva de grupo” y haga clic derecho sobre la GPO recién creada “CCN-STIC-598 Incremental Dominio categoría media” seleccionando la opción “Importar configuración...”.</p>   |
| 121. | <p>Haga clic en “Siguiente &gt;” en el “Asistente para importar configuración”.</p>                                                                                                                                                                                                                          |

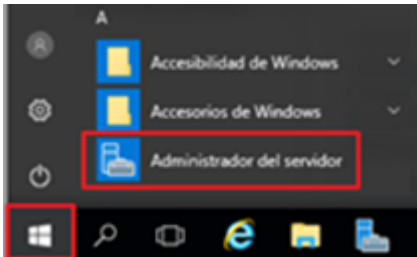
| Paso | Descripción                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 122. | <p>Haga clic en “Examinar...”.</p>                                                                                                                                         |
| 123. | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoria media” y pulse “Aceptar”.</p>  |

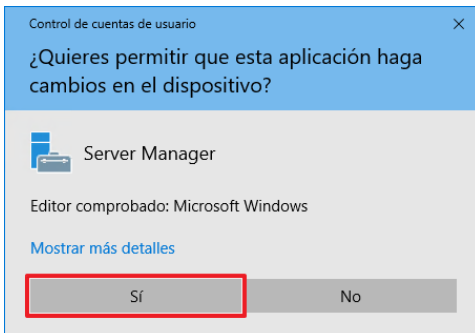
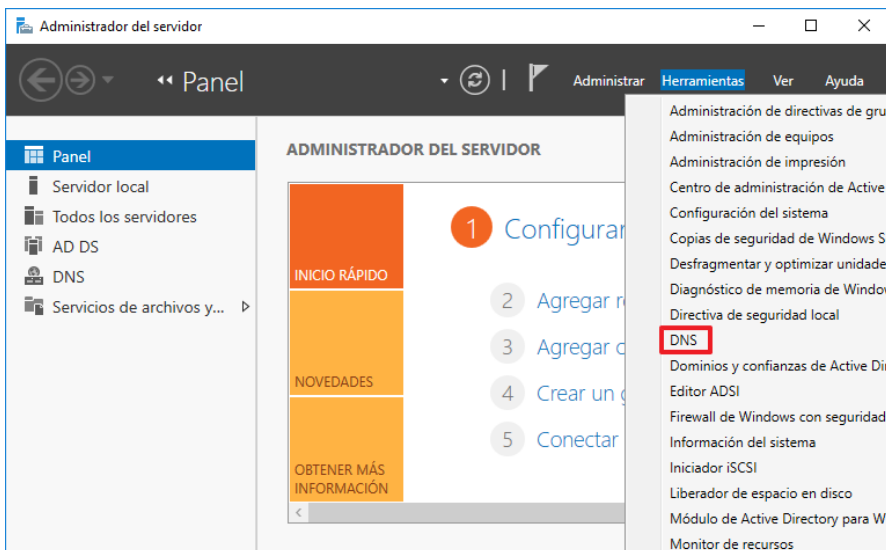
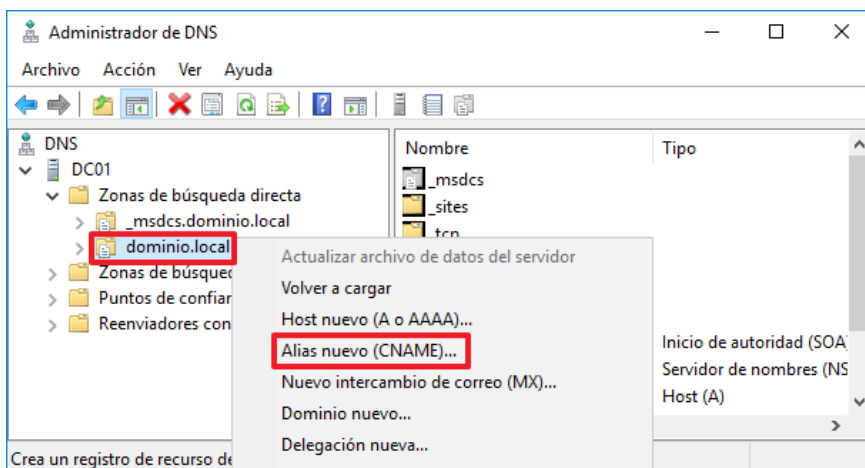
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 124. | <p>Pulse “Siguiente &gt;” para continuar con la importación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 125. | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio Categoría media” y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |

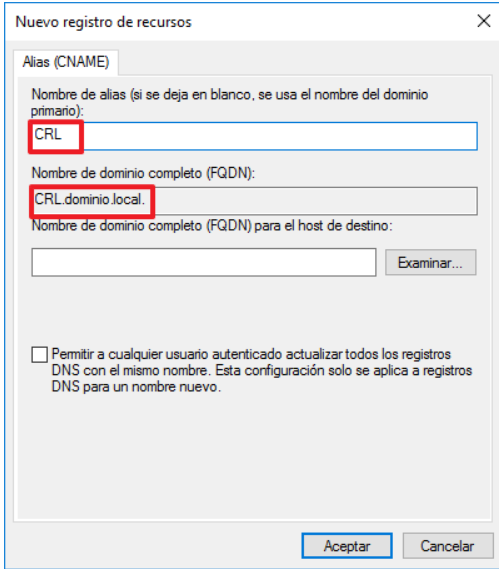
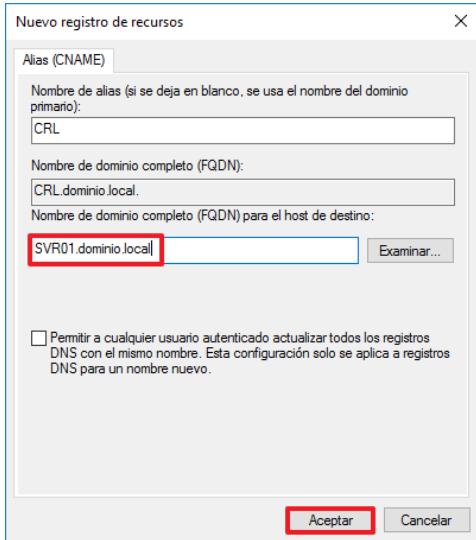
| Paso | Descripción                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 126. | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>  |
| 127. | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                    |

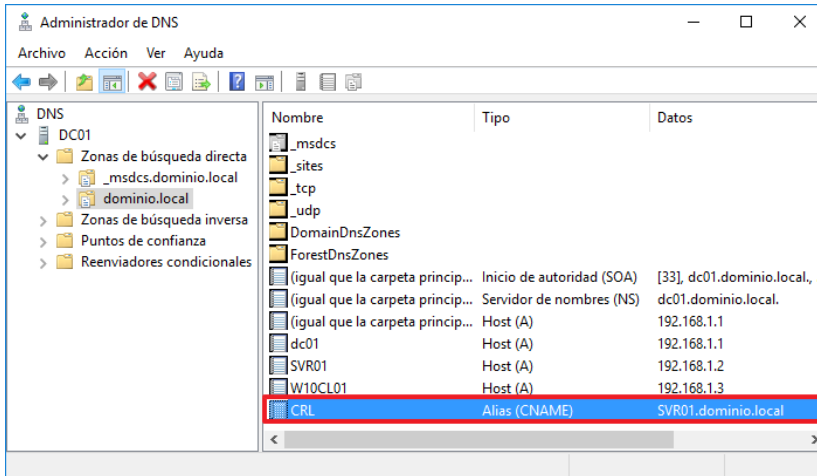
| Paso | Descripción                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 128. | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>  |
| 129. | Cierre la ventana “Administración de directivas de grupo”.                                                                                                                                                                                                         |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

| Paso | Descripción                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 130. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>    |
| 131. | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 132. | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                                                                                                                                                                        |
| 133. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>                                                                                                                                                       |
| 134. | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: <b>“&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”</b>.<br/>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>  |

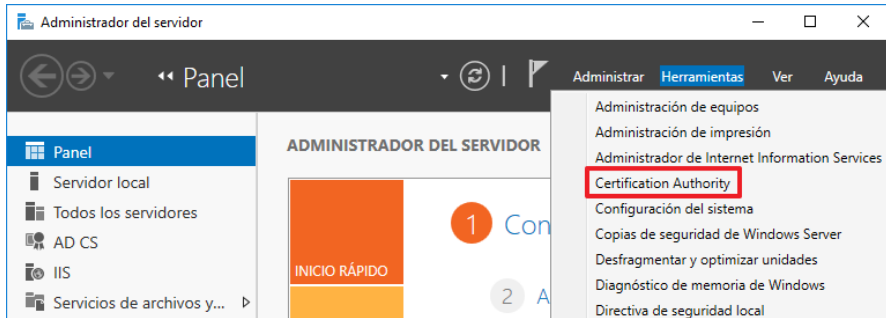
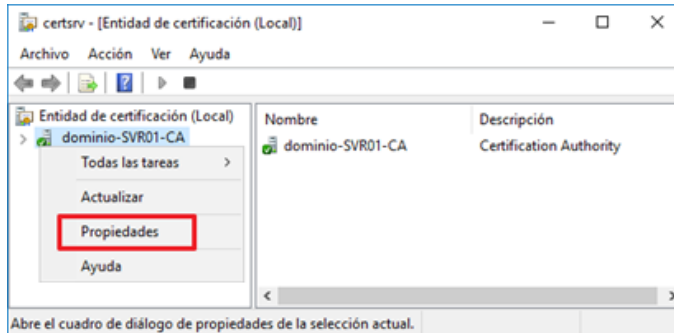
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 135. | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |
| 136. | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación subordinada de empresa y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p>         |

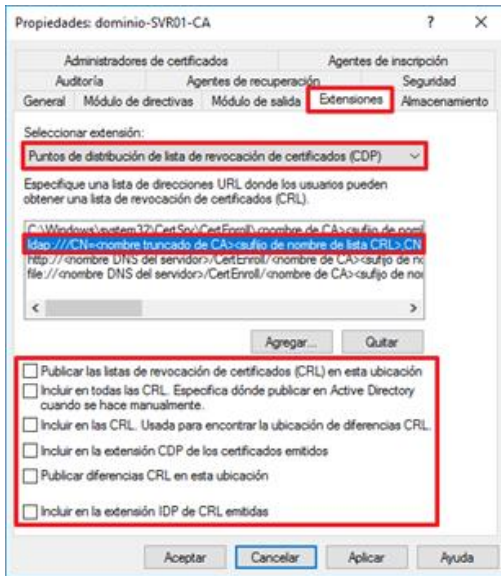
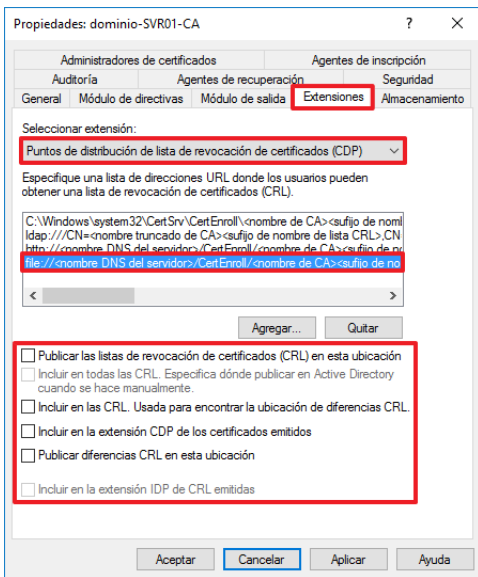
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 137. | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>  <p>The screenshot shows the 'Administrador de DNS' window. In the left pane, the tree structure is expanded to 'Zonas de búsqueda directa' &gt; 'dominio.local'. The right pane displays a list of DNS records. The record 'CRL' is highlighted with a red box. It is of type 'Alias (CNAME)' and its data field is 'SVR01.dominio.local'.</p> |

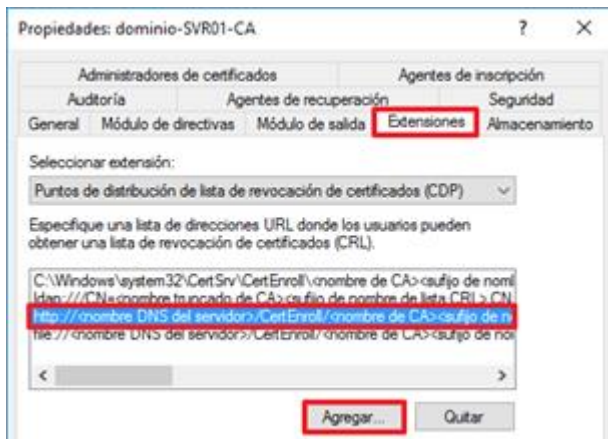
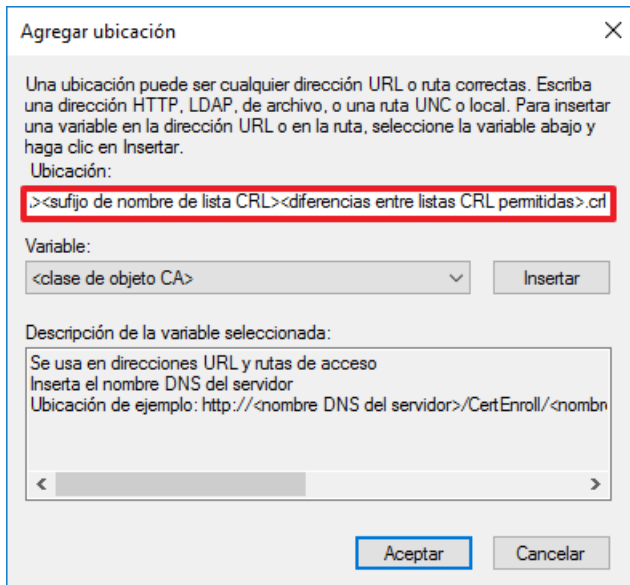
## 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.

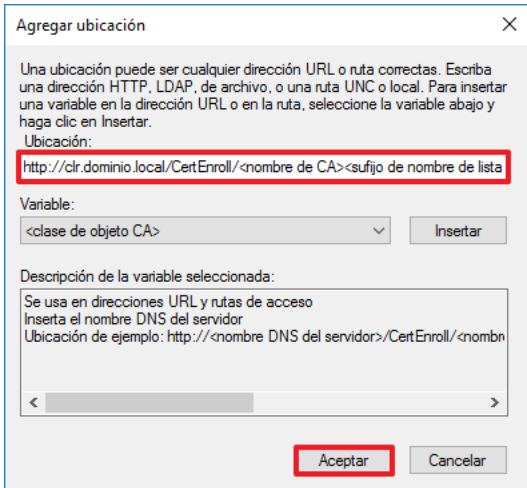
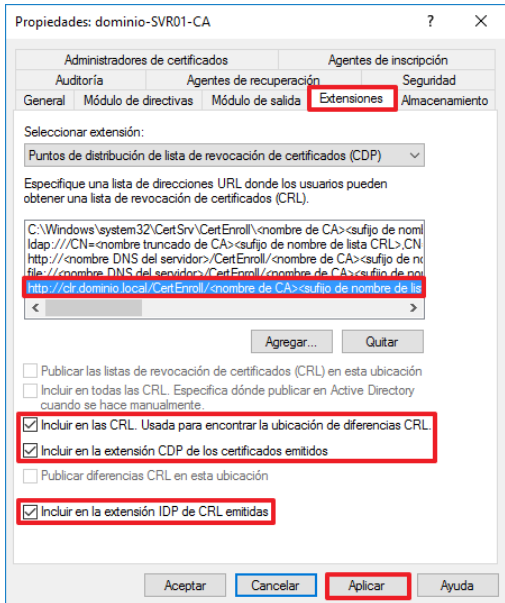
Los pasos que se describen a continuación se realizarán sobre el servidor miembro de Entidad de Certificación subordinada del dominio.

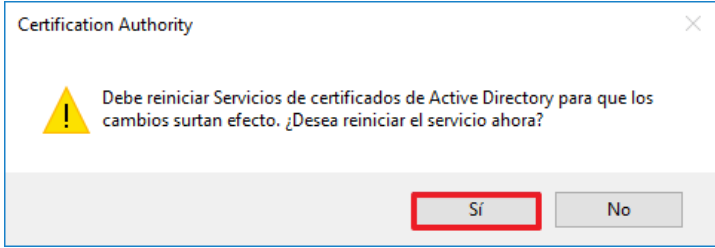
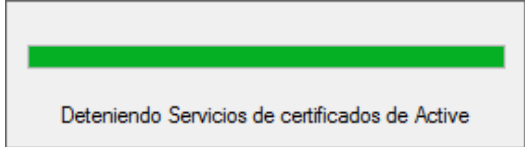
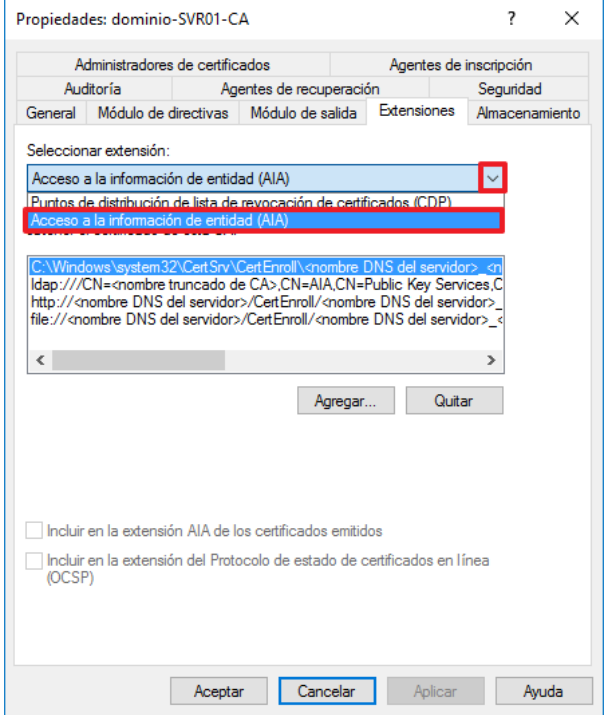
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 138. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece la Entidad Certificadora subordinada.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>                                                                                                                                                                                               |
| 139. | <p>Ejecute la consola administrativa "Certification Authority". Para ello ejecute el "Administrador del servidor" desde el icono correspondiente.</p>  <p>The screenshot shows the Windows taskbar with several icons. The icon representing the 'Administrador del servidor' (Server Manager) is highlighted with a red box.</p> |
| 140. | <p>El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.</p>                                                                                                                                                                                                                                                                                                       |

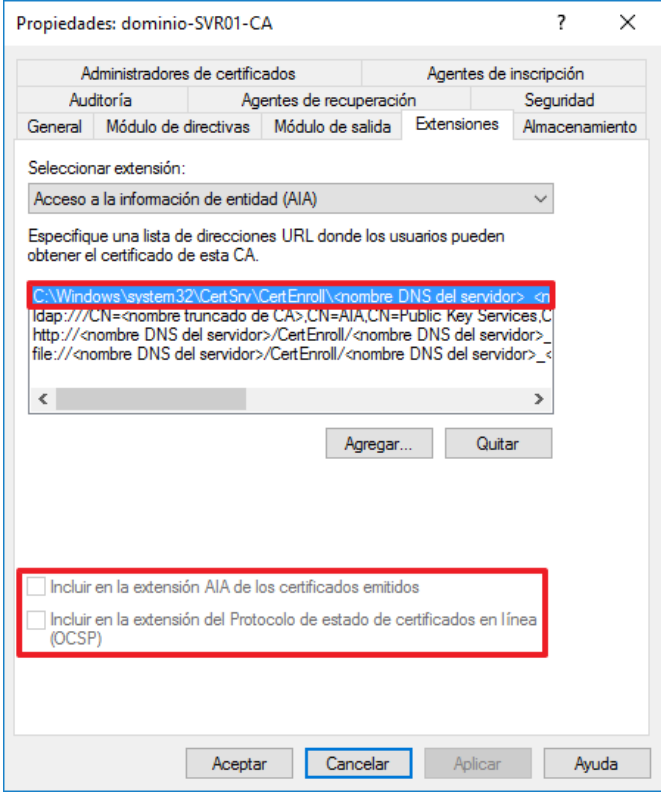
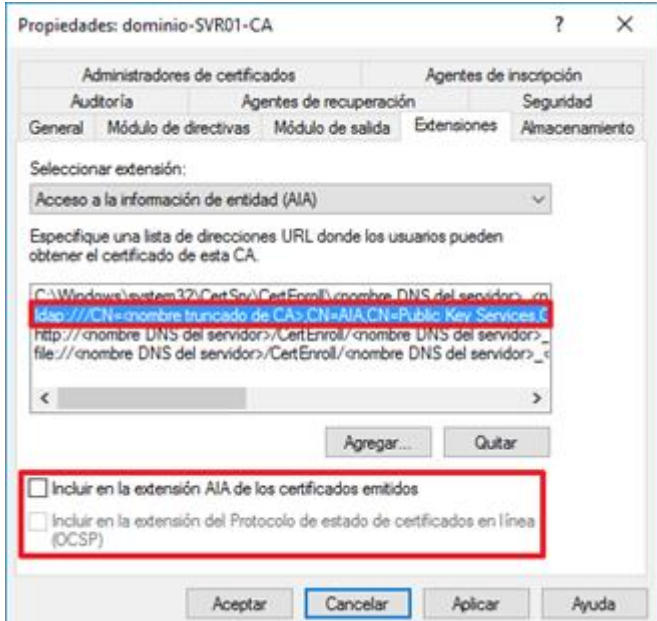
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 141. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 142. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente y con el botón derecho del ratón seleccione “Propiedades”.</p>                                                                                                                                                                                                                                                                                                                                                                                   |
| 143. | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\<nombre b="" ca&gt;&lt;="" crl="" crl&gt;&lt;diferencias="" de="" entre="" lista="" listas="" nombre="" permitidas&gt;.crl”<="" sufijo=""> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</nombre></b></p>  |

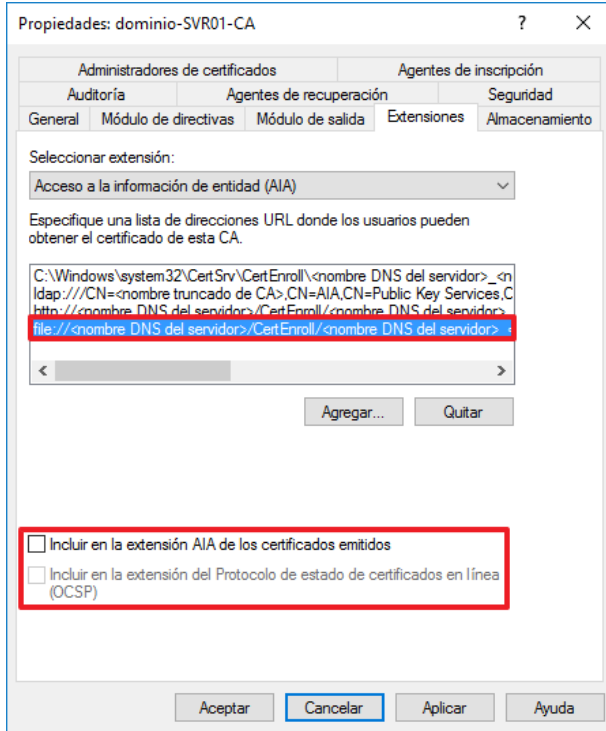
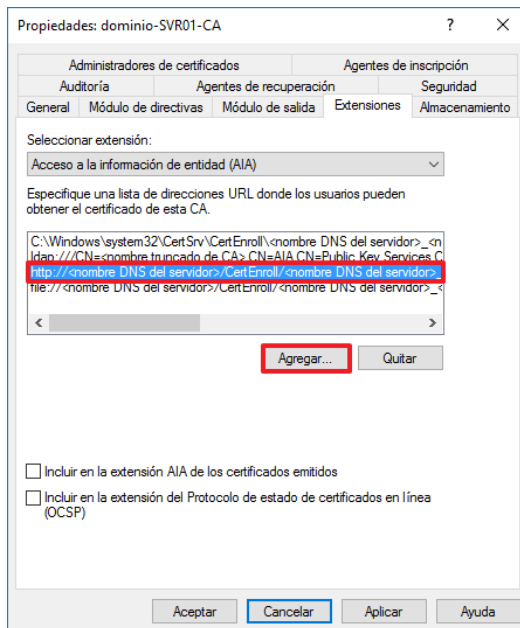
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 144. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando “<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>” y desmarcando todas las opciones.</p> <p>Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>  |
| 145. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “<b>file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y desmarque todas las opciones como muestra la siguiente figura:</p>                                                                                                                                                                  |

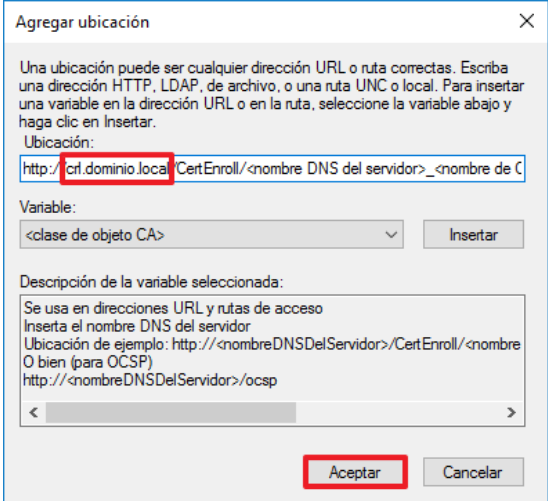
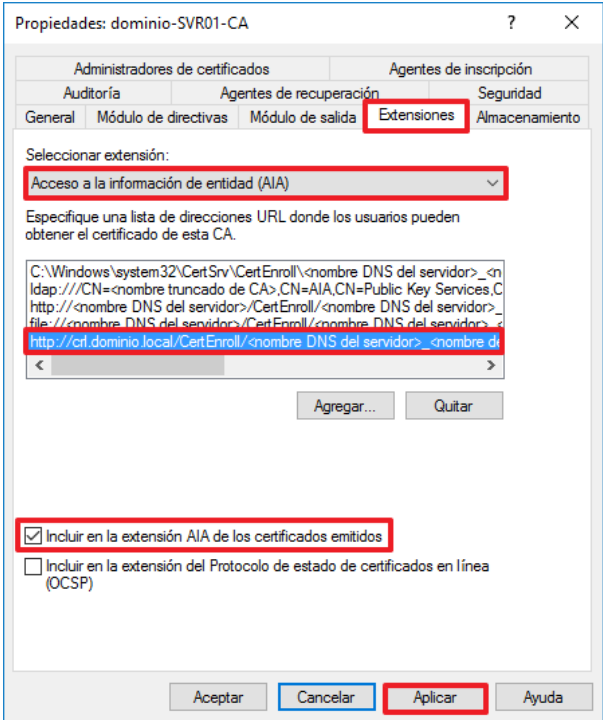
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 146. | De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto. |
| 147. | Pulse el botón “Agregar”.                                                                                                                                                                                                                                                                           |
| 148. | Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.                                                                                                                                                   |

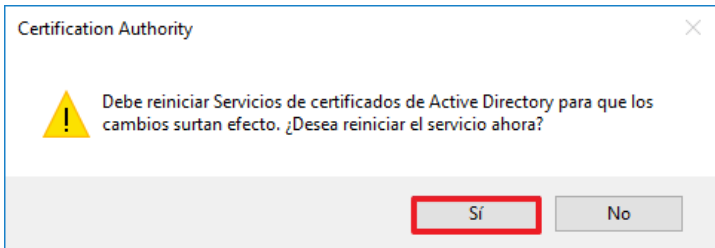
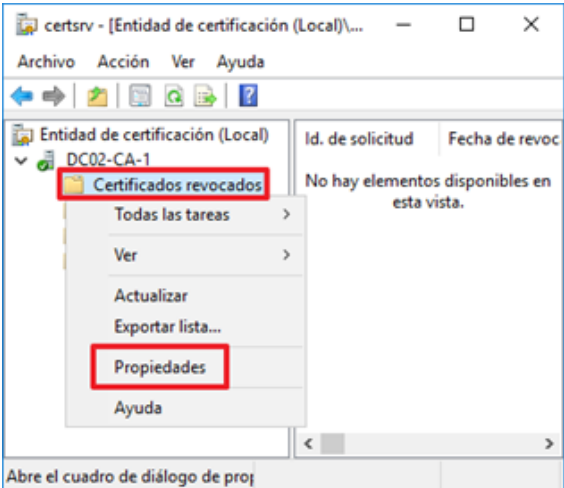
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 149. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creó anteriormente (Punto 2.3 PREPARACIÓN DEL DIRECTORIO ACTIVO) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                              |
| 150. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufrido de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos</li> <li>– Incluir en la extensión IDP de CRL emitidas</li> </ul> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

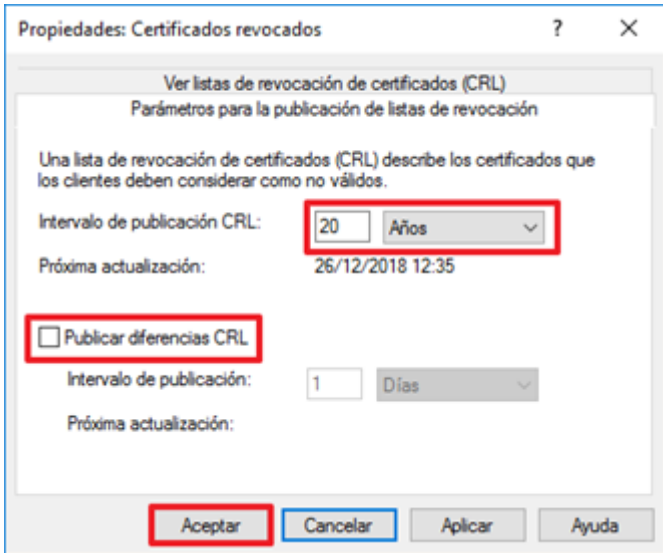
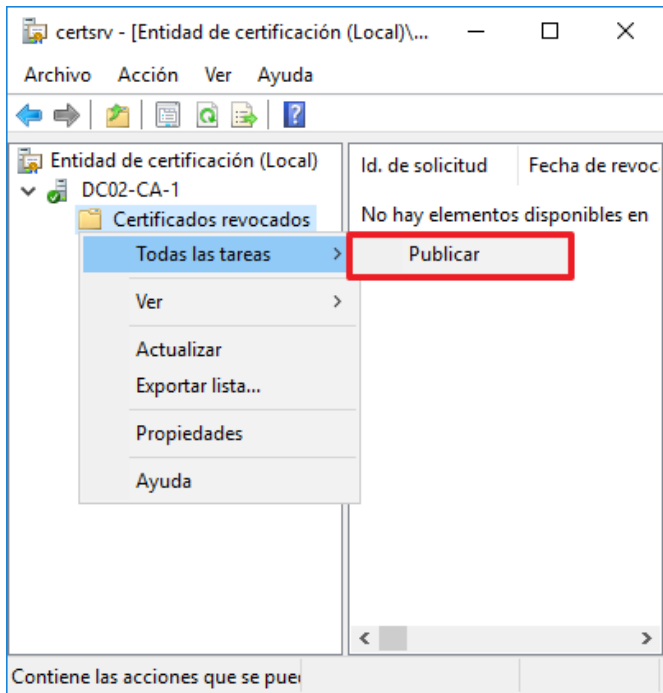
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 151. | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 152. | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 153. | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

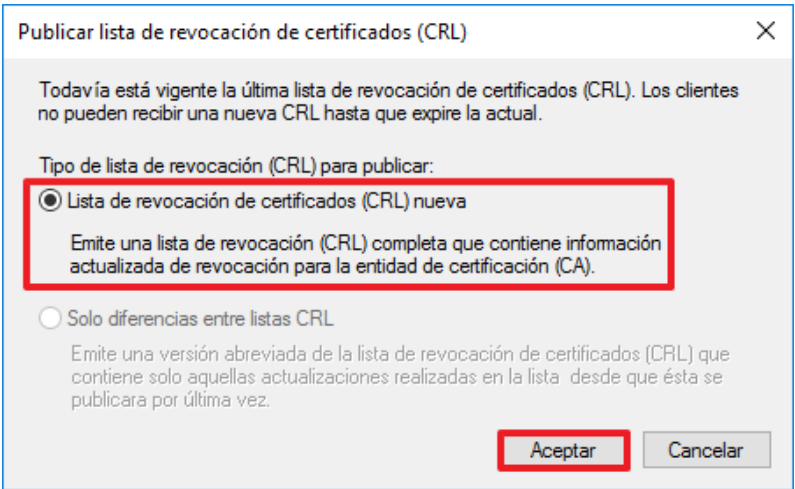
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 154. | <p>Compruebe que en el objeto <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt”</b> todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura:</p>                     |
| 155. | <p>Compruebe que en el objeto <b>“ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;”</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura:</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 156. | <p>Seleccione ahora “file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y desmarque la opción “Incluir en la extensión AIA de los certificados emitidos”.</p>  |
| 157. | <p>Seleccione “http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y copie el elemento mediante la combinación de teclas “Control + C”.</p>                                                                                                        |
| 158. | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                    |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 159. | Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.                                                                                                                                                                                                                                                                                                                                                                          |
| 160. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios:</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                      |
| 161. | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora “http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>  |

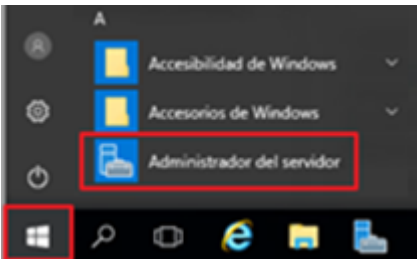
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 162. | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 163. | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 164. | <p>El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL y al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.</p>                                                                                                                                                                                                                                                                                                                                                  |
| 165. | <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:</p> <p><b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b></p> <p>Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>  |

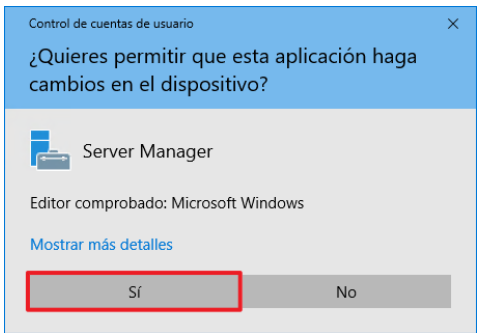
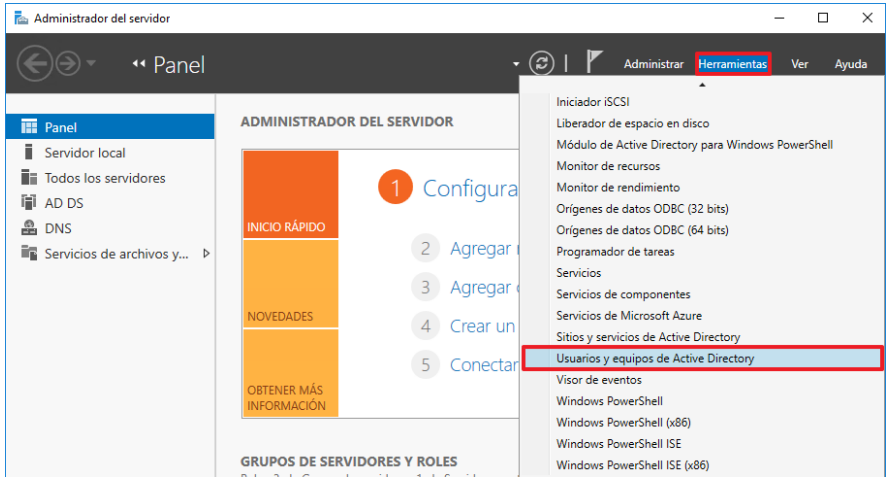
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 166. | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p>  <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p> |
| 167. | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                                                                                                                                                                                                                                                                                          |

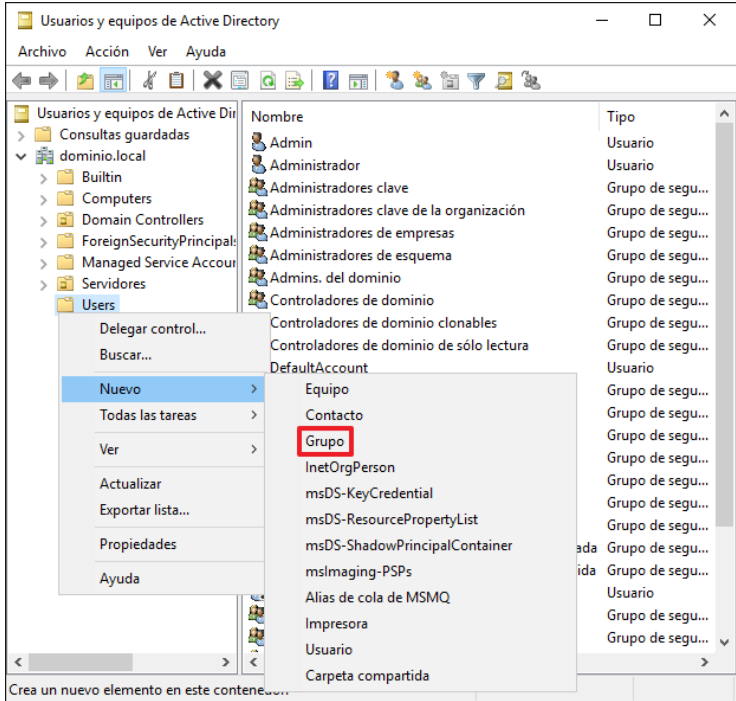
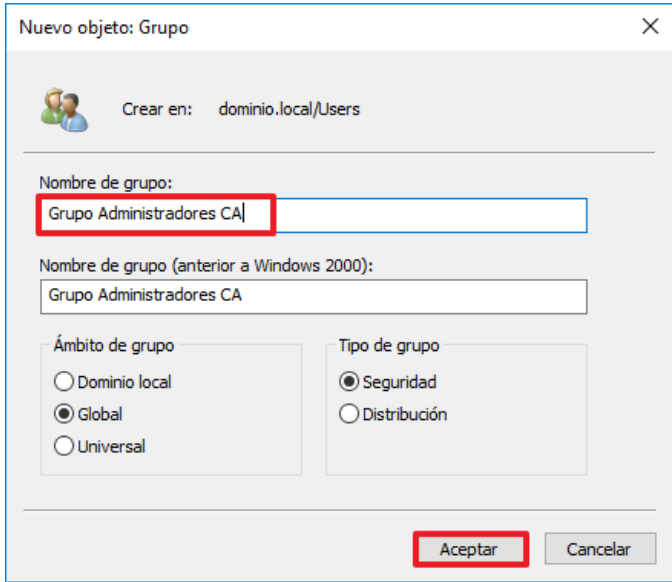
| Paso | Descripción                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 168. | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>  |

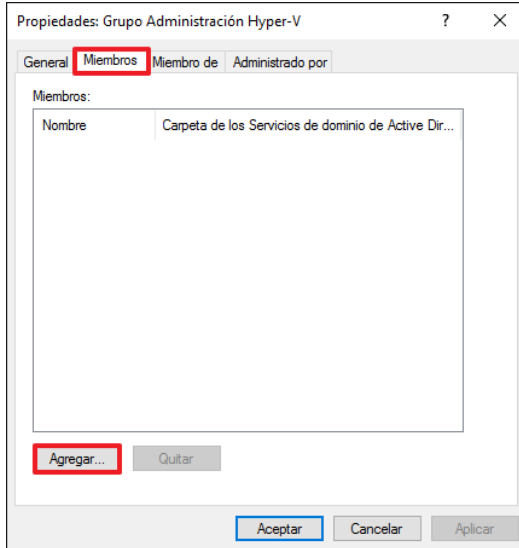
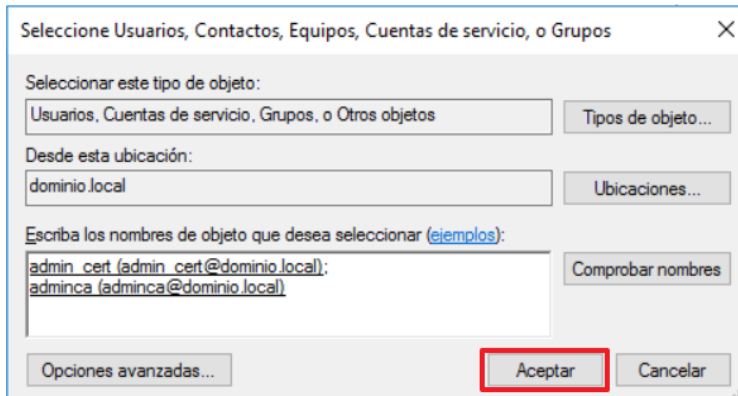
## 2.5. SEGREGACIÓN DE ROLES

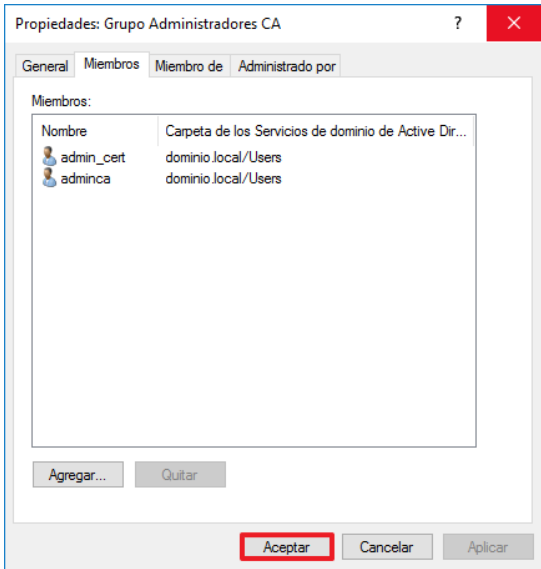
Con la aplicación del ENS para la categoría media sobre el Servidor de Certificación Subordinada de Dominio, será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar el Servidor de Certificación.

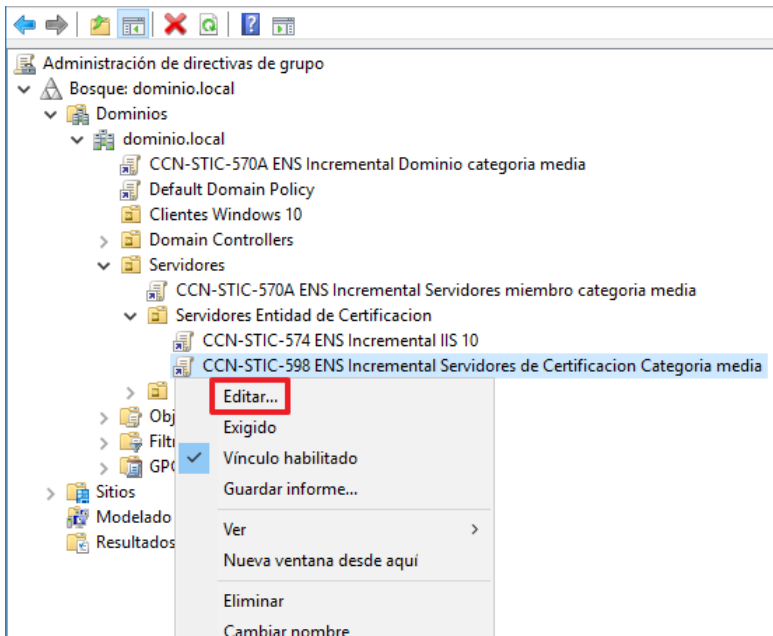
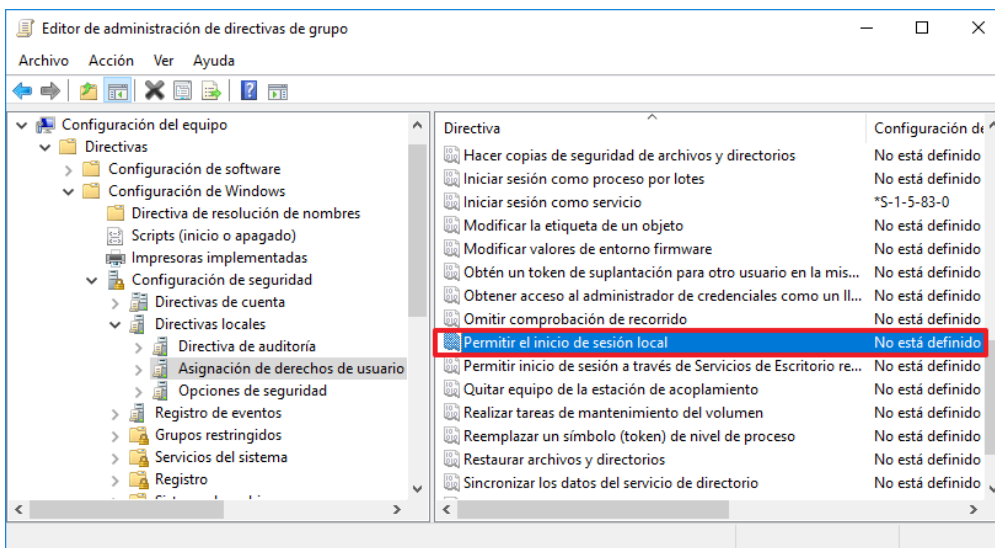
| Paso | Descripción                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 169. | <p>Inicie sesión en el servidor de certificación subordinada donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |
| 170. | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                            |

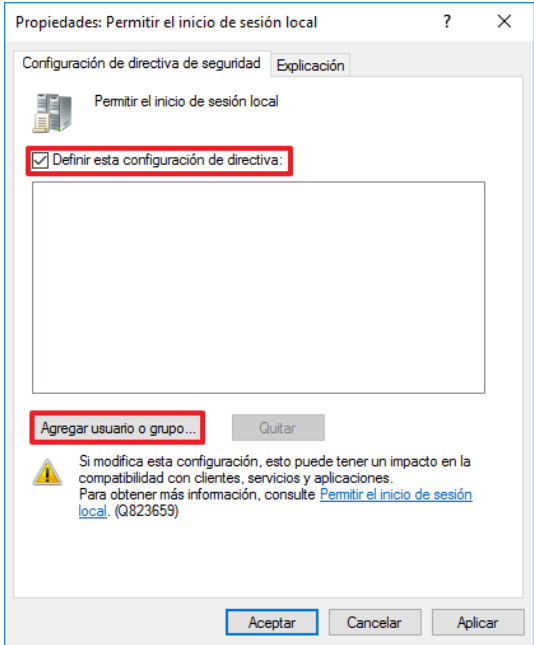
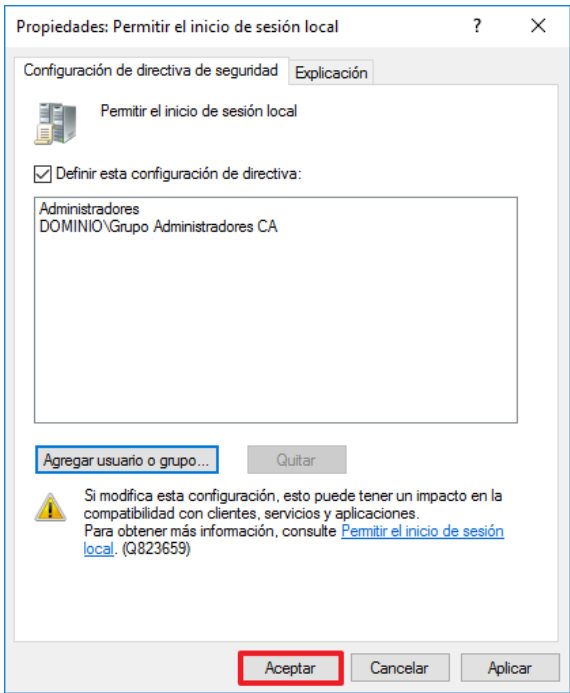
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 171. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                                    |
| 172. | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione <b>“Herramientas → Usuarios y equipos de Active Directory”</b>.</p>  |

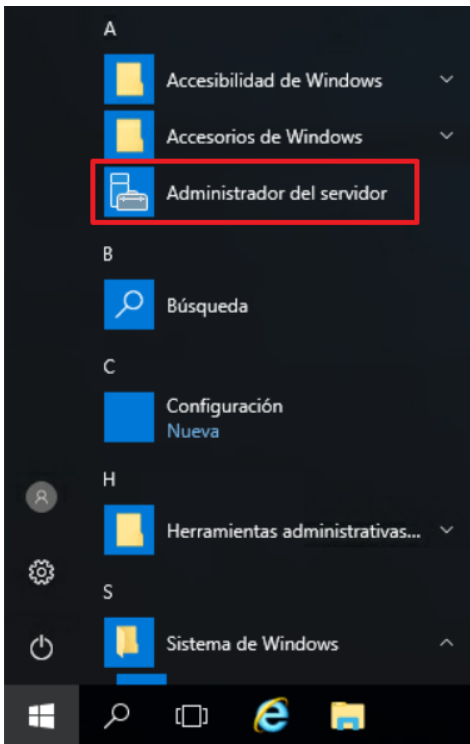
| Paso | Descripción                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 173. | <p>Despliegue el nodo “&lt;&lt;su dominio&gt;&gt; → Users”. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual “Nuevo → Grupo”.</p>       |
| 174. | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |

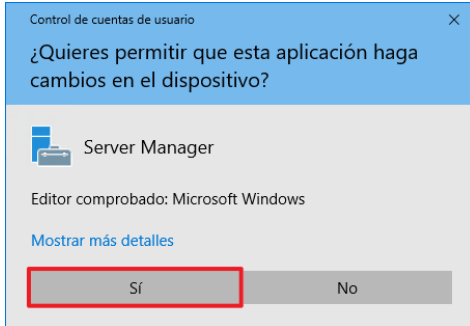
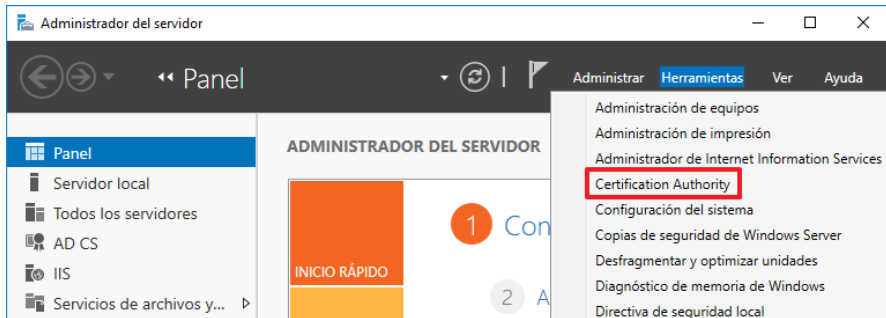
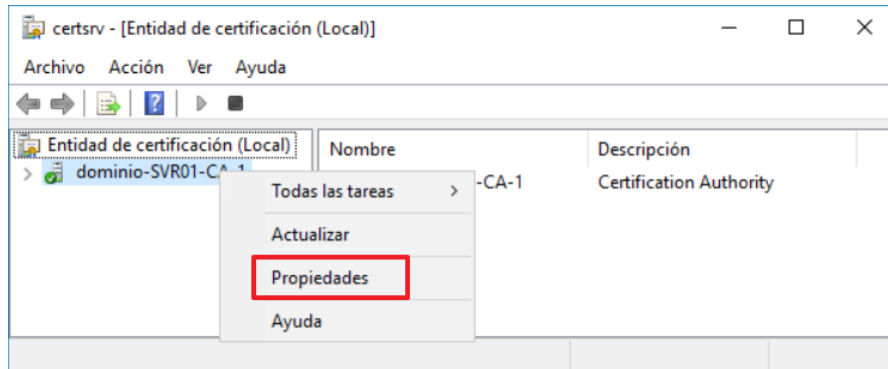
| Paso | Descripción                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 175. | <p>Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>                                              |
| 176. | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la generación de esta guía”.</p> |

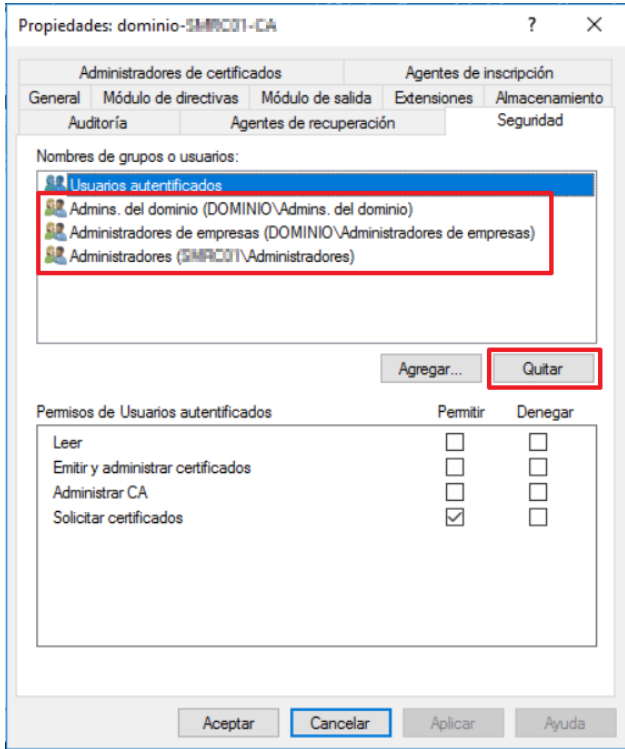
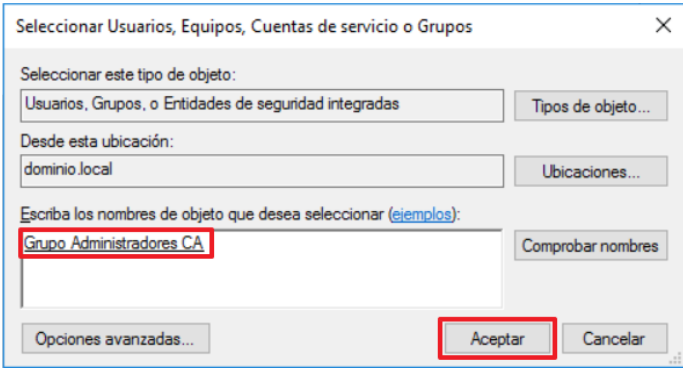
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 177. | <p>Pulse “Aceptar” cuando haya finalizado.</p>                                                                                                                                                                                                                                            |
| 178. | <p>A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione <b>“Herramientas → Administración de directivas de grupo”</b>.</p>  |

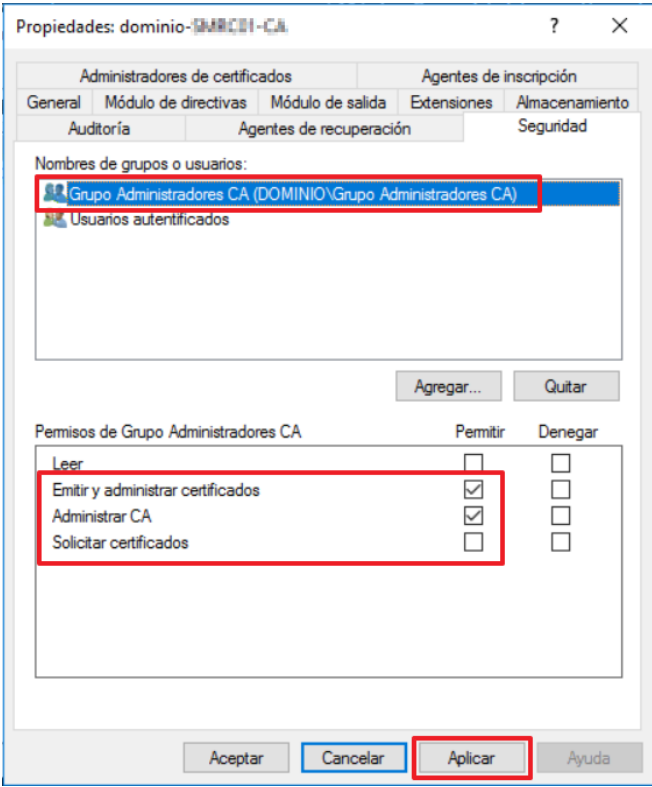
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 179. | <p>Expanda el árbol <b>“Bosque:&lt;nombre de su bosque&gt; → Dominios → &lt;nombre de su dominio&gt;”→“Servidores” → “Entidad certificadora”</b> y pulse con el botón derecho el objeto GPO denominado <b>“CCN-STIC-598 Incremental Servidor Entidad de Certificacion Categoria media”</b>, y seleccione la opción del menú contextual <b>“Editar...”</b>.</p>  |
| 180. | <p>Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. <b>“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</b>.<br/>Haga doble clic en el panel derecho sobre la directiva <b>“Permitir el inicio de sesión local”</b>.</p>      |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 181. | <p>Marque la casilla “Definir esta configuración de directiva:” y pulse sobre “Agregar usuario o grupo...”.</p>                                                                                                                                                                                                                                                     |
| 182. | <p>Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor de Entidad de Certificación. Pulse “Aceptar” cuando haya finalizado.</p>  <p><b>Nota:</b> En este ejemplo se hace uso del grupo denominado “Grupo Administración CA”. Deberá adaptar esta configuración a las necesidades de su organización.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 183. | <p>A continuación, inicie sesión en el Servidor de Entidad de Certificación Subordinada.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador del dominio.</p> |
| 184. | <p>A continuación, ejecute la consola administrativa "Certification Authority". Para ello, clic en <b>"Inicio de Windows → Administrador del servidor"</b>.</p>                  |

| Paso | Descripción                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 185. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                    |
| 186. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                            |
| 187. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “dominio-SVR01-CA-1”.</p> |

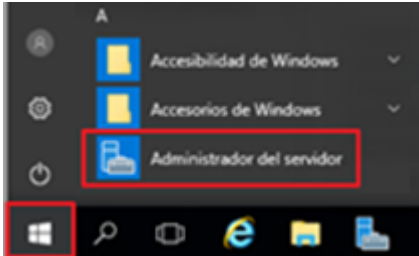
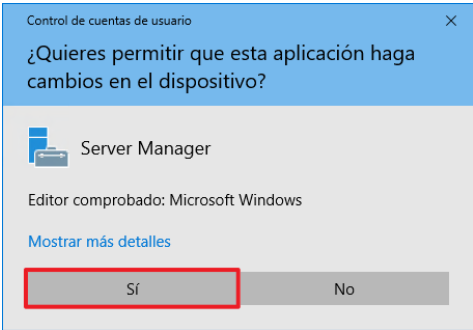
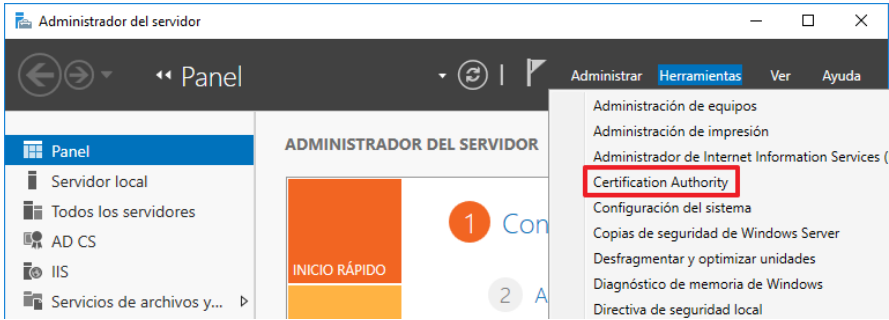
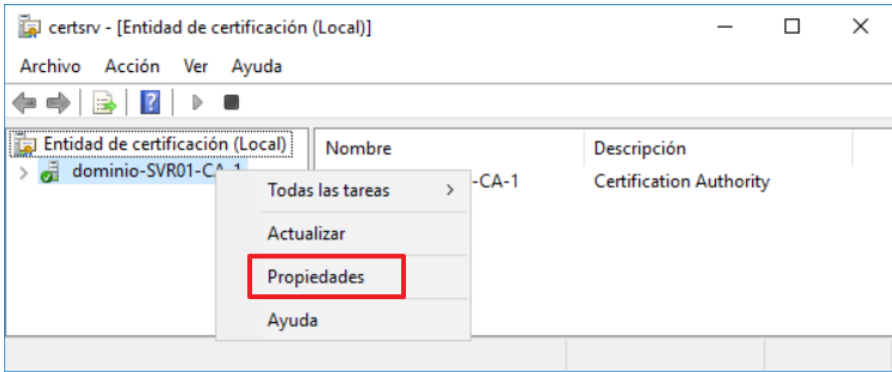
| Paso | Descripción                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 188. | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque uno a uno los grupos Administradores (del dominio, de empresa y locales) y, pulse “Quitar” para eliminar los grupos.</p>  |
| 189. | <p>A continuación, añada el grupo “Grupo Administradores CA” y pulse “Aceptar”.</p>                                                                                                                |

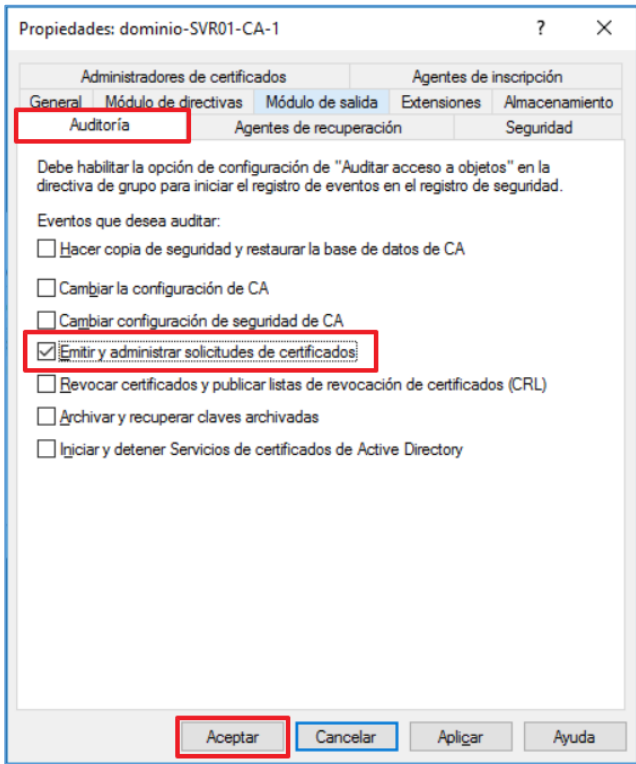
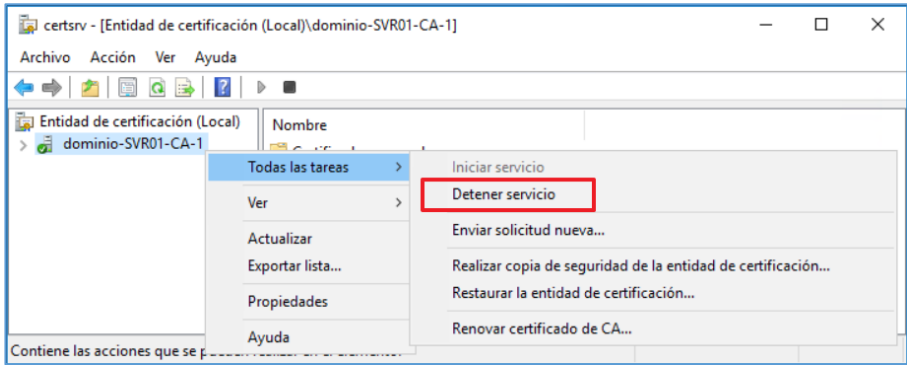
| Paso | Descripción                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 190. | <p>Seleccione el grupo recién añadido, otórguele los permisos “Emitir y administrar certificados” y “Administrar CA” y desmarque la opción “Solicitar certificados”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 191. | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                                                                 |

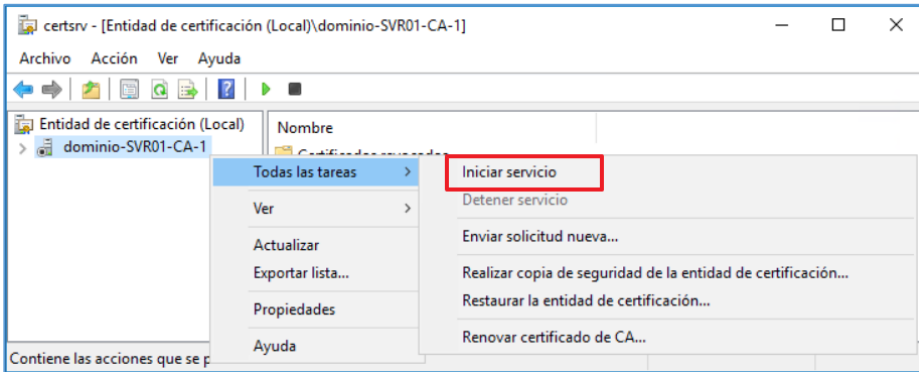
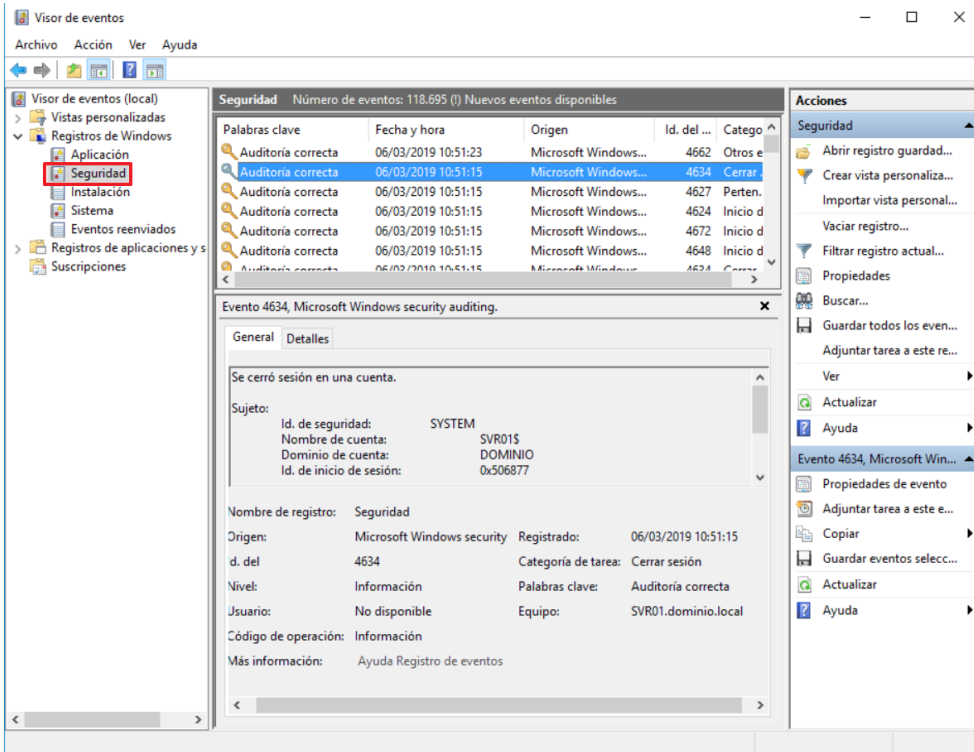
## 2.6. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

Existe la posibilidad de auditar el control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoría de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma, por lo que tendrá que repetir este punto en ambas Entidades de certificación.

| Paso | Descripción                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 192. | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 193. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                                                           |
| 194. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                |
| 195. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                           |
| 196. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “dominio-SVR01-CA-1”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 197. | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: <b>“Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales”</b>.</p> |
| 198. | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú <b>“Todas las tareas → Detener servicio”</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 199. | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú “<b>Acción → Todas las tareas → Iniciar servicio</b>” para iniciarlo de nuevo.</p>                                                                                                                                                                                                                                                                                                                        |
| 200. | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: “<b>Inicio → Herramientas administrativas → Visor de eventos</b>”. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: “<b>Visor de eventos (local) → Registro de Windows → Seguridad</b>”.</p> |

## ANEXO A.3.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.3.3 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MS WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS.

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de entidad de certificación sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría media del ENS.

### 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ

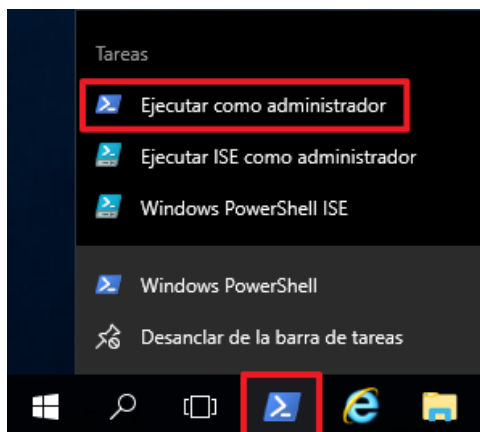
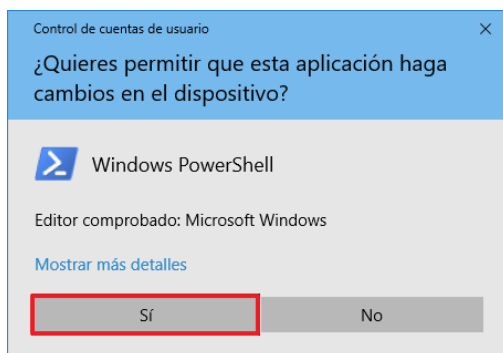
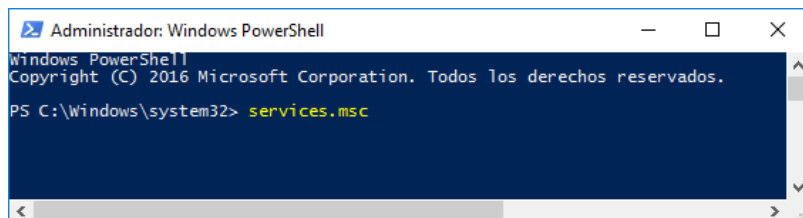
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor independiente con una cuenta de usuario que tenga privilegios de administración.

Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

- a) Consola de servicios (services.msc).
- b) Explorador de Archivos (explorer.exe)

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

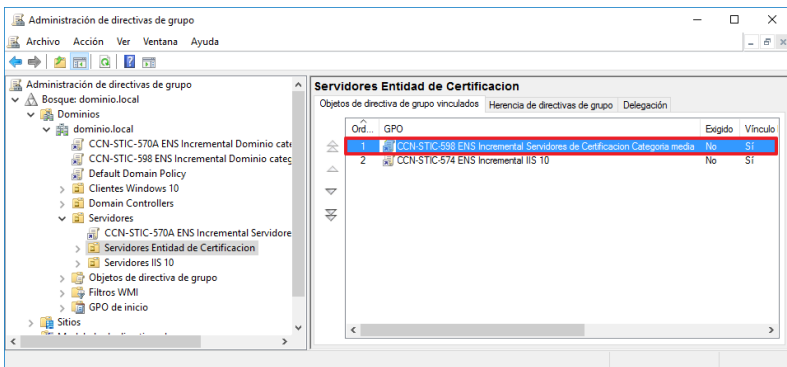
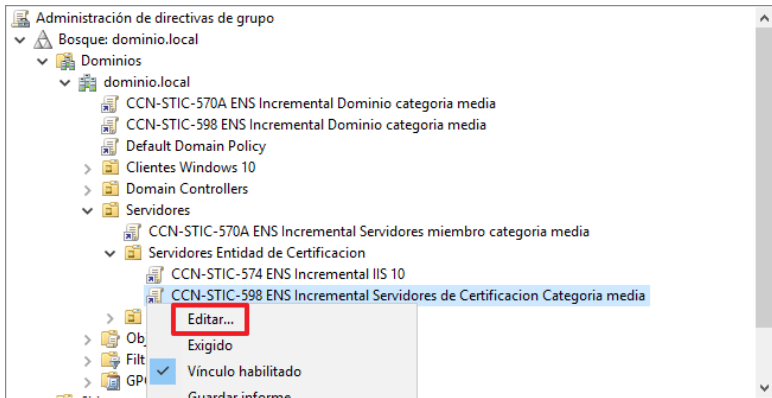
| Comprobación                                                                 | OK/NOK | Cómo hacerlo                                                                                                                      |
|------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor independiente Entidad de Certificación. raíz |        | En el servidor independiente Entidad de Certificación raíz, inicie sesión con una cuenta que tenga privilegios de administración. |

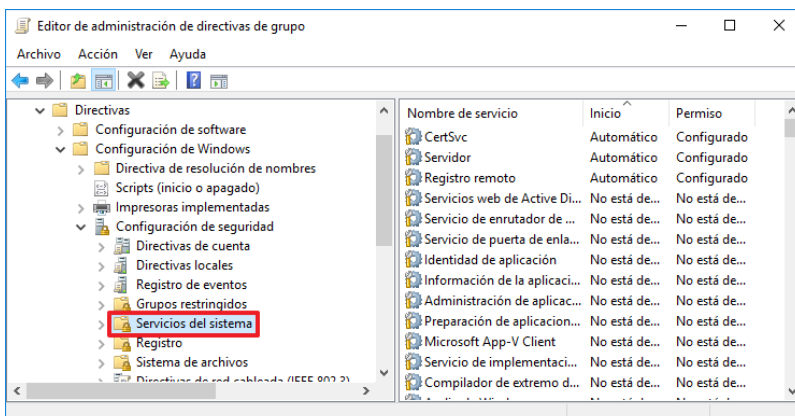
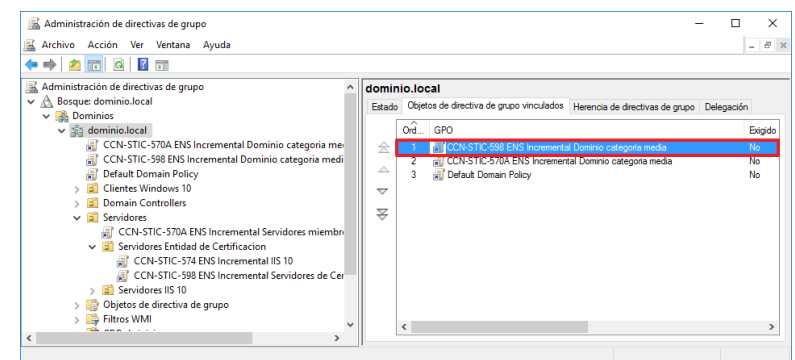
| Comprobación                                                                       | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |        |
|------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| 2. Verifique la correcta aplicación de la configuración de servicios del sistema”. |                         | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse “Sí” en la ventana de “Control de cuentas de usuario”.</p>  <p>Teclee “rsop.msc” en la consola de comandos que se ha abierto:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p> |             |        |
| Servicio (Nombre largo)                                                            | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                      | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |

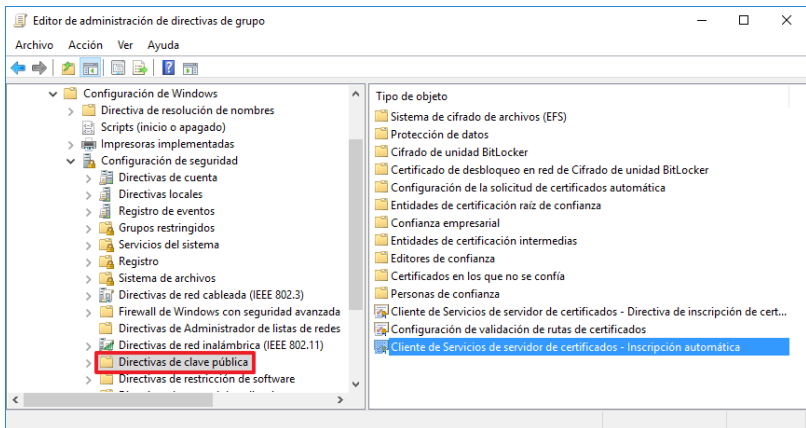
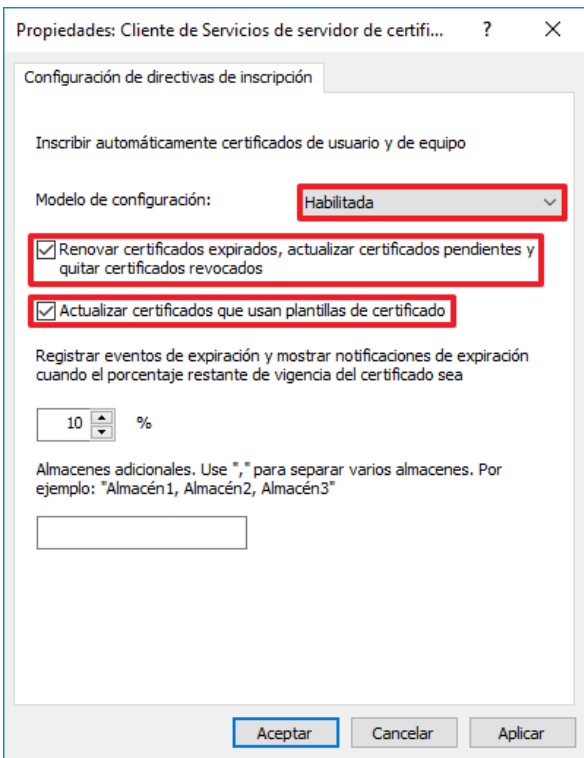
## 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO

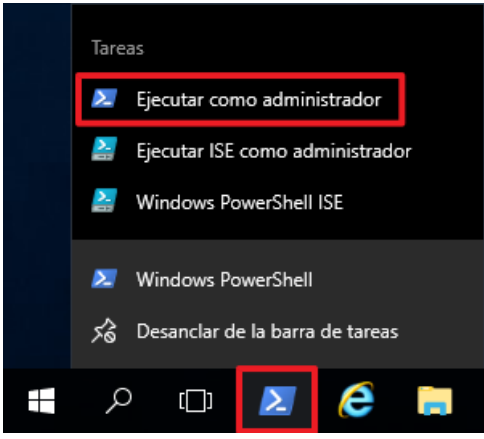
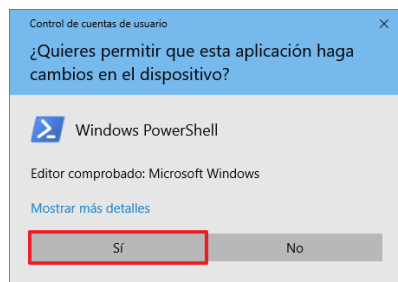
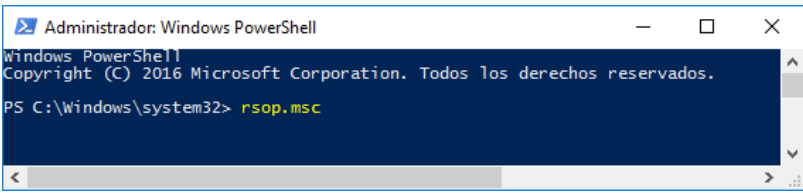
Las consolas y herramientas que se utilizarán son las siguientes:

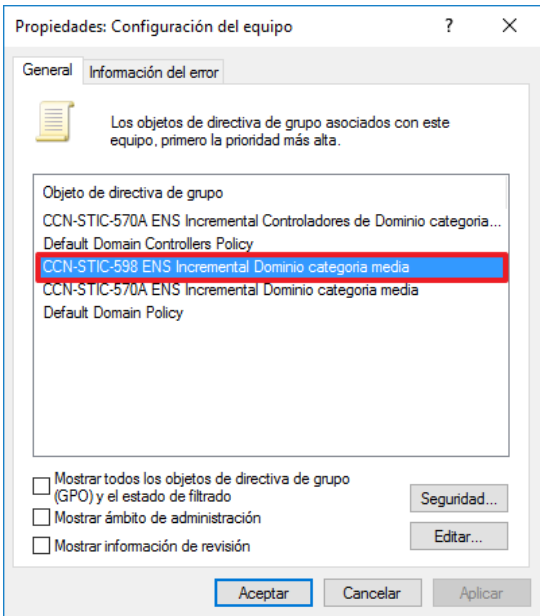
- Administrador de directivas de grupo (gpmc.msc).
- Usuarios y equipos de Active Directory (dsa.msc).
- Conjunto resultante de directivas (rsop.msc).

| Comprobación                                                                                                                       | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en un controlador de dominio.                                                                                     |        | En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”.              |        | <p>Ejecute el “Administrador de directivas de grupo” mediante la siguiente ruta:<br/> <b>“Inicio → Herramientas administrativas → Administración de directivas de grupo”</b></p> <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores Entidad de Certificación”. Verifique que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” está creada y vinculada en el primer lugar de orden de vínculo.</p>  |
| 3. Verifique los servicios del sistema de la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”. |        | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”.</p>  <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:</p>                                                                                                                                                                                                              |

| Comprobación                                                                                      | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |             |        |
|---------------------------------------------------------------------------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                   |                         | <div>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</div> <div></div> <div>Nota: Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</div>                                                                                      |             |        |
| Servicio (Nombre largo)                                                                           | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                     | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |
| Servidor                                                                                          | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |
| Registro Remoto                                                                                   | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Configurado |        |
| 4. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Dominio Categoría media”. |                         | <div>Ejecute el “Administrador de directivas de grupo” a través de la siguiente ruta:<br/>“Inicio → Herramientas administrativas → Administración de directivas de grupo”</div> <div>Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política “CCN-STIC-598 ENS Incremental Dominio categoría media” está creada y vinculada en el primer lugar de orden de vínculo.</div> <div></div> |             |        |

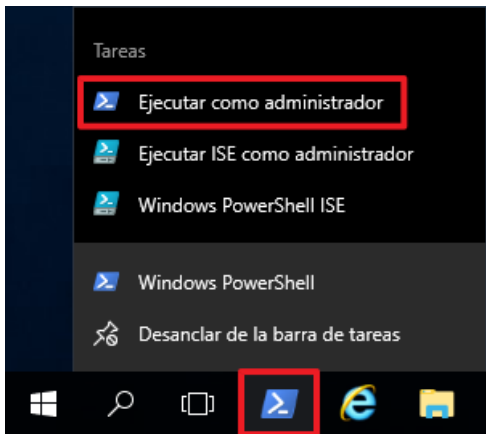
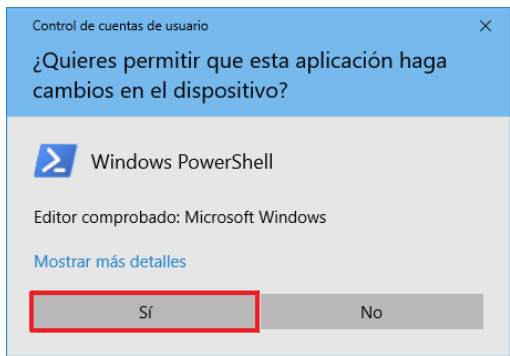
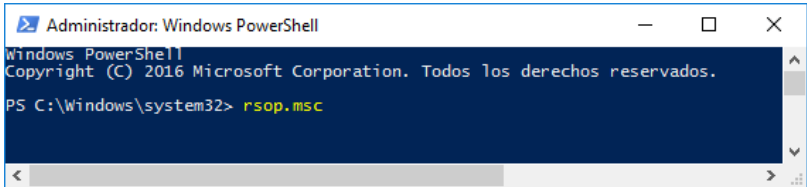
| Comprobación                                                                                                                                   | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Verifique la configuración de inscripción automática de certificados en la política "CCN-STIC-598 ENS Incremental Dominio categoria media". |        | <p>Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo". Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:</p> <p><b>Directiva CCN-STIC-598 ENS Incremental Dominio Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  <p>Haga doble clic sobre el objeto "Cliente de Servicios de servidor de certificados – Inscripción automática" y compruebe los valores correspondientes a la inscripción automática.</p>  |

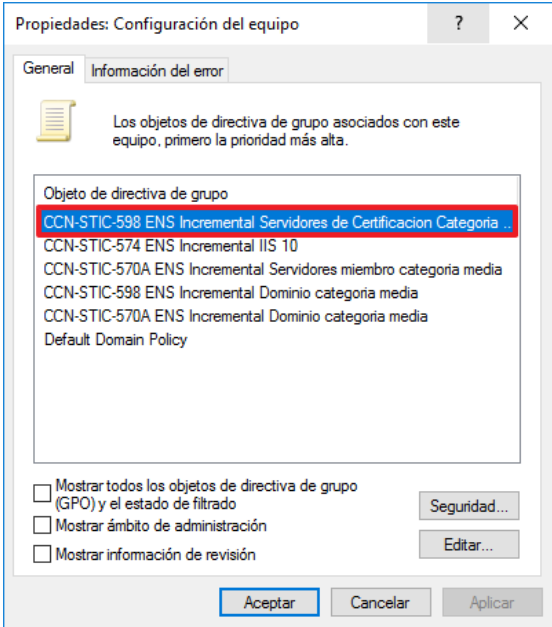
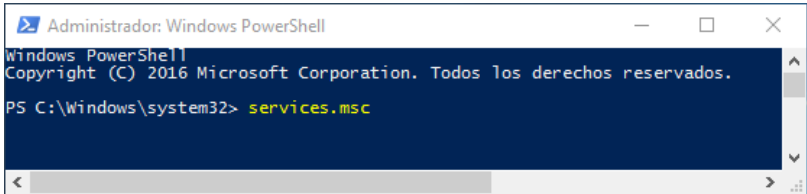
| Comprobación                                                                                                                            | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                      |        |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------|
|                                                                                                                                         |        | Configuración                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Estado               | OK/NOK |
|                                                                                                                                         |        | Modelo de configuración                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Habilitada           |        |
|                                                                                                                                         |        | Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Habilitada (marcada) |        |
|                                                                                                                                         |        | Actualizar certificados que usan plantillas de certificado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Habilitada (marcada) |        |
|                                                                                                                                         |        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                      |        |
| 6. Verifique la correcta aplicación de la política "CCN-STIC-598 Incremental Dominio categoría media" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  |                      |        |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                 |
|--------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>A continuación, haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría media” aparece en la lista como muestra la imagen.</p>  |

### 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN SUBORDINADA

| Comprobación                                                              | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación raíz de empresa. |        | En el servidor Entidad de Certificación subordinada, inicie sesión con una cuenta que tenga privilegios de administración del dominio.                                                                                                                                                                                                                                                                                 |
| 2. Verifique la correcta membresía de segregación de roles                |        | <p>Acceda a la herramienta “Usuarios y equipos de Active Directory” dentro del “Administrador del servidor” y despliegue el nodo “&lt;&lt;su dominio&gt;&gt; → Users”. Ahora, compruebe que los usuarios habilitados para labores de administración de la Entidad Certificadora pertenecen al grupo “Grupo Administración CA”.</p> <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |

| Comprobación                                                                                                                                                    | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Verifique la correcta aplicación de la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee "rsop.msc" en la consola de comandos que se ha abierto:</p>  |

| Comprobación                                                                                                                                                               | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                         |             |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                            |                         | <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media” aparece en la lista como muestra la imagen.</p>  |             |        |
| 4. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría media”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                  |             |        |
| Servicio (Nombre largo)                                                                                                                                                    | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                               | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                              | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                           | Configurado |        |
| Servidor                                                                                                                                                                   | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                           | Configurado |        |
| Registro Remoto                                                                                                                                                            | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                           | Configurado |        |

## ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

### ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

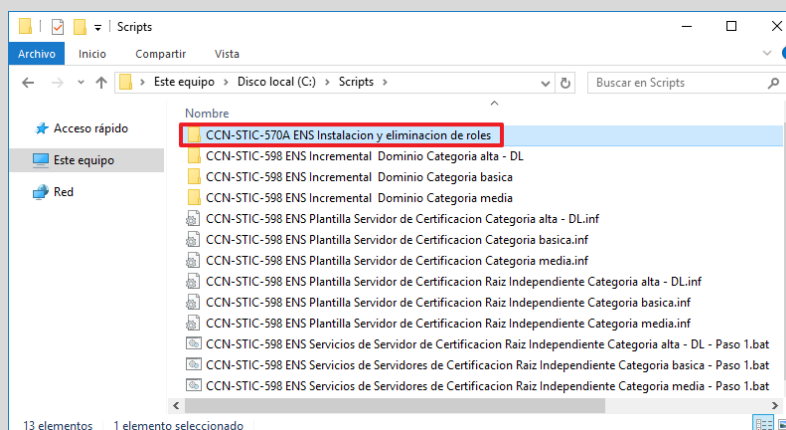
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Microsoft Windows Server 2016 con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad cumpla con los requisitos para una red clasificada con grado de clasificación Difusión Limitada. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

**Nota:** Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará uso de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho caso.

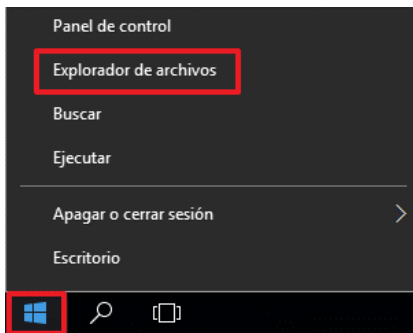
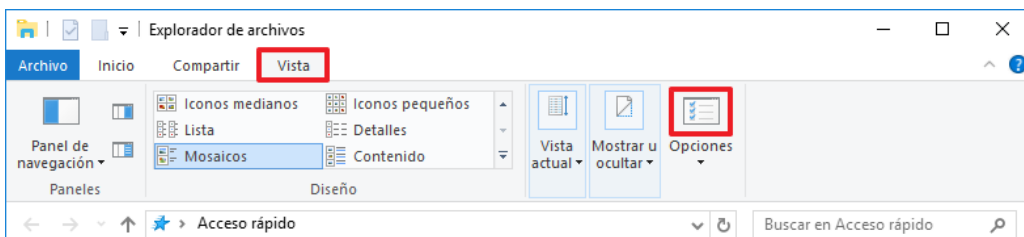
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad para comprobar su correcta funcionalidad.

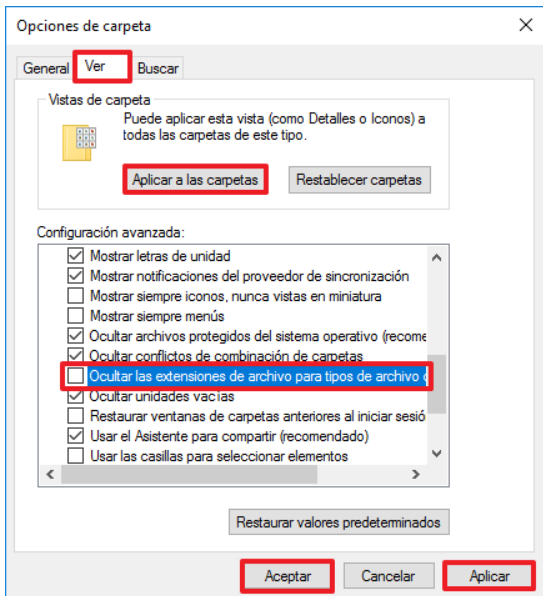
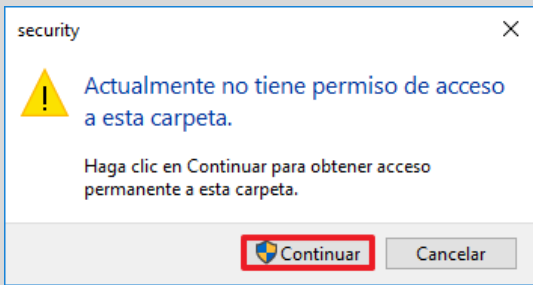
**Nota:** Si instala el Servidor Entidad de Certificación por primera vez con la guía “CCN-STIC-570A – Implementación del ENS en Windows Server 2016” aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO. En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía “CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016” encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta “Scripts” adjunta a la presente guía.

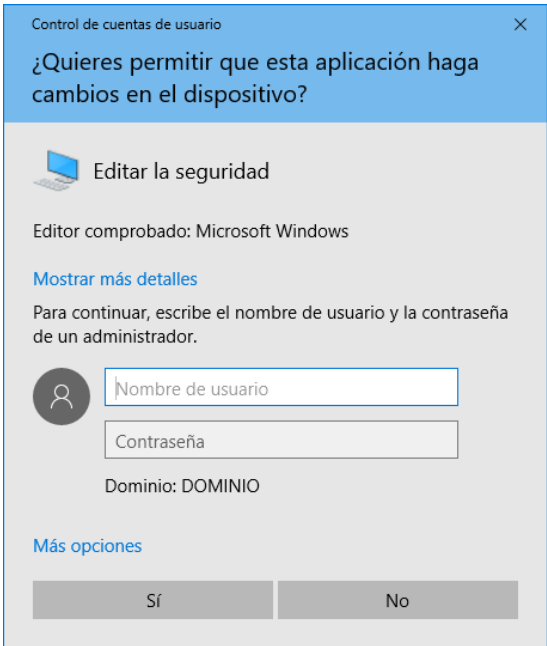
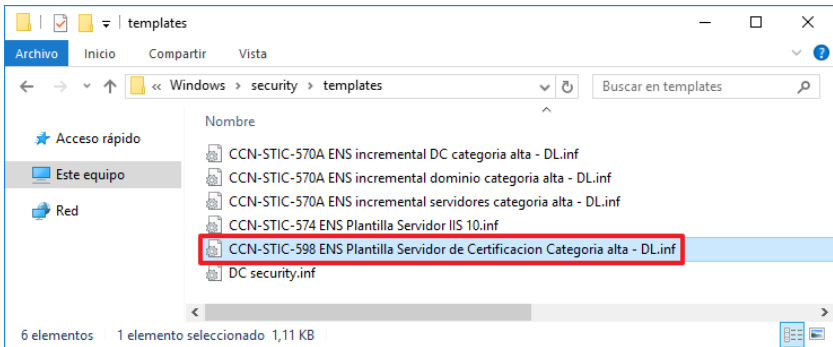
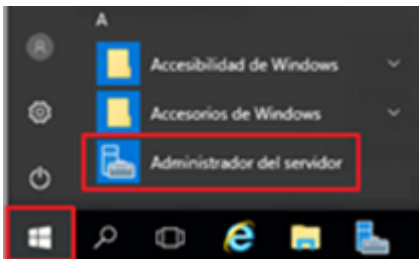


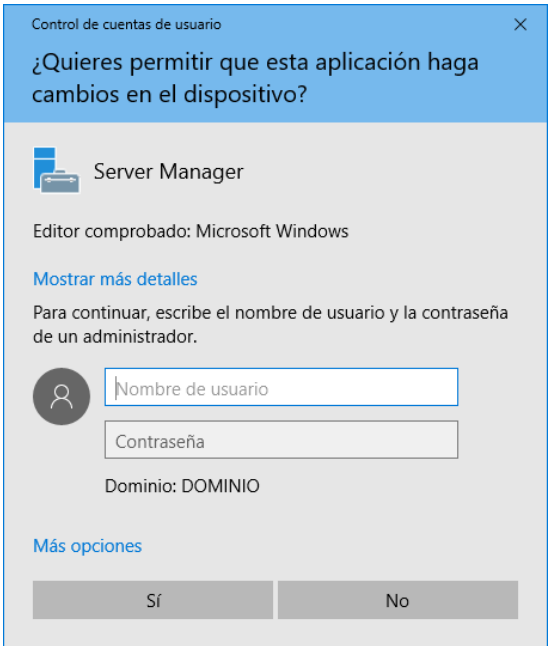
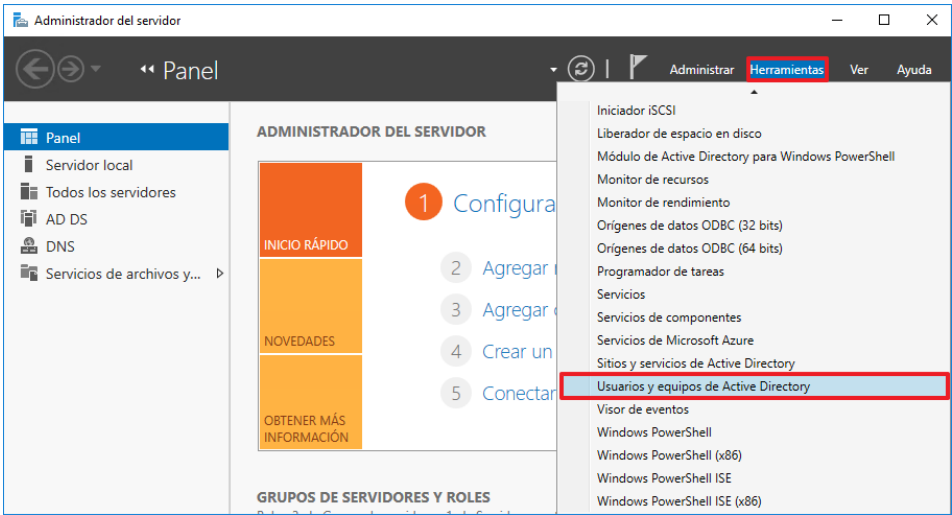
## 1. PREPARACIÓN DEL DOMINIO

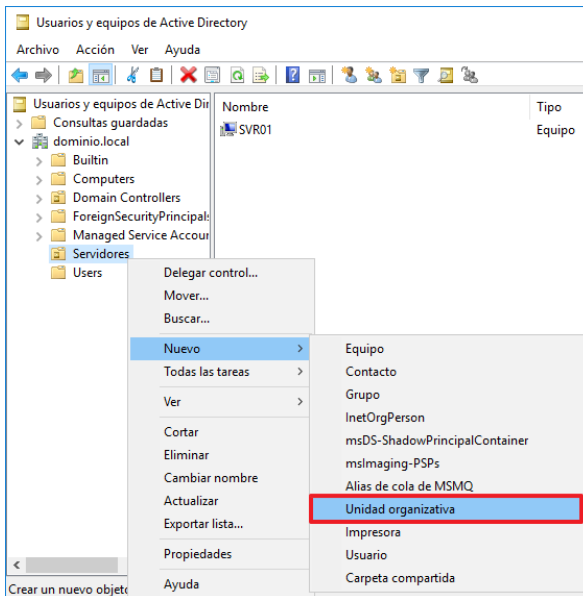
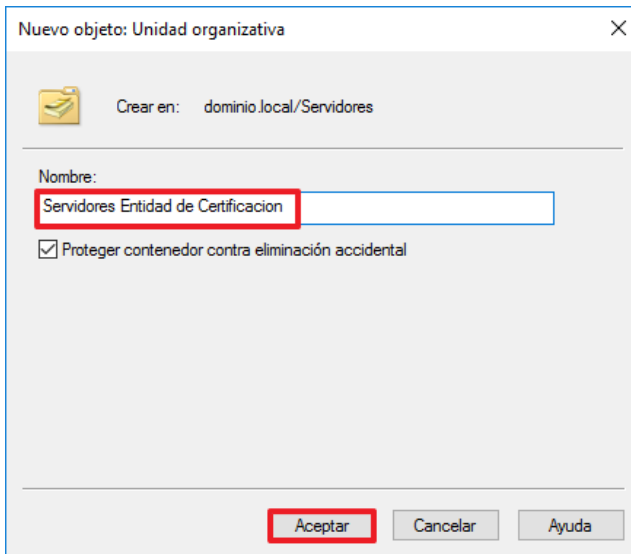
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor de Entidad de Certificación.

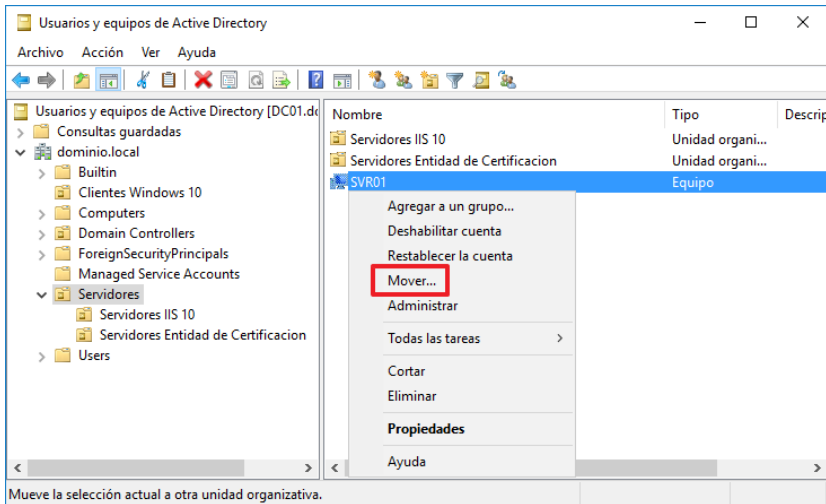
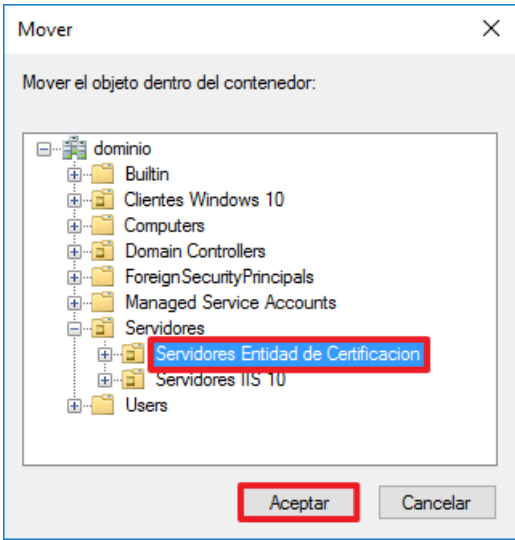
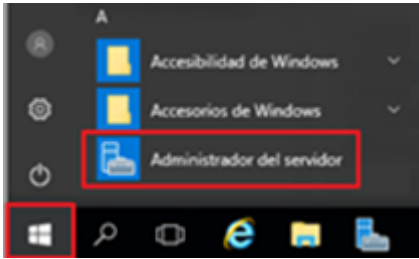
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para la Entidad de Certificación según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p>                                                                                                          |
| 2.   | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                                                                                                                                                                    |
| 3.   | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                                                                                                                                                                                                                    |
| 4.   | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>  |
| 5.   | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                     |

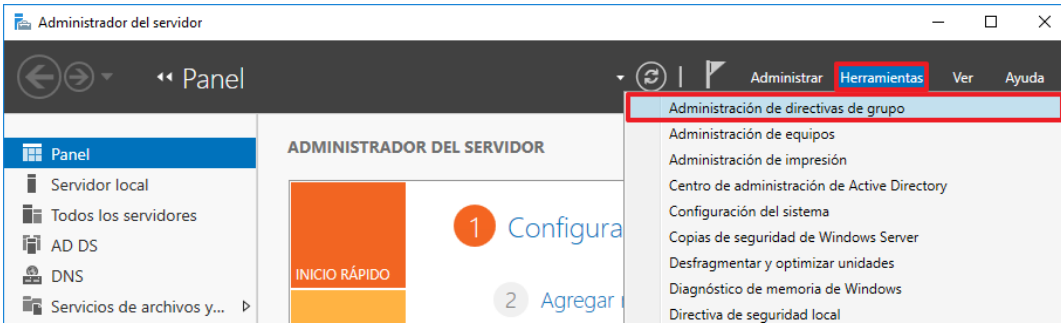
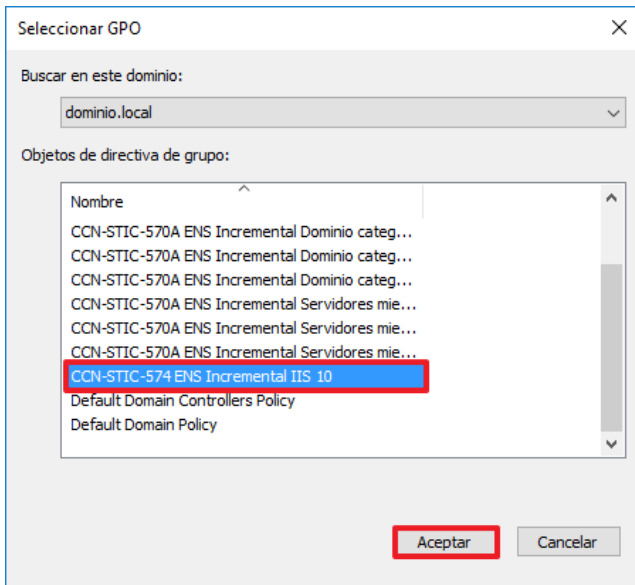
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |
| 7.   | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                            |

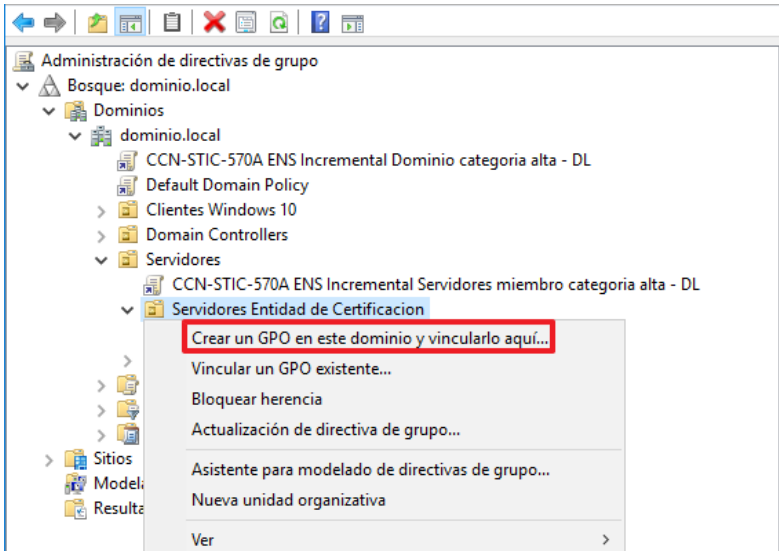
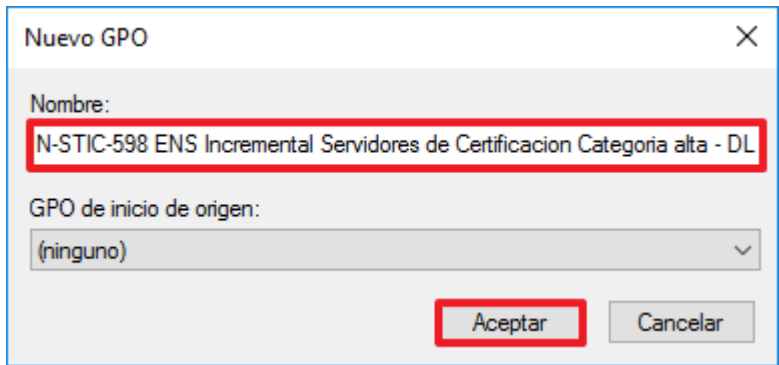
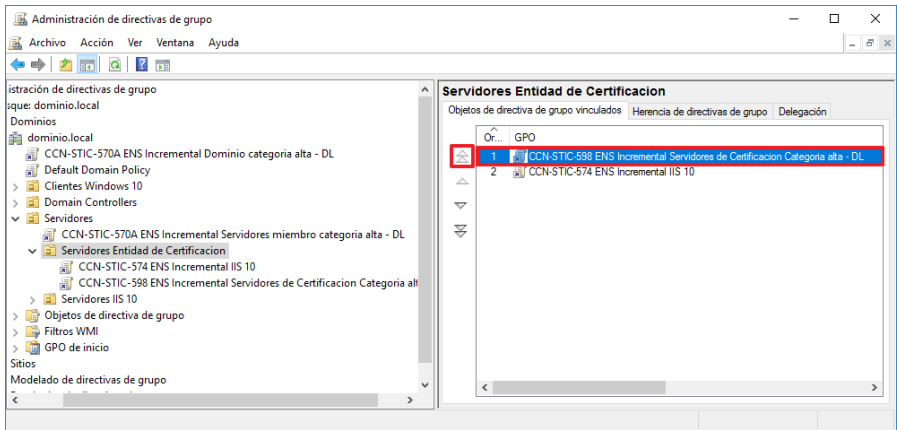
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.   | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |
| 9.   | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría alta - DL.inf” ubicada en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>                                                                                                                                                                                                                                                                                                                                                                                |
| 10.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |

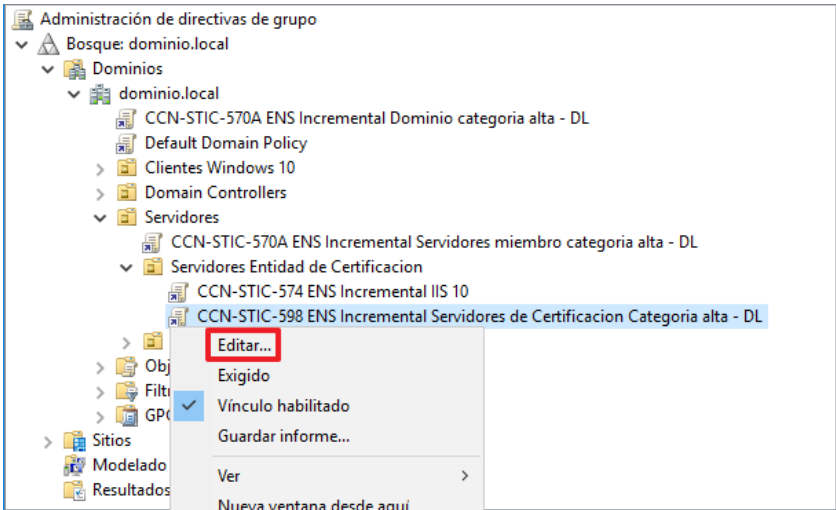
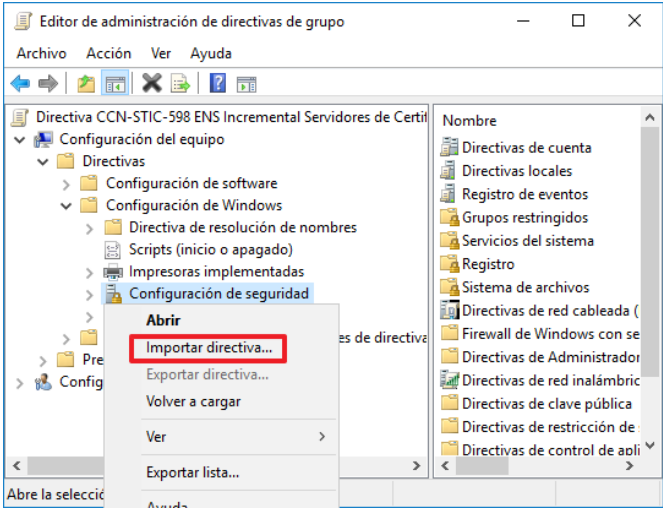
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                                    |
| 12.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione <b>“Herramientas → Usuarios y equipos de Active Directory”</b>.</p>  |

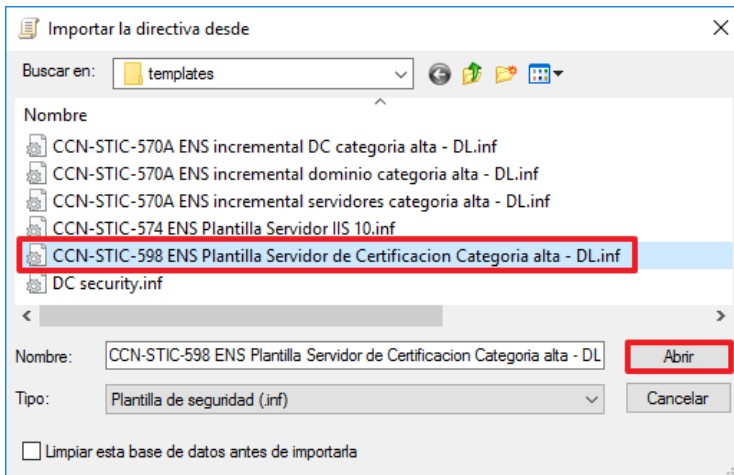
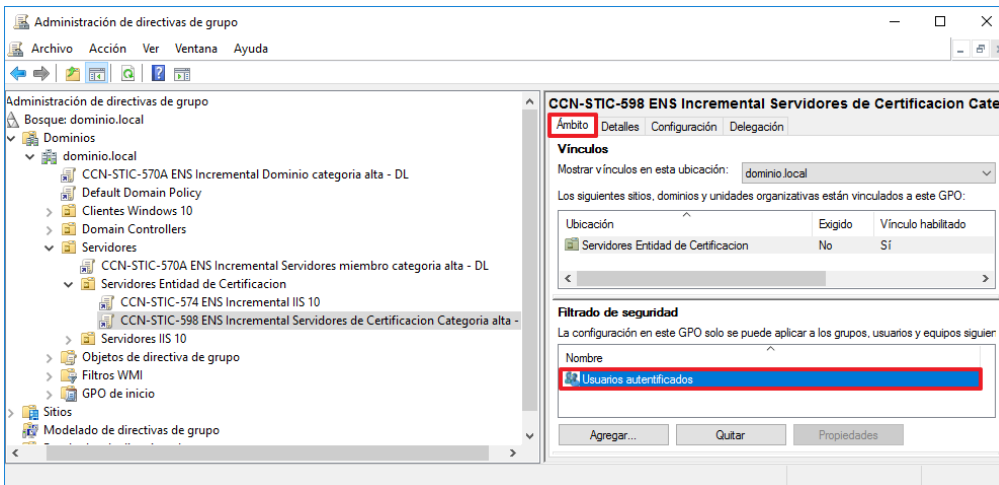
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo “&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local → Servidores”.</p> |
| 14.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

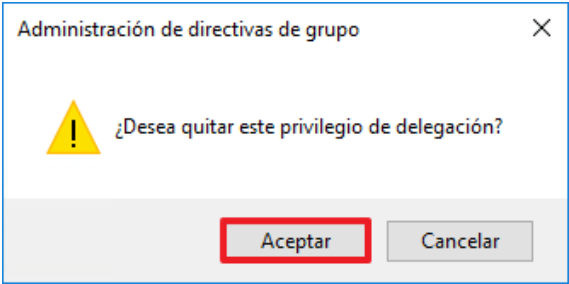
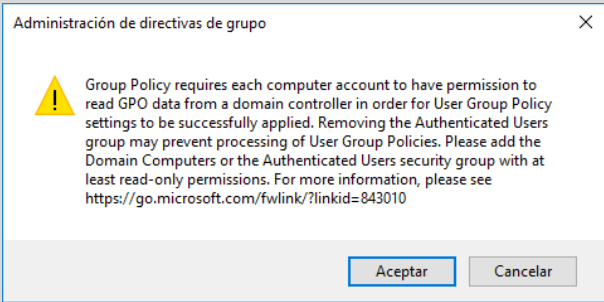
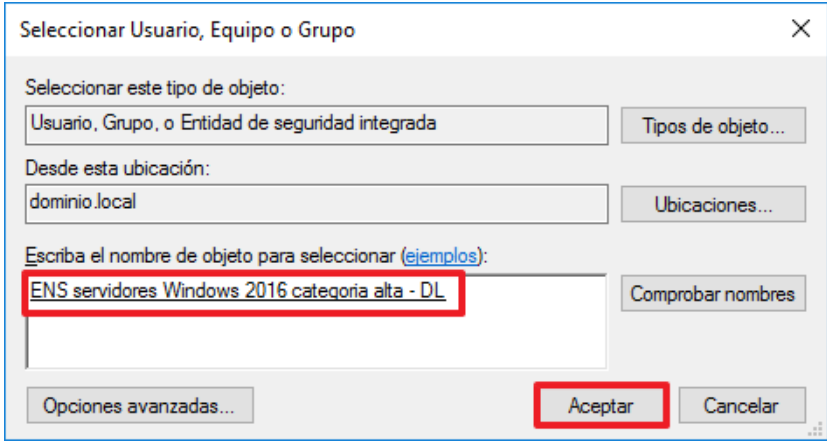
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores entidad de certificación a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |
| 16.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>                                                                                                                                                                                                                         |
| 17.  | Cierre la herramienta de “Usuarios y equipos de Active Directory”.                                                                                                                                                                                                                                                                                                                                                                  |
| 18.  | <p>A continuación, abra el “Administrador del servidor”.</p>                                                                                                                                                                                                                                                                                    |

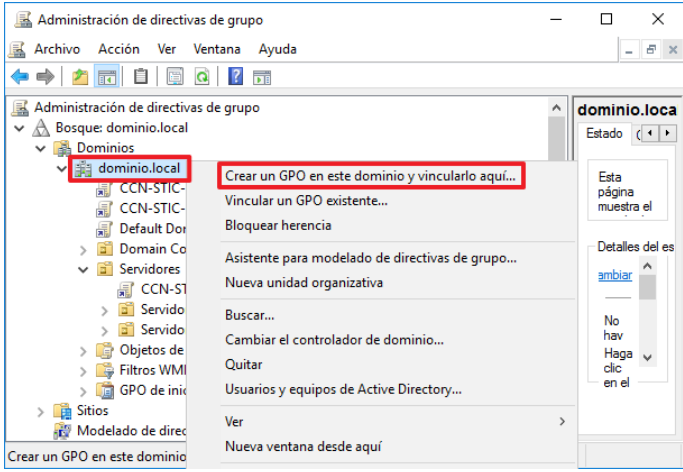
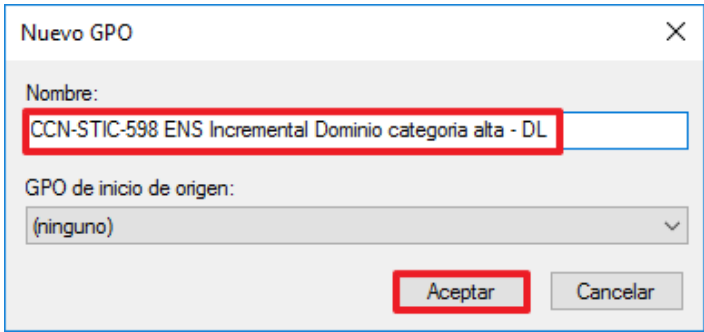
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.  | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón <b>“Herramientas → Administración de directivas de grupo”</b>.</p>                                                                                                               |
| 20.  | <p>A continuación, despliegue el nodo <b>“Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”</b>.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p>                             |
| 21.  | <p>Seleccione <b>“Vincular un GPO existente...”</b> y vincule el objeto de directiva de grupo <b>“CCN-STIC-574 ENS Incremental IIS 10”</b> a la nueva unidad organizativa <b>“Servidores Entidad de Certificación”</b>, haciendo clic con el botón derecho sobre ella.</p>  |

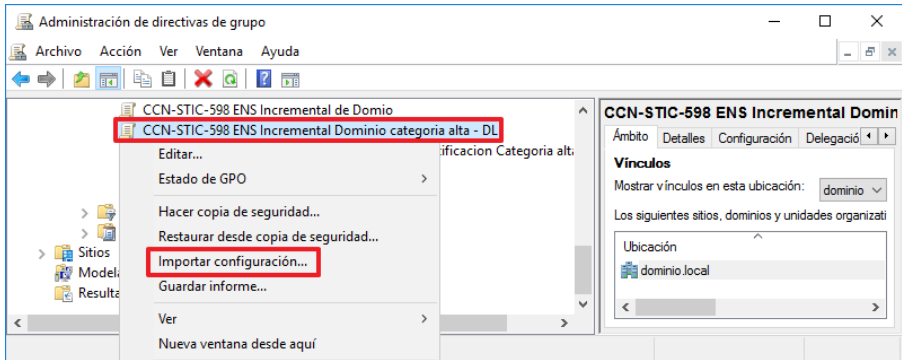
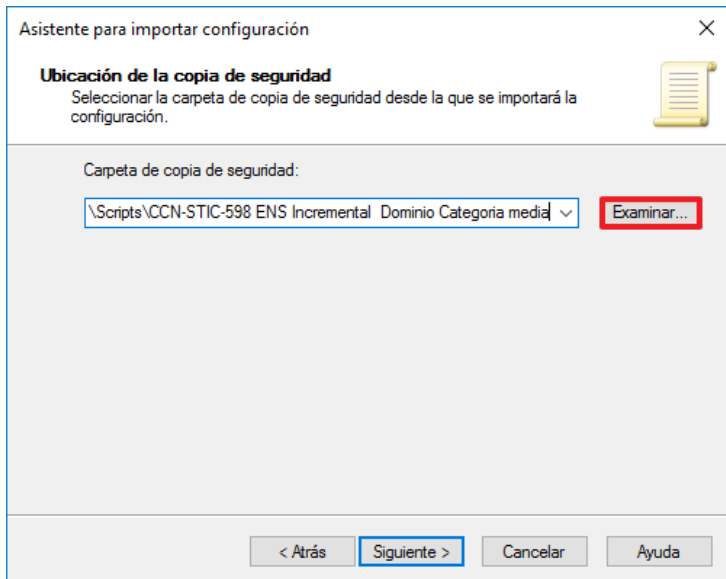
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22.  | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>       |
| 23.  | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL” y haga clic en el botón “Aceptar”.</p>                                                                                                                    |
| 24.  | <p>Seleccione la unidad organizativa “<b>Servidores Entidad de Certificación</b>”. En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  |

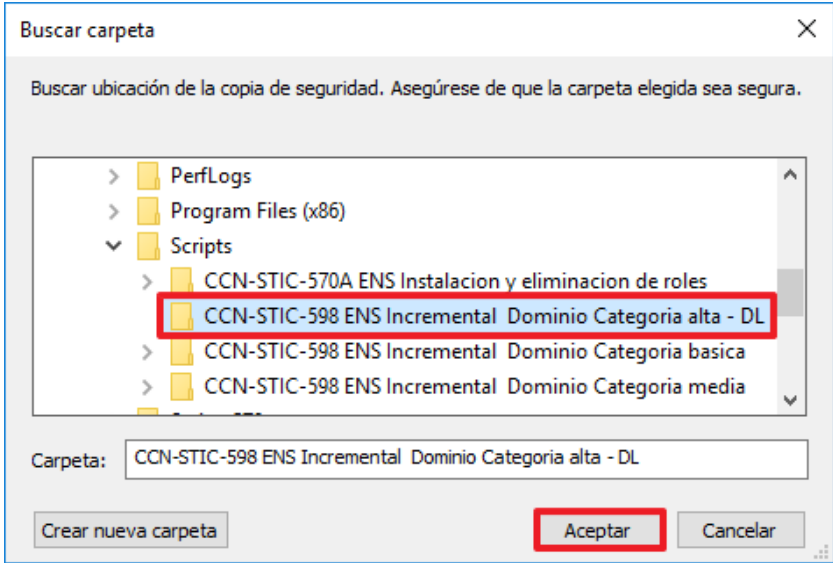
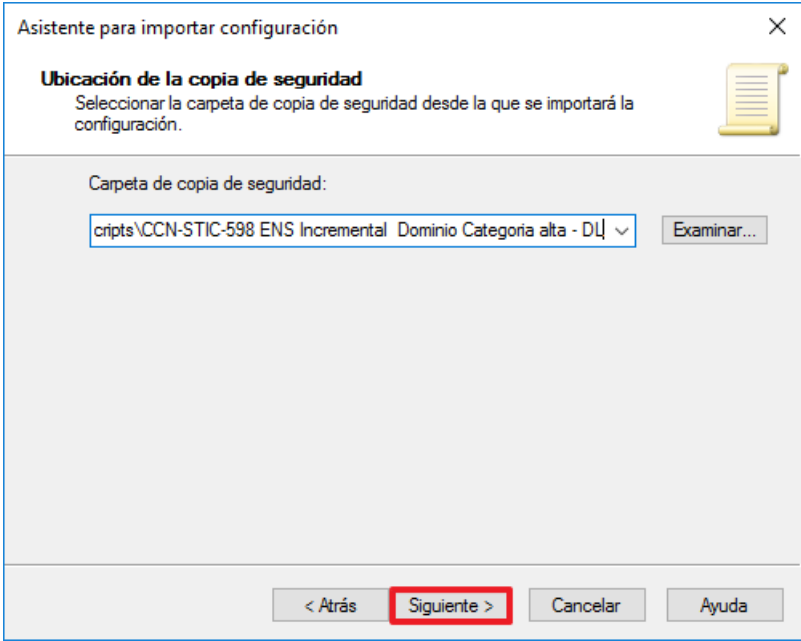
| Paso | Descripción                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25.  | De esta forma, se garantiza que la directiva se aplica correctamente.                                                                                                                                                         |
| 26.  | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción “Editar”.</p>  |
| 27.  | <p>Expanda el nodo “Configuración del equipo → Directivas→ Configuración de Windows → Configuración de seguridad”.</p>                                                                                                        |
| 28.  | <p>Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.</p>                      |

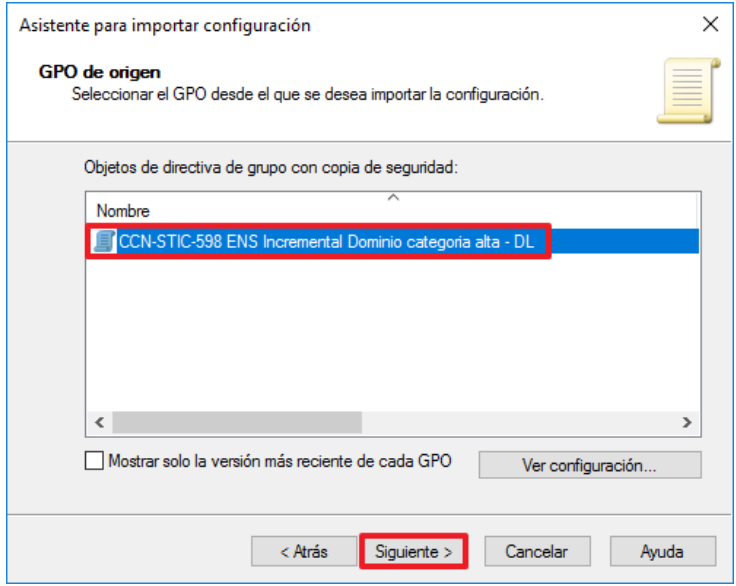
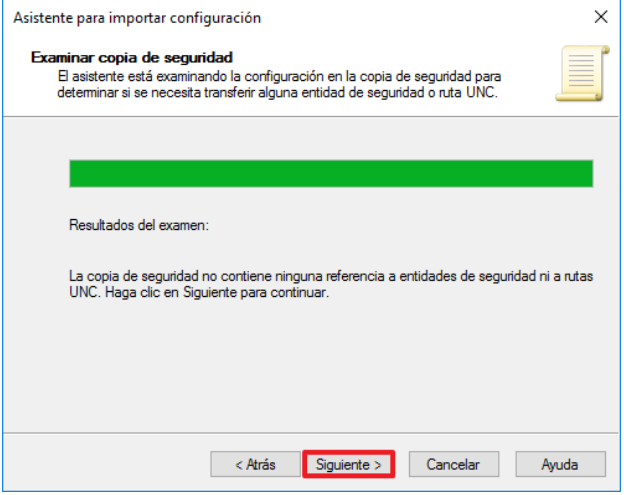
| Paso | Descripción                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29.  | <p>Seleccione la plantilla “C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría alta - DL.inf”. Haga clic en el botón “Abrir”.</p>                                                 |
| 30.  | Cierre el “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                              |
| 31.  | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>  |

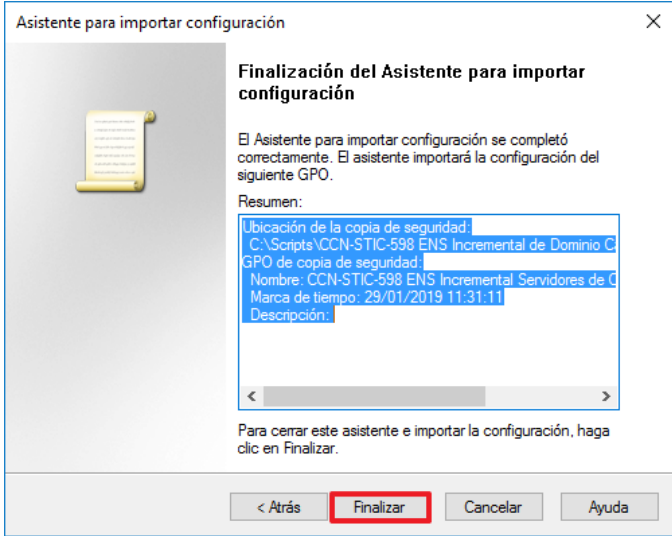
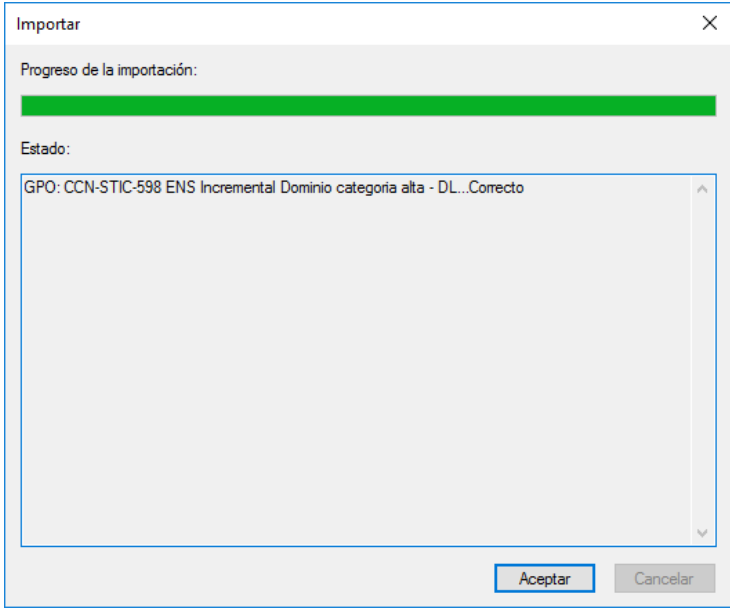
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 32.  | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>                                                                  |
| 33.  | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidores Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria alta - DL” que contiene el servidor con el rol “Servidores Entidad de Certificación”.</p> |
| 34.  | <p>Cierre la ventana “Editor de administración de directivas de grupo”.</p>                                                                                                                                                                                                                                                                                                                                                    |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 35.  | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 36.  | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 37.  | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 Incremental Dominio categoria alta - DL” y pulse el botón “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

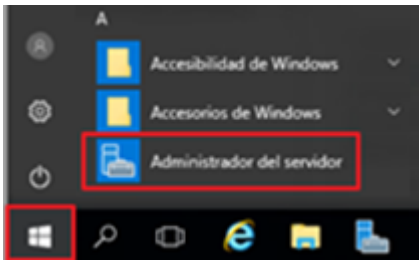
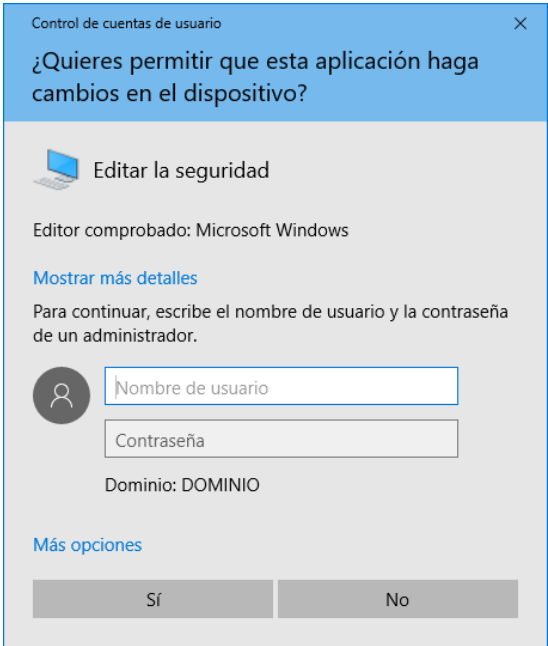
| Paso | Descripción                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 38.  | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>  |
| 39.  | <p>Haga clic en “Siguiete &gt;” en el “Asistente para importar configuración”.</p>                                                                                                                                                                                                                          |
| 40.  | <p>Haga clic en “Examinar...”.</p>                                                                                                                                                                                       |

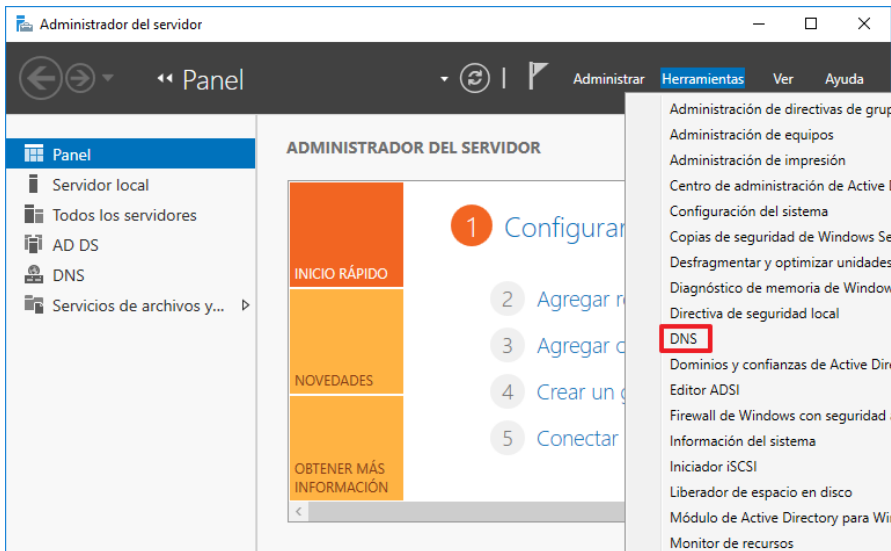
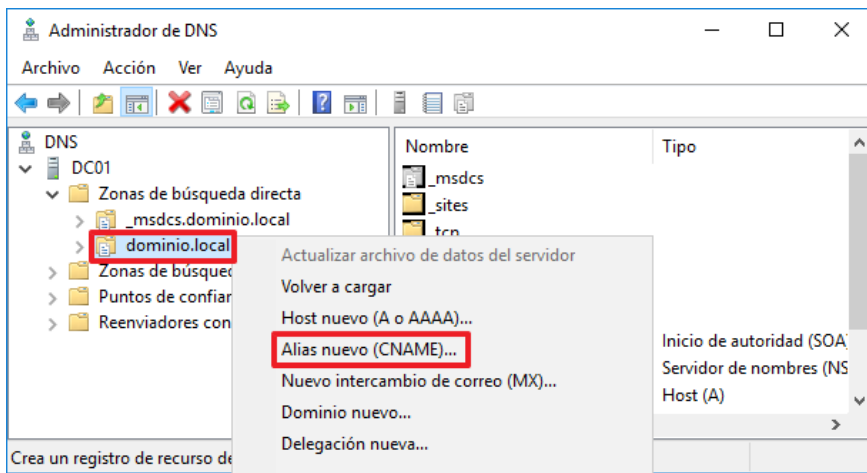
| Paso | Descripción                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 41.  | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoría alta - DL” y pulse “Aceptar”.</p>  |
| 42.  | <p>Pulse “Siguiente &gt;” para continuar con la importación.</p>                                                                                                           |

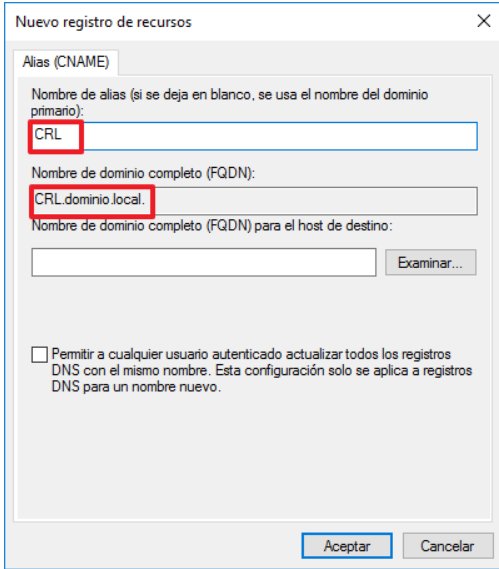
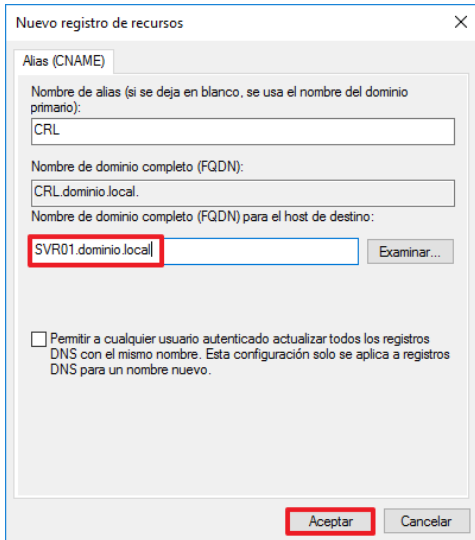
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 43.  | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio categoria alta - DL” y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |
| 44.  | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |

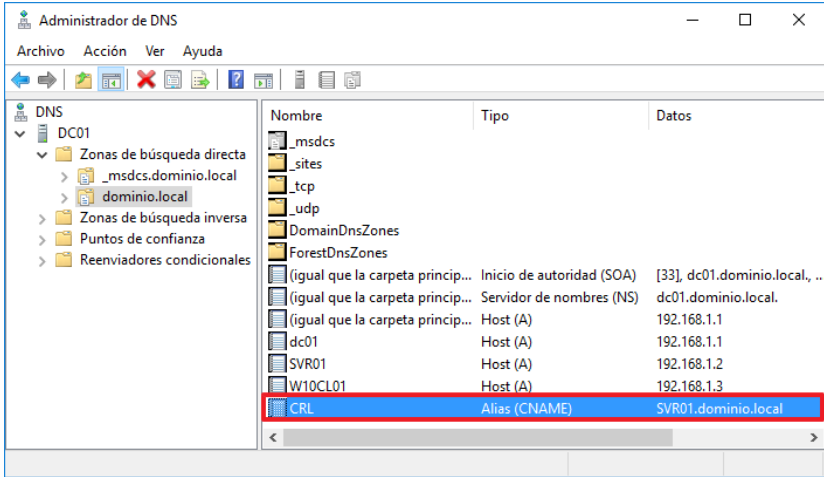
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45.  | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                                                                                                                    |
| 46.  | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>  |
| 47.  | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos.</p>                                                                         |
| 48.  | <p>Cierre la ventana “Administración de directivas de grupo”.</p>                                                                                                                                                                                                   |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

| Paso | Descripción                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 49.  | Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.                                                         |
| 50.  | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                              |
| 51.  | <p>El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>                                                                                                                                                    |
| 53.  | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: “&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”.</p> <p>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 54.  | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |
| 55.  | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p>                                |

| Paso | Descripción                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 56.  | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>  |

## 2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría alta.

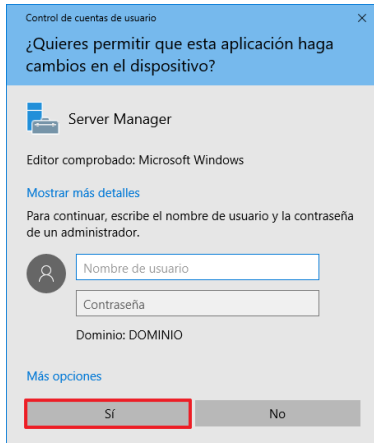
No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

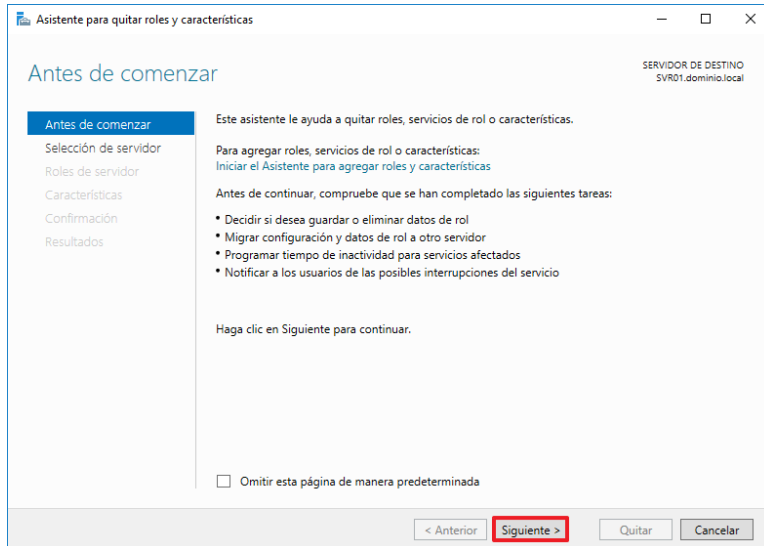
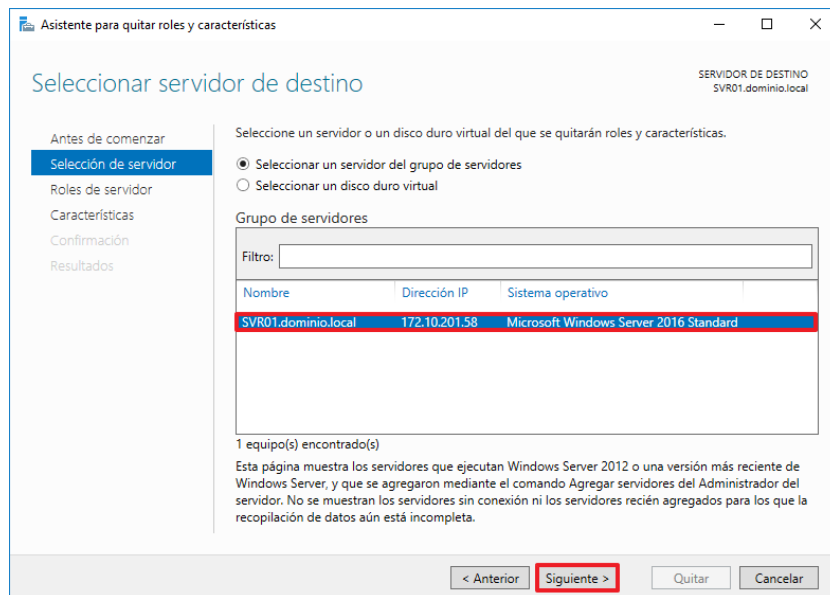
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

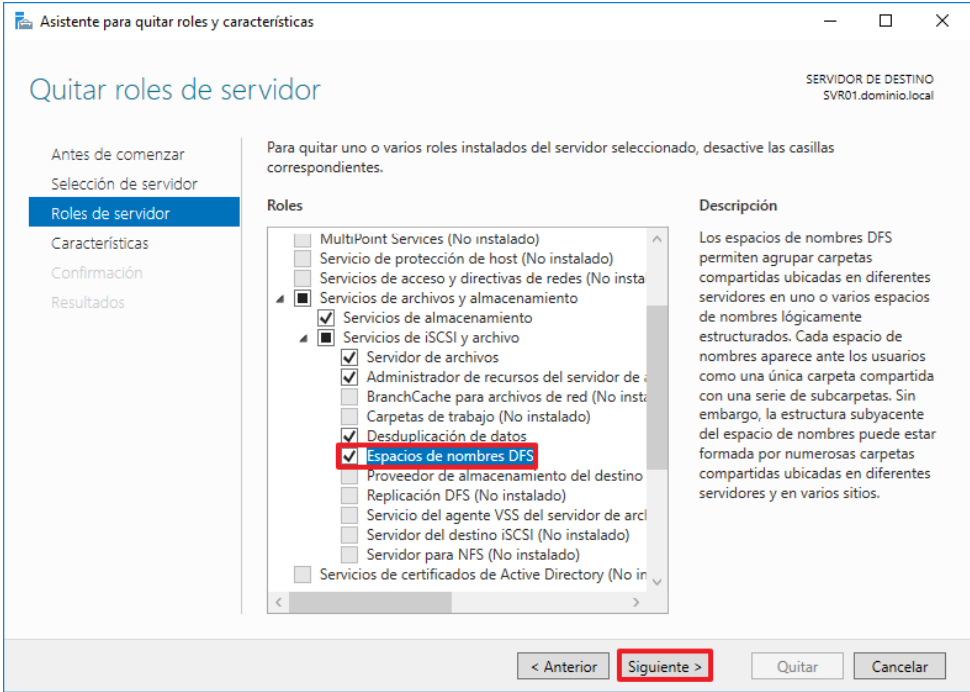
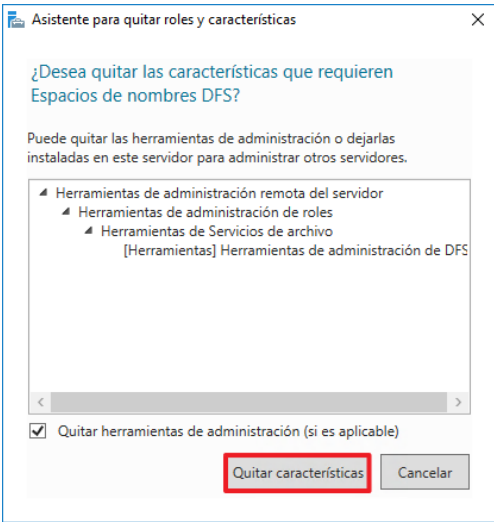
### 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

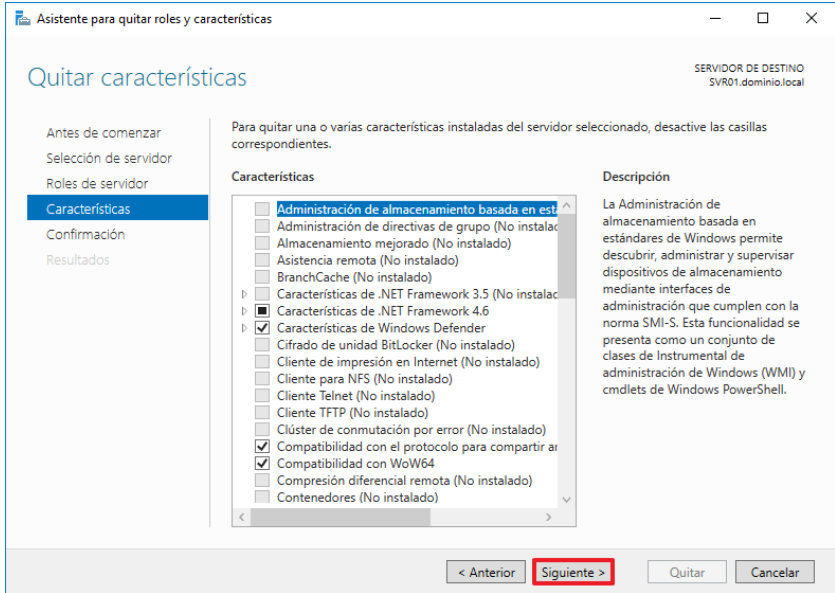
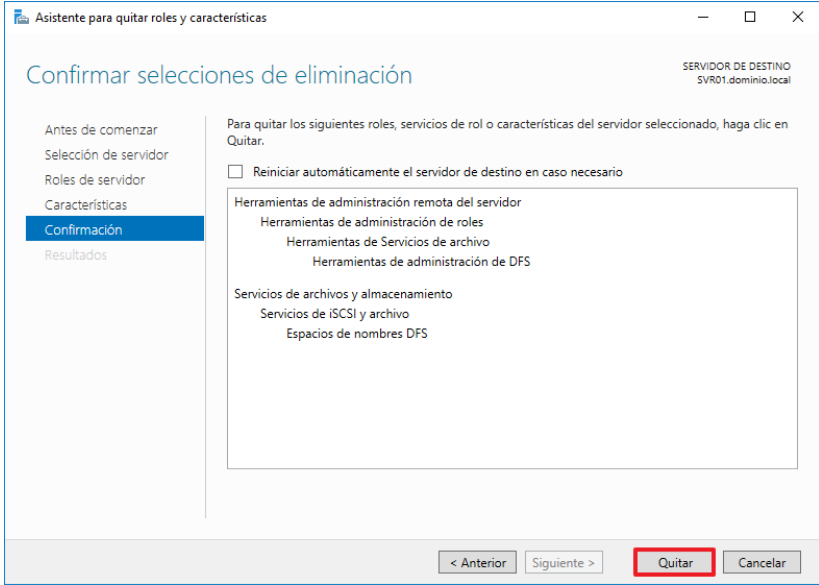
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta - DL en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

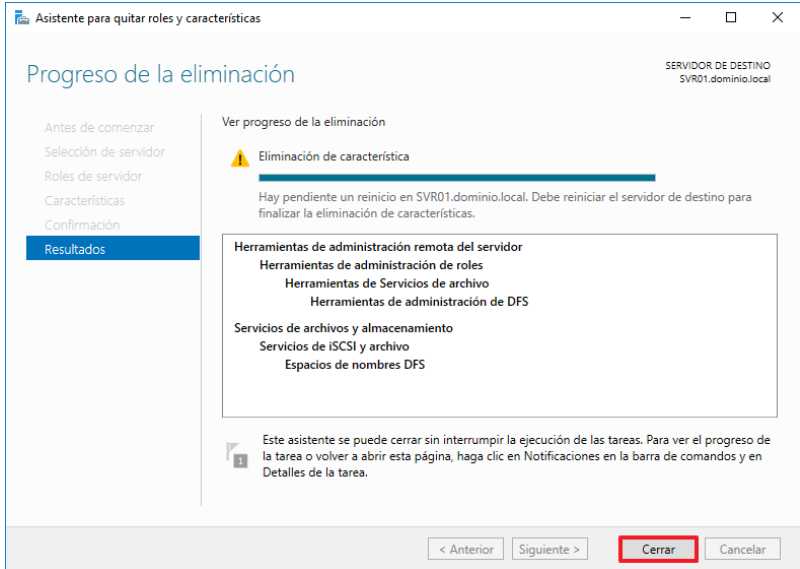
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de Certificación.

| Paso | Descripción                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Entidad de Certificación.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 58.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                       |
| 59.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                        |
| 60.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>                                                                                                           |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 61.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>                                                                              |
| 62.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p> |

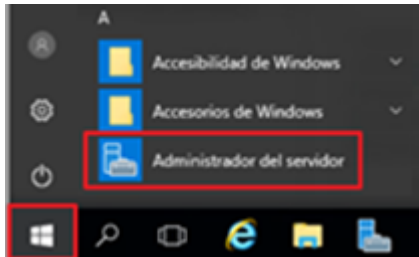
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 63.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |
| 64.  | <p>En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p>     |

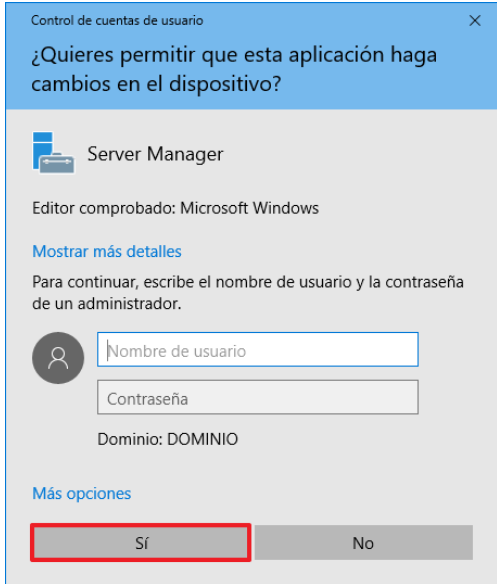
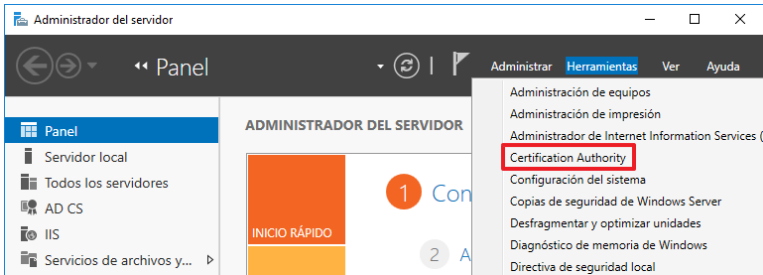
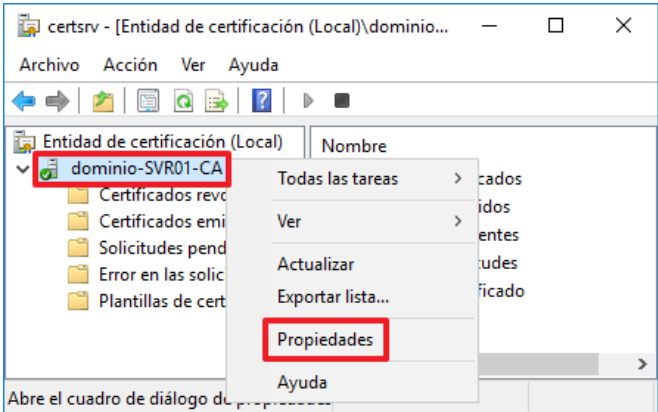
| Paso | Descripción                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 65.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>  |
| 66.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                                                                |

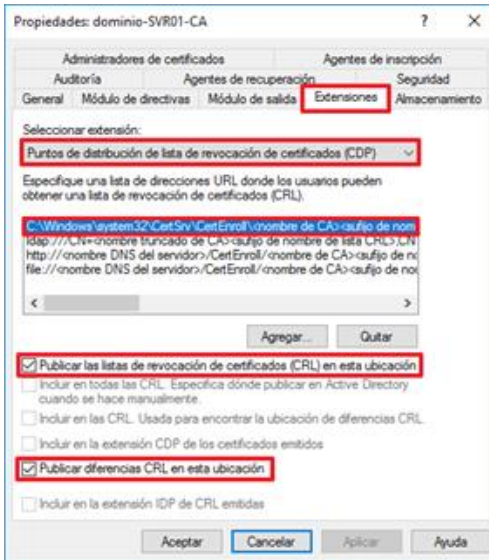
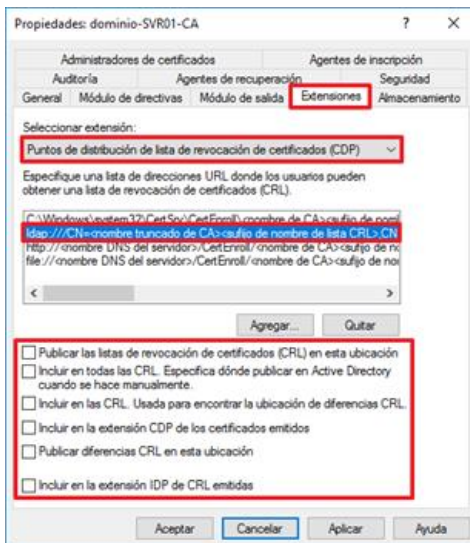
| Paso | Descripción                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 67.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 68.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                  |

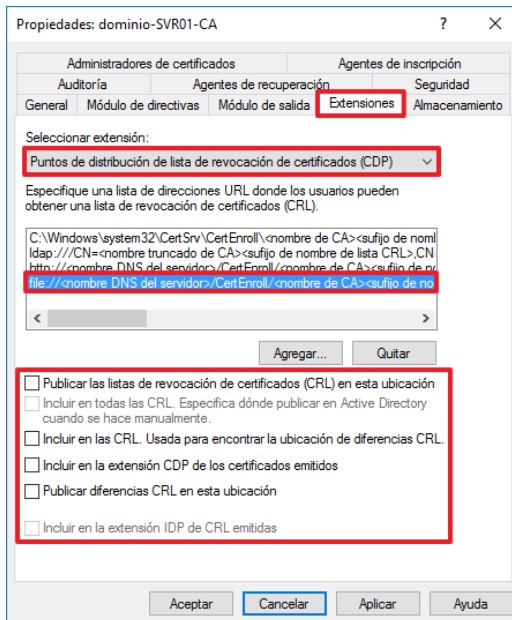
## 2.2. CONFIGURACIÓN DE LA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA

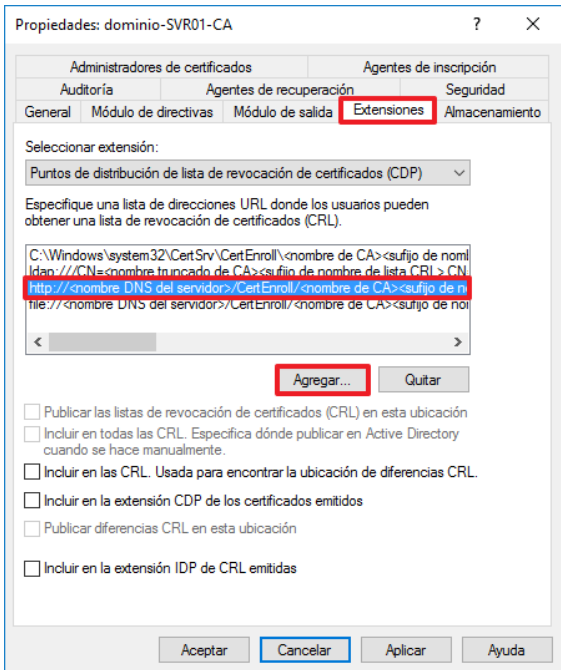
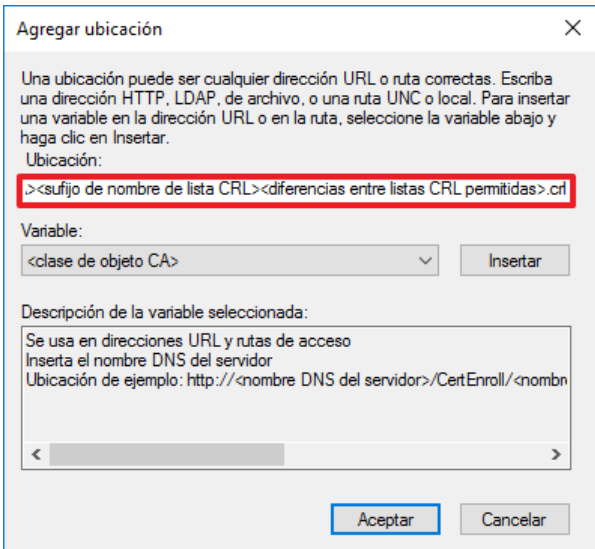
En este apartado, se establecerá la configuración que permite que un sitio web mantenga las CRLs de modo que sean accesibles por todos los clientes de la Entidad de Certificación.

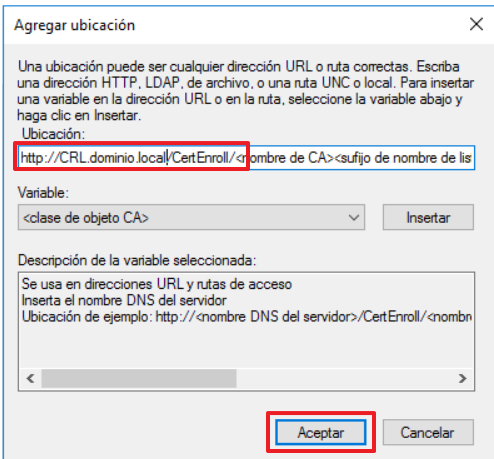
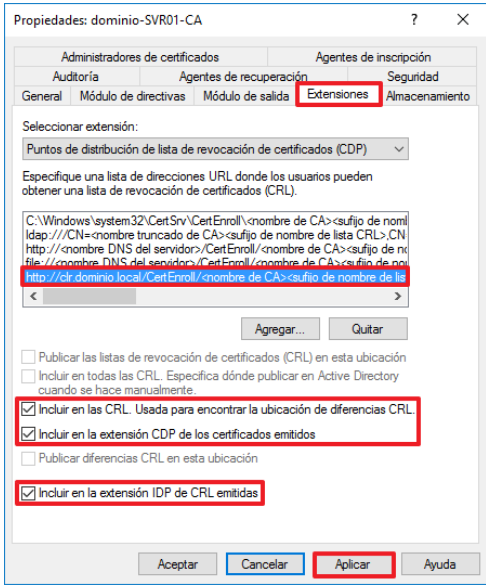
| Paso | Descripción                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 69.  | <p>Inicie sesión en el equipo que posea la Entidad de Certificación raíz de empresa.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p> |
| 70.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>               |

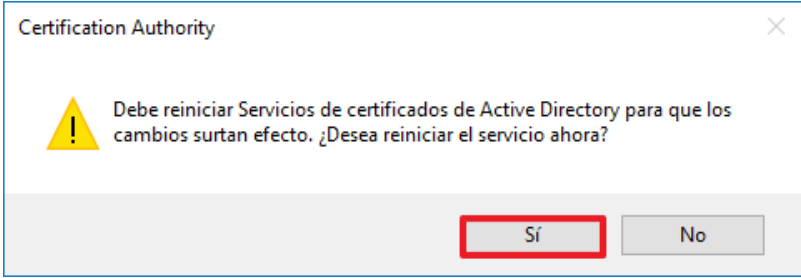
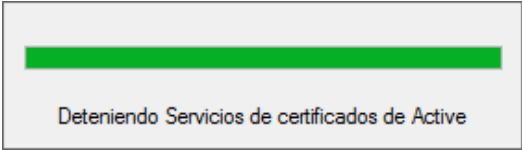
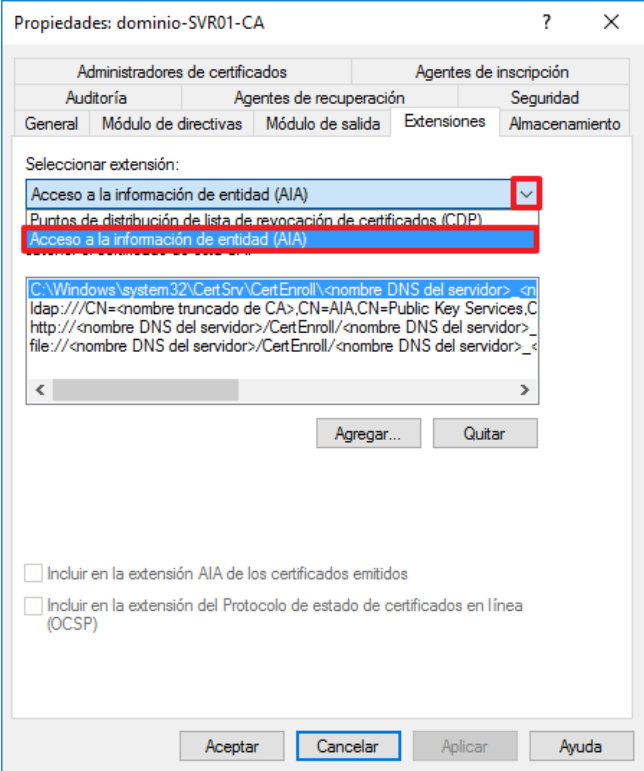
| Paso | Descripción                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 71.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio. Introduzca sus credenciales y pulse “Sí”.</p>                                                                          |
| 72.  | <p>En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                                                                  |
| 73.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado de la Entidad de Certificación configurada recientemente y, con el botón derecho del ratón selecciónela, y pulse la opción “Propiedades”.</p>  |

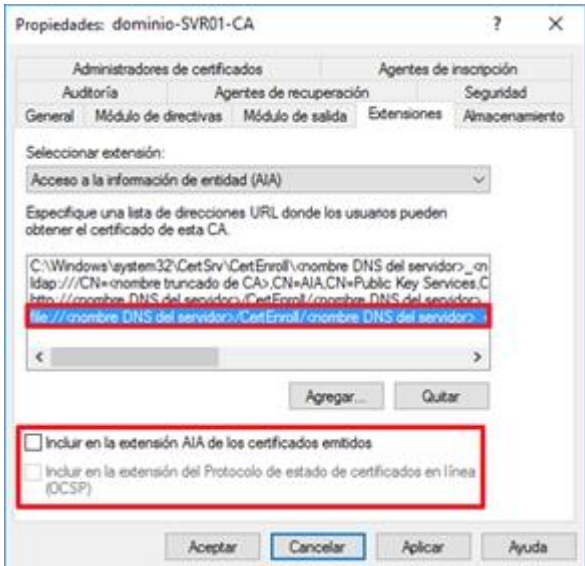
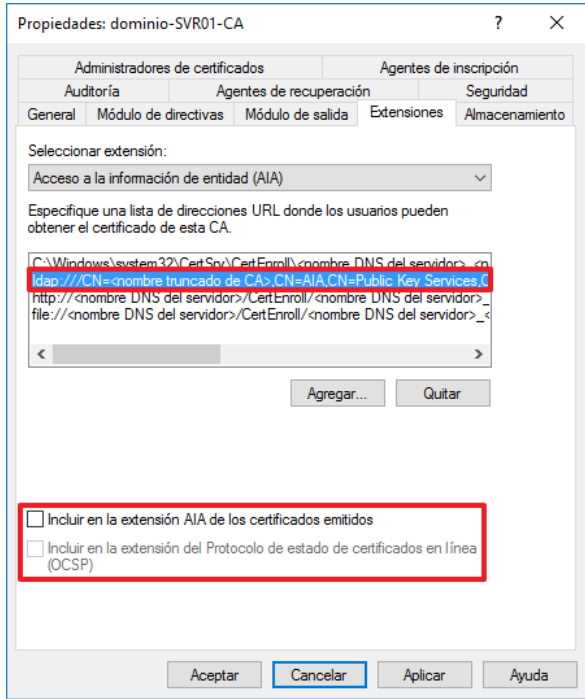
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 74.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</p>              |
| 75.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, deshabilite la publicación de CRLs mediante ldap seleccionando <b>“ldap://CN=&lt;nombre truncado de CA&gt;&lt;sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;”</b> y desmarcando todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>  |

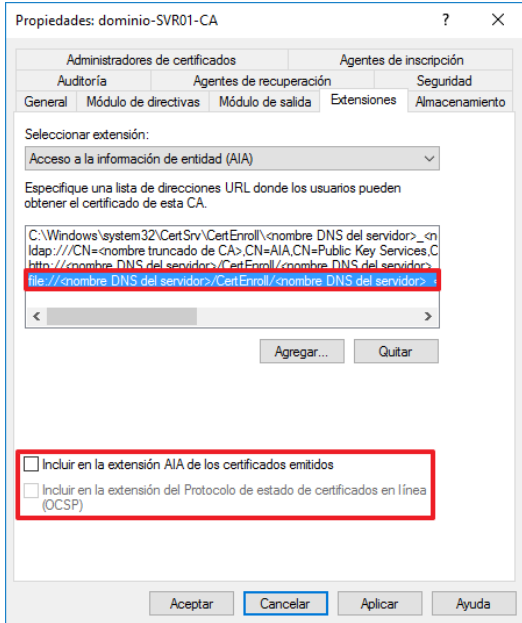
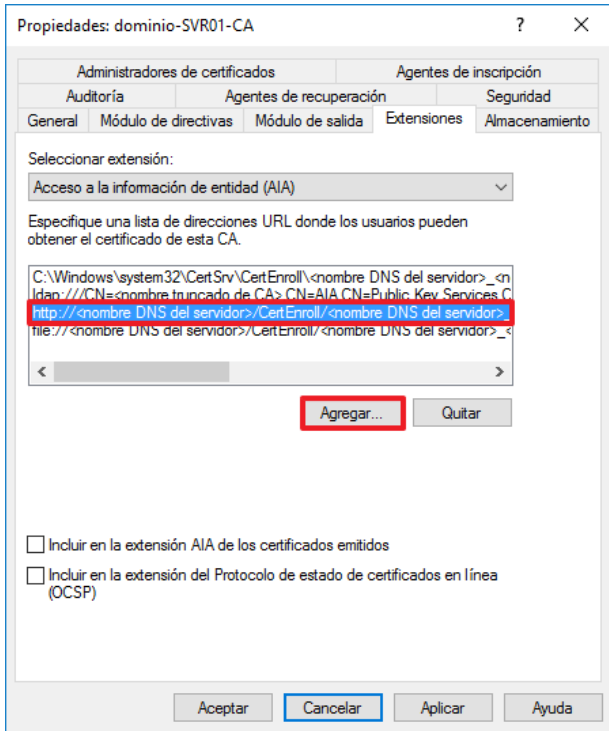
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 76.  | <p>De nuevo en “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> asegúrese que tiene todas las opciones desmarcadas tal y como aparece en la siguiente figura.</p>  |
| 77.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt;sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y copie el elemento mediante la combinación de teclas “Control + C”.</p>                                                                                                |

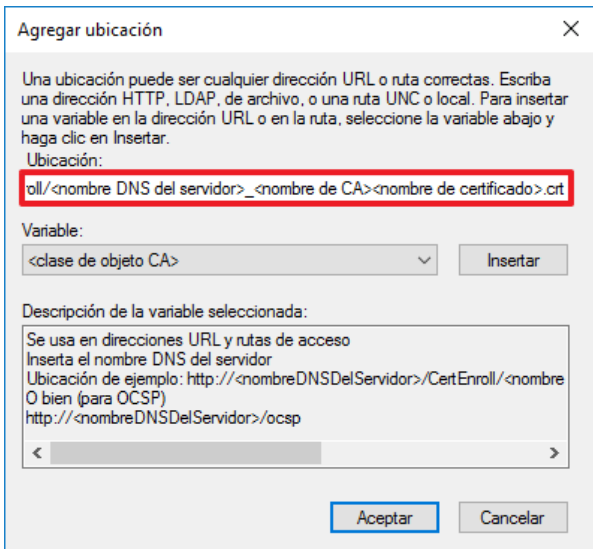
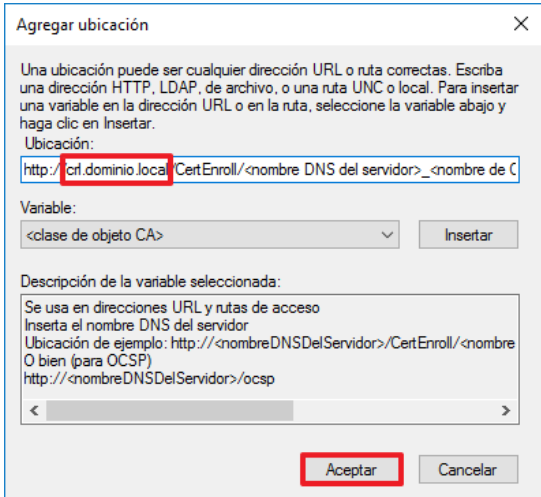
| Paso | Descripción                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 78.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                 |
| 79.  | <p>En “Agregar ubicación” coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>  |

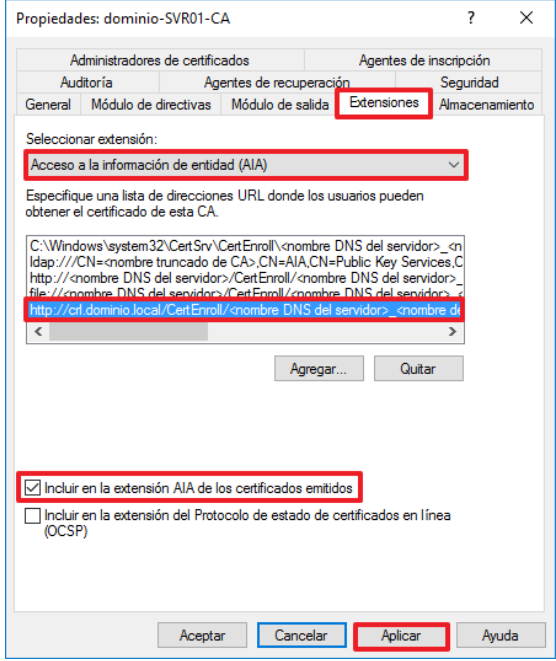
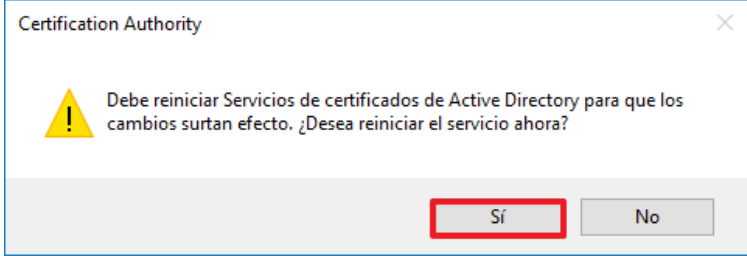
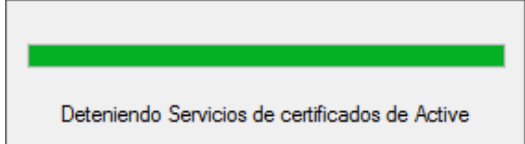
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80.  | <p>En dicha ventana, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación y que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                                                                           |
| 81.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada “http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl” y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 82.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 83.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 84.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 85.  | <p>Compruebe que en el objeto <b>"C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>                                                                    |
| 86.  | <p>Compruebe que en el objeto <b>"Idap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> están desmarcadas todas las opciones. Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.  | <p>Seleccione <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y asegúrese que todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |
| 88.  | <p>Seleccione ahora <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b>.</p>                                                                                                      |
| 89.  | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                                                                                               |

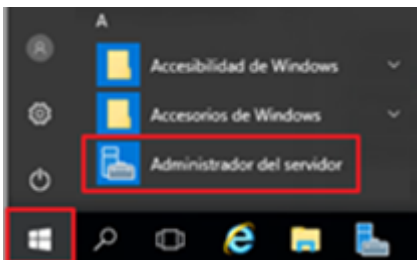
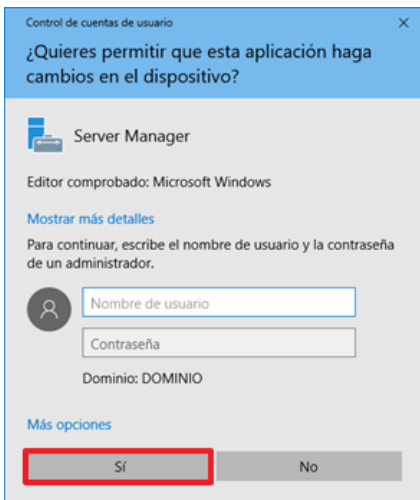
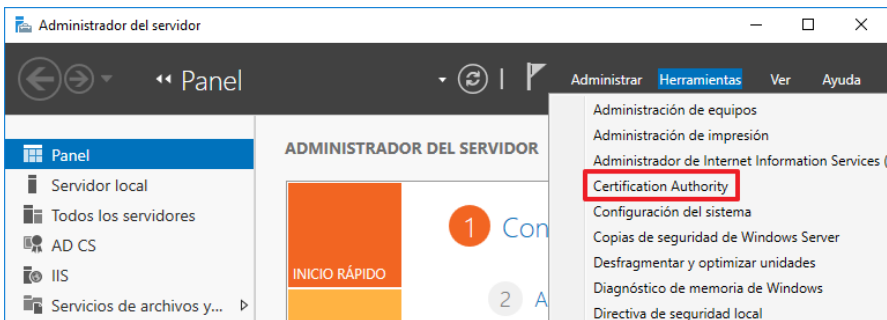
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 90.  | <p>En “Agregar ubicación” coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                                                                                                            |
| 91.  | <p>En “Agregar ubicación” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente (B.2. de la presente guía) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

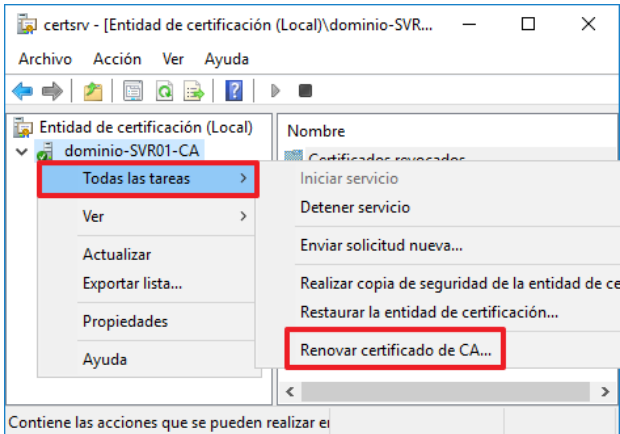
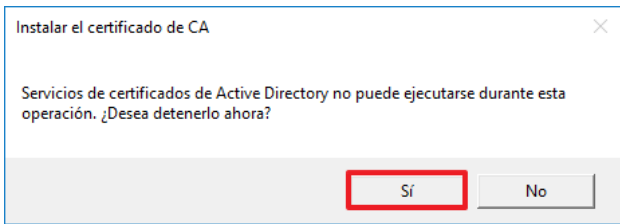
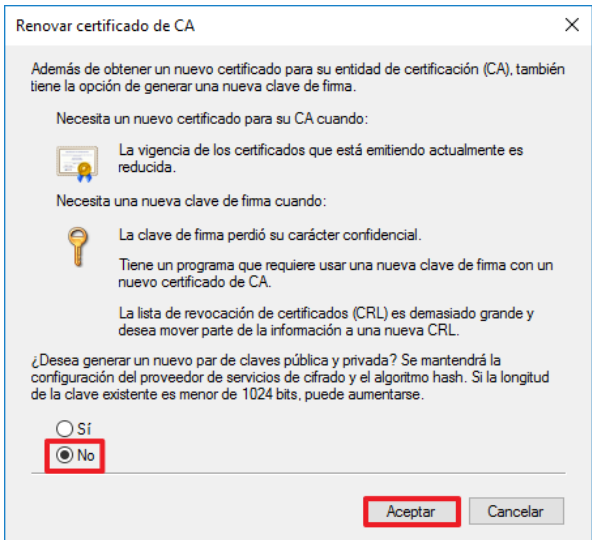
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 92.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt</b>” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”. Pulse “Aplicar” para guardar los cambios.</p>  |
| 93.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                            |
| 94.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                          |
| 95.  | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |

## 2.3. RENOVACIÓN DE CERTIFICADO DE ENTIDAD RAÍZ DE EMPRESA

Será necesario volver a generar el certificado de la Entidad de Certificación tras hacer modificaciones en las propiedades.

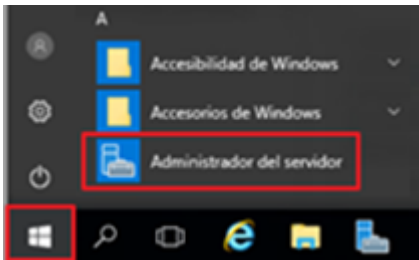
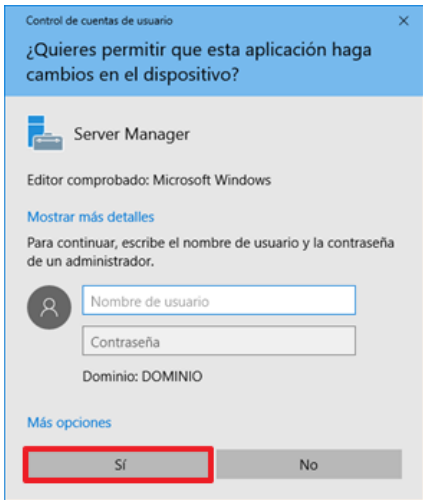
Los pasos que se definen a continuación comprenden la renovación de una Entidad de Certificación raíz de empresa.

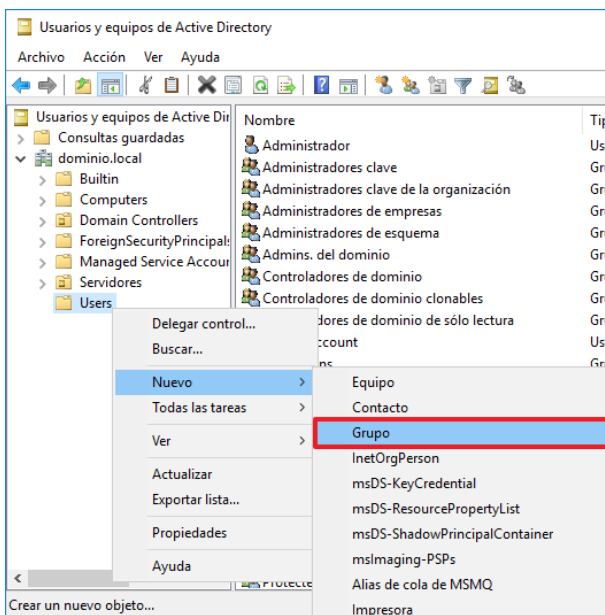
| Paso | Descripción                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Inicie sesión en el equipo Entidad de Certificación raíz.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de Administrador del Dominio.</p>                                                                           |
| 97.  | <p>Acceda al “Administrador del Servidor”. Para ello ejecute el icono correspondiente.</p>                                                                   |
| 98.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio. Introduzca sus credenciales y pulse “Sí”.</p>  |
| 99.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>        |

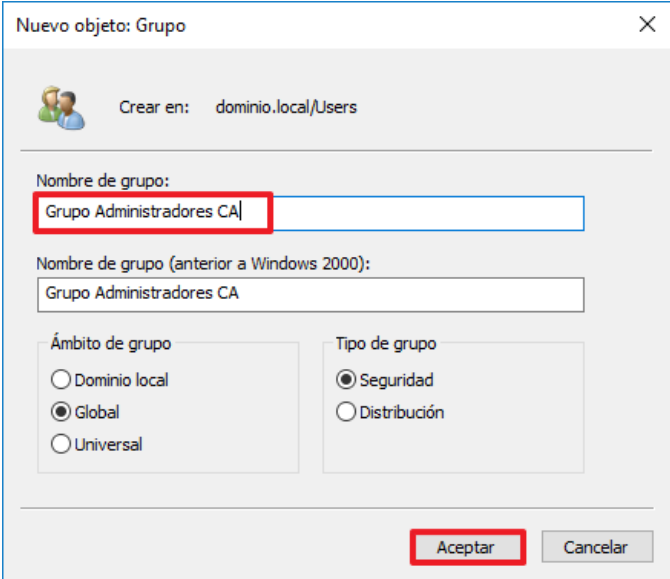
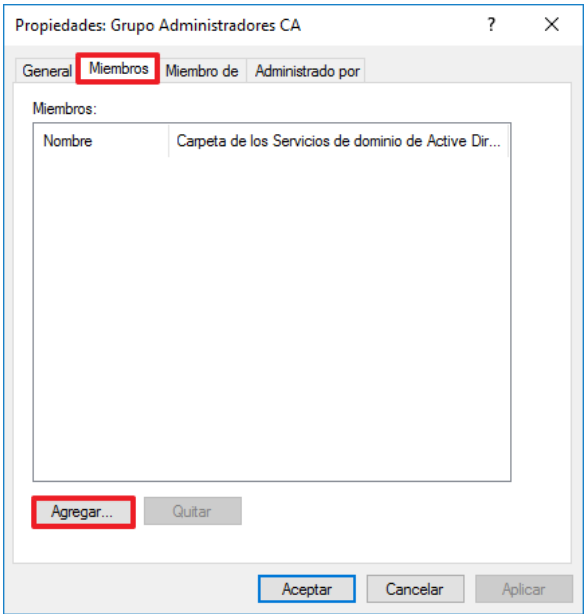
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificados y con el botón derecho del ratón selecciónela y pulse sobre <b>“Todas las tareas → Renovar certificado de CA...”</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                |
| 101. | <p>Pulse <b>“Sí”</b> en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 102. | <p>En la ventana <b>“Renovar certificado de CA”</b> seleccione <b>“No”</b> ante la pregunta de generar nuevas claves y pulse <b>“Aceptar”</b>.</p>  <p><b>Nota:</b> Si la entidad raíz es de empresa, no será necesario establecer ningún paso adicional, en caso de ser una Entidad de Certificación independiente del dominio, además de haber tenido que encenderla para realizar el proceso, será necesario extraer el fichero <b>“.CRT”</b> que se ha generado en la ruta <b>“%SYSTEMROOT%\System32\CertSrv\CertEnroll”</b> y pegarlas en la misma ruta, pero en la Entidad de Certificación subordinada de empresa.</p> |

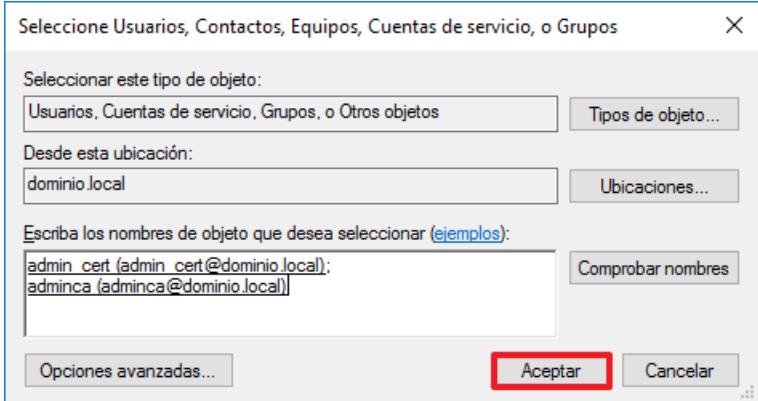
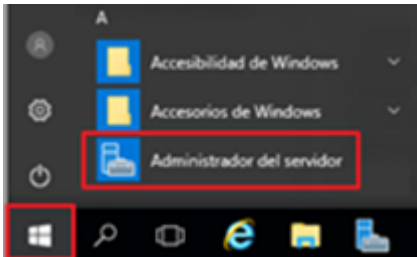
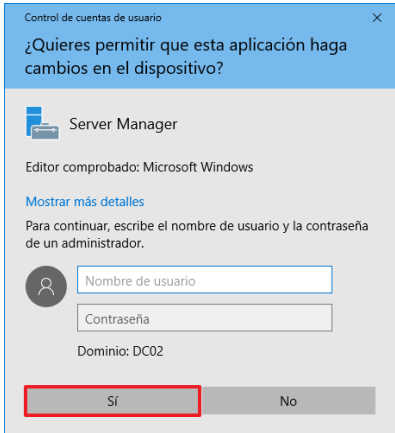
## 2.4. SEGREGACIÓN DE ROLES

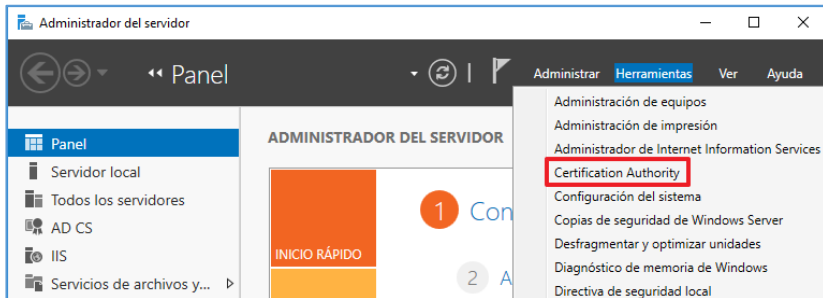
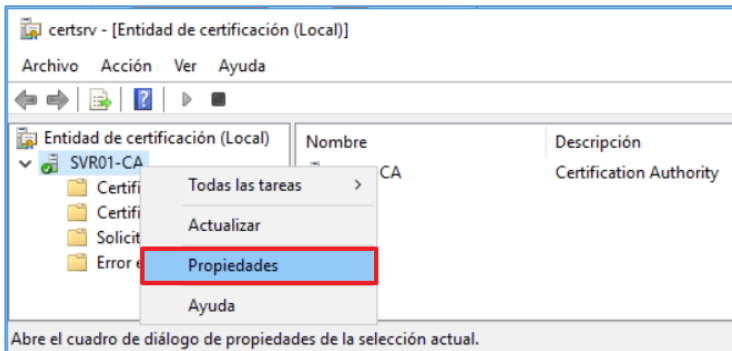
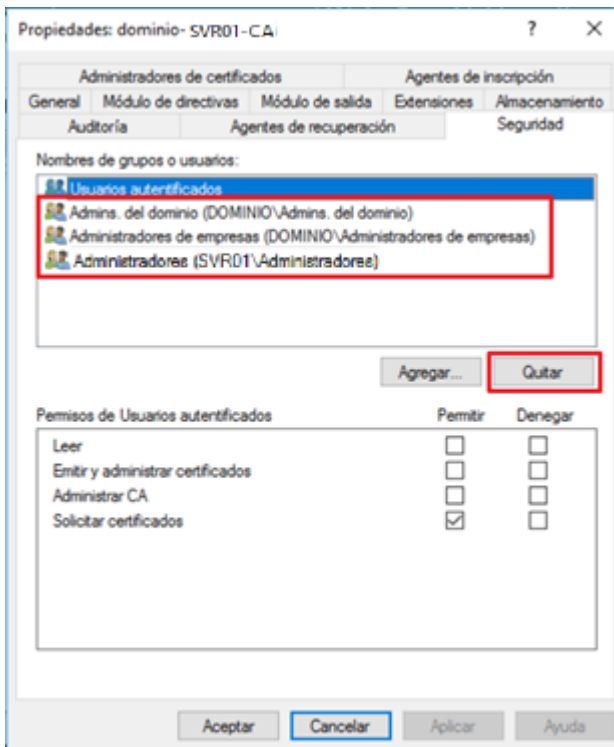
Con la aplicación del ENS para la categoría alta - DL sobre una Entidad de Certificación será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar una Entidad de Certificación.

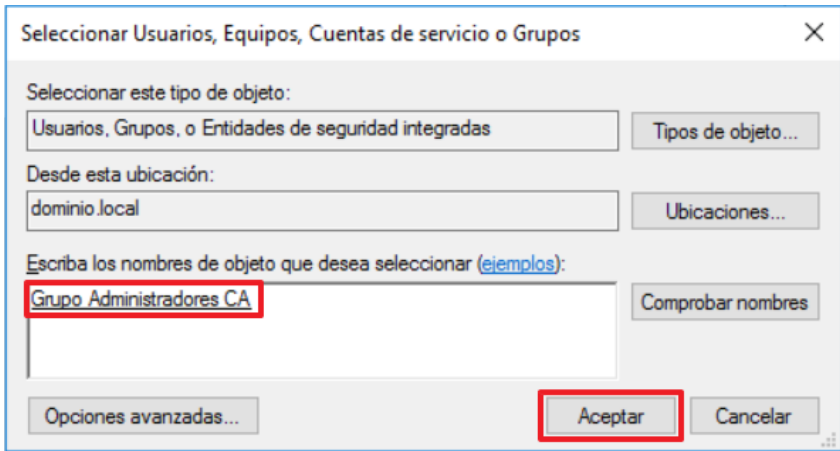
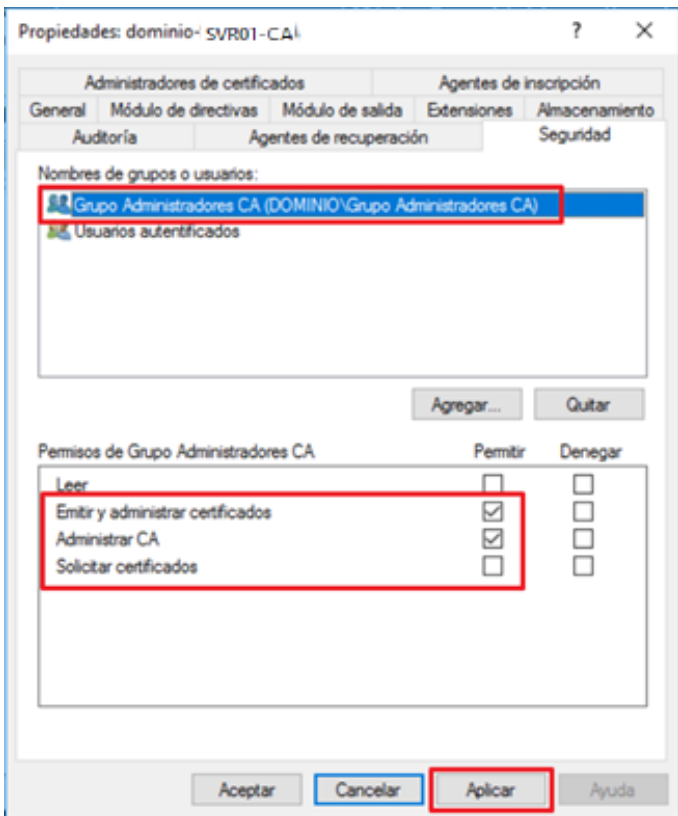
| Paso | Descripción                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 103. | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |
| 104. | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                    |
| 105. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. Introduzca sus credenciales y pulse “Sí”.</p>                                             |

| Paso | Descripción                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 106. | <p>Acceda al apartado “Herramientas” y seleccione “Usuarios y Equipos de Active Directory”.</p>                                                                 |
| 107. | <p>Despliegue el nodo “&lt;su dominio&gt; → Users”. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual “Nuevo → Grupo”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 108. | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |
| 109. | <p>Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>                  |

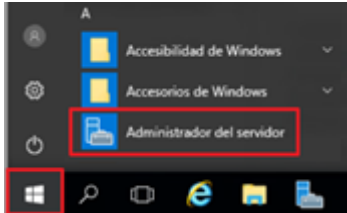
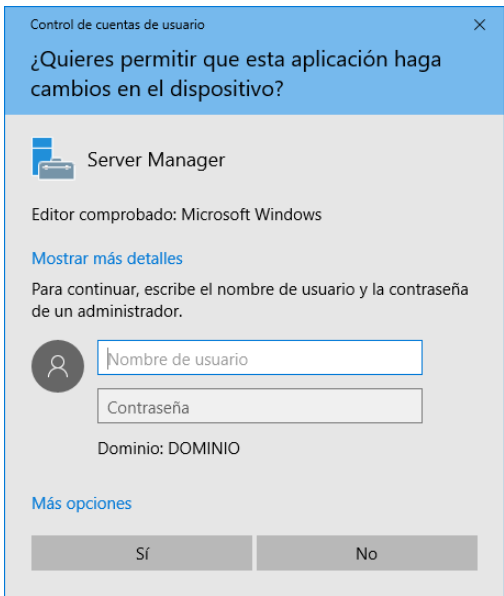
| Paso | Descripción                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 110. | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la generación de esta guía.”</p> |
| 111. | <p>A continuación, inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Entidad de Certificación.</p> <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador del dominio.</p>                                               |
| 112. | <p>A continuación, ejecute la consola administrativa “Certification Authority”. Para ello, clic en “Inicio de Windows → Administrador del servidor”.</p>                                        |
| 113. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                    |

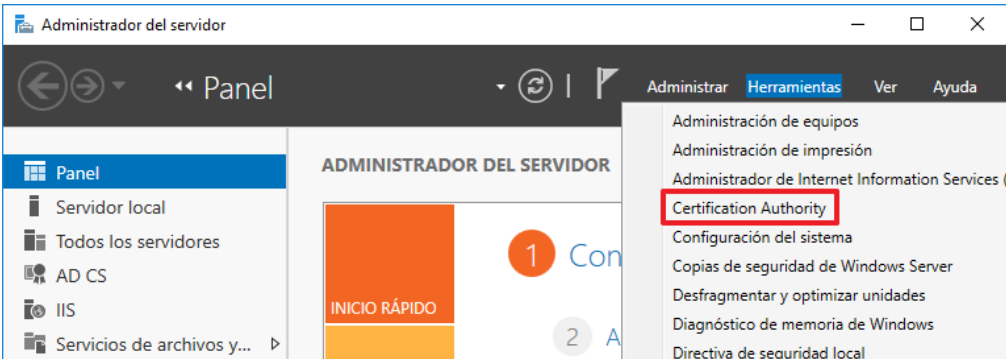
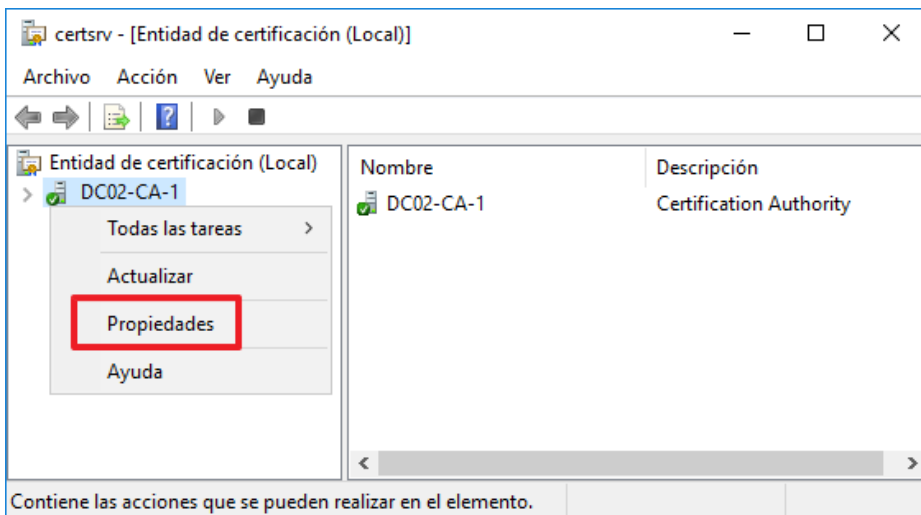
| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 114. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                   |
| 115. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>                                                                                            |
| 116. | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque uno a uno los grupos Administradores (del dominio, de empresa y locales) y, pulse “Quitar” para eliminar los grupos.</p>  |

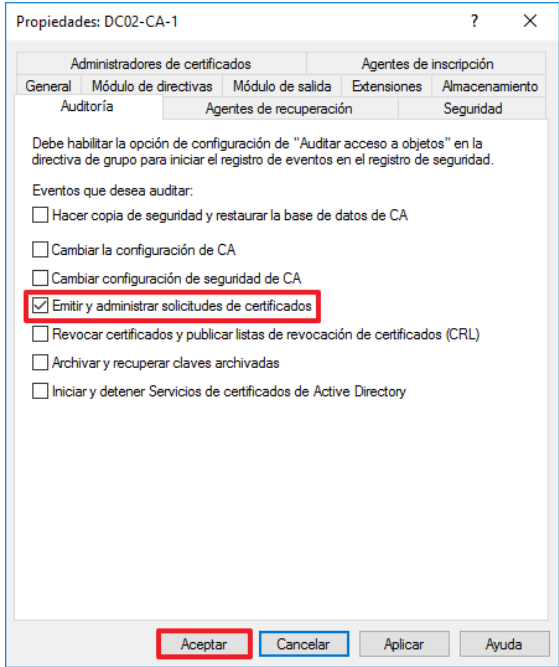
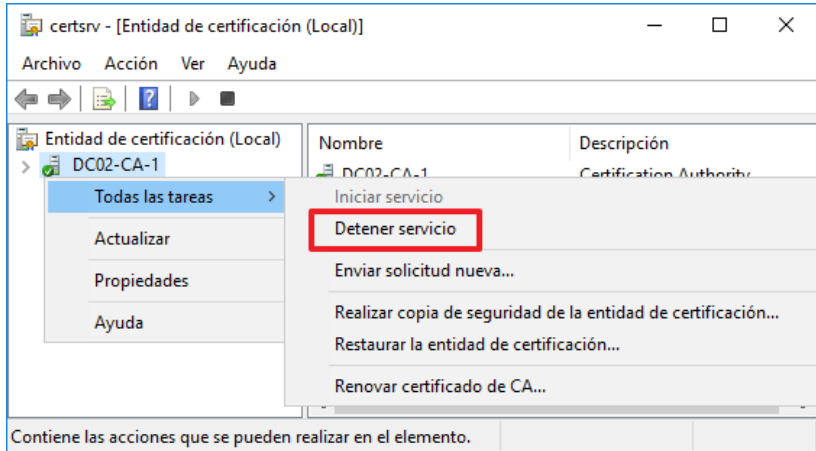
| Paso | Descripción                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 117. | <p>A continuación, añada el grupo “Grupo Administradores CA” y pulse “Aceptar”.</p>                                                                                                                                  |
| 118. | <p>Seleccione el grupo recién añadido, otórguele los permisos “Emitir y administrar certificados” y “Administrar CA” y desmarque la opción “Solicitar certificados”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 119. | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                                                                 |

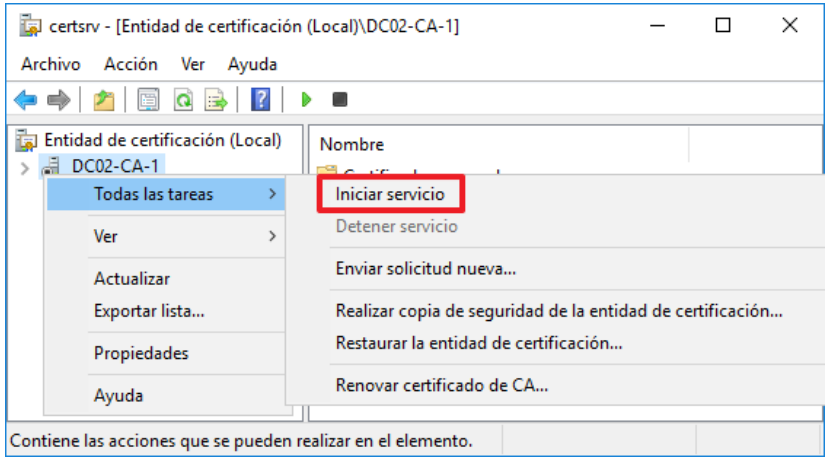
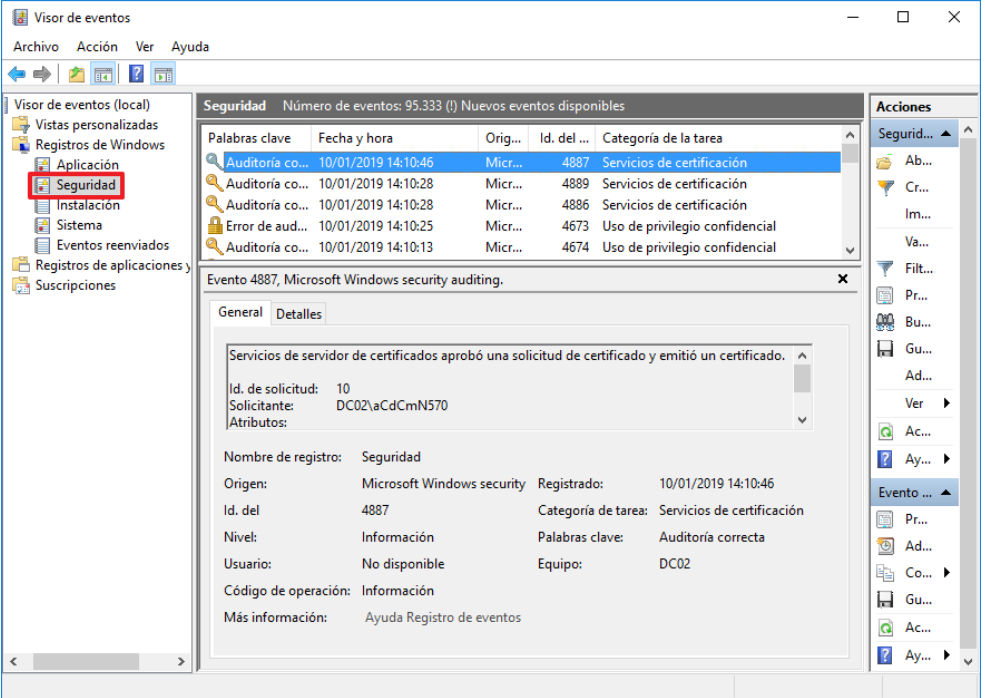
## 2.5. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

Existe la posibilidad de auditar el control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoría de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma.

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 120. | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                            |
| 121. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 122. | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.</p>                                      |

| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 123. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                   |
| 124. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 125. | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: <b>“Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales”</b>.</p> |
| 126. | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú <b>“Todas las tareas → Detener servicio”</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 127. | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú “<b>Acción → Todas las tareas → Iniciar servicio</b>” para iniciarlo de nuevo.</p>                                                                                                                                                                                                                                                                                                                        |
| 128. | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: “<b>Inicio → Herramientas administrativas → Visor de eventos</b>”. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: “<b>Visor de eventos (local) → Registro de Windows → Seguridad</b>”.</p> |

## ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en Entidad de Certificación sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría alta – Difusión Limitada del ENS / Difusión Limitada.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.4.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN MIEMBRO DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA.

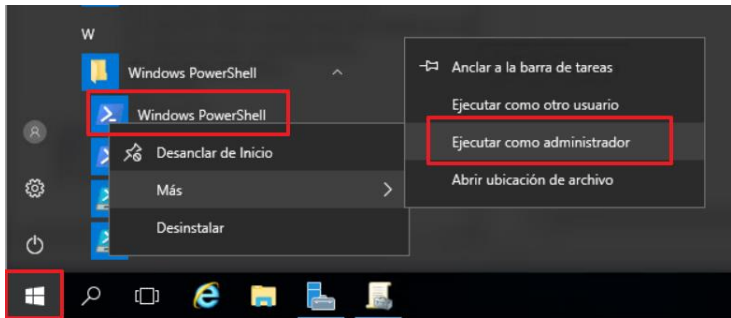
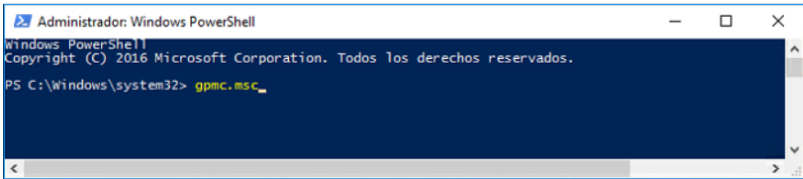
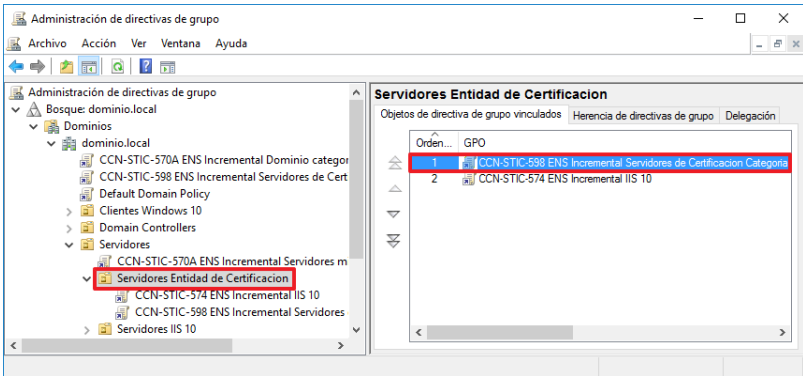
### 1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

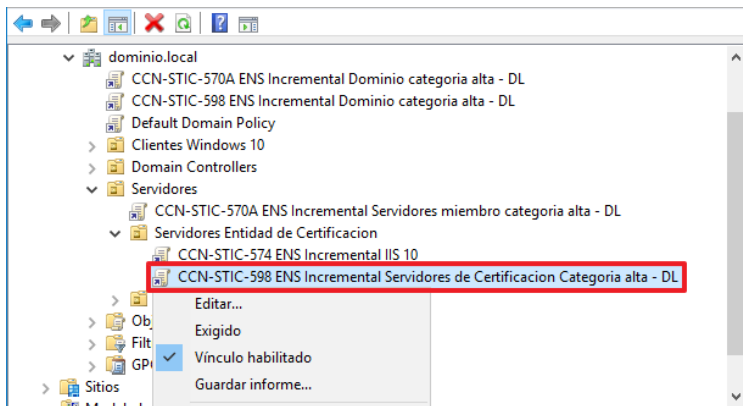
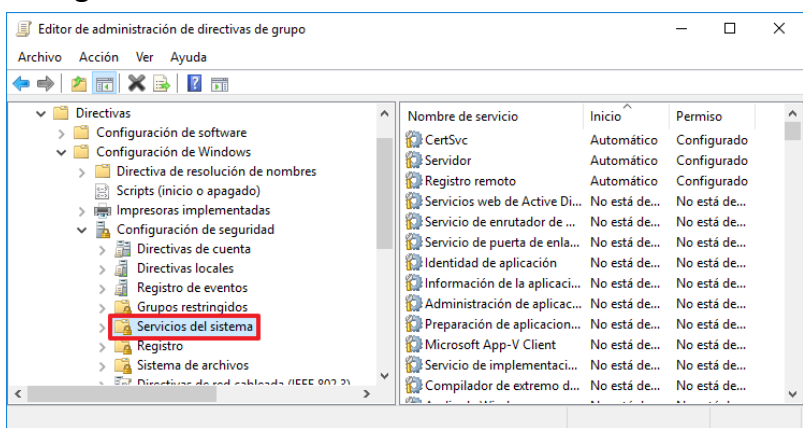
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

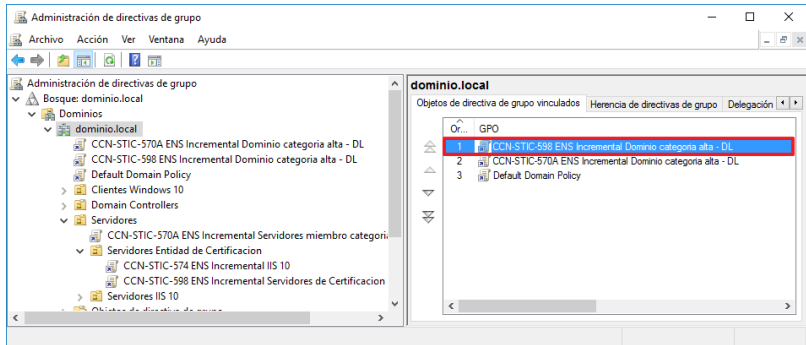
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

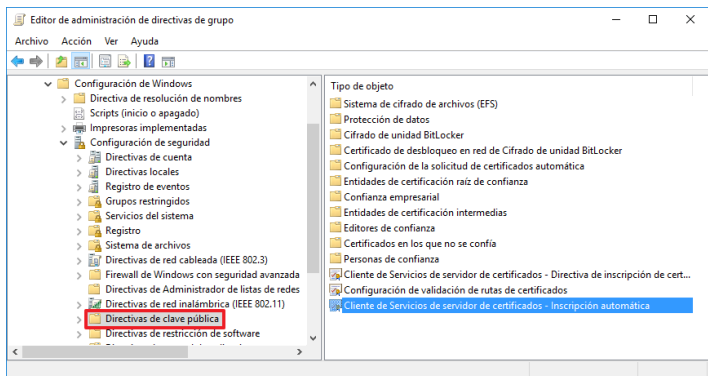
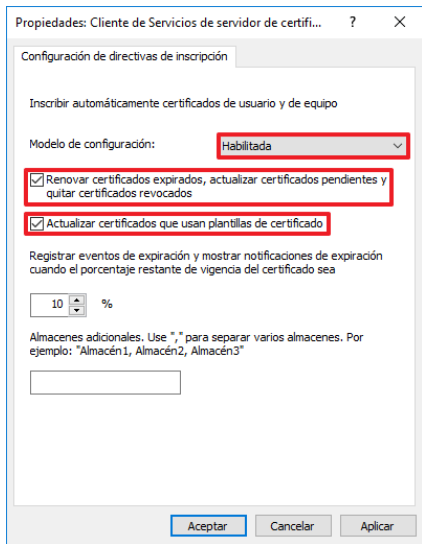
**Nota:** La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

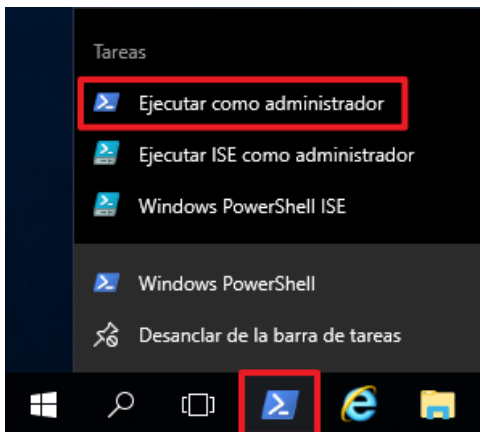
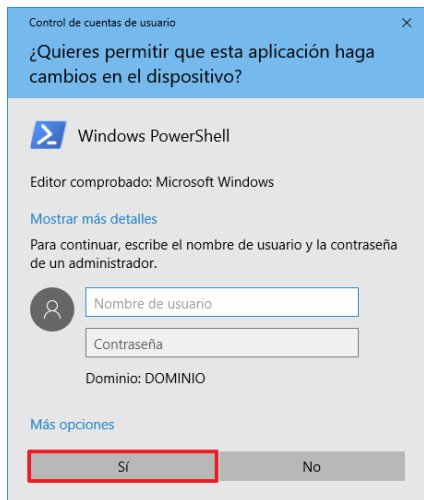
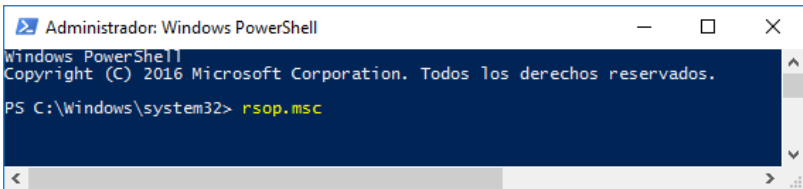
| Comprobación                                   | OK/NOK | Cómo hacerlo                                                                                                              |
|------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------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

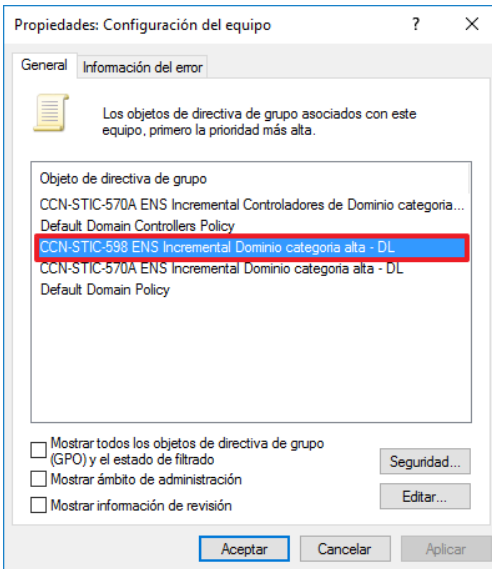
| Comprobación                                                                                                              | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Abra el administrador de directivas de grupo                                                                           |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic en “Inicio de Windows” y, con el botón derecho sobre el icono de PowerShell de la lista de programas, y, en el menú contextual que aparecerá, marque la opción "Ejecutar como administrador":</p>  <p>El control de cuentas de usuario le solicitará confirmación de ejecución, para ello, haga clic en “Sí”.</p> <p>Teclee “gpmmc.msc” en la consola de comandos que se ha abierto:</p>  |
| 3. Verifique que está creada la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL”. |        | <p>Ejecute el “Administrador de directivas de grupo” mediante la siguiente ruta:<br/> <b>“Inicio → Herramientas administrativas → Administración de directivas de grupo”</b></p> <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores Entidad de Certificación”. Verifique que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL” está creada y vinculada en el primer lugar de orden de vínculo.</p>                                                                              |

| Comprobación                                                                                                                           | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |        |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| 4. Verifique los servicios del sistema de la directiva “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL”. |                         | <p>Haga clic derecho sobre la directiva y seleccione “Editar” para ejecutar el “Editor de Administración de directivas de grupo”.</p>  <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:<br/><b>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</b></p>  <p><b>Nota:</b> Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</p> |             |        |
| Servicio (Nombre largo)                                                                                                                | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                          | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Servidor                                                                                                                               | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Registro Remoto                                                                                                                        | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |

| Comprobación                                                                                          | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Dominio categoria alta - DL". |        | <p>Ejecute el "Administrador de directivas de grupo" a través de la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b></p> <p>Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política "CCN-STIC-598 ENS Incremental Dominio categoria alta- DL" está creada y vinculada en el primer lugar de orden de vínculo.</p>  |

| Comprobación                                                                                                                                       | OK/NOK               | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------|--------|-------------------------|------------|--|----------------------------------------------------------------------------------------------------|----------------------|--|------------------------------------------------------------|----------------------|--|
| 6. Verifique la configuración de inscripción automática de certificados en la política "CCN-STIC-598 ENS Incremental Dominio categoria alta - DL". |                      | <p>Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo". Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:</p> <p><b>Directiva CCN-STIC-598 ENS Incremental Dominio categoria alta – DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  <p>Haga doble clic sobre el objeto "Cliente de Servicios de servidor de certificados – Inscripción automática" y compruebe los valores correspondientes a la inscripción automática.</p>  <table border="1"> <thead> <tr> <th>Configuración</th><th>Estado</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Modelo de configuración</td><td>Habilitada</td><td></td></tr> <tr> <td>Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados</td><td>Habilitada (marcada)</td><td></td></tr> <tr> <td>Actualizar certificados que usan plantillas de certificado</td><td>Habilitada (marcada)</td><td></td></tr> </tbody> </table> | Configuración | Estado | OK/NOK | Modelo de configuración | Habilitada |  | Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados | Habilitada (marcada) |  | Actualizar certificados que usan plantillas de certificado | Habilitada (marcada) |  |
| Configuración                                                                                                                                      | Estado               | OK/NOK                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Modelo de configuración                                                                                                                            | Habilitada           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados                                                 | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Actualizar certificados que usan plantillas de certificado                                                                                         | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |

| Comprobación                                                                                                                                | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. Verifique la correcta aplicación de la política "CCN-STIC-598 Incremental Dominio categoría alta - DL" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Introduzca sus credenciales y pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                     |
|--------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>A continuación, haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría alta - DL” aparece en la lista como muestra la imagen.</p>  |

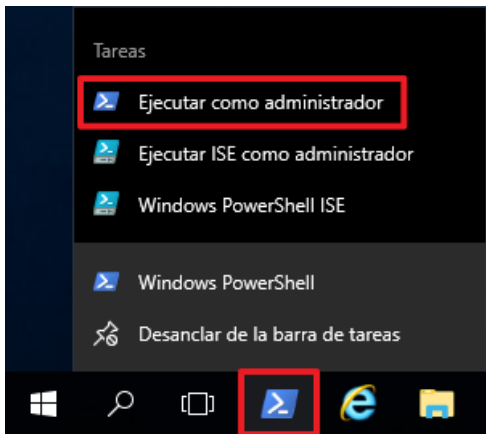
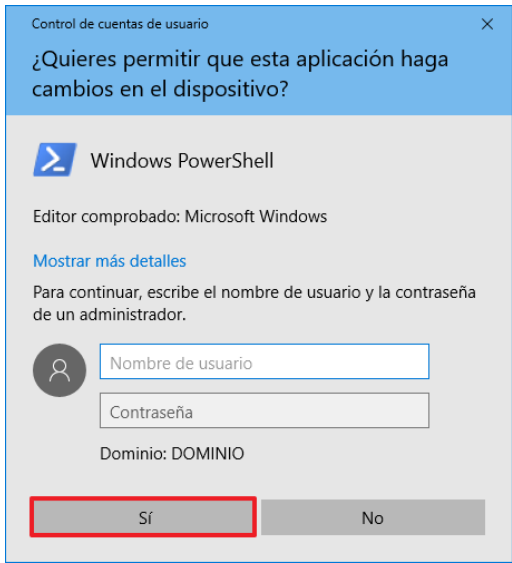
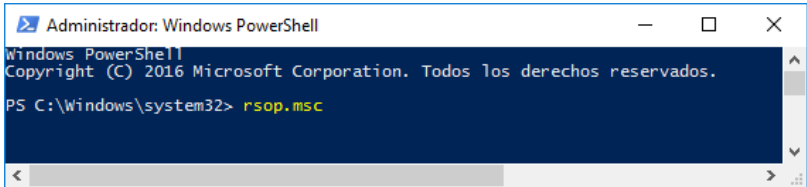
## 2. COMPROBACIONES EN SERVIDOR MIEMBRO

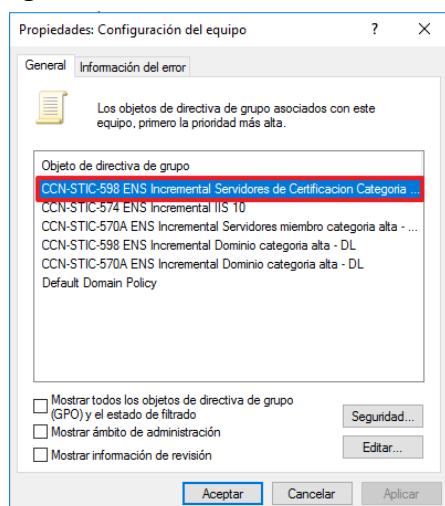
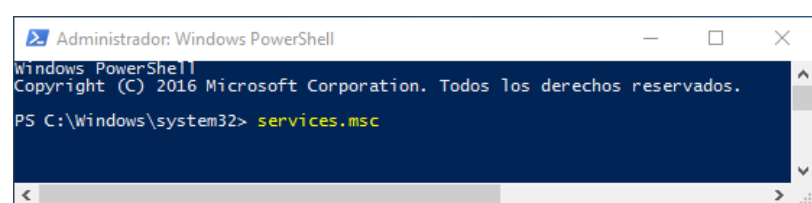
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

Para realizar las comprobaciones pertinentes en los servidores miembros se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

- Administrador del Servidor
- Conjunto resultante de directivas (rsop.msc)
- Consola de servicios (services.msc)

| Comprobación                                                              | OK/NOK | Cómo hacerlo                                                                                                                               |
|---------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación raíz de empresa. |        | En el servidor Entidad de Certificación raíz de empresa, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |

| Comprobación                                                                                                                                                        | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Verifique la correcta aplicación de la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL" en un equipo miembro del dominio. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario".</p>  <p>Teclee "rsop.msc" en la consola de comandos que se ha abierto:</p>  |

| Comprobación                                                                                                                                                                   | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                            |             |        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                                |                         | <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL” aparece en la lista como muestra la imagen.</p>  |             |        |
| 3. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                     |             |        |
| Servicio (Nombre largo)                                                                                                                                                        | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                  | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                                  | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                              | Configurado |        |
| Servidor                                                                                                                                                                       | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                              | Configurado |        |
| Registro Remoto                                                                                                                                                                | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                              | Configurado |        |

### ANEXO A.4.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tengan que aplicar medidas de seguridad sobre una entidad de certificación en Microsoft Windows Server 2016 independientes con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

**Nota:** Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará uso de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho caso.

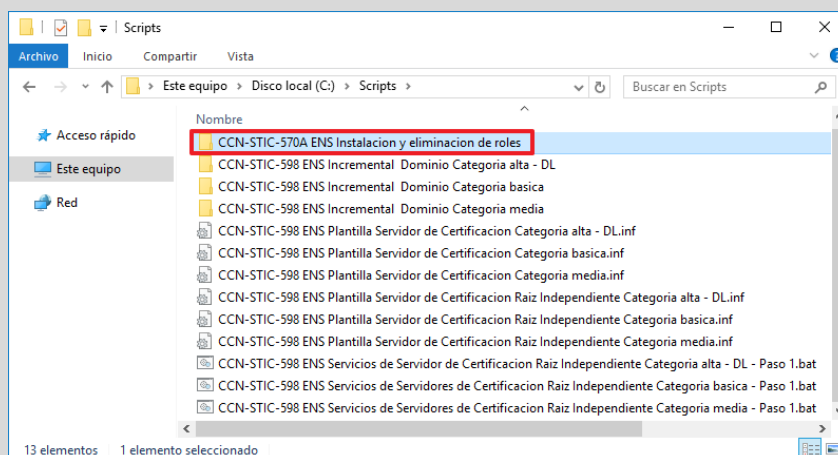
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad para comprobar su correcta funcionalidad.

Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

- a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad media.
- b) Un servidor independiente del dominio preparado siguiendo la guía CCN-STIC-570B Anexo A con una categorización de seguridad media.
- c) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad media.

**Nota:** Si instala el Servidor entidad de certificación por primera vez con la guía “CCN-STIC-570A – Implementación del ENS en Windows Server 2016” aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.

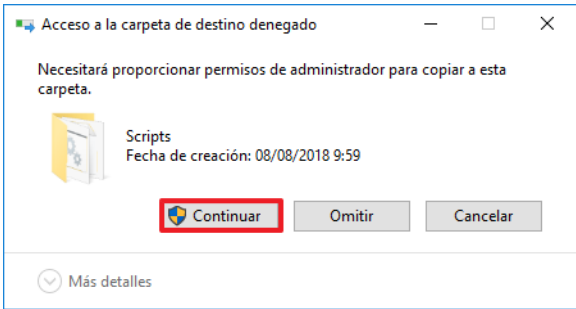
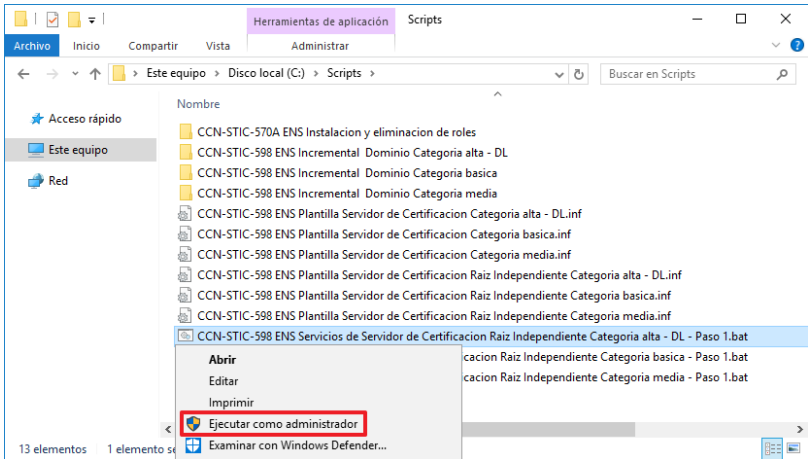
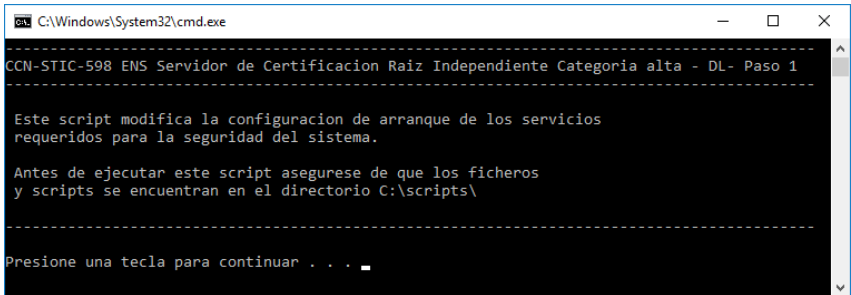
En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía “CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016” encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta “Scripts” adjunta a la presente guía.

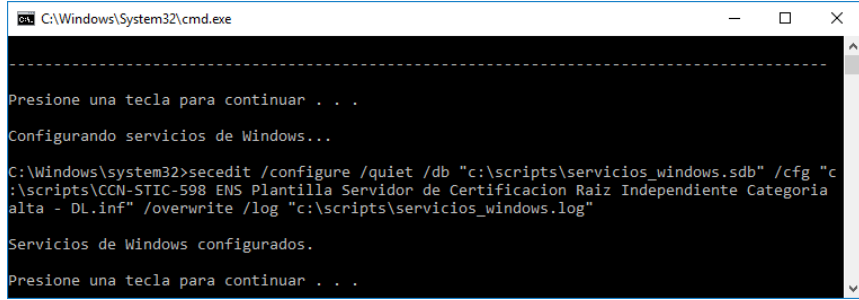
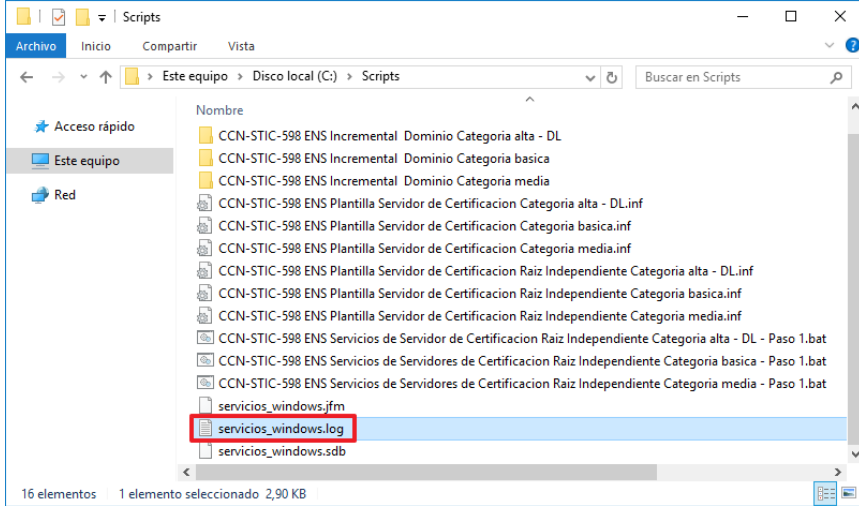
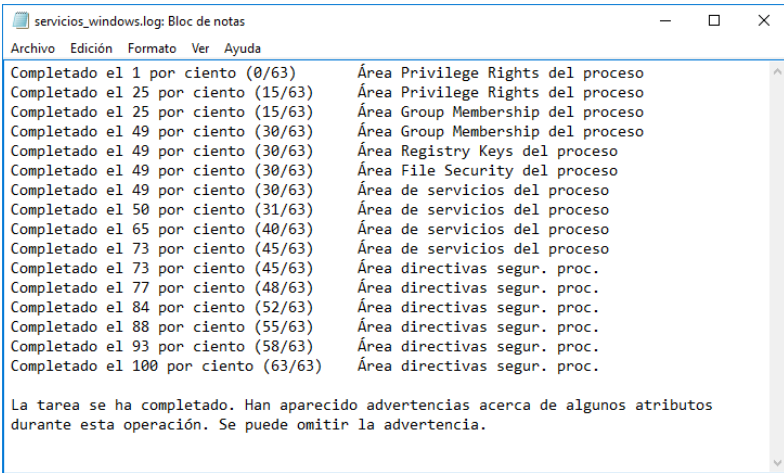


## 1. CONFIGURACIONES DE SEGURIDAD SOBRE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE DEL DOMINIO

Los pasos que se describen a continuación se realizarán en todos aquellos servidores Entidad de Certificación raíz independiente del dominio sobre Microsoft Windows Server 2016, que implementen servicios o información de categoría alta – DL y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

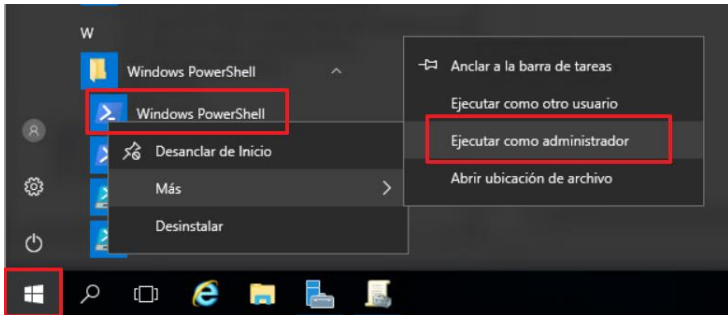
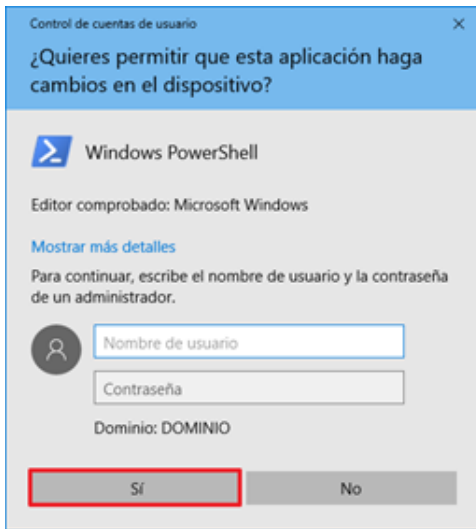
| Paso | Descripción                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor independiente donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que tenga privilegios de Administrador.</p> |
| 2.   | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                        |

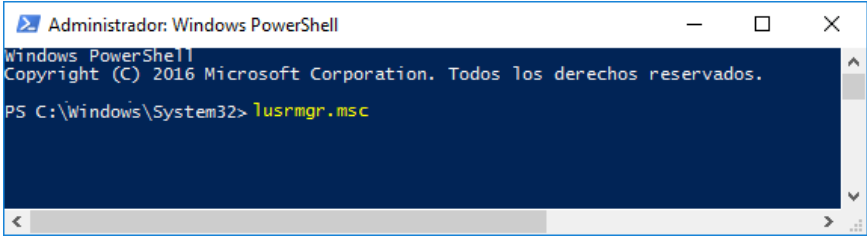
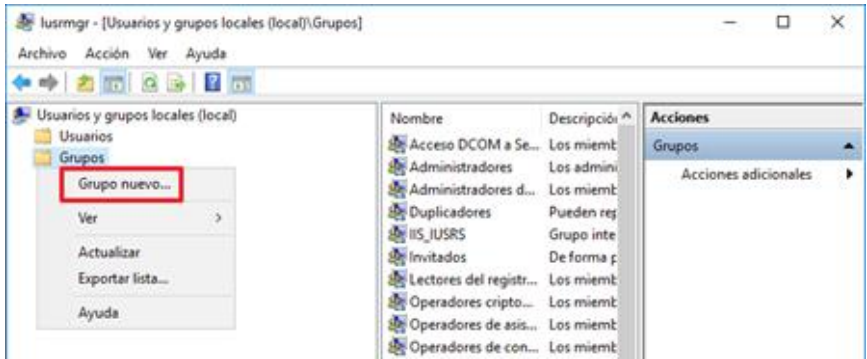
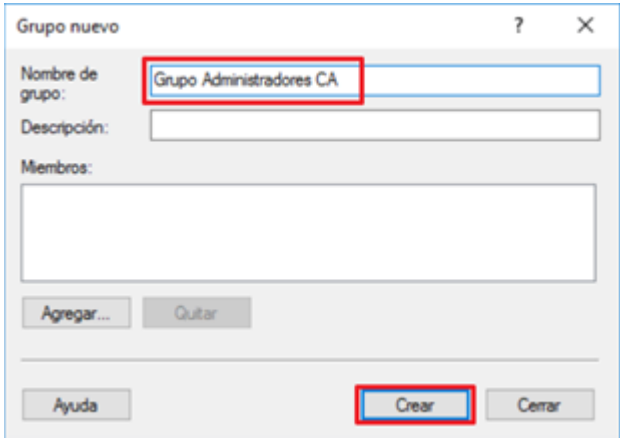
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.   | <p>Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.</p>  <p><b>Nota:</b> Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Haga clic en el botón “Continuar” e introduzca las credenciales.</p>                                                                                                                                                                                                                                                                                                                                                                     |
| 4.   | <p>A continuación, diríjase a la carpeta “C:\Scripts” y ejecute con permisos de administrador el script “CCN-STIC ENS Servicios de Certificacion Raíz Independiente Categoría alta - DL – Paso 1.bat”. Este script aplica al sistema la plantilla de servicios para la seguridad del sistema.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.</p> |
| 5.   | <p>Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría alta - DL del ENS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

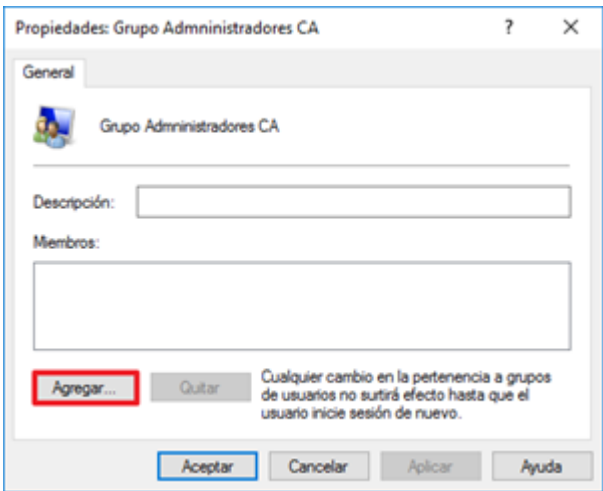
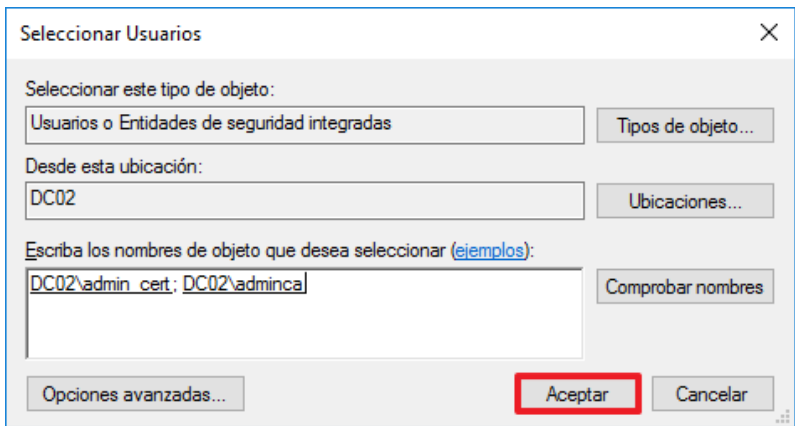
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | <p>Una vez completado el proceso, deberá pulsar una tecla para continuar.</p>  |
| 7.   | <p>Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta "C:\Scripts" con el nombre de "servicios_windows.log".</p>                                                                                                                                                                                                                                                                                                  |
| 8.   | <p>Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.</p>                                                                                                                                                                                                                                                                                               |

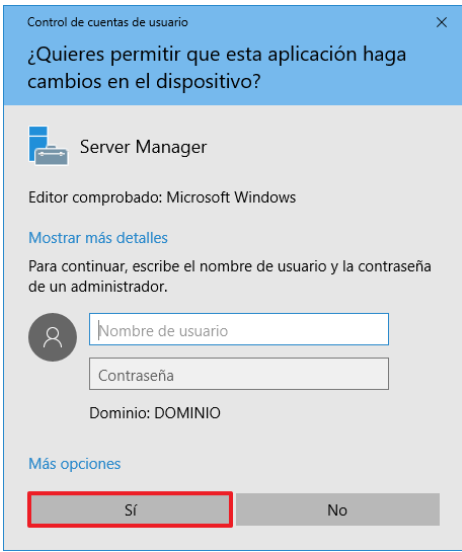
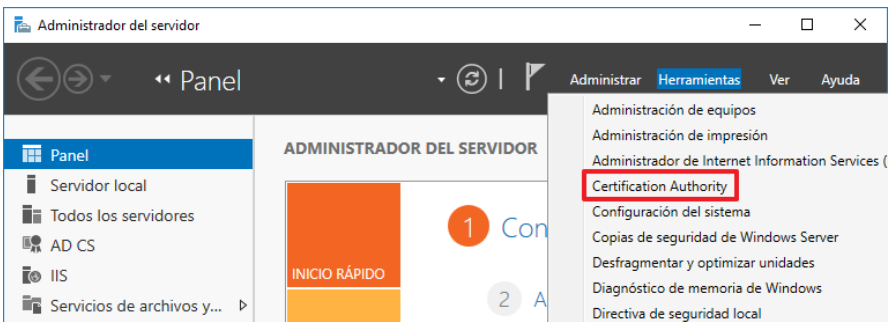
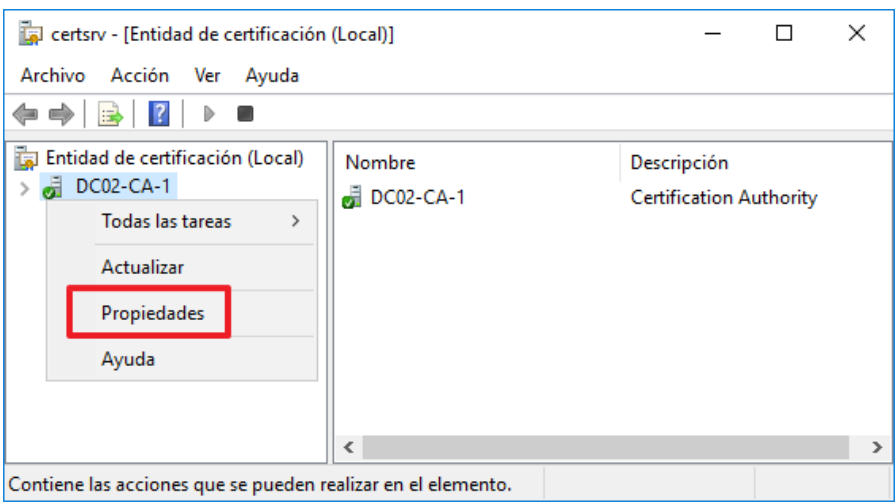
## 1.1. SEGREGACIÓN DE ROLES

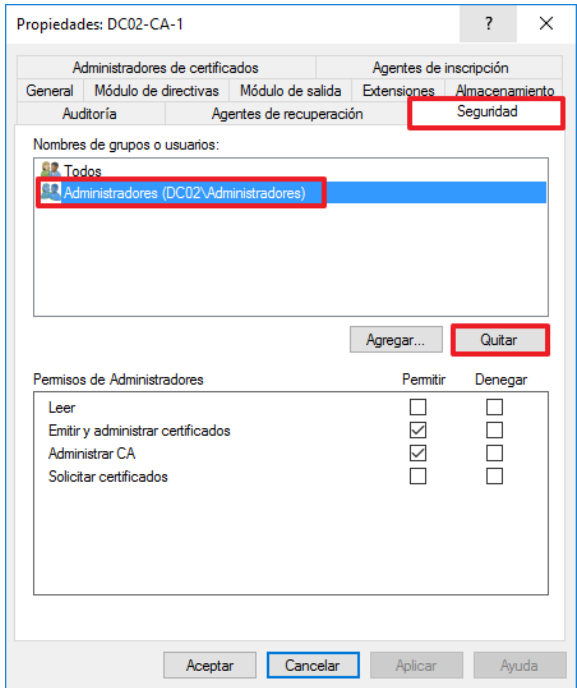
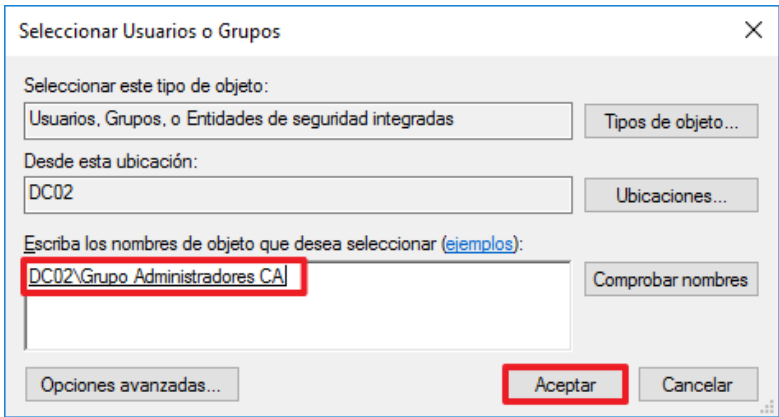
Con la aplicación del ENS para la categoría alta - DL sobre el Servidor de Certificación Raíz Independiente será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar el Servidor de Certificación.

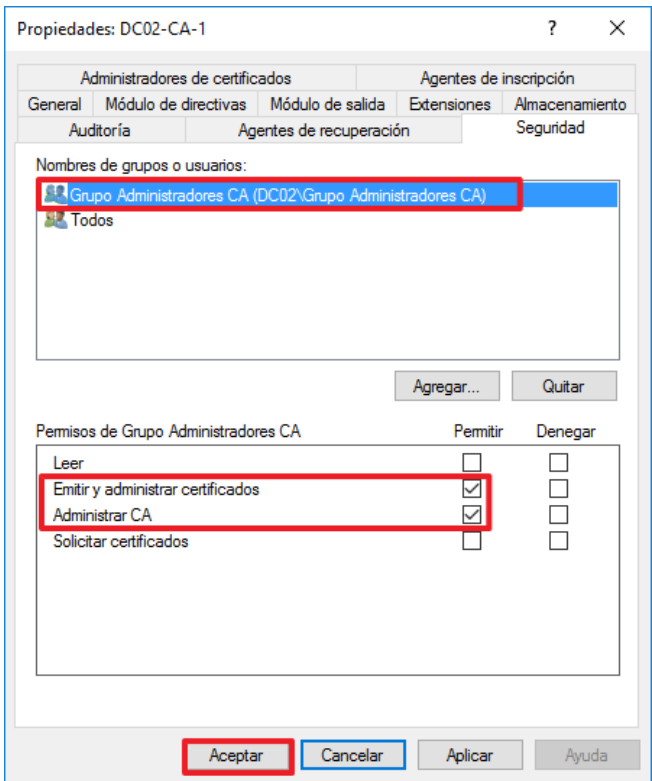
| Paso | Descripción                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.   | <p>Inicie sesión en Servidor de Certificación raíz independiente.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador local.</p>                                                                             |
| 10.  | <p>Ejecute la consola de PowerShell. Para ello pulse sobre “Inicio”, seleccione <b>“Windows Powershell → Windows Powershell”</b> con el botón derecho y pulse sobre la opción <b>“Más → Ejecutar como administrador”</b>.</p>  |
| 11.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                |

| Paso | Descripción                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.  | <p>Teclee “lusrmgr.msc” en la consola de comandos que se ha abierto.</p>                                                                                                    |
| 13.  | <p>Pulse con el botón derecho sobre “Grupos” y seleccione la opción del menú contextual “Grupo nuevo...”.</p>                                                              |
| 14.  | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.  | <p>Haga doble clic sobre el grupo recién creado y pulse la pestaña “Agregar grupo...”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>                                      |
| 16.  | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la creación de esta guía.”</p> |
| 17.  | <p>A continuación, ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                          |

| Paso | Descripción                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18.  | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca sus credenciales y pulse “Sí” para continuar.</p>                                                          |
| 19.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                  |
| 20.  | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p> |

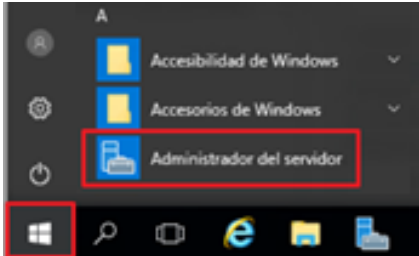
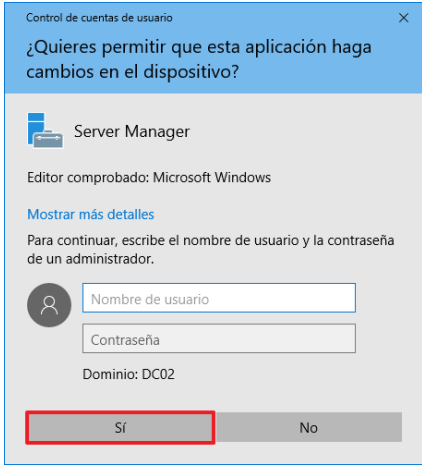
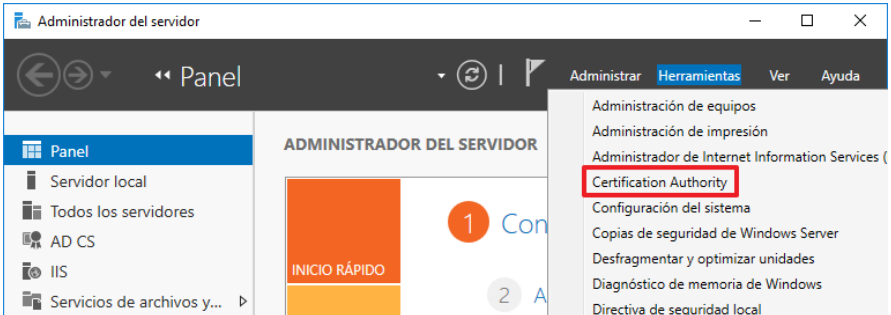
| Paso | Descripción                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21.  | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque el grupo Administradores. Pulse “Quitar” para eliminar el grupo Administradores.</p>  |
| 22.  | <p>A continuación, añada el grupo recién creado y pulse “Aceptar”.</p>                                                                                         |

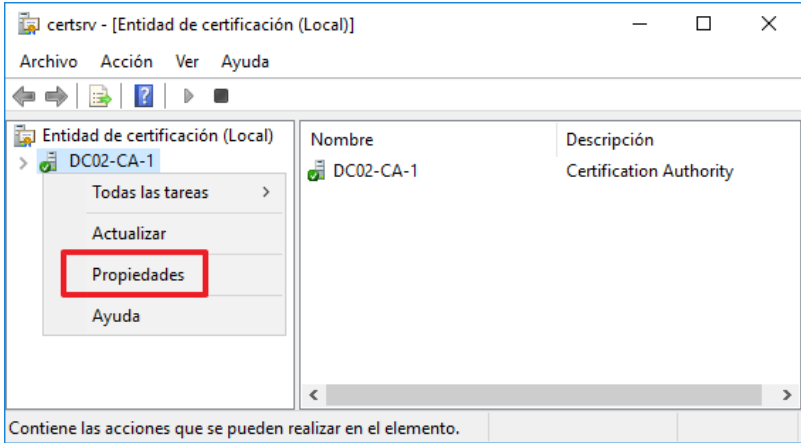
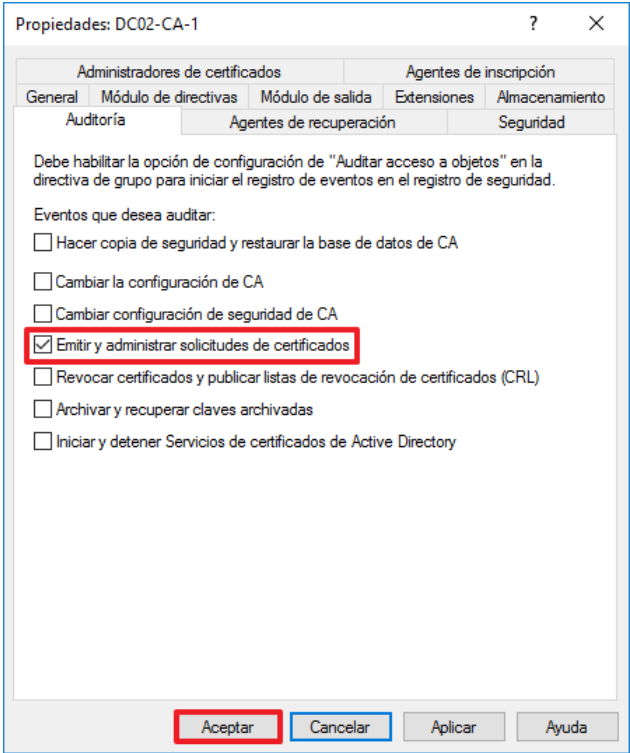
| Paso | Descripción                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23.  | <p>Seleccione el grupo recién añadido y otórguele los permisos “Emitir y administrar certificados” y “Administrar CA”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 24.  | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                   |

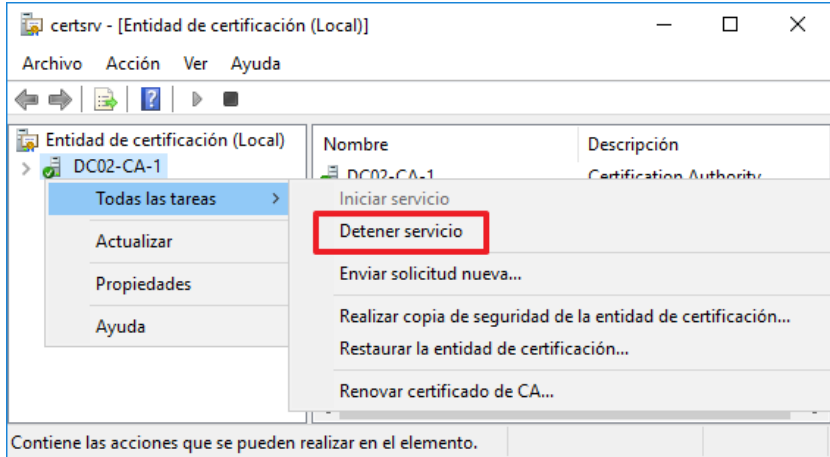
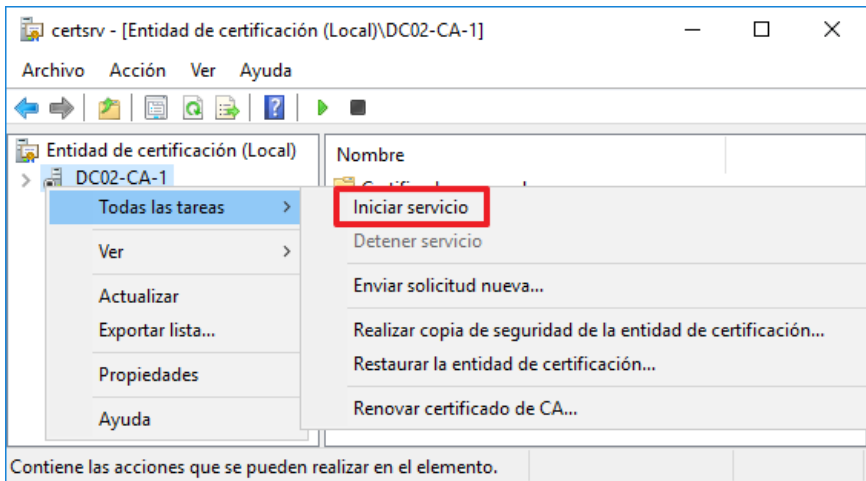
## 1.2. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

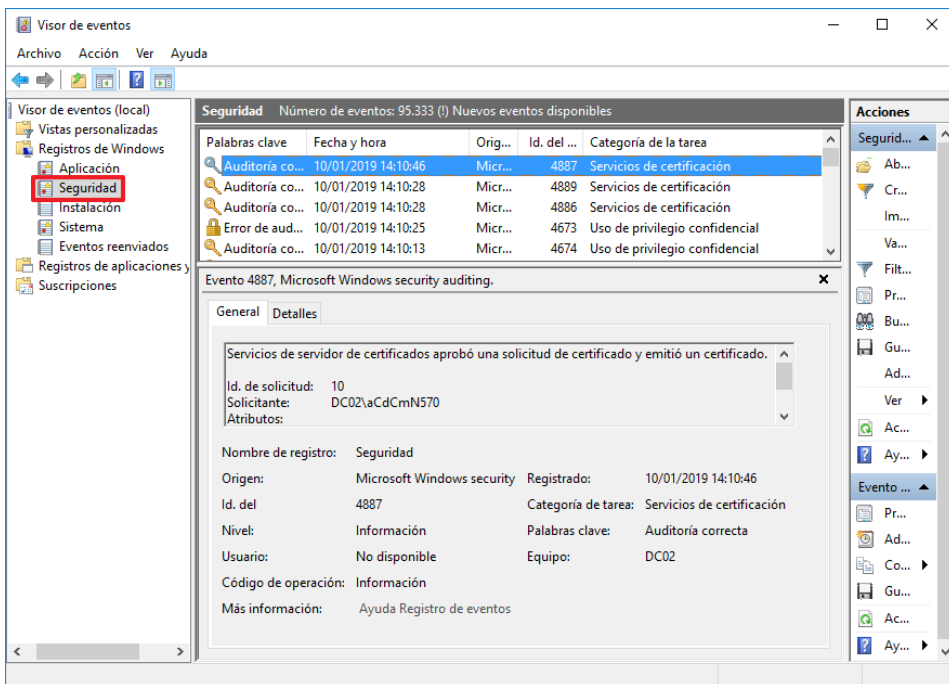
Existe la posibilidad que auditores lleven un control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoría de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma.

| Paso | Descripción                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25.  | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                         |
| 27.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”</p>  |
| 28.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                         |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29.  | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “DC02-CA-1”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 30.  | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31.  | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú <b>“Todas las tareas → Detener servicio”</b>.</p>                                         |
| 32.  | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú <b>“Acción → Todas las tareas → Iniciar servicio”</b> para iniciarlo de nuevo.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33.  | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: <b>"Inicio → Herramientas administrativas → Visor de eventos"</b>. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: <b>"Visor de eventos (local) → Registro de Windows → Seguridad"</b>.</p> |

## 2. CONSIDERACIONES DE SEGURIDAD SOBRE EL DOMINIO

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría alta.

No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

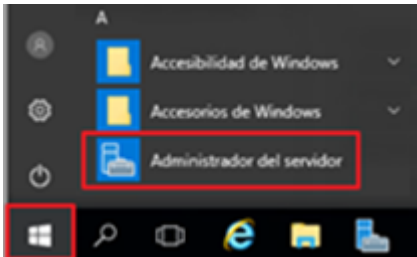
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

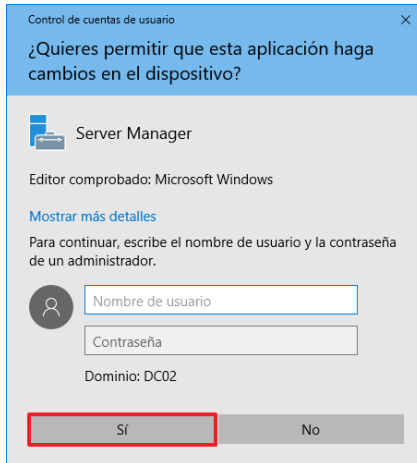
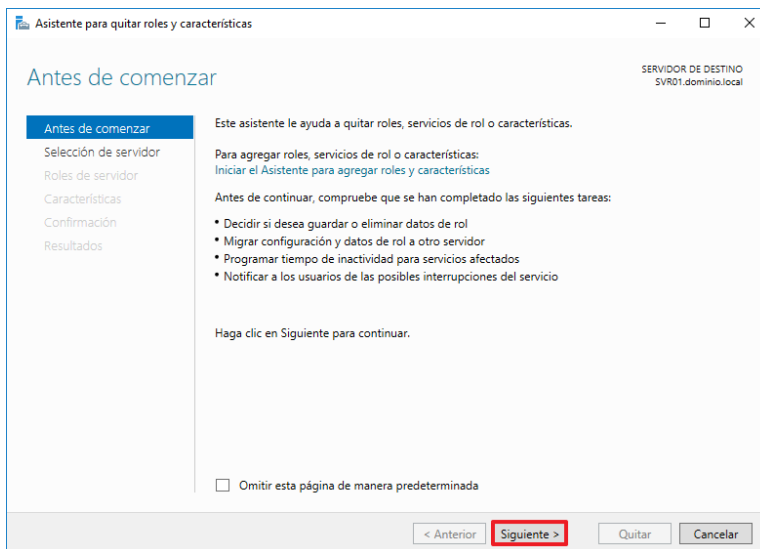
## 2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

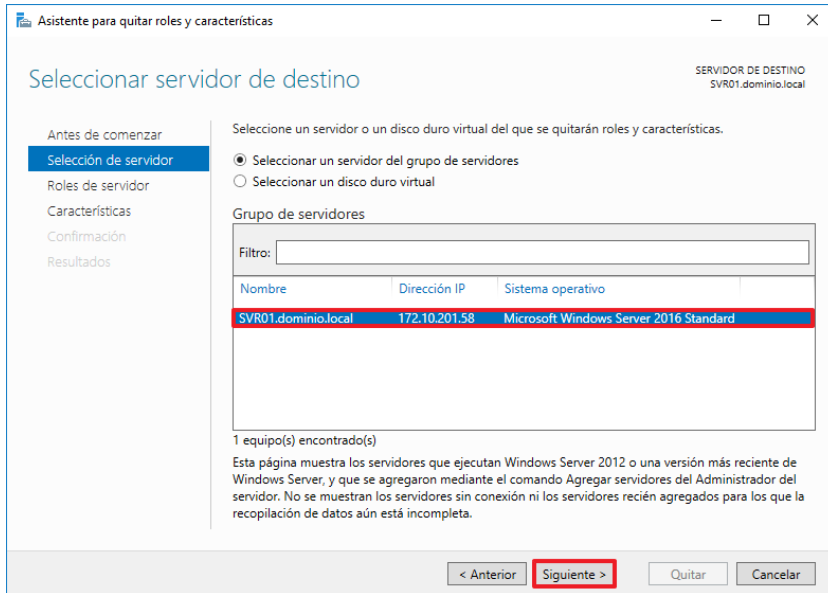
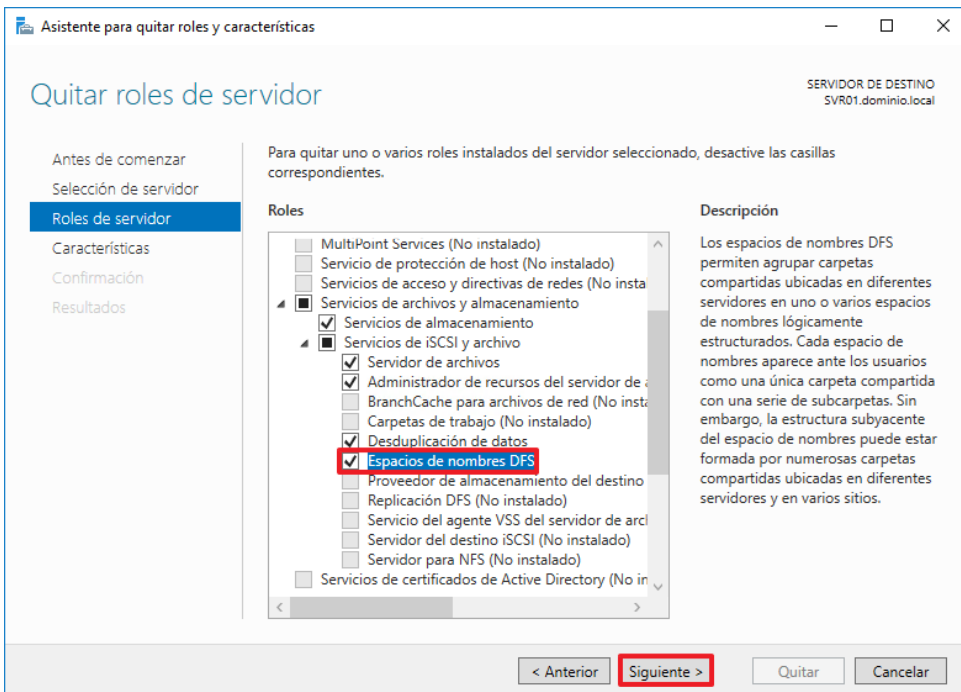
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

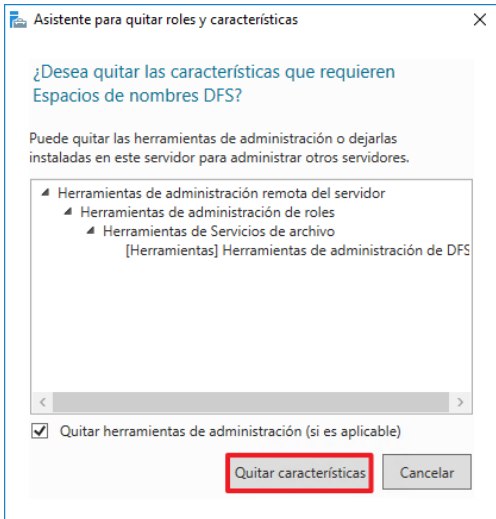
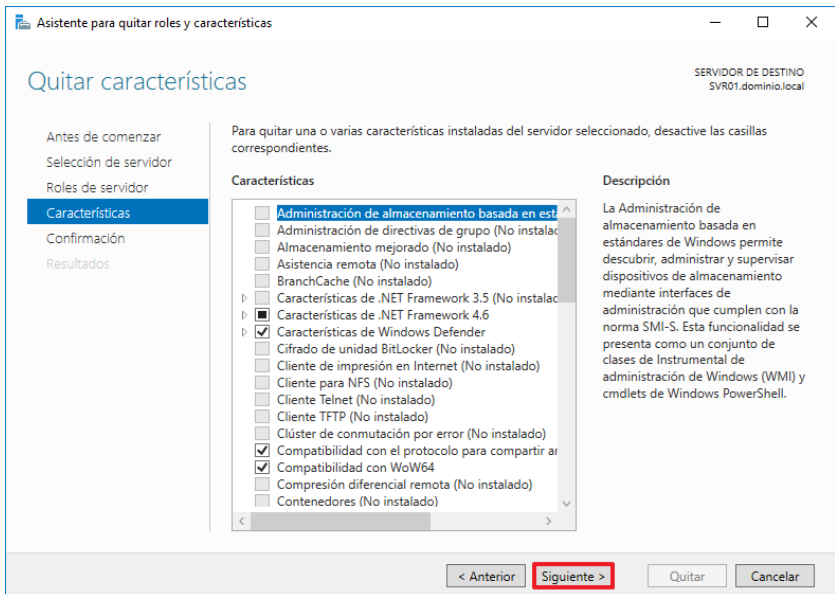
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de Certificación.

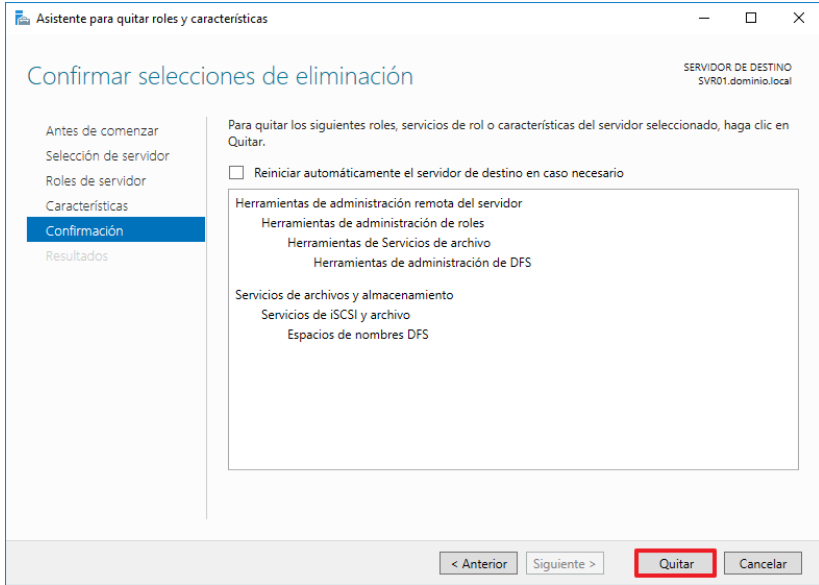
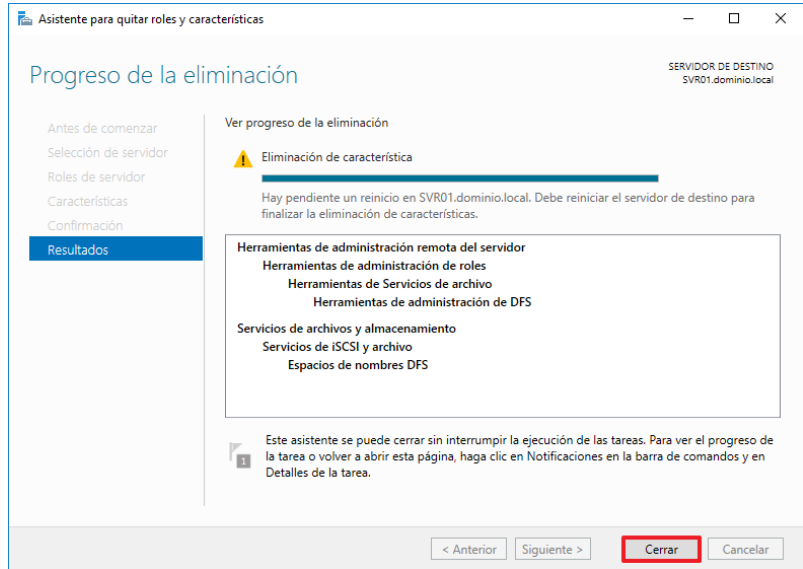
**Nota:** Para continuar con el siguiente paso a paso deberá realizar previamente el “ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR MIEMBRO O CONTROLADOR DE DOMINIO QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA O ALTA DEL ENS” de la guía “CCN-STIC-570A - Implementación del ENS en Microsoft Windows Server 2016” y una vez finalizado deberá desvincular y/o eliminar la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” creada en dicho anexo.

| Paso | Descripción                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34.  | <p>Inicie sesión en el servidor miembro donde tenga instalado el rol Entidad Certificadora.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.</p> |
| 35.  | <p>Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                                                   |

| Paso | Descripción                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 36.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>  |
| 37.  | <p>A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.</p>                                                                 |
| 38.  | <p>Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente &gt;” para continuar.</p>                                                    |

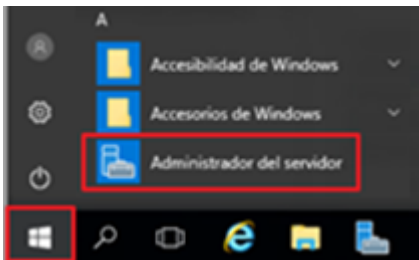
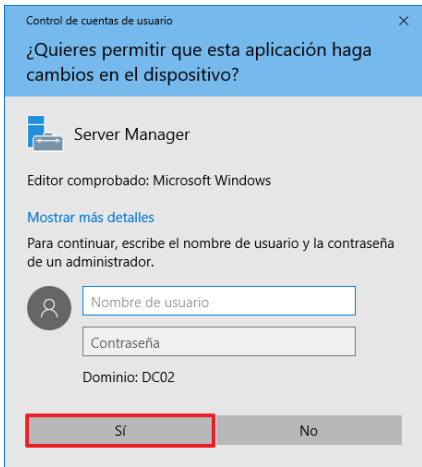
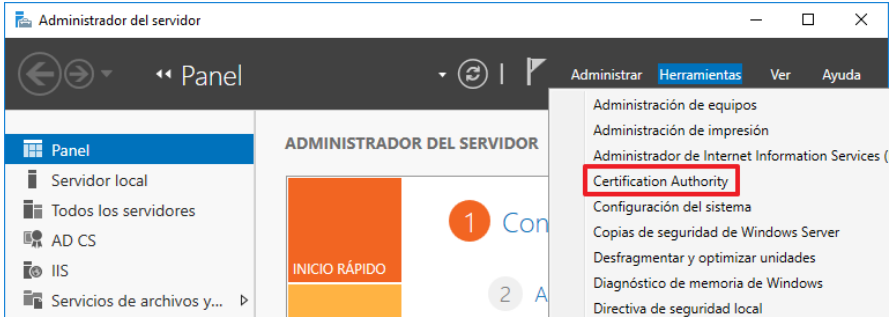
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 39.  | <p>Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el servidor con el nombre “SVR01”.</p>                                                       |
| 40.  | <p>En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> En este ejemplo se desinstala el rol “Espacios de nombres DFS”.</p> |

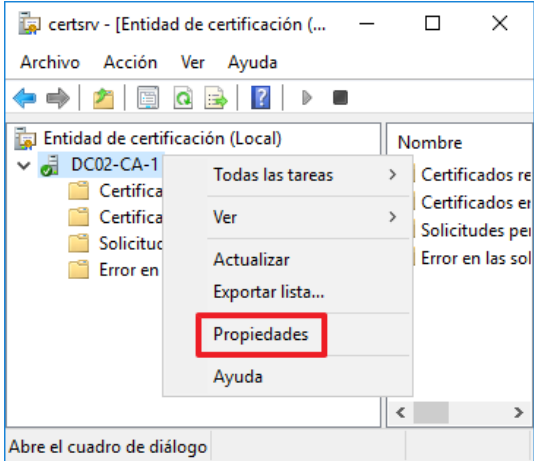
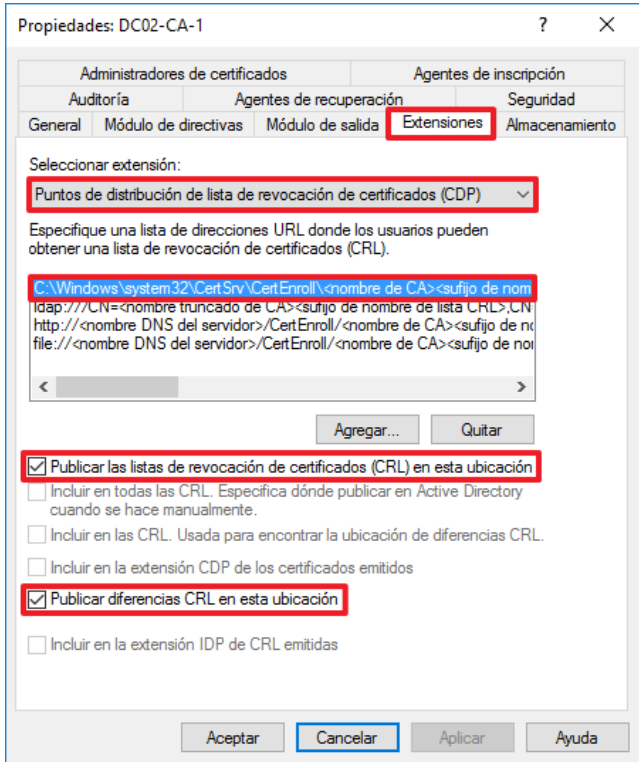
| Paso | Descripción                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 41.  | <p>En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.</p>  <p><b>Nota:</b> En este ejemplo se eliminan las características que dependen del rol.</p> |
| 42.  | <p>En la ventana de características pulse el botón “Siguiente &gt;”. En este ejemplo no se desinstala ninguna característica adicional.</p>                                                                                                      |

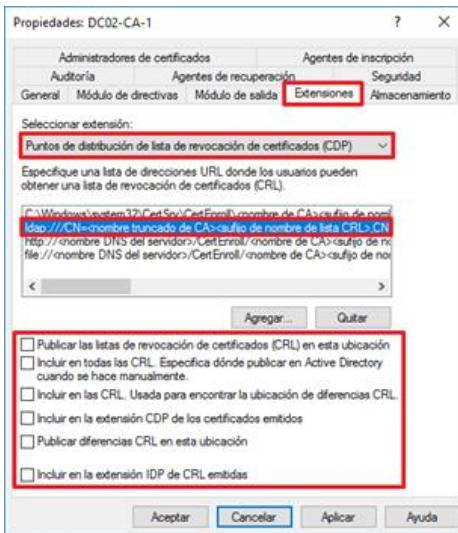
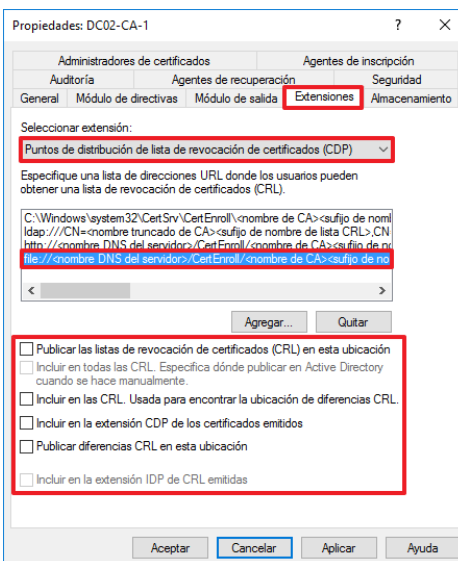
| Paso | Descripción                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 43.  | <p>En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.</p>                     |
| 44.  | <p>Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar.</p>  |
| 45.  | <p>En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.</p>                                                    |

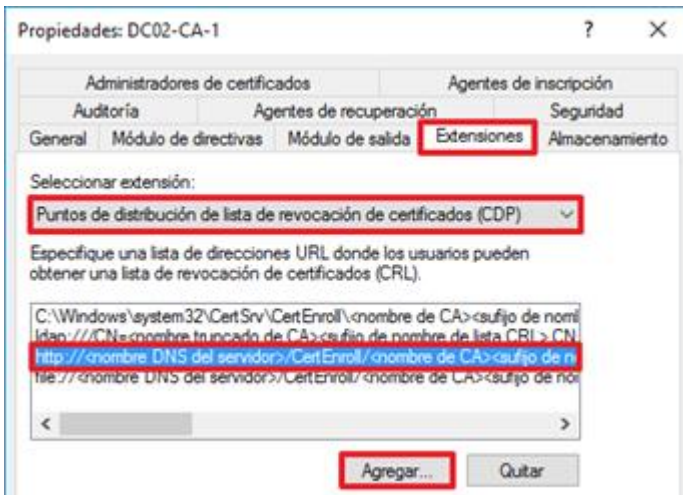
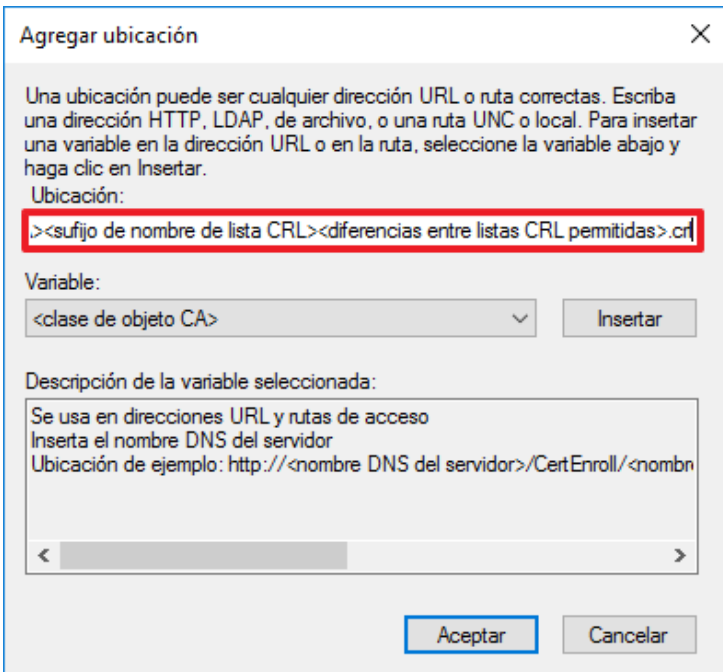
## 2.2. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL)

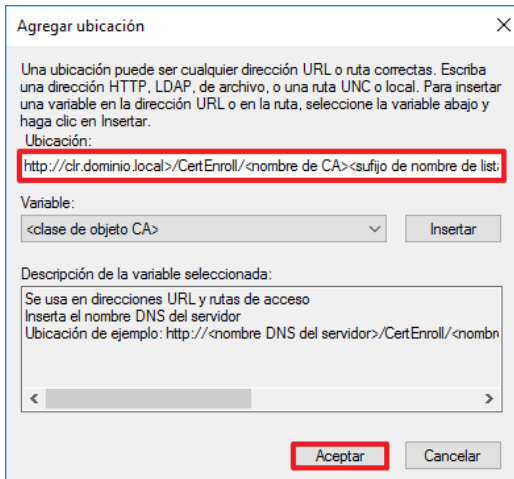
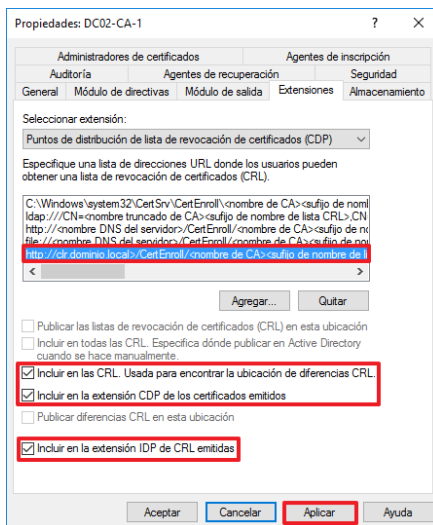
Los pasos que se describen a continuación se realizarán sobre el servidor Entidad de Certificación independiente del dominio.

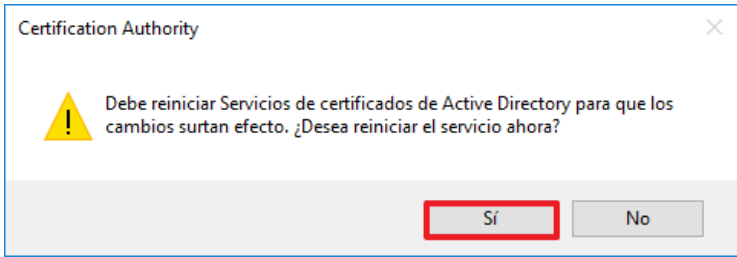
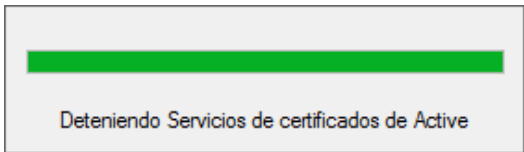
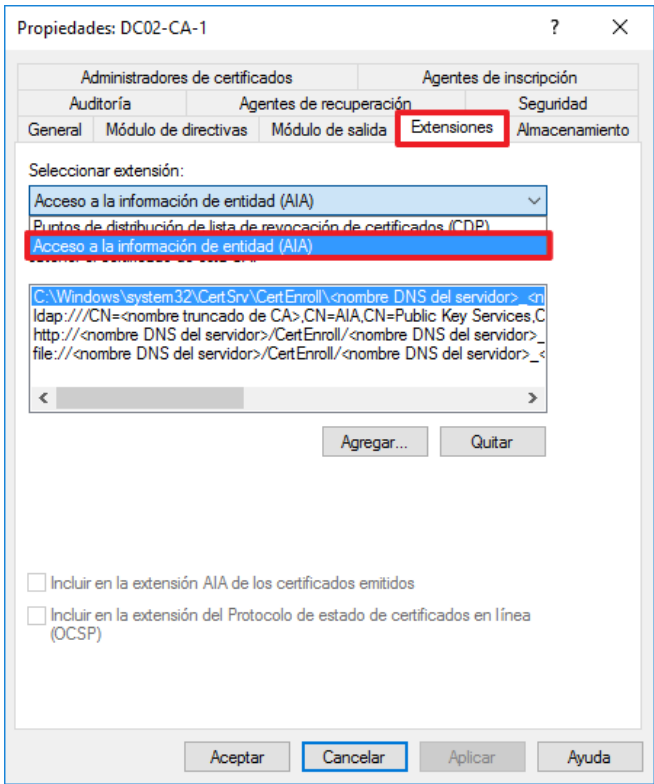
| Paso | Descripción                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46.  | Si no lo ha hecho anteriormente, inicie sesión en el equipo donde se va a instalar el servidor independiente Entidad de Certificación raíz.<br><br><b>Nota:</b> Deberá iniciar sesión con una cuenta con permisos de administrador local.                                         |
| 47.  | Acceda al “administrador del servidor” mediante el icono de la barra de tareas.<br><br>                                                                                                         |
| 48.  | El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”.<br><br> |
| 49.  | En el menú de la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.<br><br>                                                              |

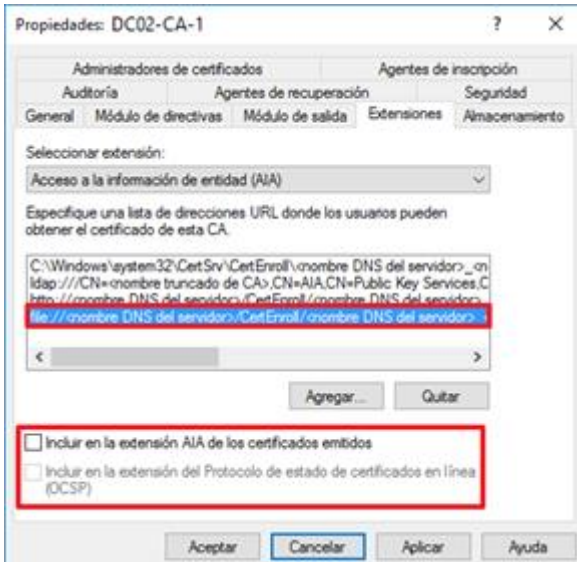
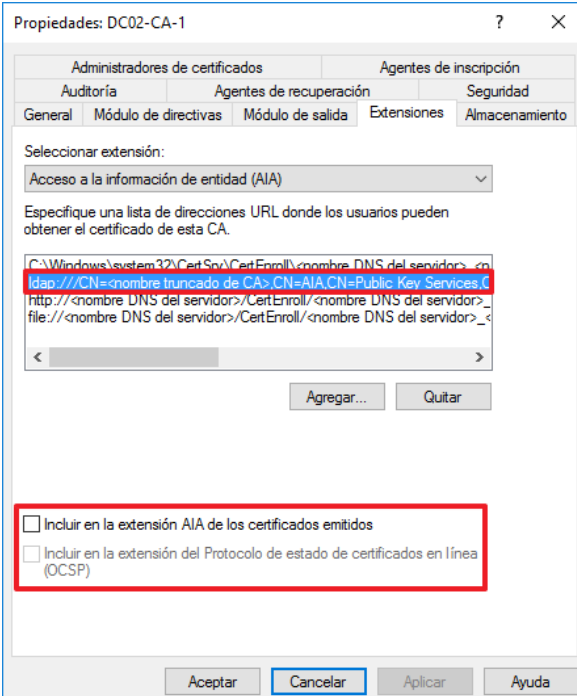
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 50.  | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente, con el botón derecho del ratón selecciónelo y pulse sobre “Propiedades”.</p>                                                                                                                                                                                                                                                                                                                                |
| 51.  | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</p>  |

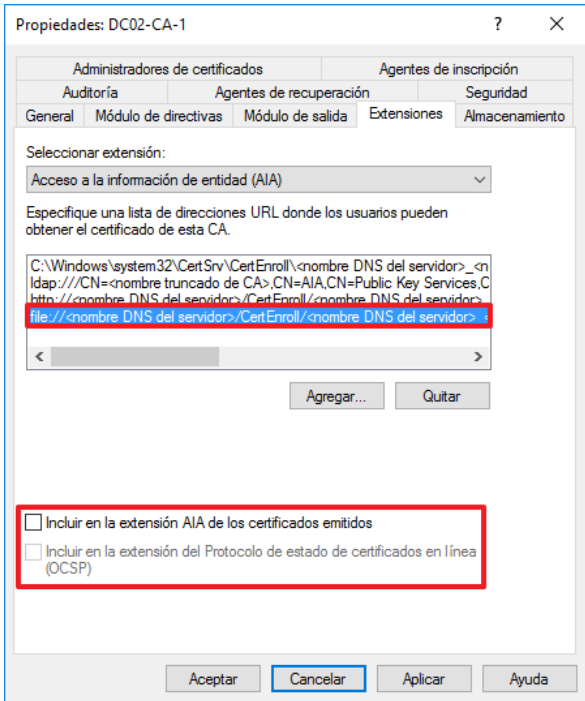
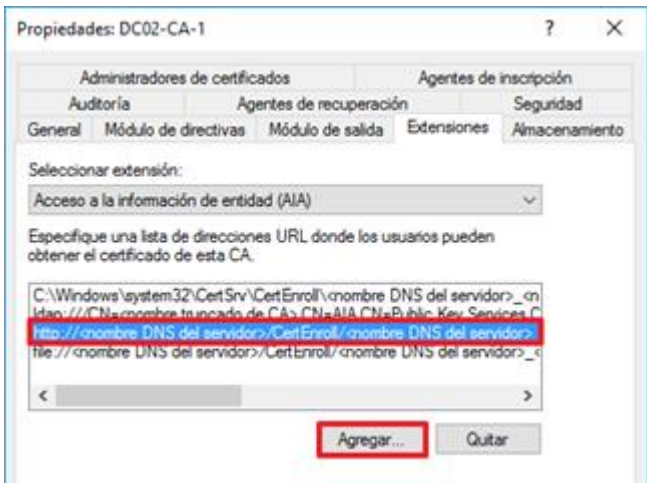
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando “<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>” y desmarque todas las opciones.</p> <p>Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>  |
| 53.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “<b>file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y desmarque todas las opciones como muestra la siguiente figura:</p>                                                                                                                                                                |

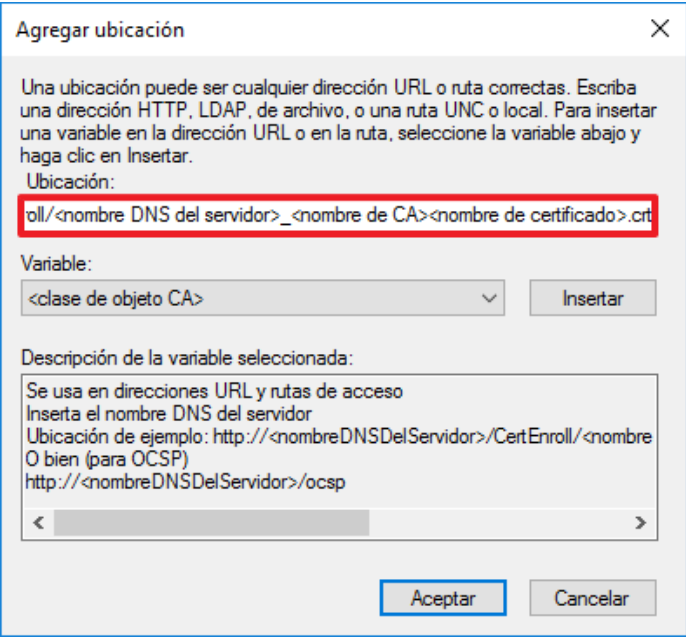
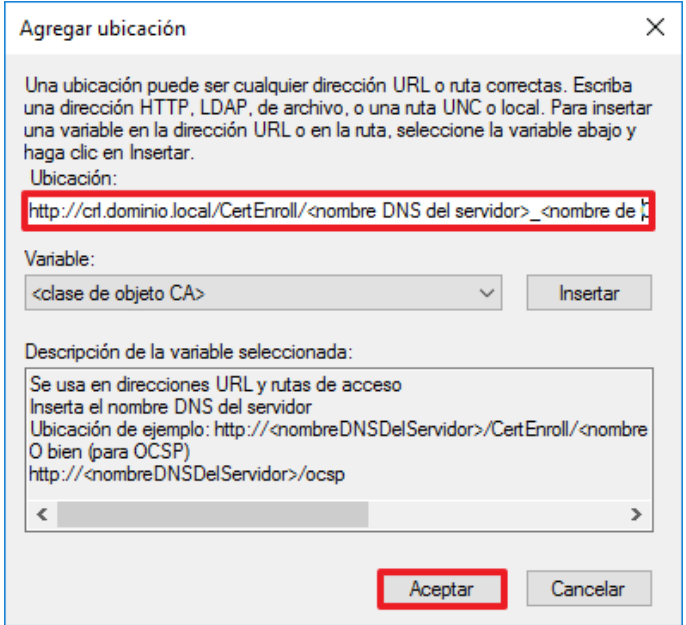
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 54.  | De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto. |
| 55.  | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                                                                   |
| 56.  | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                            |

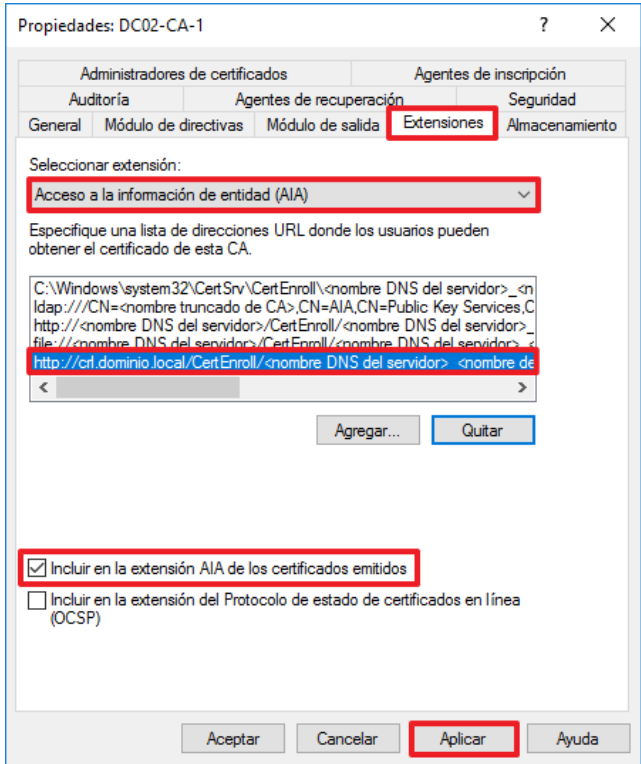
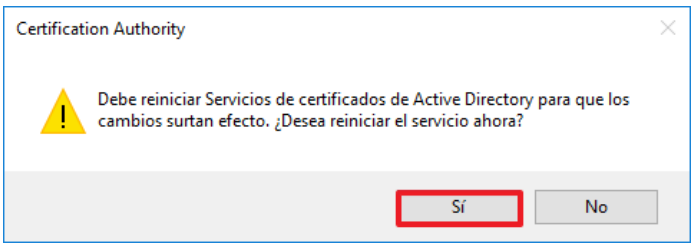
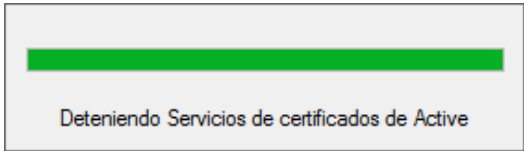
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                                             |
| 58.  | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y marque los siguientes elementos:</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos.</li> <li>– Incluir en la extensión IDP de CRL emitidas.</li> </ul> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 59.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 60.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 61.  | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

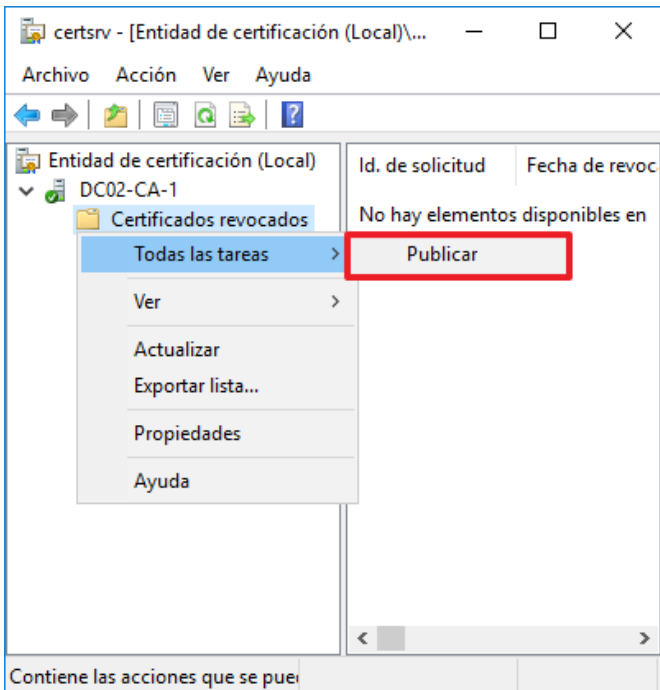
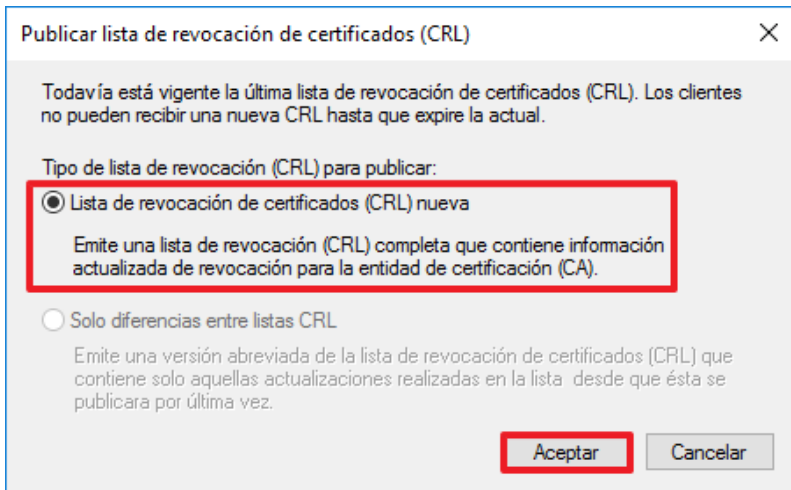
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 62.  | <p>Compruebe que en el objeto <b>"C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt"</b> todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.</p>                      |
| 63.  | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |

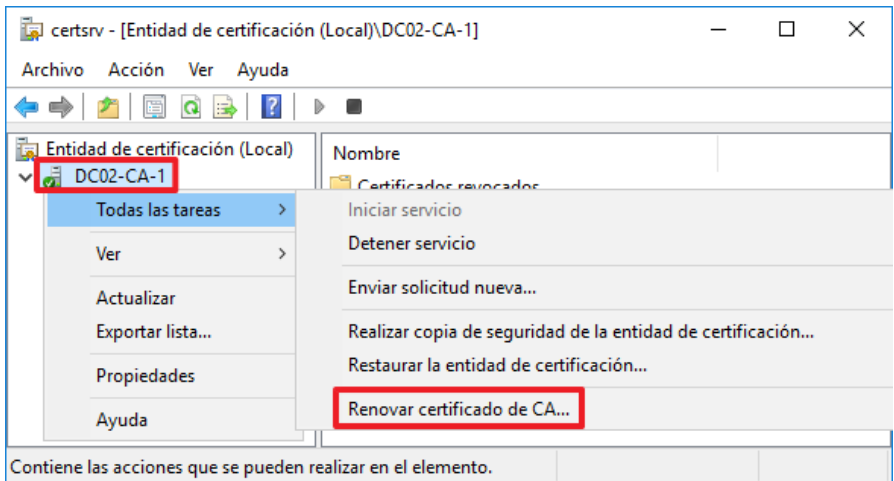
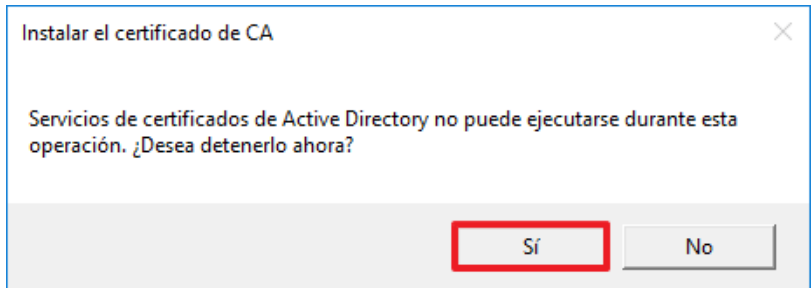
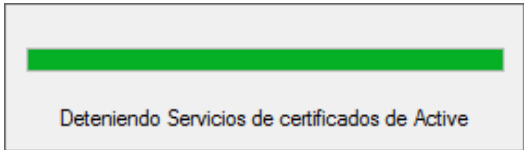
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64.  | <p>Seleccione ahora <b>“file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y desmarque la opción <b>“Incluir en la extensión AIA de los certificados emitidos”</b>.</p>  |
| 65.  | <p>Seleccione ahora <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt”</b> y copie el elemento mediante la combinación de teclas <b>“Control + C”</b>.</p>                                                                                                  |
| 66.  | <p>Pulse el botón <b>“Agregar”</b>.</p>                                                                                                                                                                                                                           |

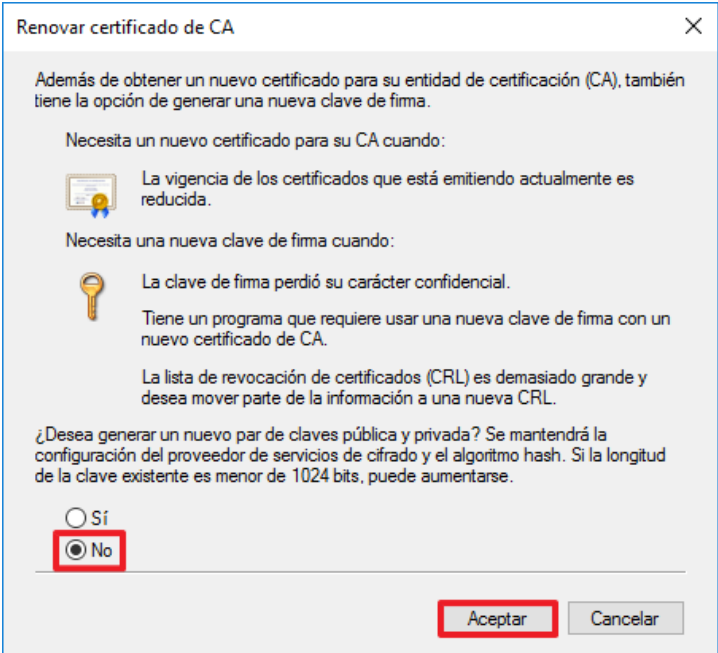
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 67.  | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                                                                                                                                    |
| 68.  | <p>En “Agregar ubicación” y pulsando la tecla “Inicio” diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creará posteriormente en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 69.  | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt</b>” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”.</p> <p>Pulse “Aplicar” para guardar los cambios.</p>  |
| 70.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                          |
| 71.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                                                                                                                                                                                                                                                                                        |
| 72.  | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 73.  | El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL, al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.                                                                                                                                                                                                                                              |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 74.  | <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:</p> <p><b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b></p> <p>Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p> |
| 75.  | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p> <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p>                                        |

| Paso | Descripción                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 76.  | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>  |
| 77.  | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>                                                                 |

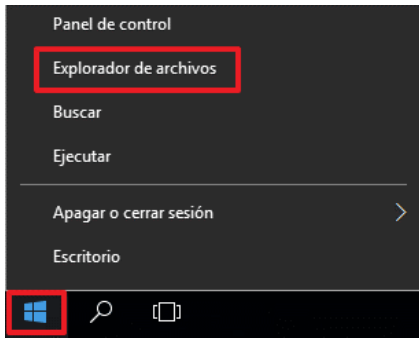
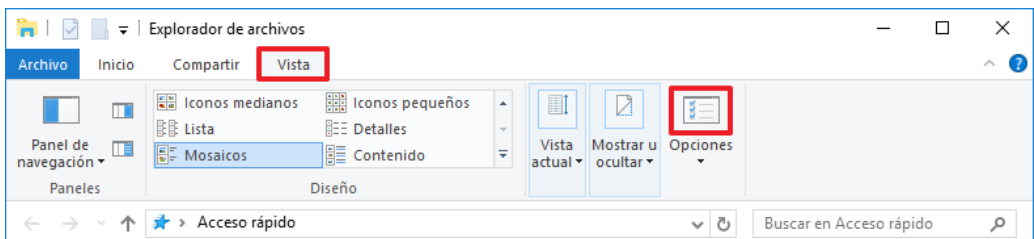
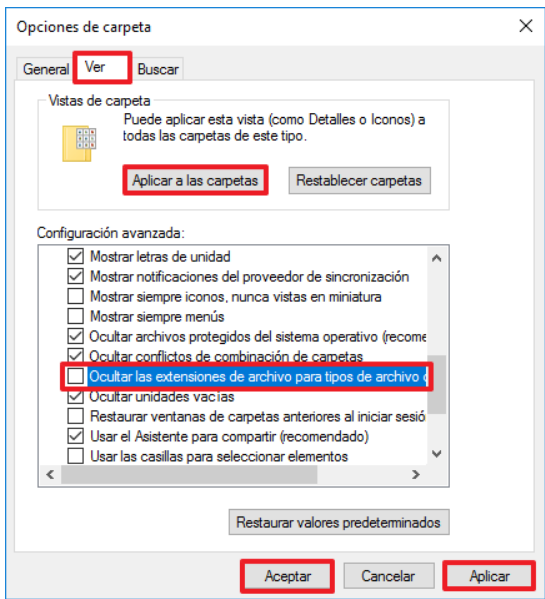
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 78.  | <p>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 <b>“Todas las tareas → Renovar certificado de CA...”</b>.</p>  |
| 79.  | <p>Pulse <b>“Sí”</b> en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                 |
| 80.  | <p>Tras unos segundos, se reiniciarán los <b>“Servicios de certificados”</b>.</p>                                                                                                                                                                                                        |

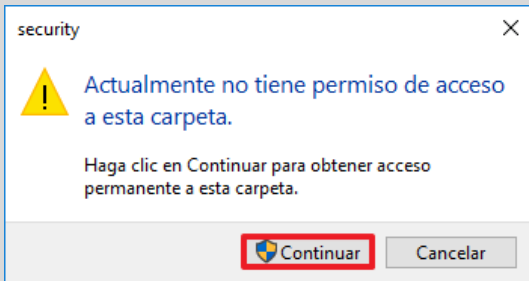
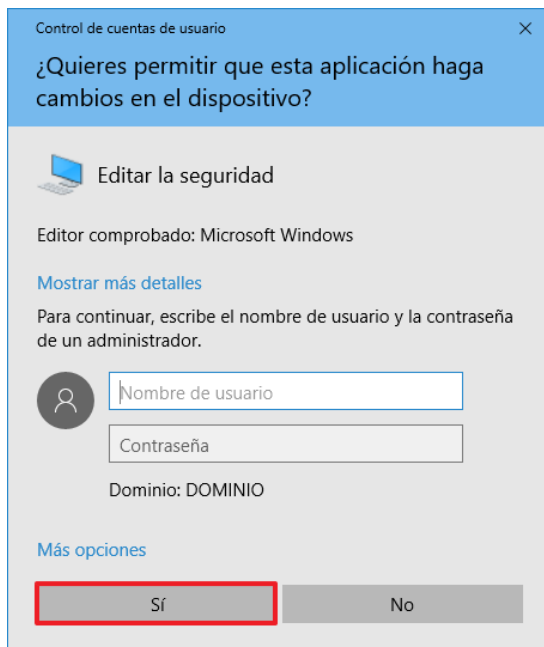
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 81.  | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Este proceso comienza en segundo plano y puede tardar unos minutos. No debe cerrar la ventana hasta que finalice el proceso.</p> |

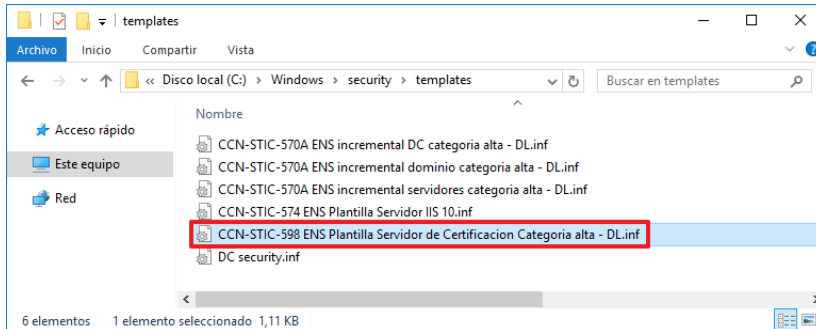
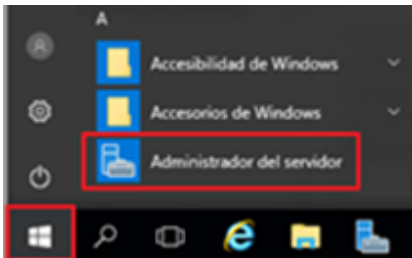
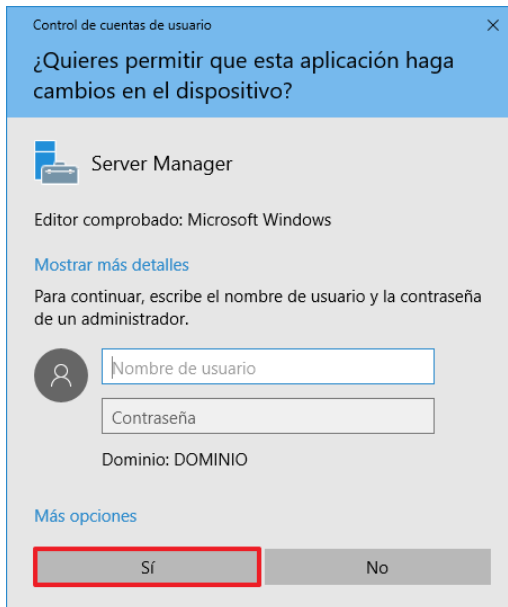
### 2.3. PREPARACIÓN DEL DIRECTORIO ACTIVO

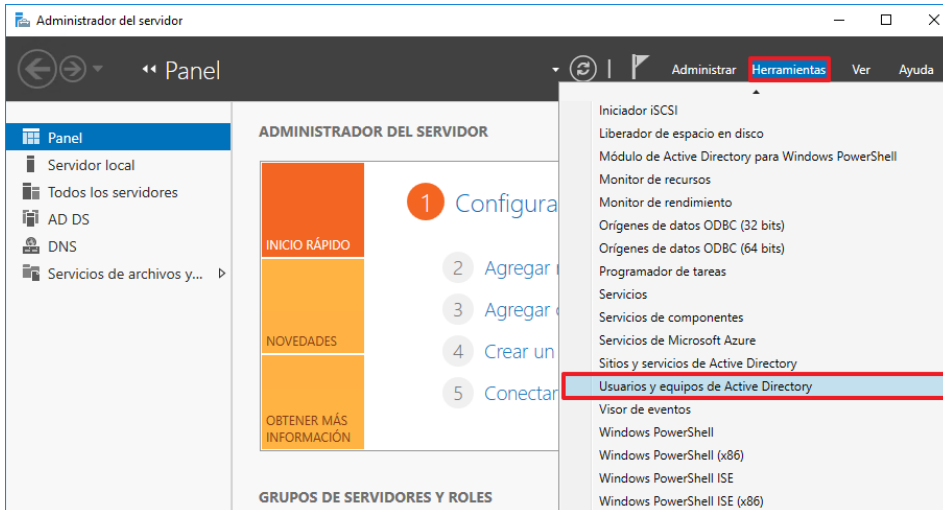
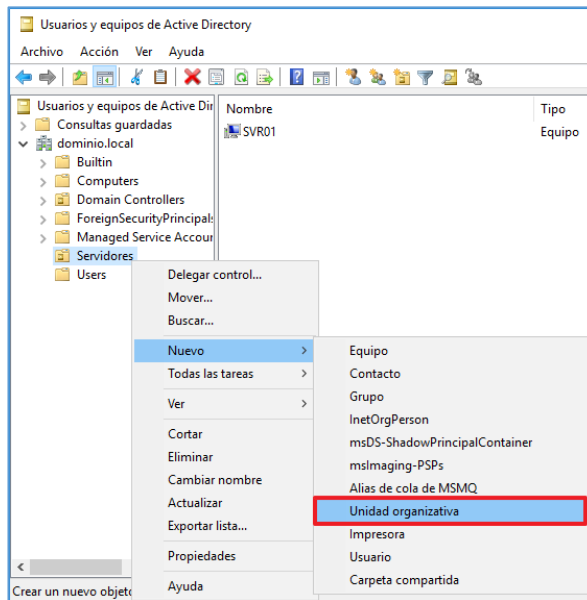
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que va a pertenecer el servidor de Entidad de Certificación subordinada.

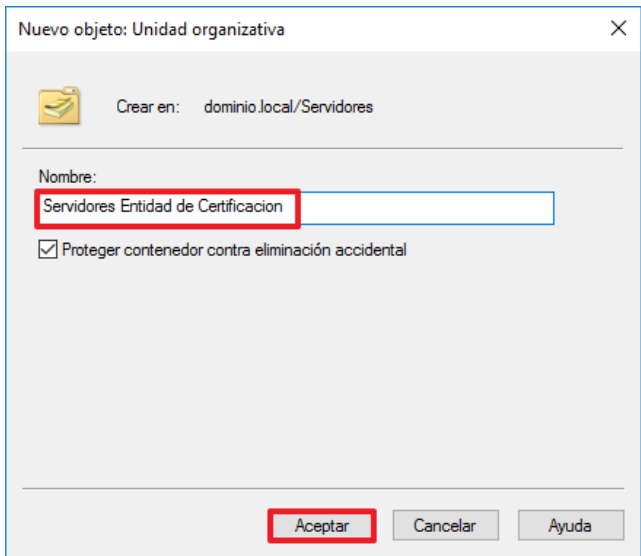
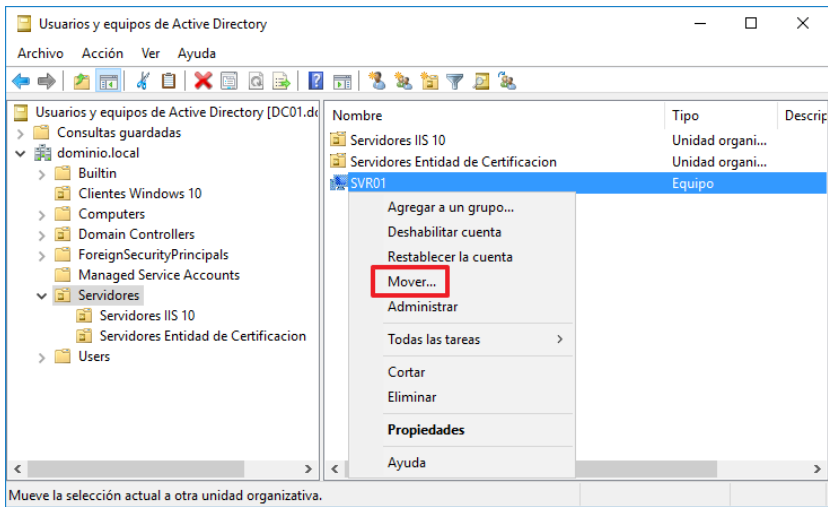
| Paso | Descripción                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 82.  | <p>Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |
| 83.  | Cree el directorio “Scripts” en la unidad “C:\”.                                                                                                                                                                                                                                            |
| 84.  | Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.                                                                                                                                                                                            |

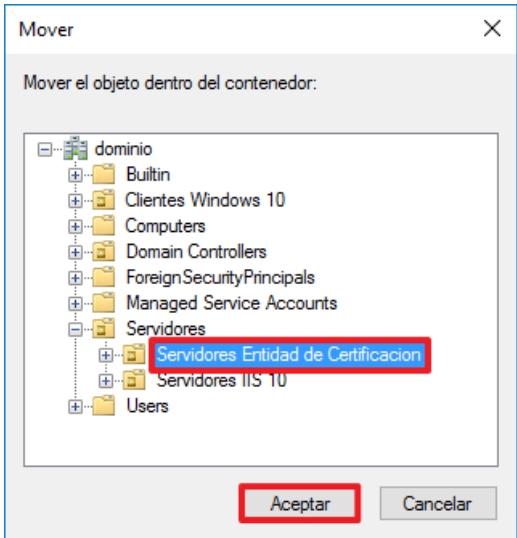
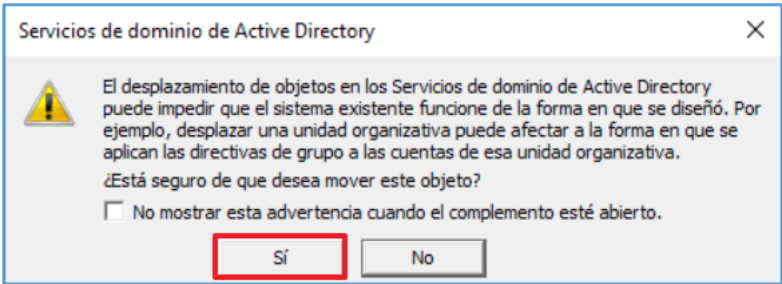
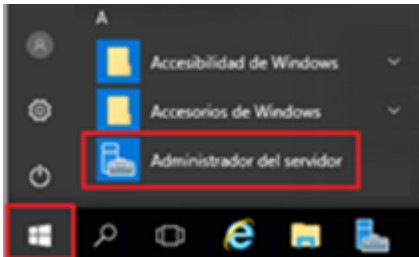
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 85.  | <p>Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”.</p>                         |
| 86.  | <p>En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”.</p>                                                                                                                                                                                                                                           |
| 87.  | <p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p>  |

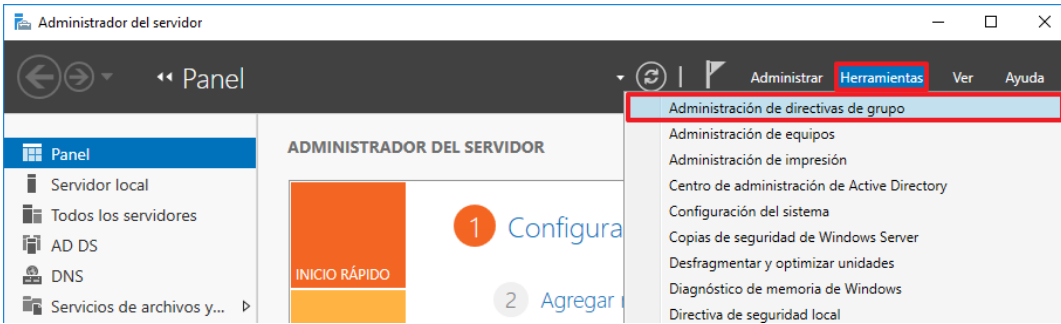
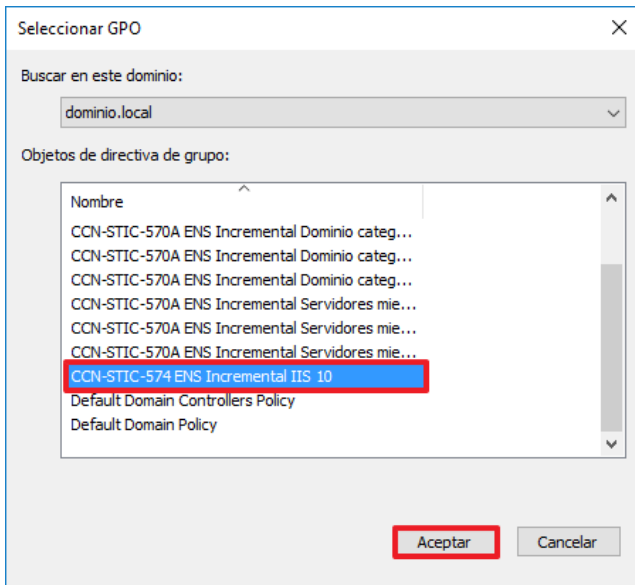
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88.  | <p>Adicionalmente acceda al directorio “C:\Windows\Security\Templates”.</p> <p><b>Nota:</b> Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.</p>                                                                                                                                                                                                                                                                                                              |
| 89.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>  <p><b>Nota:</b> En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña</p> |

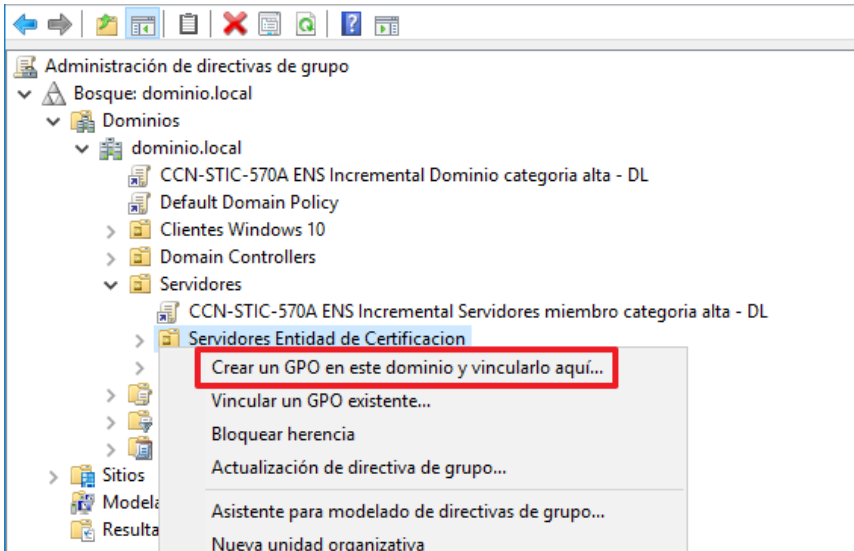
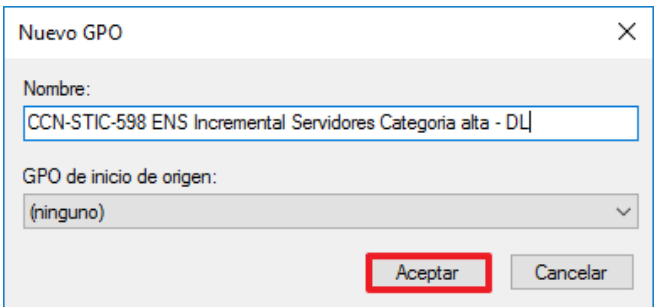
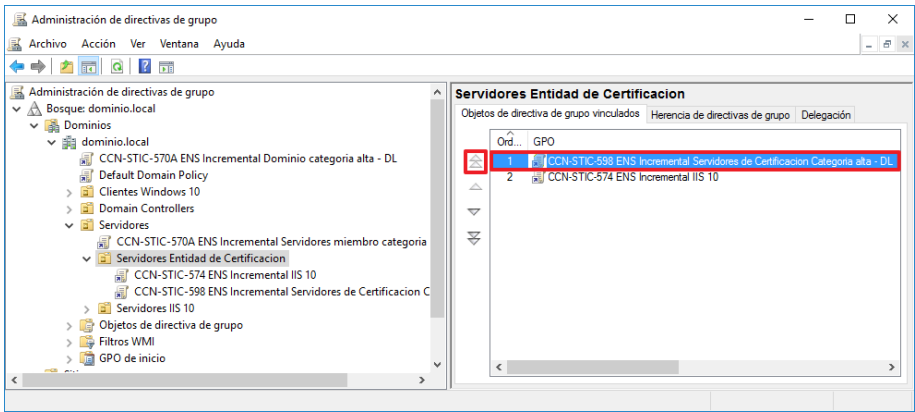
| Paso | Descripción                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 90.  | <p>Copie el fichero “CCN-STIC-598 ENS Plantilla de Servidor de Certificación Categoría alta - DL.inf” ubicada en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”.</p>             |
| 91.  | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                             |
| 92.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”.</p>  |

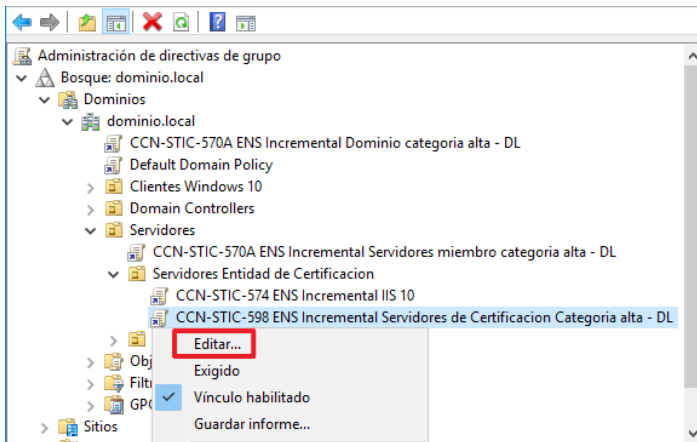
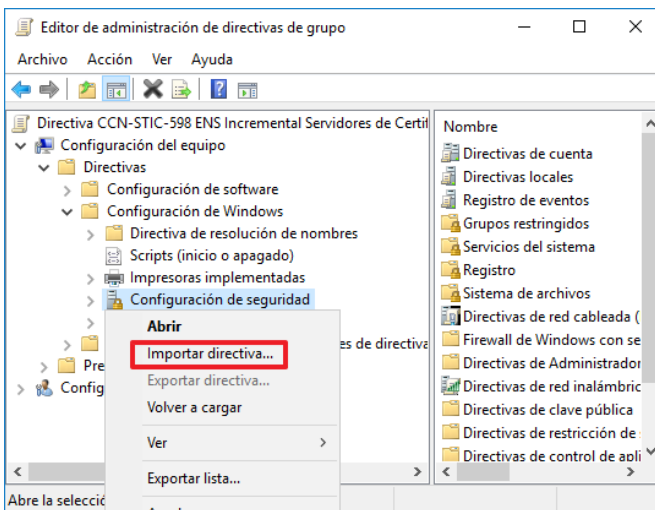
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93.  | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione <b>“Herramientas → Usuarios y equipos de Active Directory”</b>.</p>                                                                                                                                                                                                                                                                                                                                          |
| 94.  | <p>En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo <b>“&lt;&lt;dominio&gt;&gt; → &lt;&lt;unidad organizativa&gt;&gt;”</b>, y desplegando el menú contextual con el botón derecho, seleccione la opción <b>“Nuevo → Unidad organizativa”</b>.</p>  <p><b>Nota:</b> En este ejemplo, la unidad organizativa de servidores se encuentra en <b>“dominio.local → Servidores”</b>.</p> |

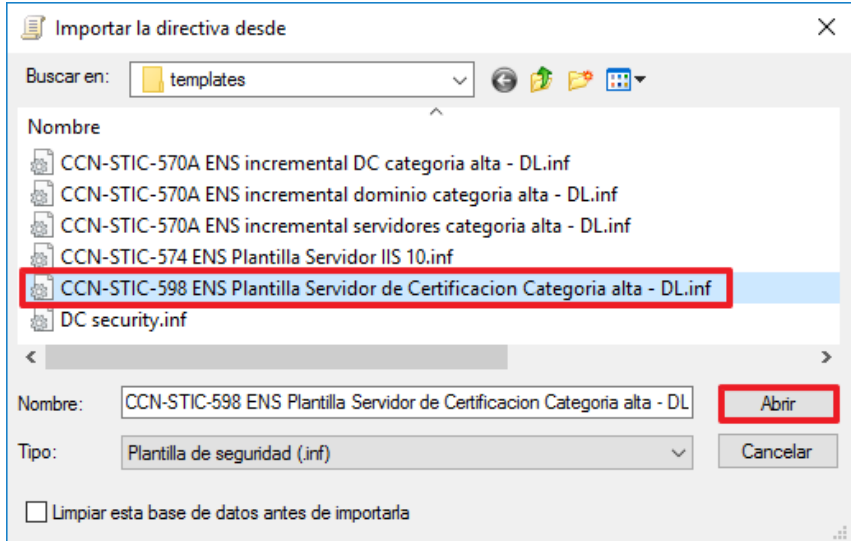
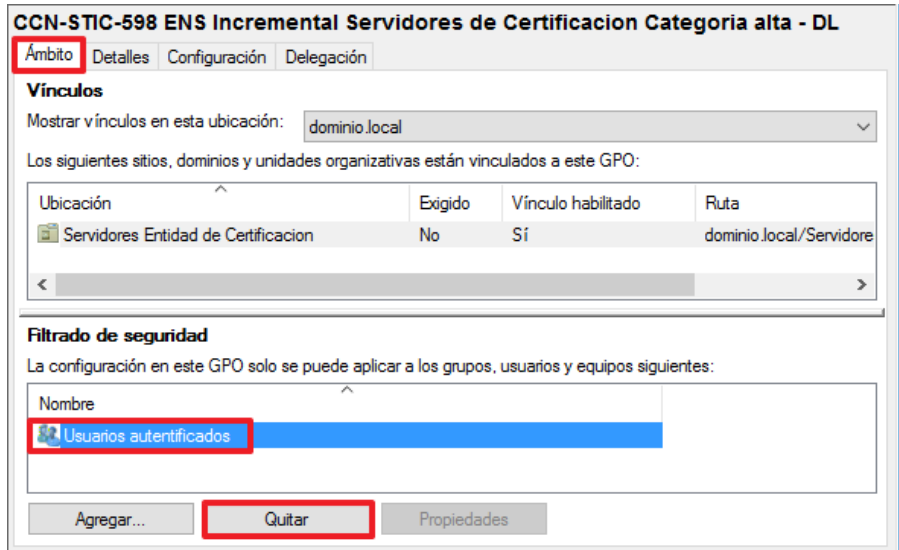
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 95.  | <p>Introduzca el nombre “Servidores Entidad de Certificación” tal y como se muestra en la imagen y pulse sobre “Aceptar”.</p>                                                                                                                                                                                              |
| 96.  | <p>Una vez creada la nueva unidad organizativa, deberá mover los servidores a la unidad organizativa “Servidores Entidad de Certificación”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa.</p>  |

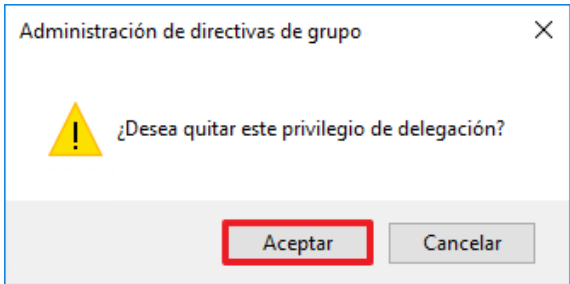
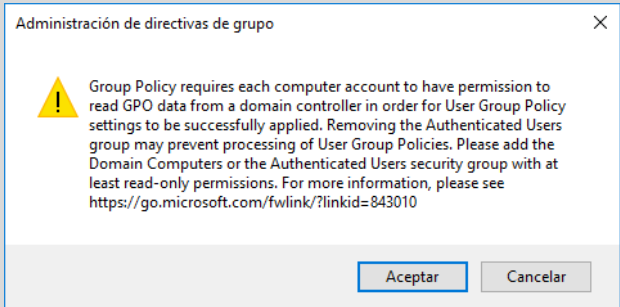
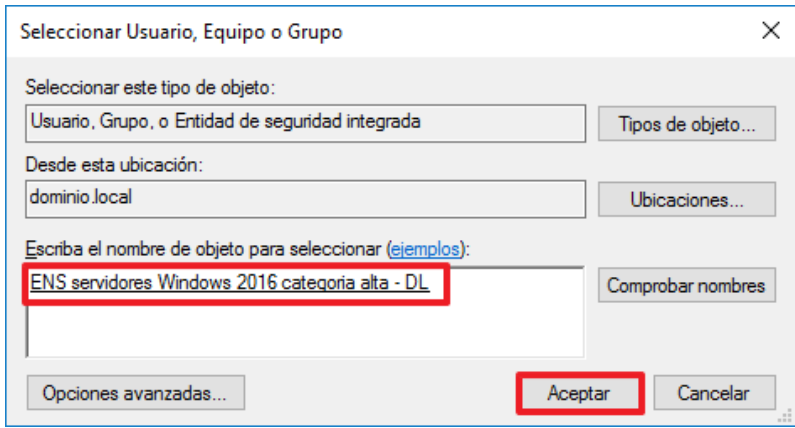
| Paso | Descripción                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 97.  | <p>A continuación, seleccione la unidad organizativa “Servidores Entidad de Certificación” y pulse sobre “Aceptar”.</p>  |
| 98.  | <p>Acepte el mensaje de advertencia</p>                                                                                 |
| 99.  | Cierre la herramienta de “Usuarios y equipos de Active Directory”.                                                                                                                                         |
| 100. | <p>A continuación, abra el “Administrador del servidor”.</p>                                                           |

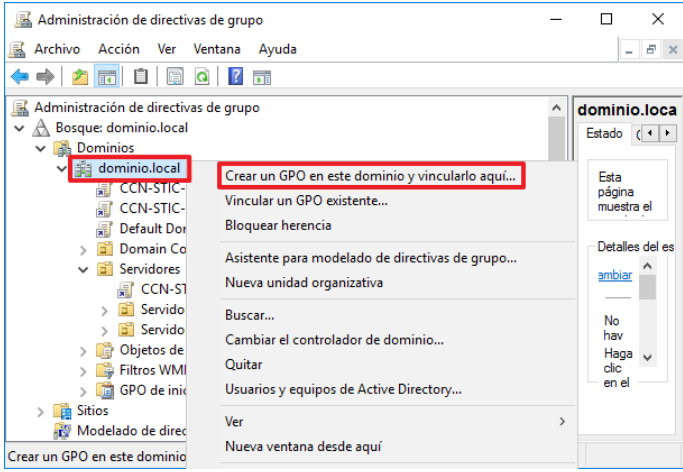
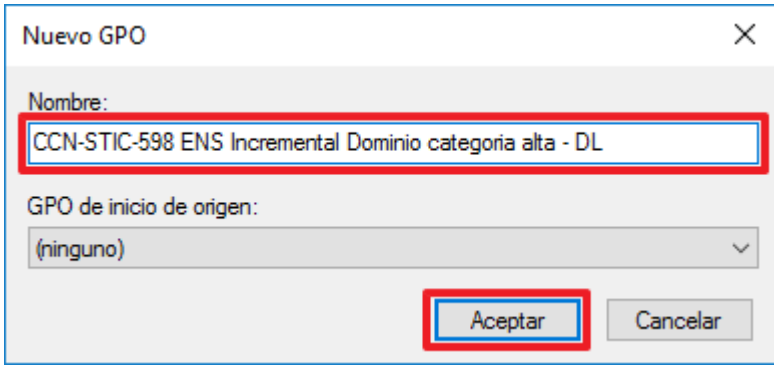
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 101. | <p>Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón <b>“Herramientas → Administración de directivas de grupo”</b>.</p>                                                                                          |
| 102. | <p>A continuación, despliegue el nodo <b>“Bosque: &lt;&lt;nombre de bosque&gt;&gt; → Dominios → &lt;&lt;nombre de dominio&gt;&gt; → Servidores → Servidores Entidad de Certificación”</b>.</p> <p><b>Nota:</b> En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina “Servidores”.</p>        |
| 103. | <p>Seleccione “Vincular un GPO existente...” y vincule el objeto de directiva de grupo “CCN-STIC-574 ENS Incremental IIS 10” a la nueva unidad organizativa “Servidores Entidad de Certificación”, haciendo clic con el botón derecho sobre ella.</p>  |

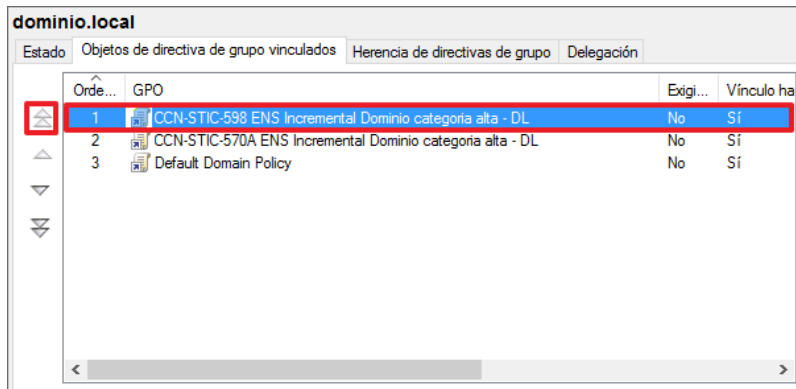
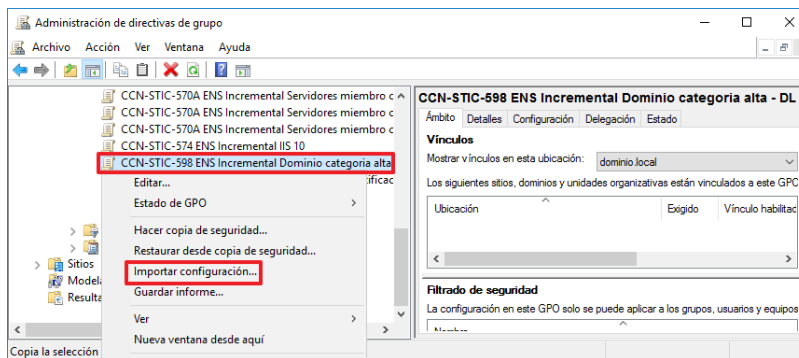
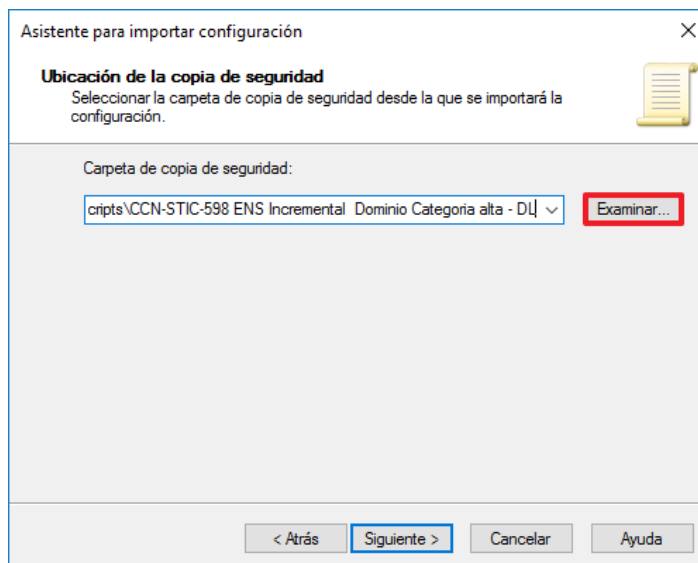
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 104. | <p>A continuación, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores de Entidad de Certificación”, haciendo clic con el botón derecho sobre ella y seleccionando en el menú “Crear un GPO en este dominio y vincularlo aquí...”.</p>       |
| 105. | <p>Escriba el nombre de la GPO “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL” y haga clic en el botón “Aceptar”.</p>                                                                                                                    |
| 106. | <p>Seleccione la unidad organizativa “<b>Servidores Entidad de Certificación</b>”. En el panel de la derecha de la consola, seleccione la directiva que acaba de crear y sitúela en el primer nivel de aplicación utilizando las flechas para establecer el orden.</p>  |
| 107. | <p>De esta forma, se garantiza que la directiva se aplica correctamente.</p>                                                                                                                                                                                                                                                                                |

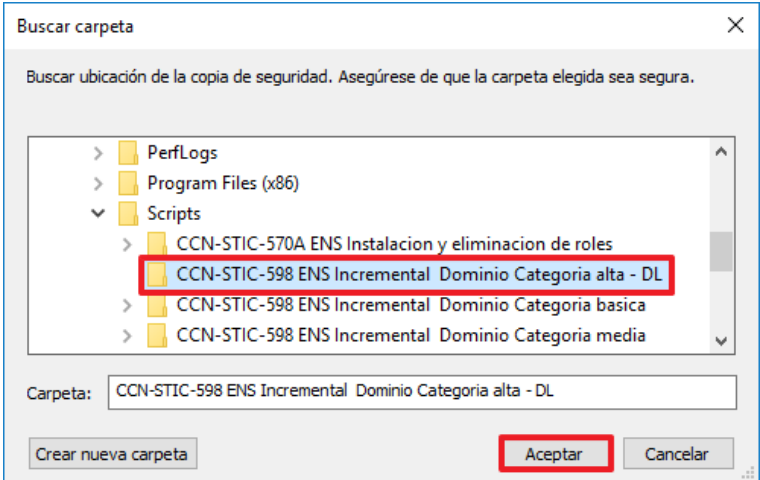
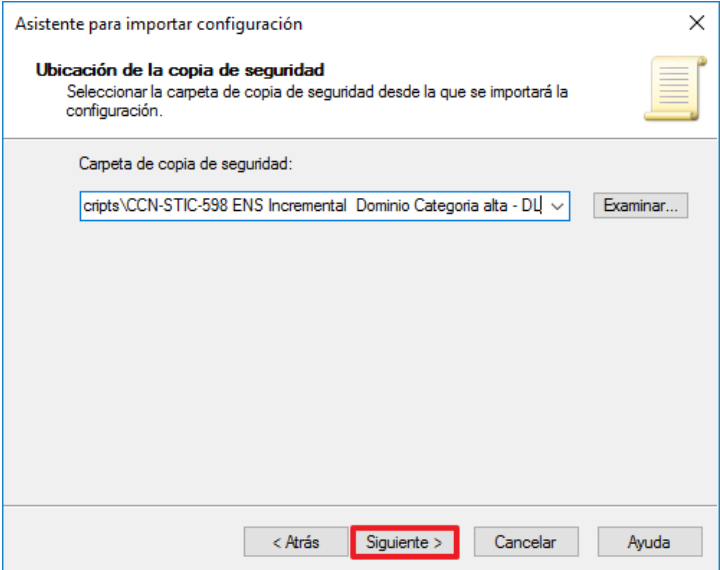
| Paso | Descripción                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 108. | <p>Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción “Editar”.</p>  |
| 109. | <p>Expanda el nodo “Configuración del equipo → Directivas→ Configuración de Windows → Configuración de seguridad”.</p>                                                                                                        |
| 110. | <p>Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.</p>                      |

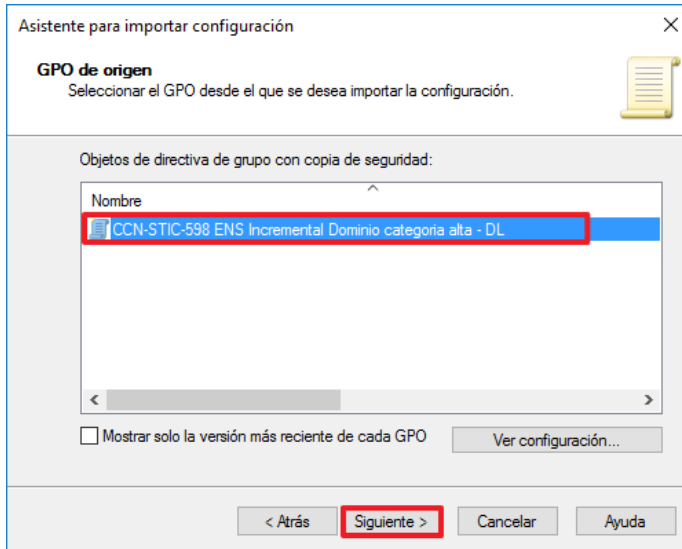
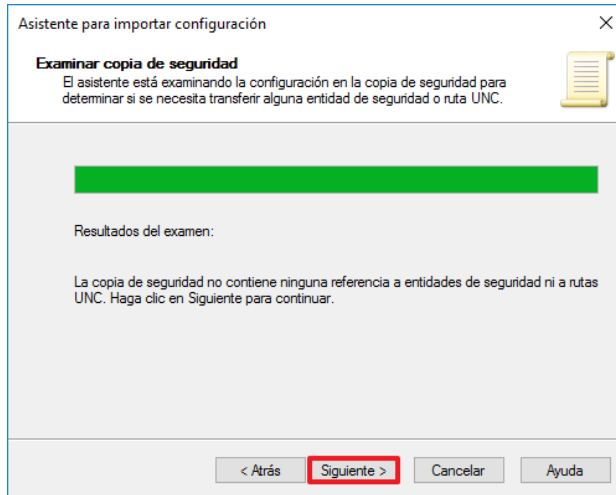
| Paso | Descripción                                                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 111. | <p>Seleccione la plantilla “C:\Windows\Security\Templates\CCN-STIC-598 Plantilla Servidor de Certificación Categoría alta - DL.inf”. Haga clic en el botón “Abrir”.</p>                                                 |
| 112. | Cierre el “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                              |
| 113. | <p>Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”.</p>  |

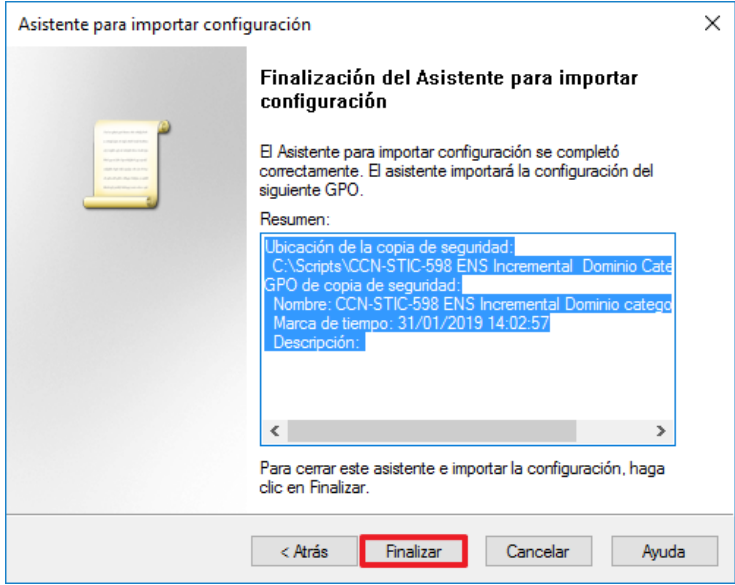
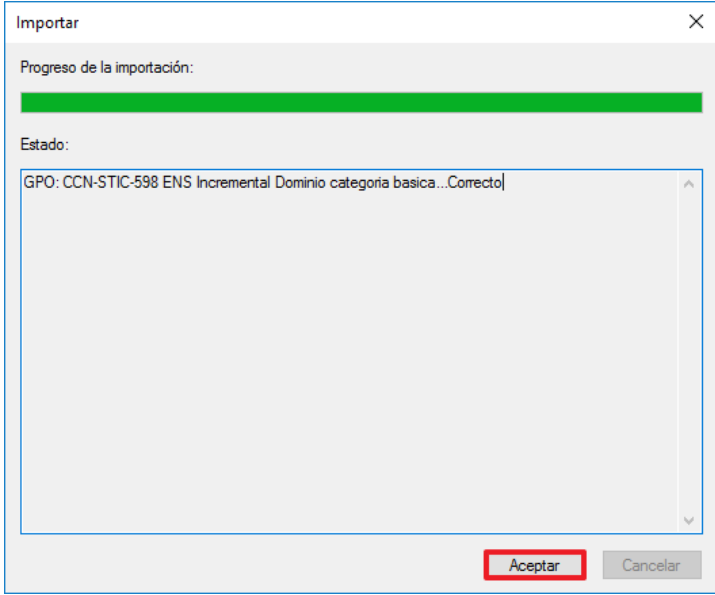
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 114. | <p>Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.</p>  <p><b>Nota:</b> Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”.</p>                                                                   |
| 115. | <p>Agregue los grupos de usuarios que contengan los equipos con el rol “Servidor de Entidad de Certificación” y pulse “Aceptar” para finalizar.</p>  <p><b>Nota:</b> Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria alta - DL” que contiene el servidor con el rol “Servidor de entidad de certificación”</p> |
| 116. | Cierre la ventana “Editor de administración de directivas de grupo”.                                                                                                                                                                                                                                                                                                                                                            |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 117. | <p>A continuación, se va a configurar una directiva incremental que habilita los procesos de inscripción automática y renovación automática de certificados para usuarios y equipos de todo el dominio, siempre y cuando, la plantilla correspondiente así lo establezca en su configuración de seguridad.</p> <p><b>Nota:</b> Si no desea que se habilite la inscripción y renovación automática de certificados, no ejecute los siguientes pasos. Sin embargo, se recomienda habilitar esta funcionalidad ya que permite que, de forma transparente para los usuarios y haciendo uso de Kerberos como protocolo de autenticación de usuarios y equipos de Directorio Activo, se emitan y se renueven certificados en todo el dominio. Independientemente de ello, en las plantillas de certificados se pueden establecer los requerimientos de emisión de los certificados y la pertenencia a los grupos de seguridad para cada tipo de certificado.</p> |
| 118. | <p>Seleccione el nodo raíz del dominio de su organización y, haciendo clic con el botón derecho, seleccione la opción “Crear un GPO en este dominio y vincularlo aquí...”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 119. | <p>Escriba, como nombre de la nueva política, “CCN-STIC-598 Incremental Dominio categoria alta - DL” y pulse el botón “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

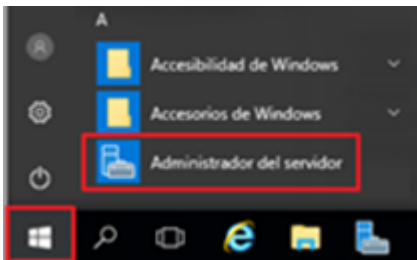
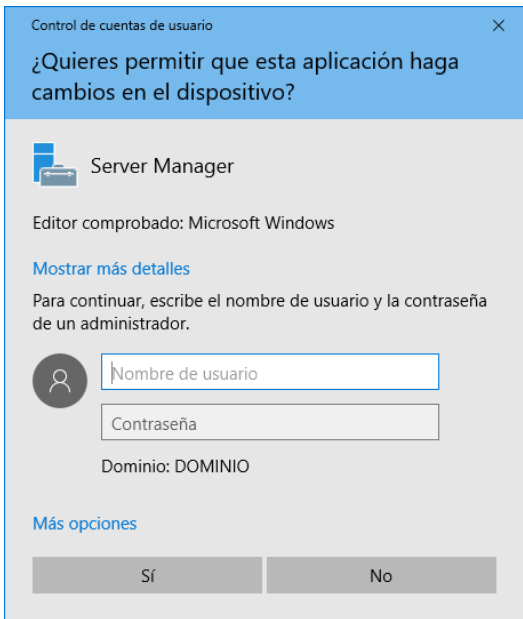
| Paso | Descripción                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 120. | <p>Sitúese sobre el contenedor correspondiente al dominio, seleccione la GPO recién creada y pulsando sobre la doble flecha sitúe dicha GPO en el primer lugar en el orden de vínculos tal y como muestra la imagen.</p>     |
| 121. | <p>Despliegue el contenedor “Objetos de directiva de grupo” y haga clic derecho sobre la GPO recién creada “CCN-STIC-598 Incremental Dominio categoría alta - DL” seleccionando la opción “Importar configuración...”.</p>  |
| 122. | <p>Haga clic en “Siguiete &gt;” en el “Asistente para importar configuración”.</p>                                                                                                                                                                                                                             |
| 123. | <p>Haga clic en “Examinar...”.</p>                                                                                                                                                                                         |

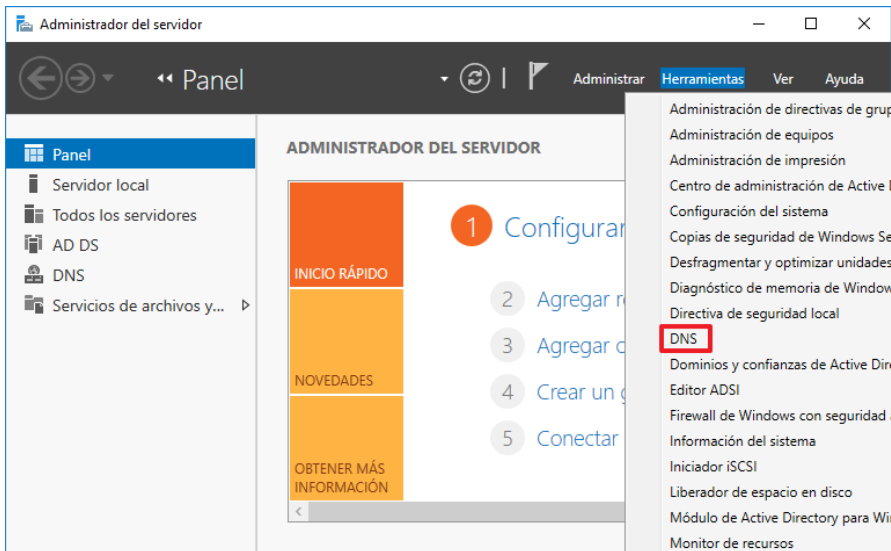
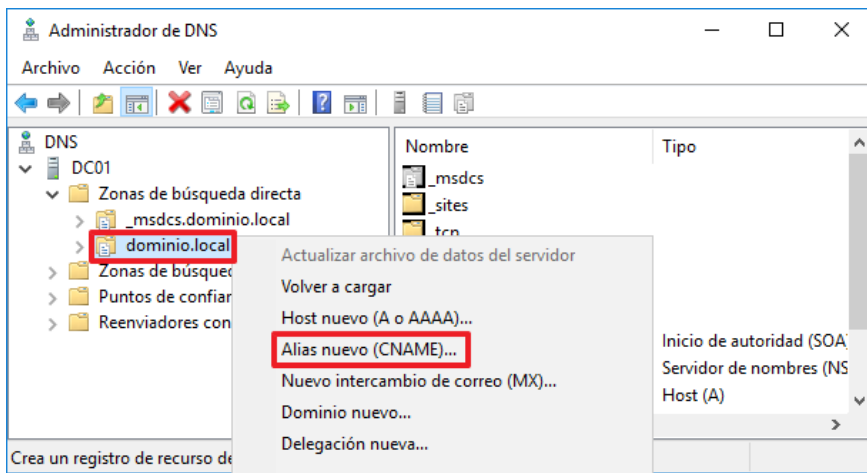
| Paso | Descripción                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 124. | <p>En la ventana “Buscar carpeta” seleccione la ubicación de la copia de seguridad “C:\Scripts\CCN-STIC-598 Incremental Dominio Categoría alta - DL” y pulse “Aceptar”.</p>  |
| 125. | <p>Pulse “Siguiente &gt;” para continuar con la importación.</p>                                                                                                            |

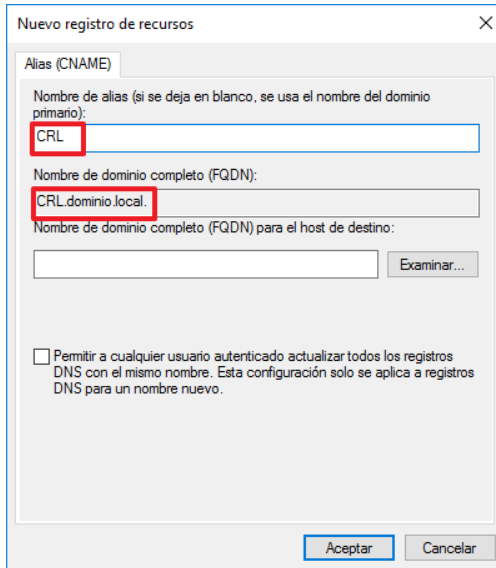
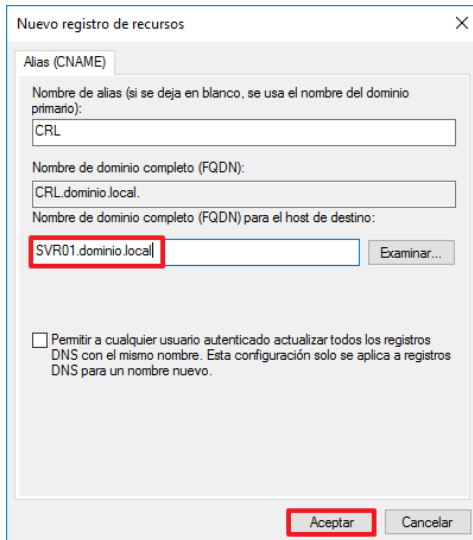
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 126. | <p>En “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-598 Incremental Dominio Categoría alta - DL” y pulse “Siguiente &gt;”.</p>  <p><b>Nota:</b> Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Éste es un fichero oculto y debe mostrarse a través de “opciones de carpeta”, con la opción “Mostrar archivos, carpetas y unidades ocultos”.</p> |
| 127. | <p>En la pantalla de “Resultados del examen” pulse el botón “Siguiente &gt;”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |

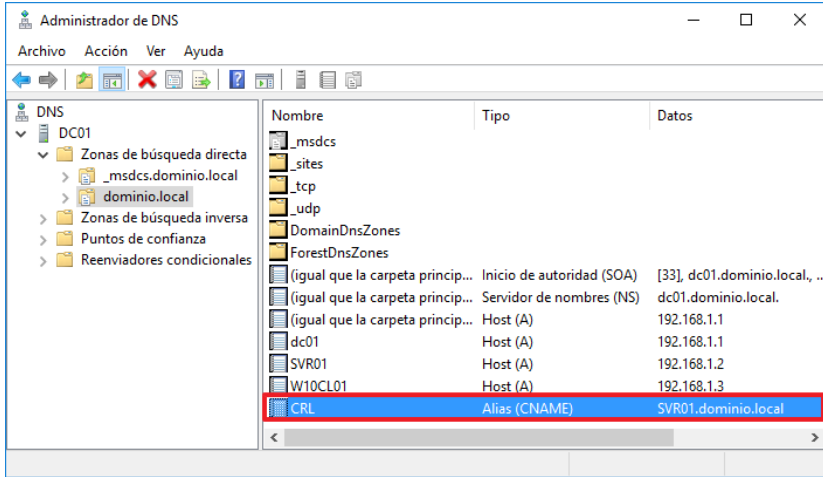
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 128. | <p>Para completar el asistente pulse el botón “Finalizar”.</p>                                                                                                                    |
| 129. | <p>Deberá aparecer un mensaje indicando que la importación se ha realizado correctamente. Pulse finalmente “Aceptar” para cerrar el asistente de importación de políticas.</p>  |
| 130. | <p>Cierre la ventana “Administración de directivas de grupo”.</p>                                                                                                                                                                                                   |

En el siguiente apartado, se configurará el servidor Entidad de Certificación y el sitio web que mantendrá las listas de revocación de certificados (CRLs). Previo a estas configuraciones se va a establecer un nombre DNS para el sitio web donde se publicarán dichas CRLs.

| Paso | Descripción                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 131. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>  |
| 132. | <p>Ejecute la consola administrativa “DNS”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 133. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                  |

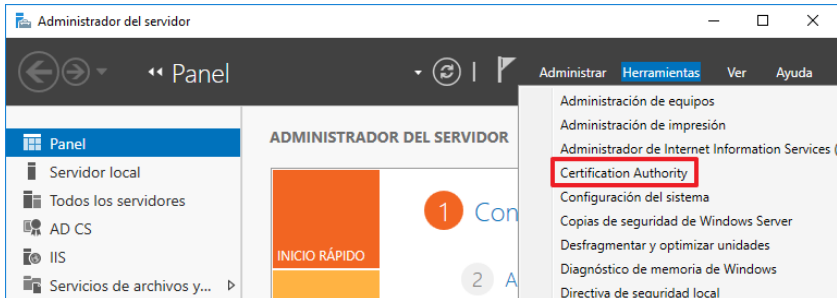
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 134. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “DNS”.</p>                                                                                                                                                    |
| 135. | <p>Navegue hasta el objeto con el nombre del dominio, mediante la siguiente ruta: “&lt;nombre de controlador de dominio&gt; → Zonas de búsqueda directa → &lt;Nombre de dominio&gt;”.</p> <p>Pulse con el botón derecho sobre él para seleccionar “Alias nuevo (CNAME)...”.</p>  |

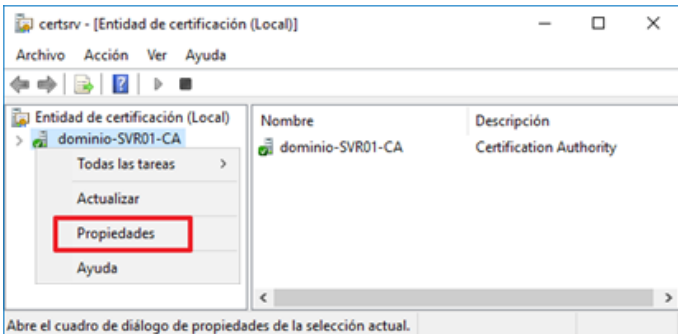
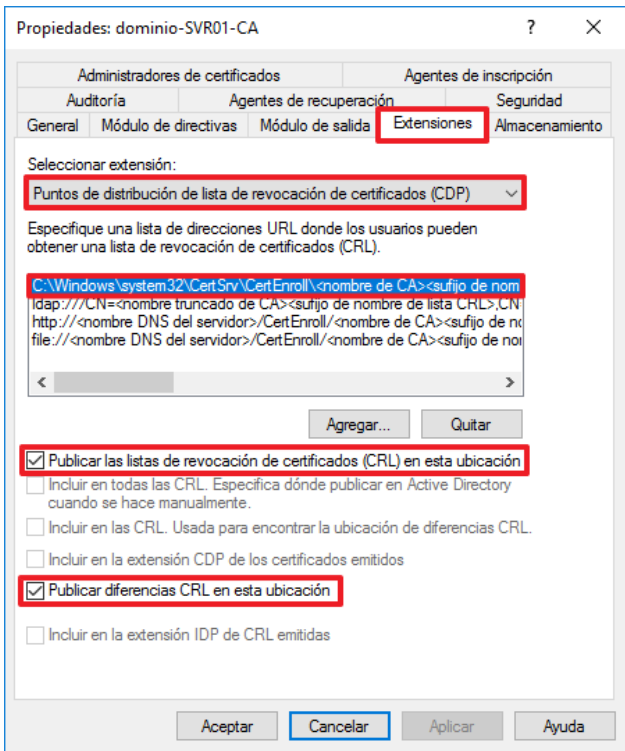
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 136. | <p>En la ventana “Nuevo registro de recursos”, escriba el nombre DNS del sitio web repositorio de CRLs.</p>  <p><b>Nota:</b> En el ejemplo se define “CRL.dominio.local”. En el campo “Nombre de alias” solamente será necesario escribir “CRL”, ya que se autocompletará el FQDN con el nombre del dominio de manera automática.</p> |
| 137. | <p>En el campo “Nombre de dominio completo (FQDN) para el host de destino:” deberá introducir el FQDN del servidor Entidad de Certificación subordinada de empresa y pulse aceptar.</p>  <p><b>Nota:</b> En el ejemplo se introduce “SVR01.dominio.local” que corresponde al FQDN del equipo usado para este escenario.</p>         |

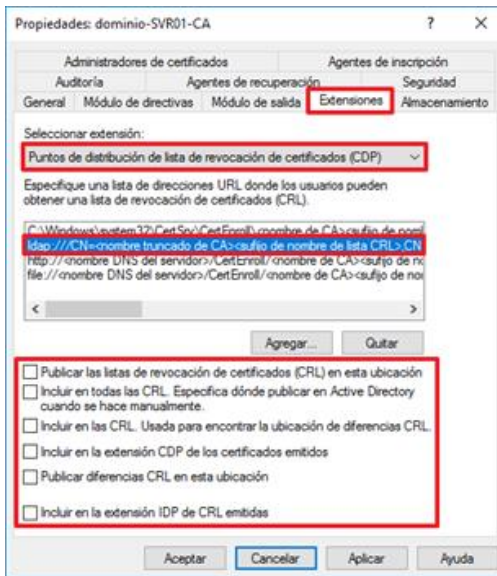
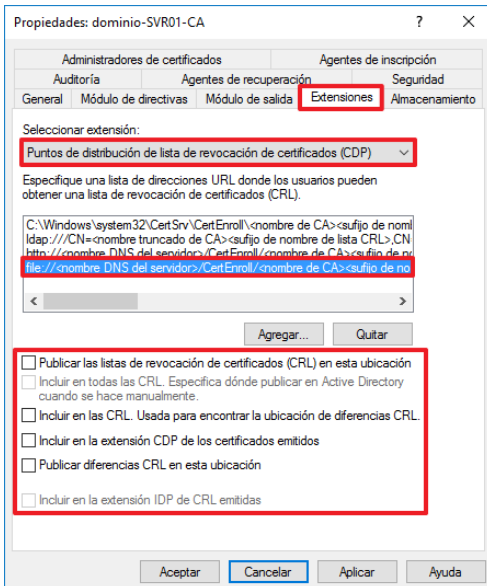
| Paso | Descripción                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 138. | <p>Compruebe que el objeto CNAME se ha creado correctamente y que apunta al objeto de tipo HOST (A) correspondiente.</p>  |

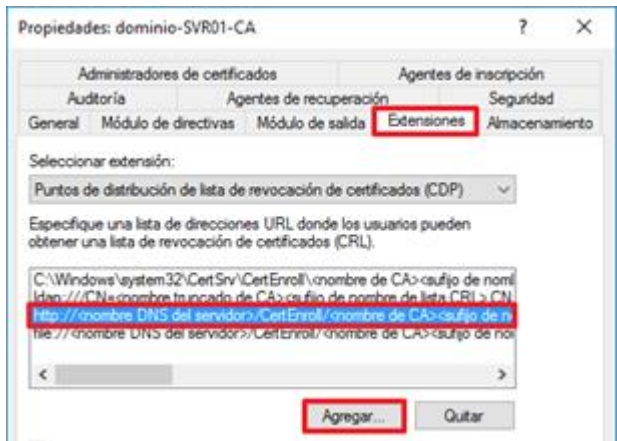
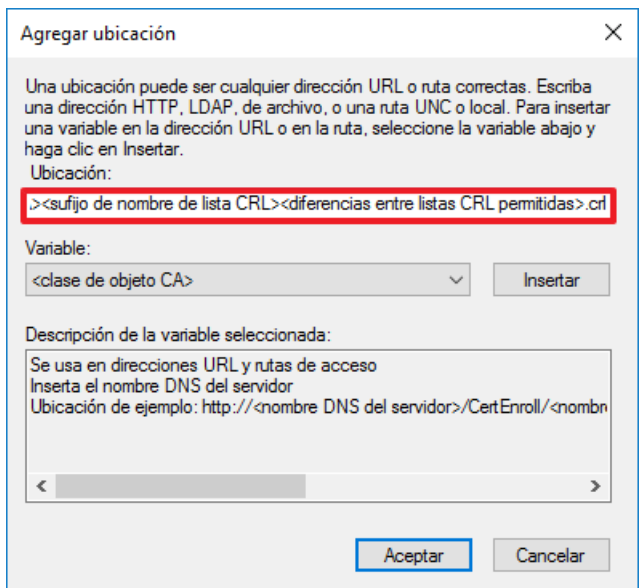
## 2.4. CONFIGURACIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL) EN LA ENTIDAD SUBORDINADA.

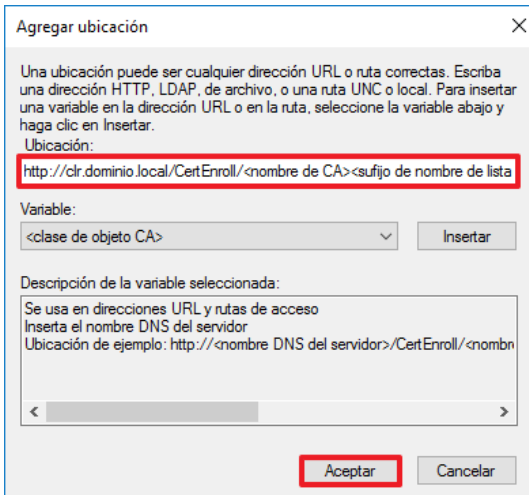
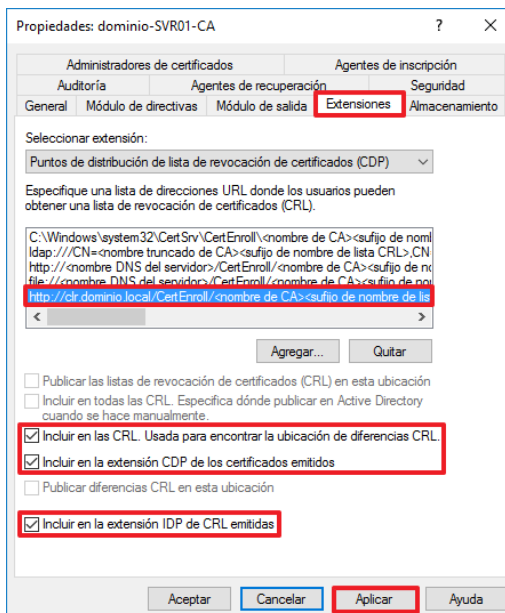
Los pasos que se describen a continuación se realizarán sobre el servidor miembro de Entidad de Certificación subordinada del dominio.

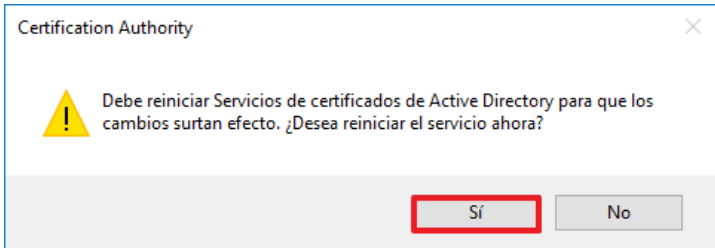
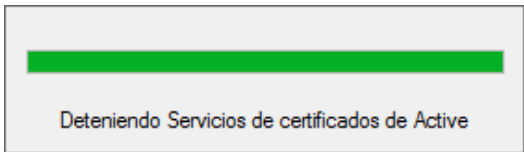
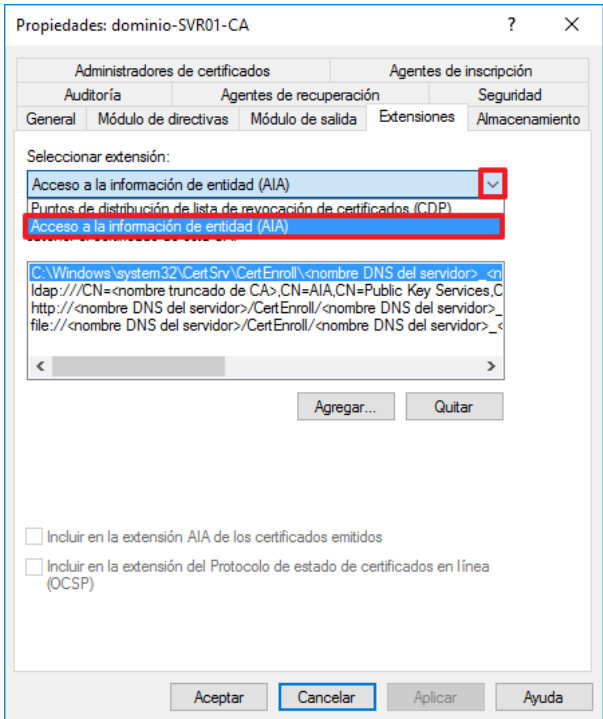
| Paso | Descripción                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 139. | <p>Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p>                        |
| 140. | <p>Ejecute la consola administrativa "Certification Authority". Para ello ejecute el "Administrador del servidor" desde el icono correspondiente.</p>  |
| 141. | <p>El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "S".</p>                                                      |
| 142. | <p>En el "Administrador del servidor" despliegue el menú superior derecho "Herramientas" y a continuación seleccione "Certification Authority".</p>    |

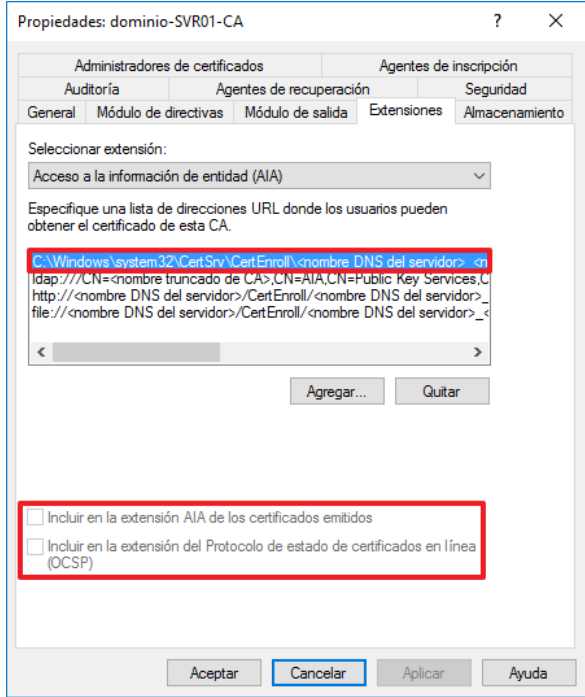
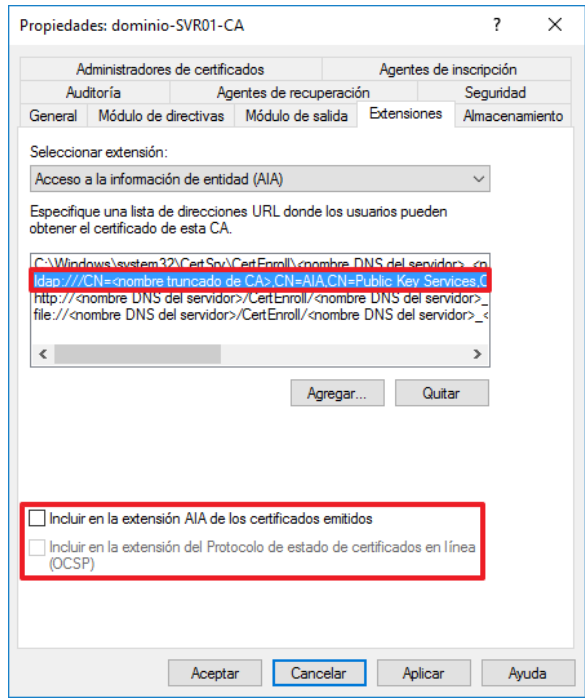
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 143. | <p>Despliegue el menú de la izquierda hasta llegar a los servicios de certificado del servidor Entidad de Certificación configurado recientemente y con el botón derecho del ratón seleccione “Propiedades”.</p>                                                                                                                                                                                                                                                                                                                                               |
| 144. | <p>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 <b>“C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y mantenga las opciones marcadas por defecto. Ambas casillas deben quedar marcadas tal y como se muestra en la siguiente figura.</p>  |

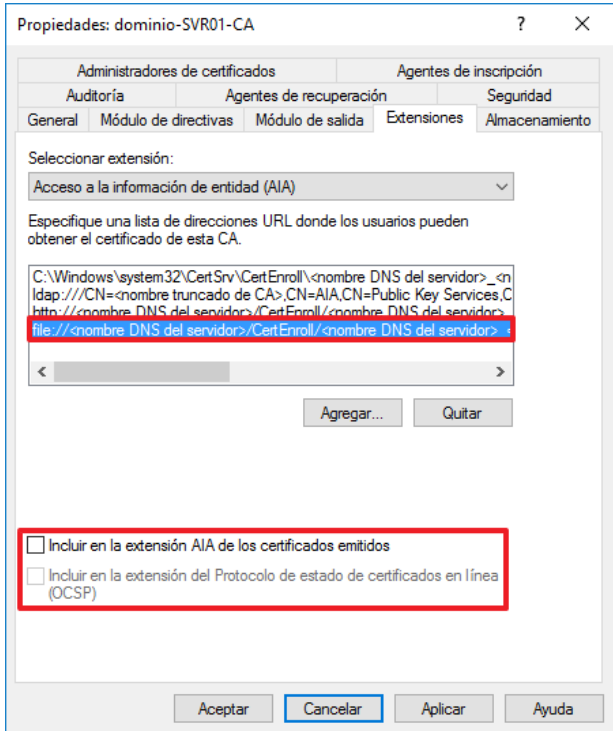
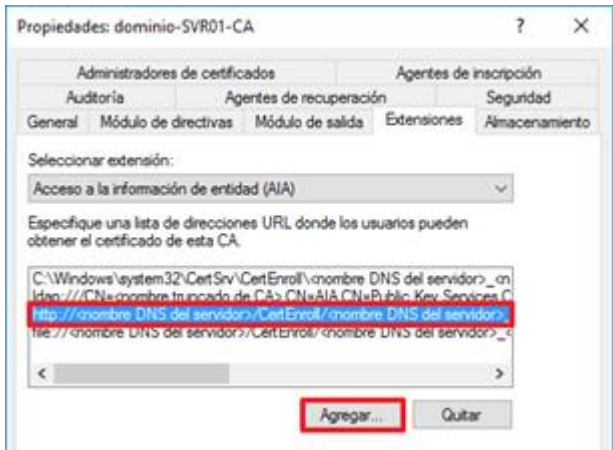
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 145. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)” deshabilite la publicación de CRLs mediante LDAP seleccionando “<b>ldap://CN=&lt;nombre truncado de CA&gt;&lt; sufijo de nombre de lista CRL&gt;,CN=nombre corto del servidor,CN=CDP,CN=Public Key Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CDP&gt;</b>” y desmarcando todas las opciones.</p> <p>Todas las casillas deben quedar desmarcadas tal y como se muestra en la siguiente figura:</p>  |
| 146. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione “<b>file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl</b>” y desmarque todas las opciones como muestra la siguiente figura.</p>                                                                                                                                                                  |

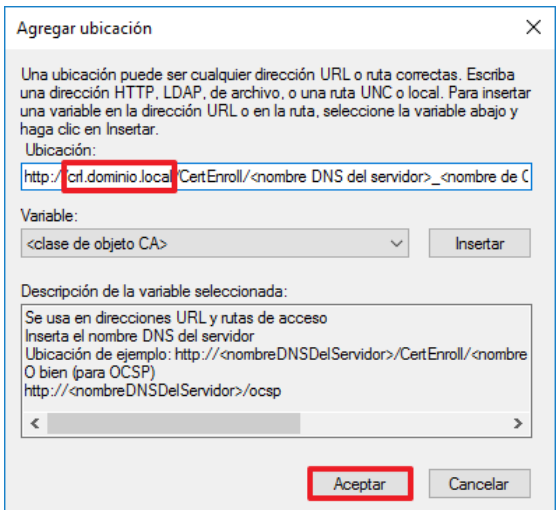
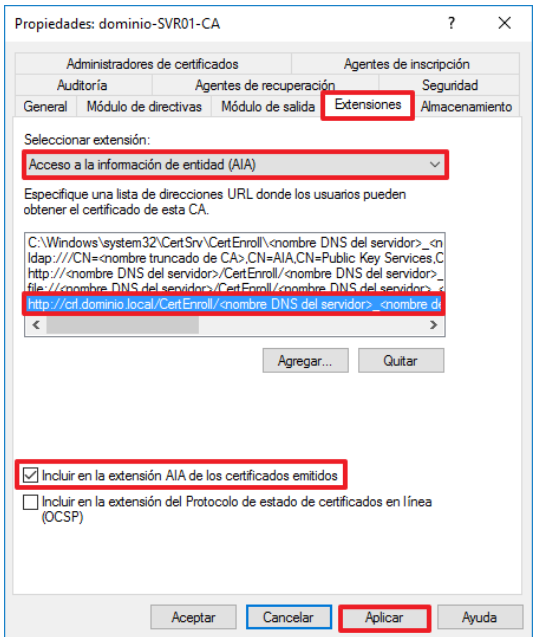
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 147. | De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione <b>“http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre de CA&gt;&lt; sufijo de nombre de lista CRL&gt;&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y pulse “Control + C”, para copiar el objeto. |
| 148. | Pulse el botón “Agregar”.<br>                                                                                                                                                                                                                                                                       |
| 149. | Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.<br>                                                                                                                                               |

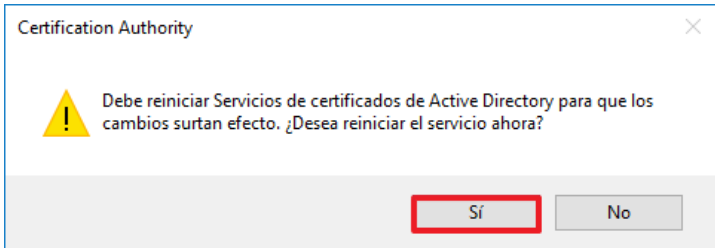
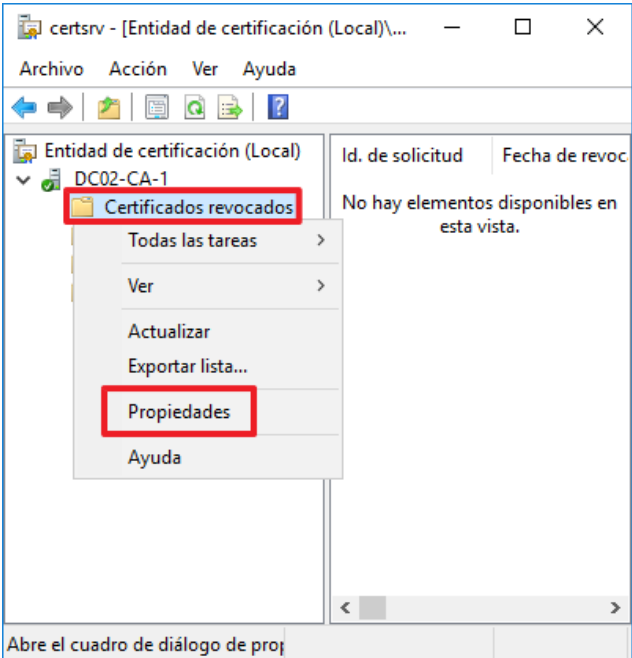
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 150. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación que se creó anteriormente (Punto 2.3 PREPARACIÓN DEL DIRECTORIO ACTIVO) en la Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                                                                                                                                                      |
| 151. | <p>De nuevo en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Puntos de distribución de lista de revocación de certificados (CDP)”, seleccione la ubicación recién creada <b>“http://CRL.dominio.local/CertEnroll/&lt;nombre de CA&gt;/sufijo de nombre de lista CRL&lt;diferencias entre listas CRL permitidas&gt;.crl”</b> y marque los siguientes elementos. Pulse “Aplicar” para guardar los cambios.</p> <ul style="list-style-type: none"> <li>– Incluir en las CRL. Usada para encontrar la ubicación de diferencias CRL.</li> <li>– Incluir en la extensión CDP de los certificados emitidos</li> <li>– Incluir en la extensión IDP de CRL emitidas</li> </ul>  |

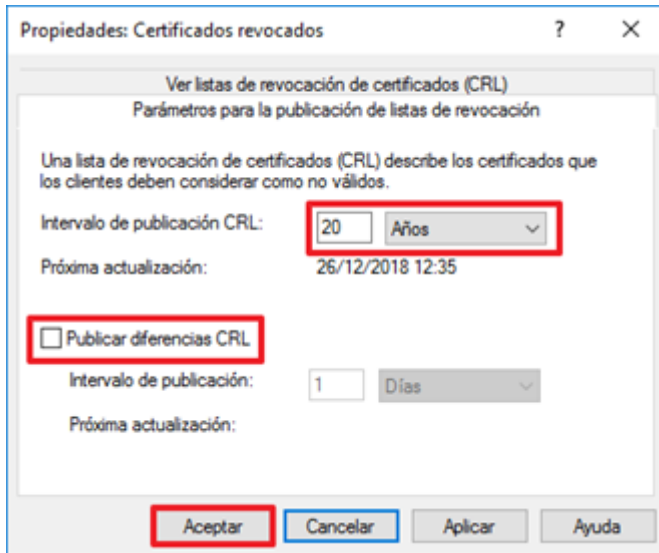
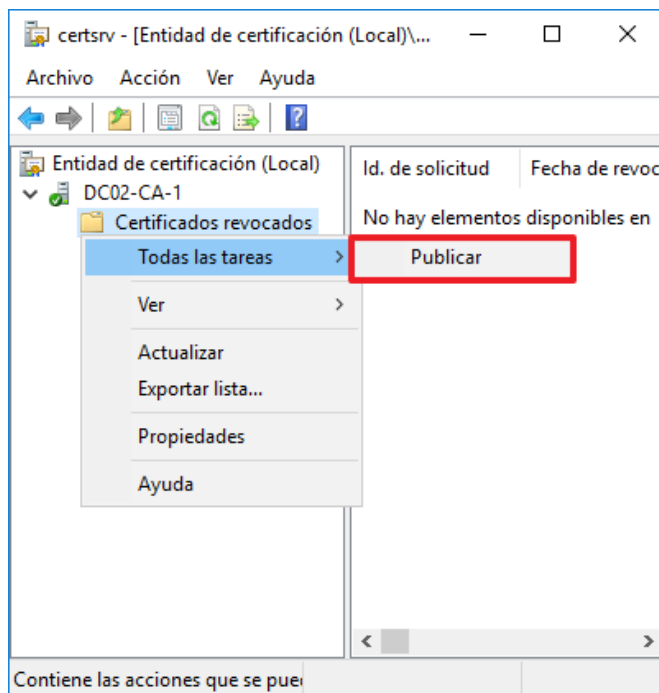
| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 152. | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                          |
| 153. | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                                                                                        |
| 154. | <p>De nuevo en la pestaña “Extensiones”, seleccione la flecha para desplegar el campo “Seleccionar extensión” y haga clic sobre “Acceso a la información de entidad (AIA)”.</p>  |

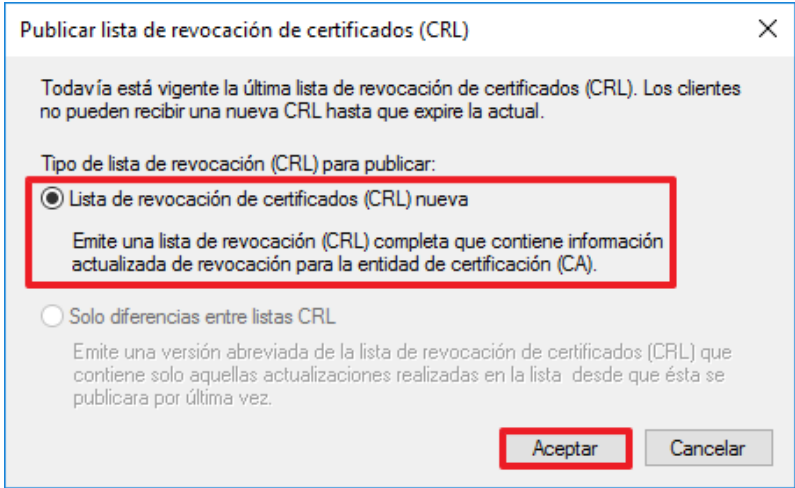
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 155. | <p>Compruebe que en el objeto <b>"C:\Windows\System32\CertSrv\CertEnroll\&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;Nombre de certificado&gt;.crt"</b> todas las casillas están desmarcadas, tal y como se muestra en la siguiente figura.</p>                     |
| 156. | <p>Compruebe que en el objeto <b>"ldap://CN=&lt;nombre truncado de CA&gt;,CN=AIA,CN=Public Key Services,CN=Services,&lt;contenedor de configuración&gt;&lt;clase de objeto CA&gt;"</b> todas las casillas están desmarcadas tal y como se muestra en la siguiente figura.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 157. | <p>Seleccione ahora “file://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y desmarque la opción “Incluir en la extensión AIA de los certificados emitidos”.</p>  |
| 158. | <p>Seleccione “http://&lt;nombre DNS del servidor&gt;/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt” y copie el elemento mediante la combinación de teclas “Control + C”.</p>                                                                                                        |
| 159. | <p>Pulse el botón “Agregar”.</p>                                                                                                                                                                                                                    |
| 160. | <p>Coloque el cursor sobre el campo vacío bajo “Ubicación:” y pulse la combinación de teclas “Control + V” para pegar el contenido recién copiado.</p>                                                                                                                                                                                  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 161. | <p>En “Agregar ubicación”, diríjase al comienzo de la línea de texto y sustituya el valor “&lt;nombre DNS del servidor&gt;” por el nombre DNS completo que corresponderá al servidor web de Entidad de Certificación subordinada. Pulse “Aceptar” para guardar los cambios.</p>  <p><b>Nota:</b> En el ejemplo, se ha utilizado el nombre CRL.dominio.local.</p>                                                                                     |
| 162. | <p>De nuevo, en la pestaña “Extensiones” y manteniendo seleccionada la extensión “Acceso a la información de entidad (AIA)”, seleccione la ubicación recién creada ahora “<b>http://CRL.dominio.local/CertEnroll/&lt;nombre DNS del servidor&gt;_&lt;nombre de CA&gt;&lt;nombre de certificado&gt;.crt</b>” y marque el elemento “Incluir en la extensión AIA de los certificados emitidos”.</p> <p>Pulse “Aplicar” para guardar los cambios.</p>  |

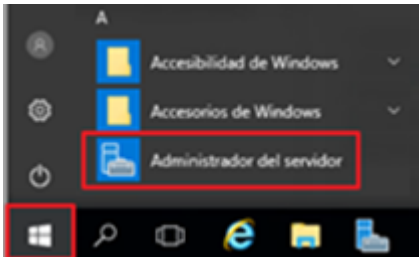
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 163. | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 164. | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 165. | <p>El siguiente paso será establecer un período de caducidad para la lista de revocación de certificados (CRL), si caduca la CRL y al no poder comprobar si un certificado está en vigor o no, no será posible hacer uso de dicho certificado del mismo modo que si éste estuviera caducado.</p> <p>Para establecer el período de caducidad de las CRLs, en el “Administrador del Servidor” que ya se había abierto para las configuraciones anteriores, se deberá navegar hasta alcanzar el contenedor de “Certificados revocados” que se encuentra en la siguiente ruta:</p> <p><b>“Administrador del Servidor → Herramientas → Entidad de certificación → &lt;nombre de la Entidad de Certificación&gt; → Certificados revocados”</b></p> <p>Pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>  |

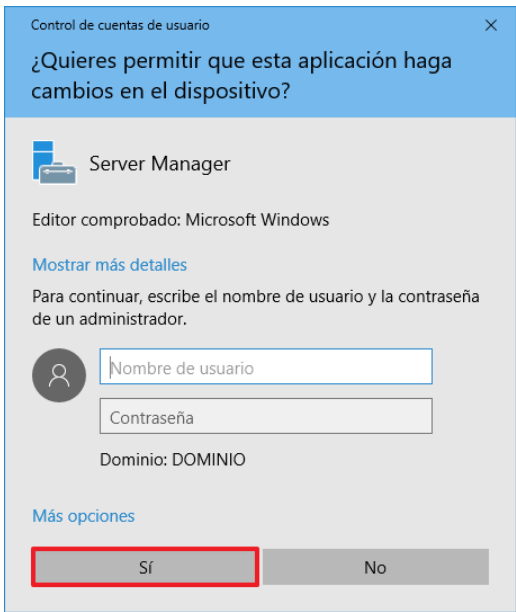
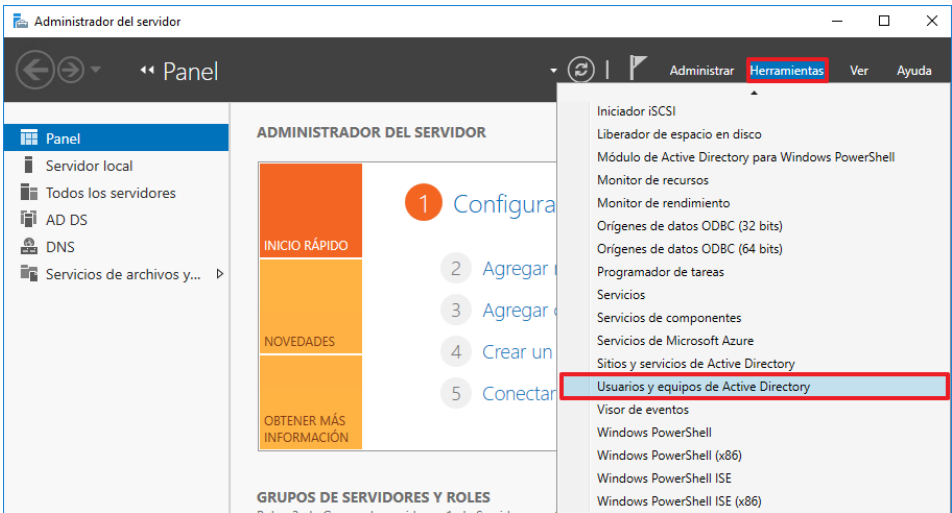
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 166. | <p>En “Intervalo de publicación CRL” introduzca el intervalo que indica cada cuánto tiempo se publicará la CRL. Establezca el intervalo de publicación y pulse “Aceptar” para cerrar la ventana de “Propiedades: Certificados revocados”.</p>  <p><b>Nota:</b> En el ejemplo, se ha indicado un periodo de validez igual al del certificado (20 años). Así mismo y debido al propósito de esta entidad, no será necesario el uso de “Diferencias CRL” y, por tanto, se mantendrá desmarcado como indica la figura.</p> |
| 167. | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                                                                                                                                                                                                                                                                                          |

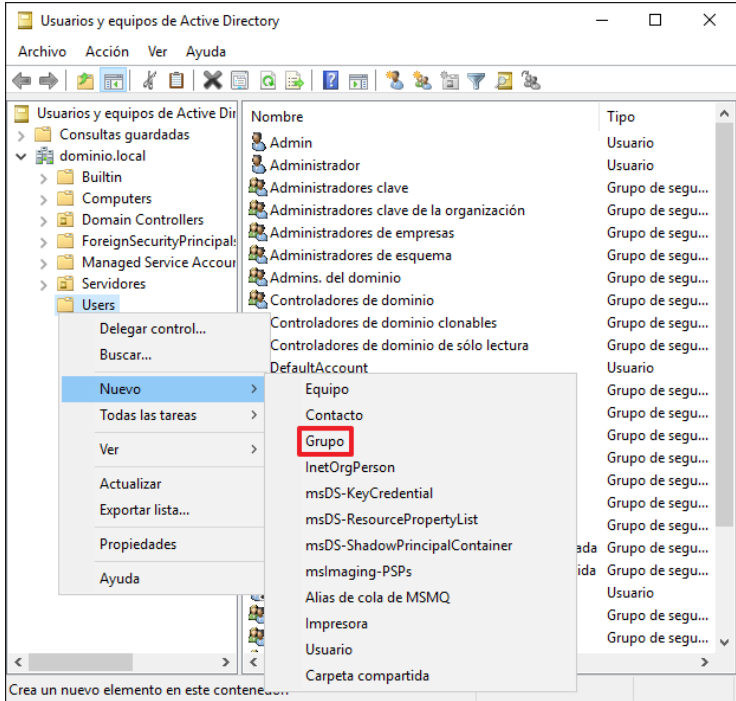
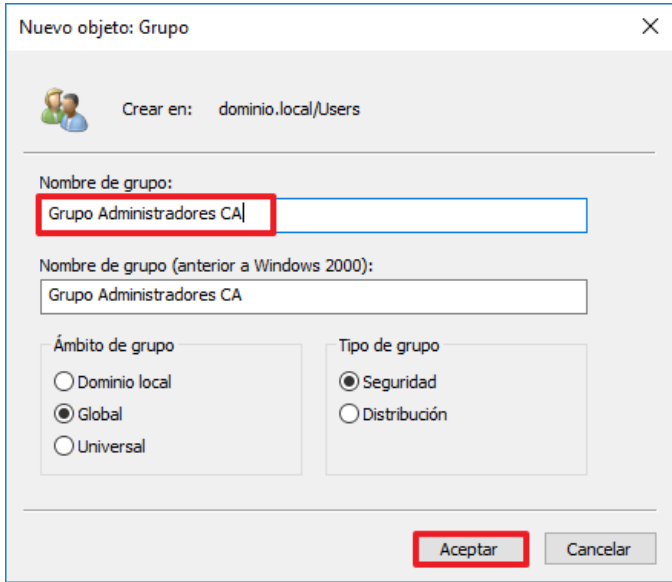
| Paso | Descripción                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 168. | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>  |

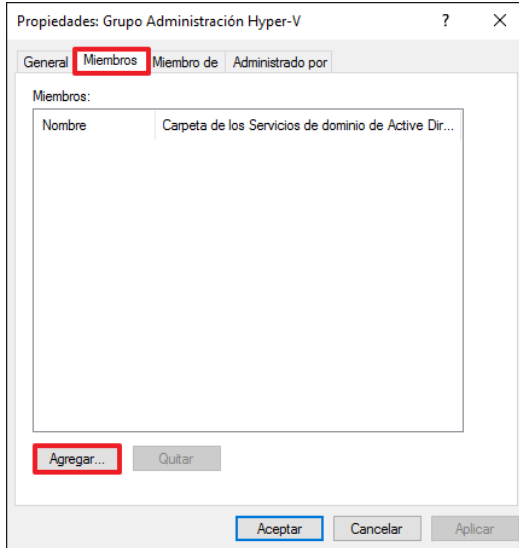
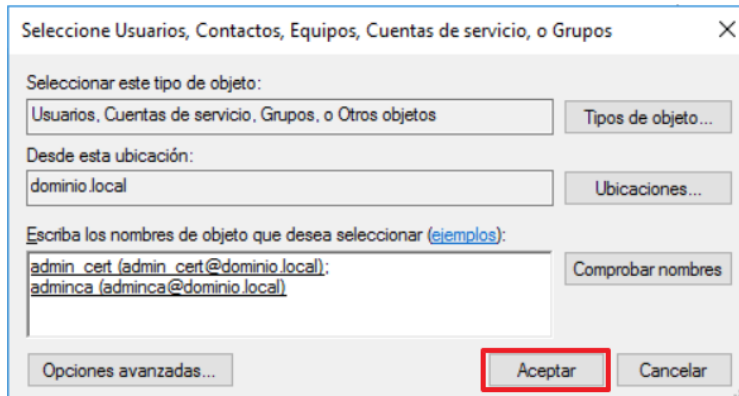
## 2.5. SEGREGACIÓN DE ROLES

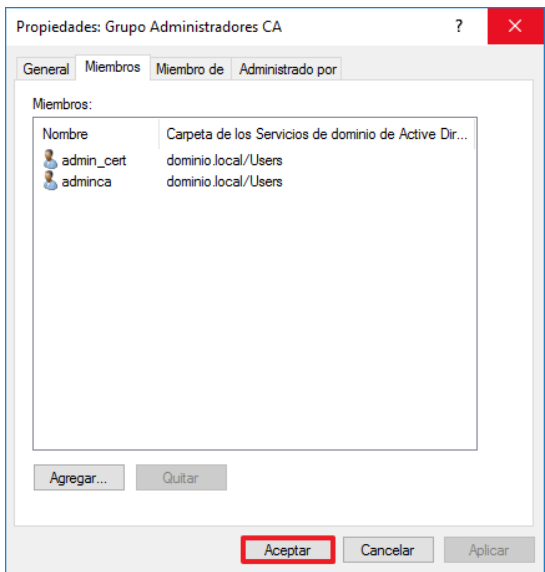
Con la aplicación del ENS para la categoría alta - DL sobre el Servidor de Certificación subordinada de Dominio, será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar el Servidor de Certificación.

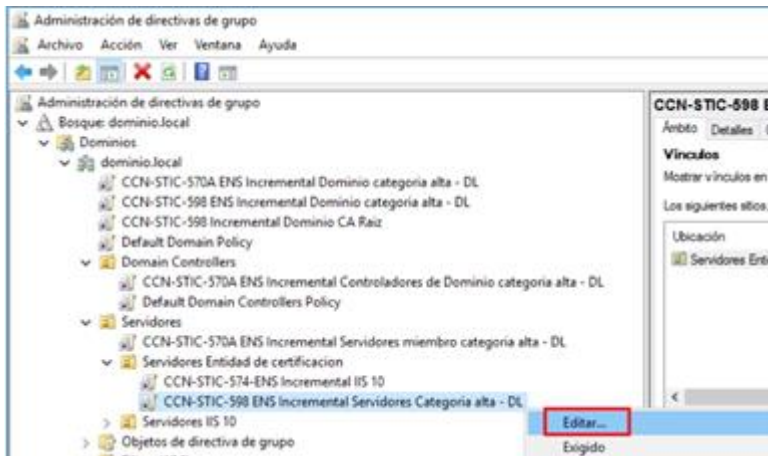
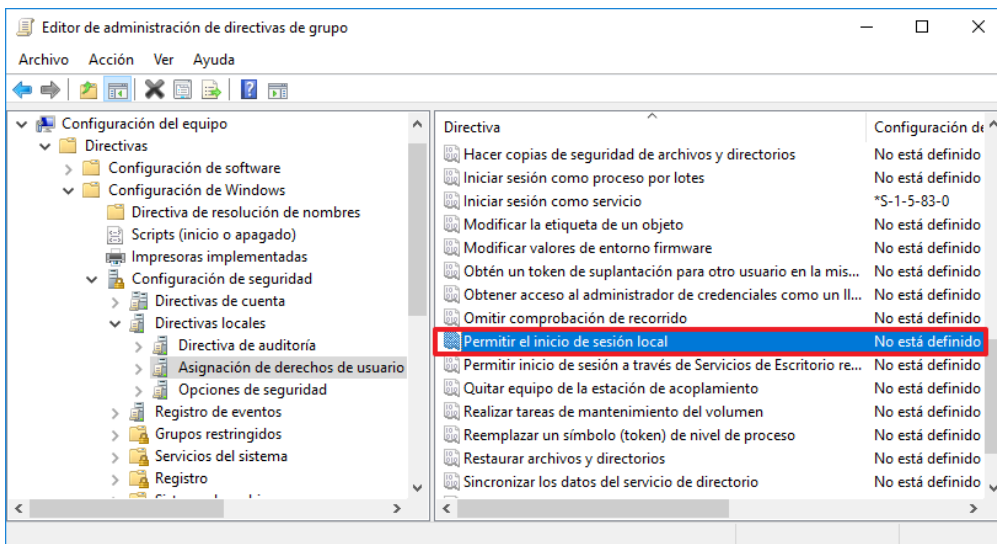
| Paso | Descripción                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 169. | <p>Inicie sesión en el servidor de certificación subordinada donde se va a aplicar seguridad según criterios de ENS.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea Administrador del Dominio.</p> |
| 170. | <p>A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.</p>                                                                            |

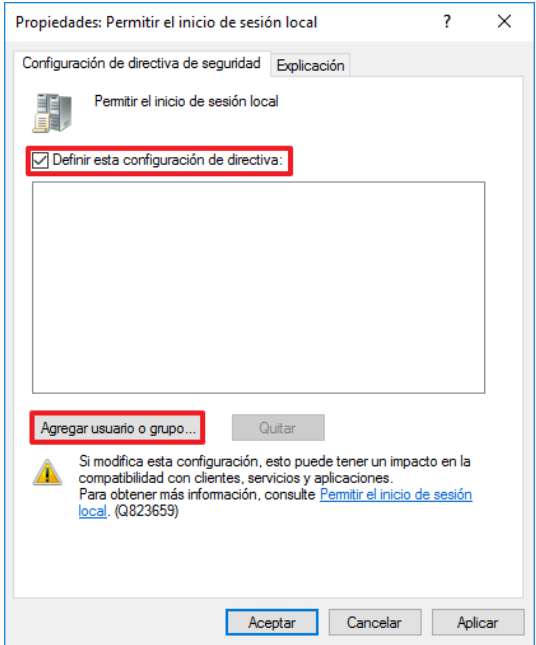
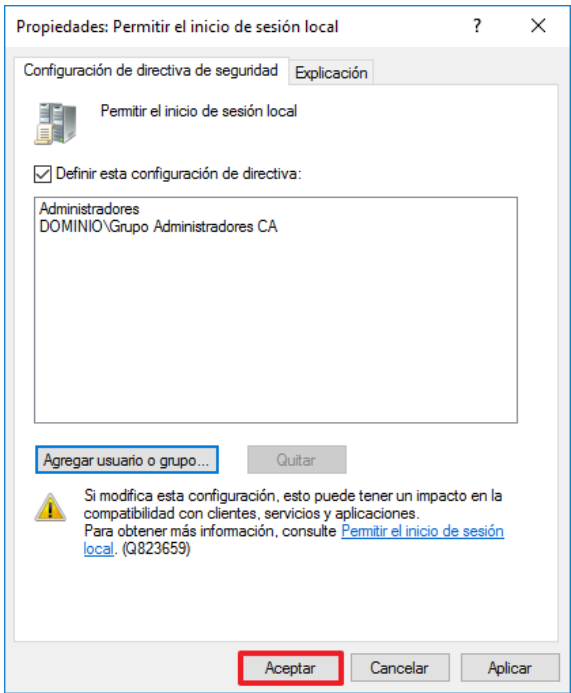
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 171. | <p>El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.</p>                                                                                                                                                     |
| 172. | <p>A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione <b>“Herramientas → Usuarios y equipos de Active Directory”</b>.</p>  |

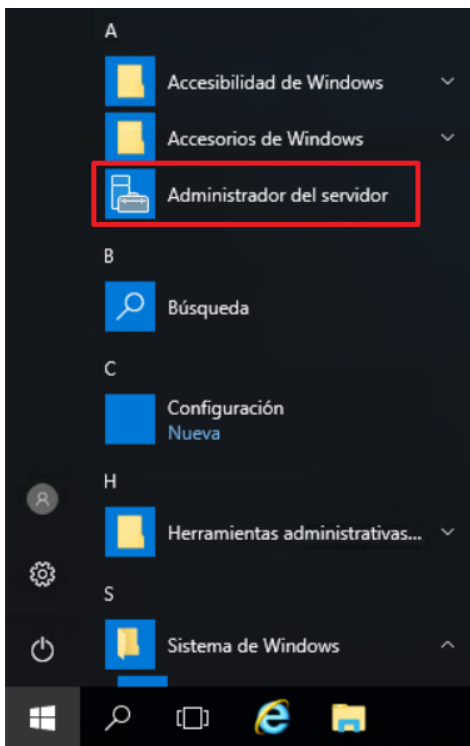
| Paso | Descripción                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 173. | <p>Despliegue el nodo “&lt;&lt;su dominio&gt;&gt; → Users”. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual “Nuevo → Grupo”.</p>       |
| 174. | <p>Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p> |

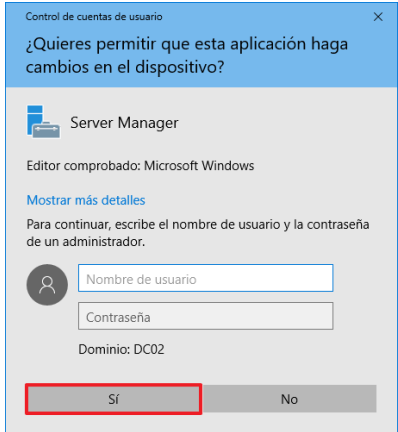
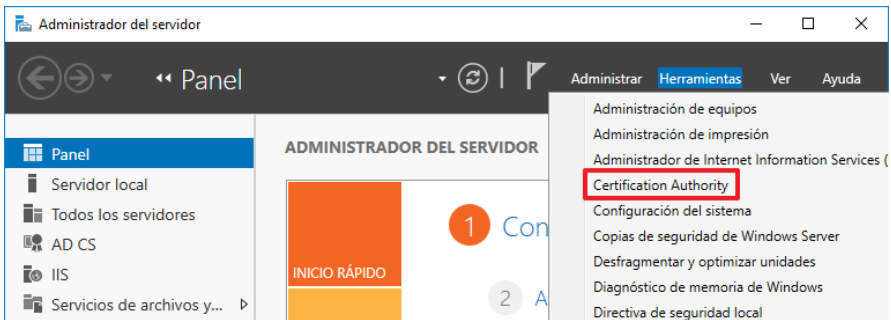
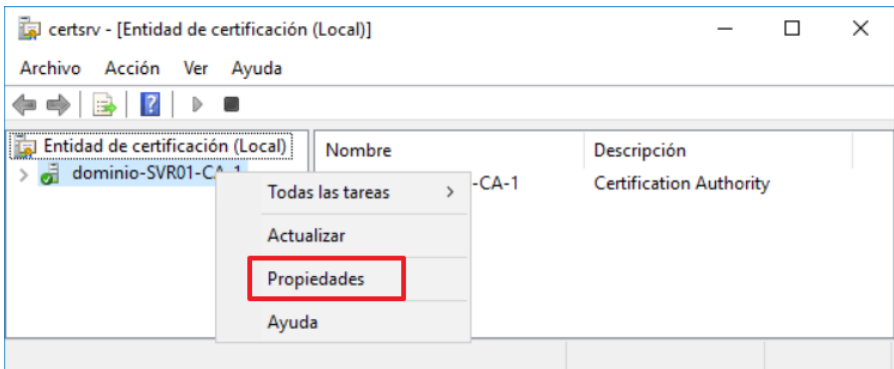
| Paso | Descripción                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 175. | <p>Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo.</p>                                              |
| 176. | <p>Añada los usuarios que desee al grupo y pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se añaden los usuarios “adminca” y “admin_cert” utilizados para la generación de esta guía”.</p> |

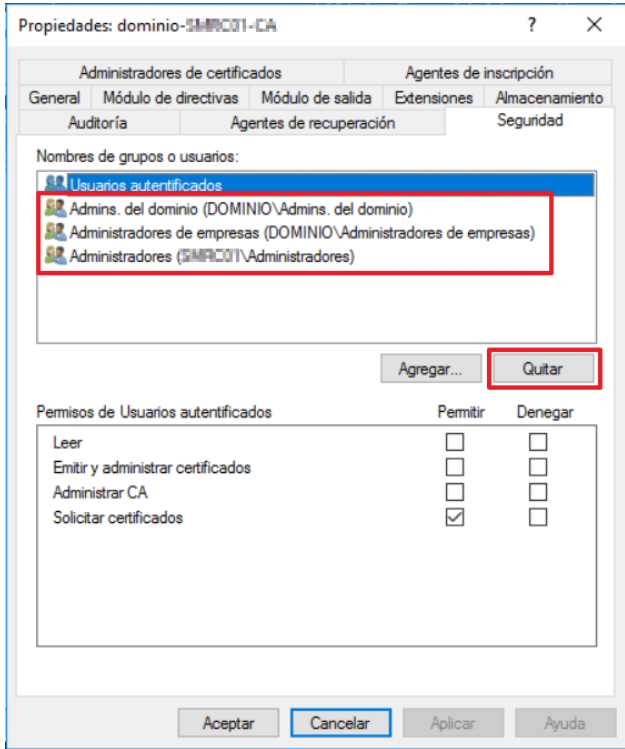
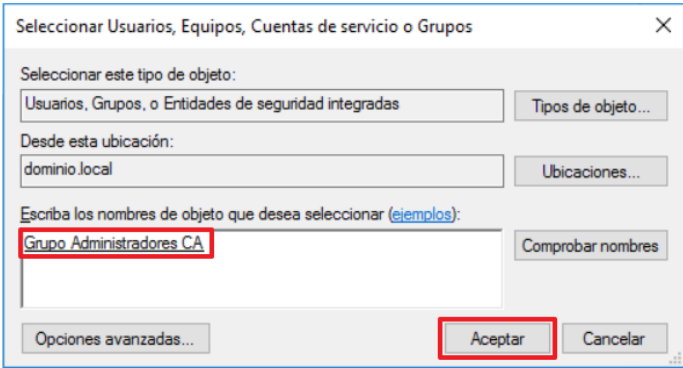
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 177. | <p>Pulse “Aceptar” cuando haya finalizado.</p>                                                                                                                                                                                                                                            |
| 178. | <p>A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione <b>“Herramientas → Administración de directivas de grupo”</b>.</p>  |

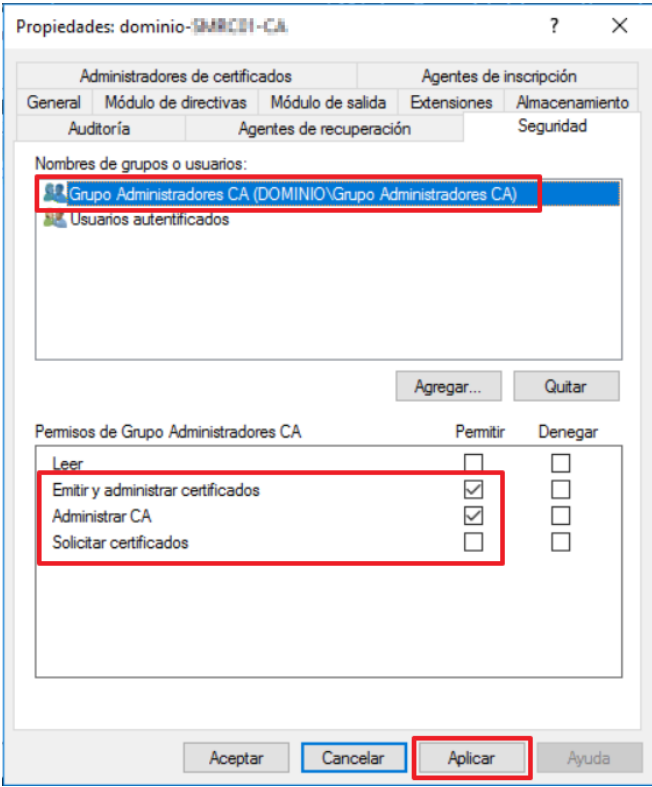
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 179. | <p>Expanda el árbol <b>“Bosque:&lt;nombre de su bosque&gt; → Dominios → &lt;nombre de su dominio&gt;”→“Servidores” → “Entidad certificadora”</b> y pulse con el botón derecho el objeto GPO denominado <b>“CCN-STIC-598 Incremental Servidor Entidad de Certificación Categoría alta - DL”</b>, y seleccione la opción del menú contextual <b>“Editar...”</b>.</p>  |
| 180. | <p>Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. <b>“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</b>.</p> <p>Haga doble clic en el panel derecho sobre la directiva <b>“Permitir el inicio de sesión local”</b>.</p>      |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 181. | <p>Marque la casilla “Definir esta configuración de directiva:” y pulse sobre “Agregar usuario o grupo...”.</p>                                                                                                                                                                                                                                                     |
| 182. | <p>Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor de Entidad de Certificación. Pulse “Aceptar” cuando haya finalizado.</p>  <p><b>Nota:</b> En este ejemplo se hace uso del grupo denominado “Grupo Administración CA”. Deberá adaptar esta configuración a las necesidades de su organización.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 183. | <p>A continuación, inicie sesión en el Servidor de Entidad de Certificación Subordinada.</p>  <p><b>Nota:</b> Inicie sesión con una cuenta que sea administrador del dominio.</p> |
| 184. | <p>A continuación, ejecute la consola administrativa "Certification Authority". Para ello, clic en <b>"Inicio de Windows → Administrador del servidor"</b>.</p>                  |

| Paso | Descripción                                                                                                                                                                                                                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 185. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                    |
| 186. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                            |
| 187. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “dominio-SVR01-CA-1”.</p> |

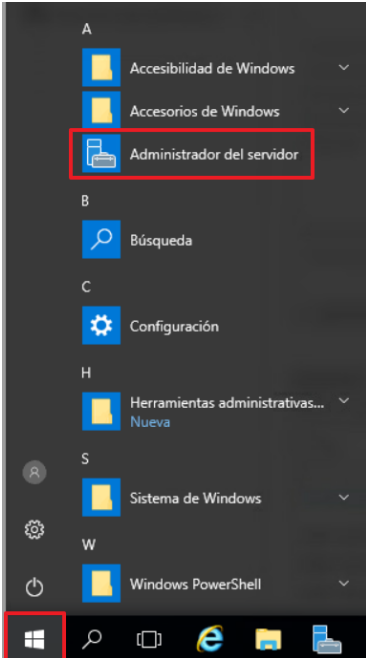
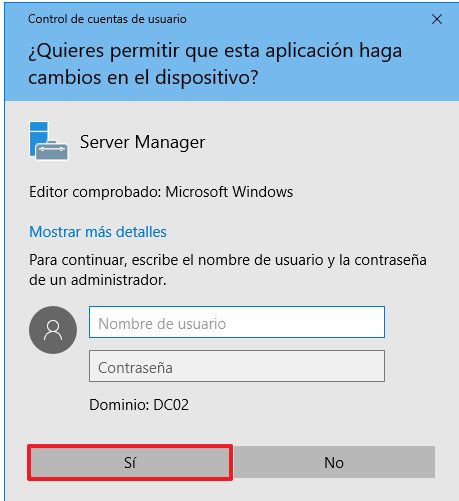
| Paso | Descripción                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 188. | <p>En la ventana “Propiedades” seleccione la pestaña “Seguridad” y marque uno a uno los grupos Administradores (del dominio, de empresa y locales) y, pulse “Quitar” para eliminar los grupos.</p>  |
| 189. | <p>A continuación, añada el grupo “Grupo Administradores CA” y pulse “Aceptar”.</p>                                                                                                                |

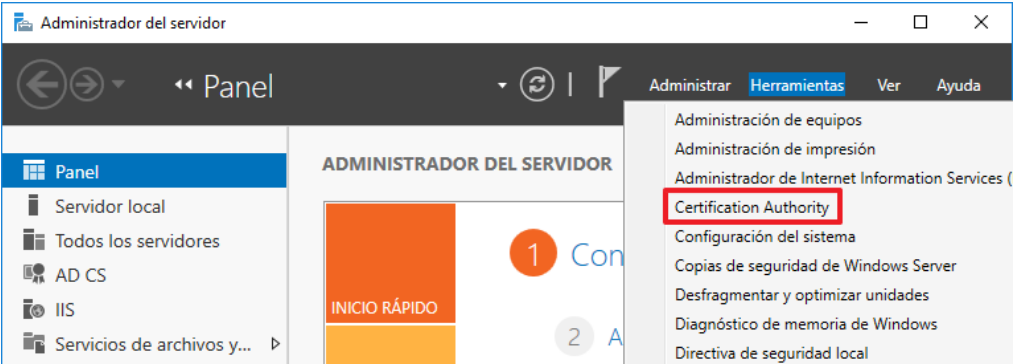
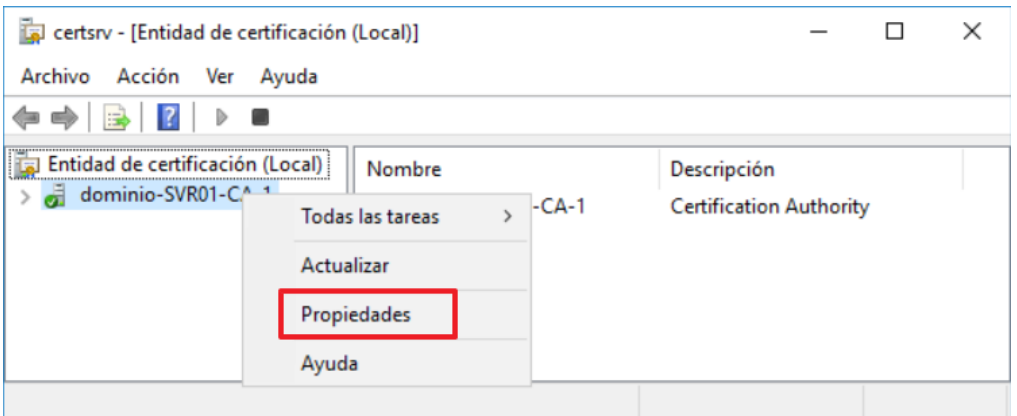
| Paso | Descripción                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 190. | <p>Seleccione el grupo recién añadido, otórguele los permisos “Emitir y administrar certificados” y “Administrar CA” y desmarque la opción “Solicitar certificados”. Pulse “Aceptar” para guardar los cambios.</p>  |
| 191. | <p>A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración CA” podrán acceder al servidor de CA y administrar dicho rol.</p>                                                                                                                                 |

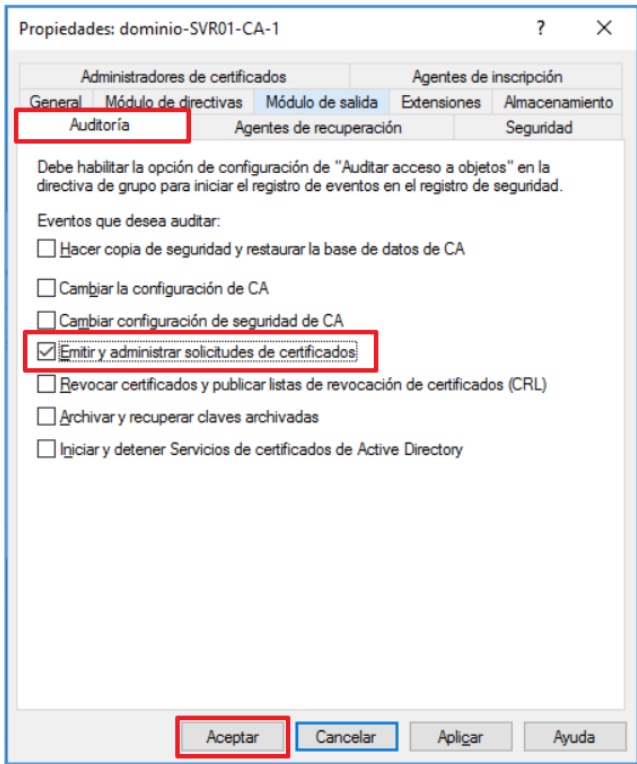
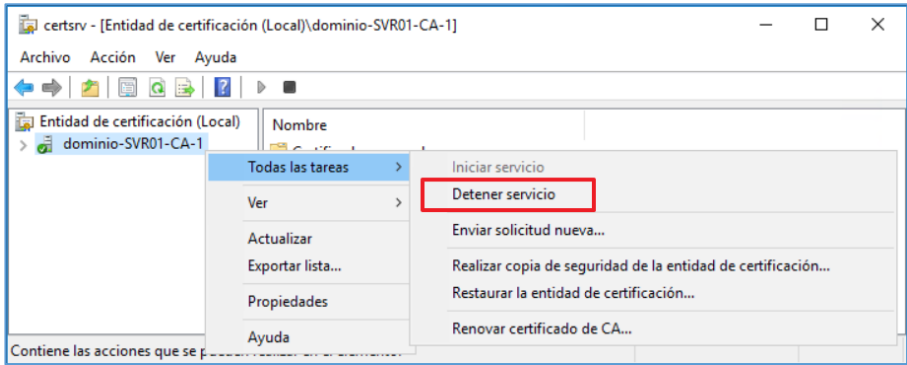
## 2.6. AUDITORÍA DE LAS OPERACIONES DE LA ENTIDAD DE CERTIFICACIÓN

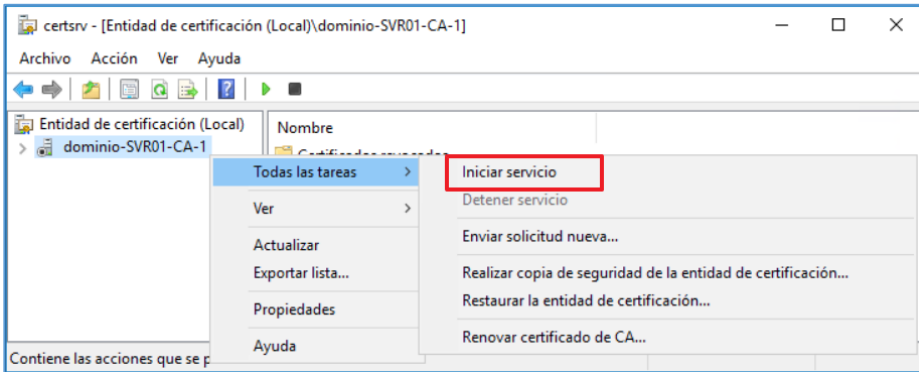
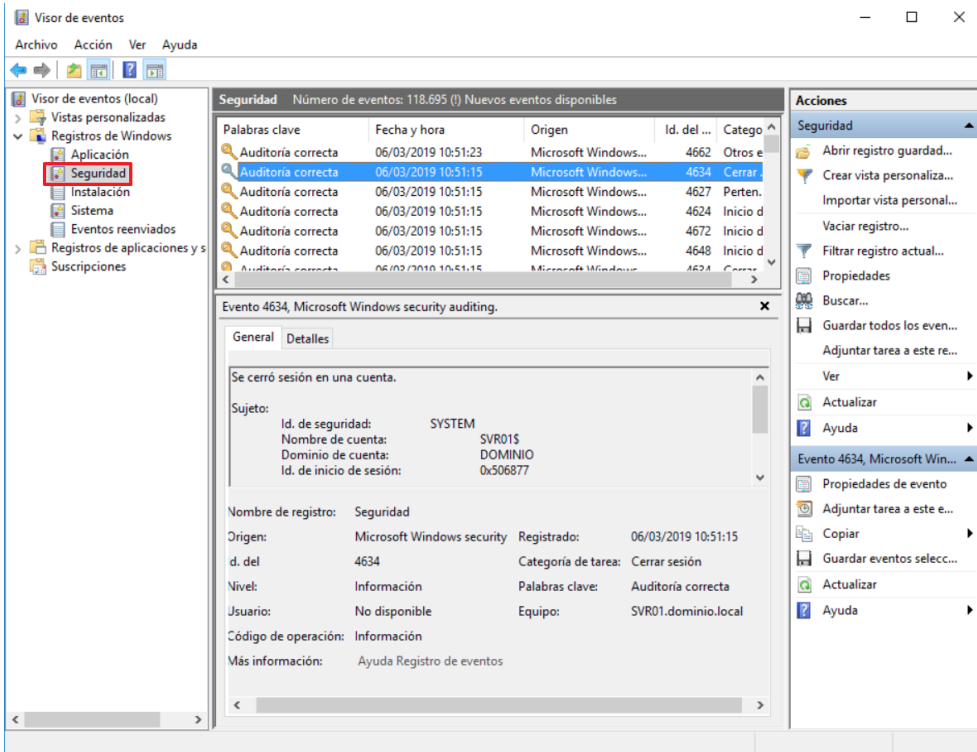
Existe la posibilidad que auditores lleven un control de las diferentes tareas que se realizan a través de la Entidad de Certificación. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoria de eventos de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma, por lo que tendrá que repetir este punto en ambas Entidades de certificación.

| Paso | Descripción                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 192. | <p>Inicie sesión en la Entidad de Certificación para configurar la auditoría.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 193. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                          |
| 194. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 195. | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                            |
| 196. | <p>Pulse con el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>  <p><b>Nota:</b> En este ejemplo el nombre de la Entidad Certificadora es “dominio-SVR01-CA-1”.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 197. | <p>En la ventana “Propiedades” seleccione la pestaña “Auditoría”, marque la opción “Emitir y administrar solicitudes de certificados” y a continuación pulse “Aceptar”.</p>  <p><b>Nota:</b> En este ejemplo se ha decidido seleccionar la pestaña “Emitir y administrar solicitudes de certificados”. La elección de marcar diferentes opciones de auditoría dependerá de las necesidades de la organización. Para que sea posible la captura de eventos de la Entidad de Certificación, el equipo debe estar configurado para auditar también el acceso a objetos. Las opciones de directiva de auditoría se pueden ver y administrar en una directiva de grupo local o de dominio en la siguiente ruta: <b>“Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales”</b>.</p> |
| 198. | <p>A continuación, pulse el botón derecho del ratón sobre la Entidad de Certificación, en el menú <b>“Todas las tareas → Detener servicio”</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 199. | <p>Una vez que el servicio esté parado, en la ventana de “Administrador del servidor” pulse en el menú “<b>Acción → Todas las tareas → Iniciar servicio</b>” para iniciarlo de nuevo.</p>                                                                                                                                                                                                                                                                                                                        |
| 200. | <p>A partir de este momento, el sistema capturará los eventos que hayan sido seleccionado, tal y como muestra la siguiente imagen.</p>  <p><b>Nota:</b> Para visualizar los eventos de la Entidad de Certificación, vaya al menú inicio: “<b>Inicio → Herramientas administrativas → Visor de eventos</b>”. Una vez dentro navegue por el árbol de la izquierda hasta llegar al apartado de seguridad y a través de la siguiente ruta: “<b>Visor de eventos (local) → Registro de Windows → Seguridad</b>”.</p> |

#### ANEXO A.4.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA ENTIDAD DE CERTIFICACIÓN SOBRE MS WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE

**Nota:** Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía “ANEXO A.4.3.IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA ENTIDAD DE CERTIFICACIÓN INDEPENDIENTE SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS”.

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores con rol de Entidad de Certificación sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

### 1. COMPROBACIONES EN EL SERVIDOR INDEPENDIENTE ENTIDAD DE CERTIFICACIÓN RAÍZ

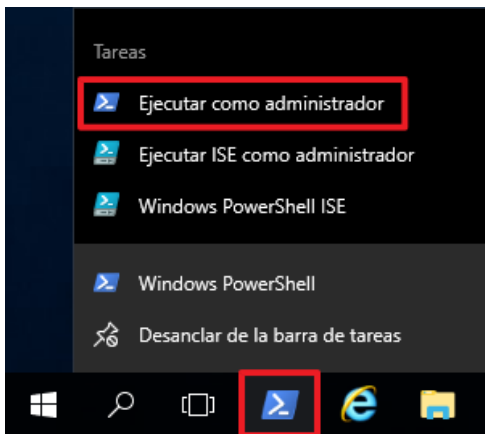
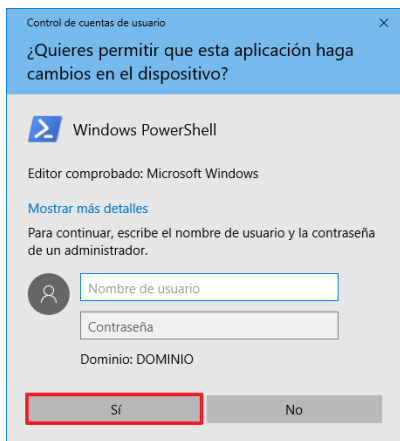
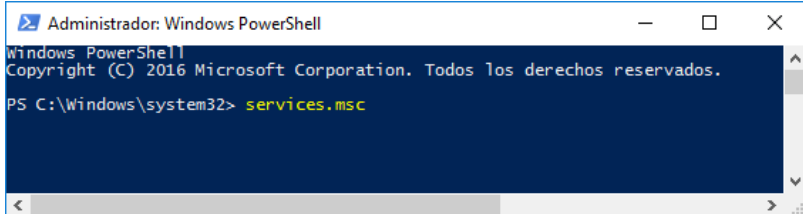
Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor independiente con una cuenta de usuario que tenga privilegios de administración.

Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

- a) Consola de servicios (services.msc)
- b) Explorador de Archivos (explorer.exe)

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

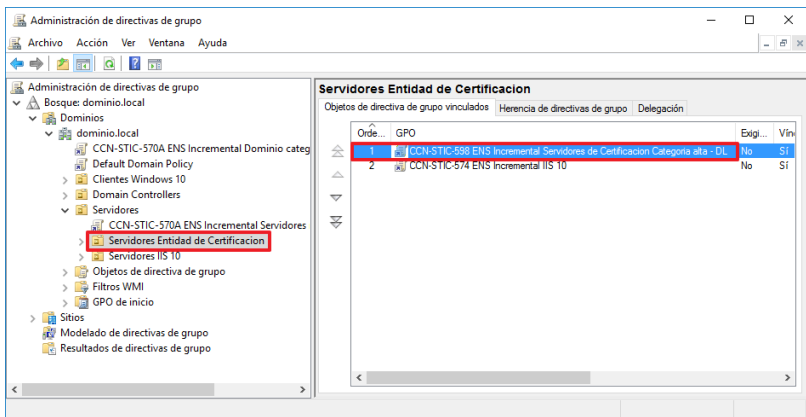
| Comprobación                                                            | OK/NOK | Cómo hacerlo                                                                                                                      |
|-------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor independiente Entidad de Certific. raíz |        | En el servidor independiente Entidad de Certificación raíz, inicie sesión con una cuenta que tenga privilegios de administración. |

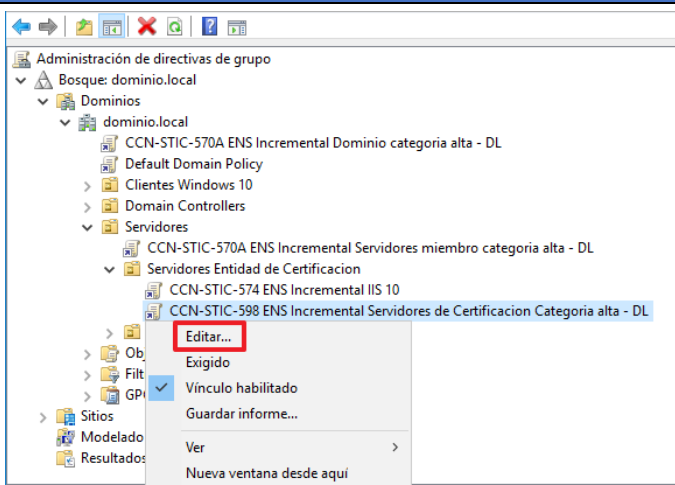
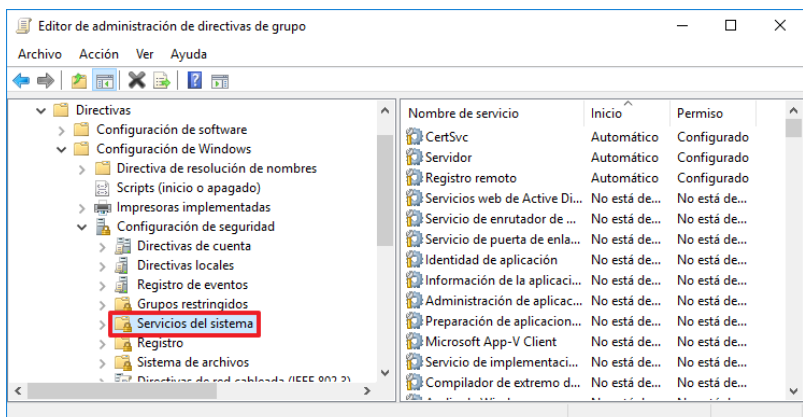
| Comprobación                                                                       | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |             |        |
|------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
| 2. Verifique la correcta aplicación de la configuración de servicios del sistema". |                         | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>  <p>Teclee “rsop.msc” en la consola de comandos que se ha abierto:</p>  <p>En la consola de “Servicios”, compruebe los siguientes valores.</p> |             |        |
| Servicio (Nombre largo)                                                            | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                      | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Configurado |        |

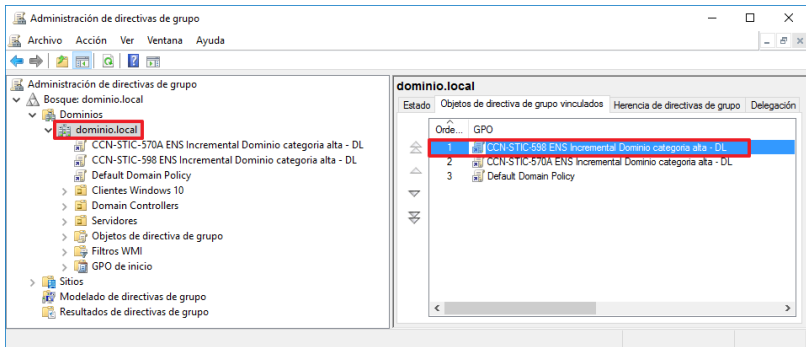
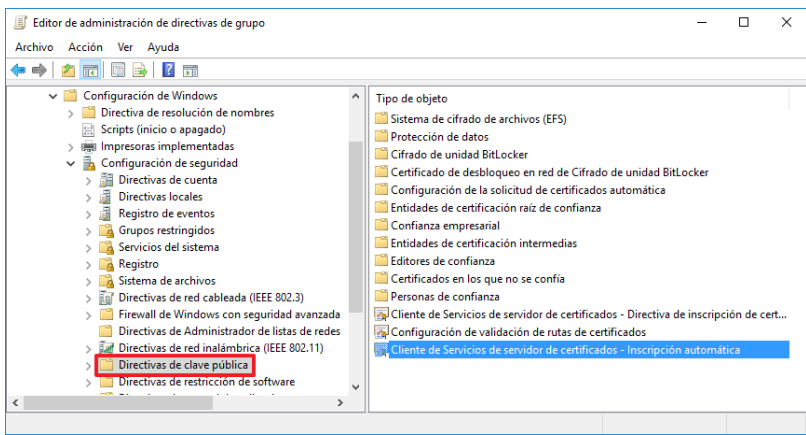
## 2. COMPROBACIONES EN EL CONTROLADOR DE DOMINIO

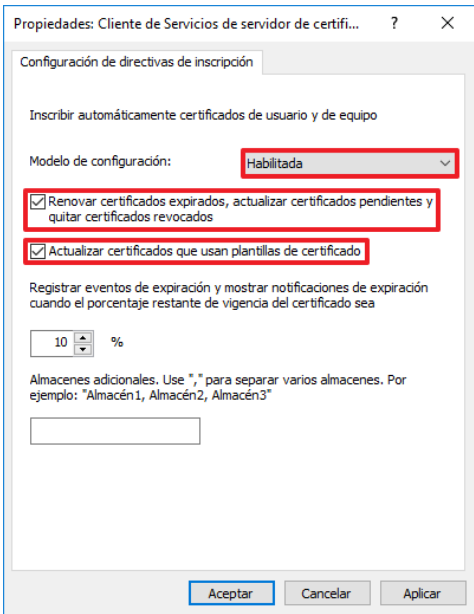
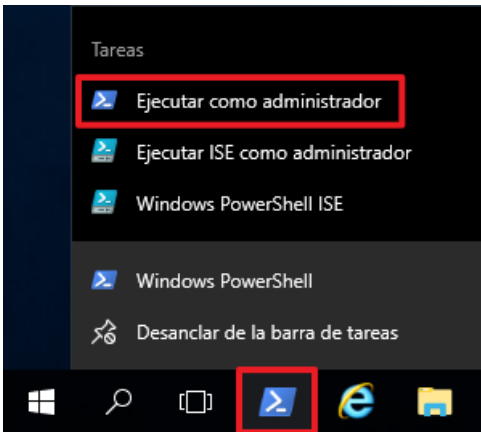
Las consolas y herramientas que se utilizarán son las siguientes:

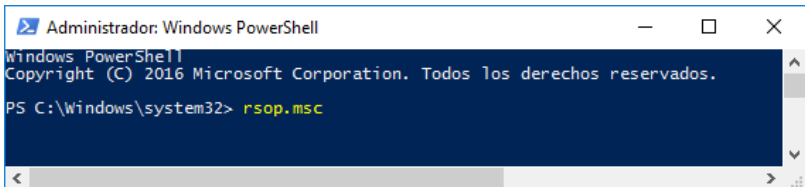
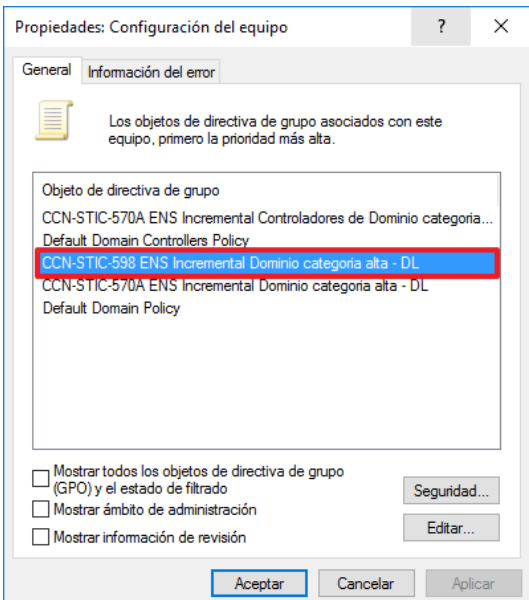
- Administrador de directivas de grupo (gpmc.msc).
- Usuarios y equipos de Active Directory (dsa.msc).
- Conjunto resultante de directivas (rsop.msc).

| Comprobación                                                                                                                           | OK/NOK                          | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                          |                                 |            |                                                                                |    |    |                                       |    |    |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------|------------|--------------------------------------------------------------------------------|----|----|---------------------------------------|----|----|
| 1. Inicie sesión en un controlador de dominio.                                                                                         |                                 | En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                          |                                 |            |                                                                                |    |    |                                       |    |    |
| 2. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL".              |                                 | <p>Ejecute el "Administrador de directivas de grupo" mediante la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b></p> <p>Despliegue el menú en árbol hasta llegar a la unidad organizativa "Servidores Entidad de Certificación". Verifique que la política "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL" está creada y vinculada en el primer lugar de orden de vínculo.</p>  <table border="1"> <caption>Servidores Entidad de Certificación</caption> <thead> <tr> <th>Objetos de directiva de grupo vinculados</th> <th>Herencia de directivas de grupo</th> <th>Delegación</th> </tr> </thead> <tbody> <tr> <td>1 CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL</td> <td>No</td> <td>SI</td> </tr> <tr> <td>2 CCN-STIC-574 ENS Incremental IIS 10</td> <td>No</td> <td>SI</td> </tr> </tbody> </table> | Objetos de directiva de grupo vinculados | Herencia de directivas de grupo | Delegación | 1 CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL | No | SI | 2 CCN-STIC-574 ENS Incremental IIS 10 | No | SI |
| Objetos de directiva de grupo vinculados                                                                                               | Herencia de directivas de grupo | Delegación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                          |                                 |            |                                                                                |    |    |                                       |    |    |
| 1 CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL                                                         | No                              | SI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                          |                                 |            |                                                                                |    |    |                                       |    |    |
| 2 CCN-STIC-574 ENS Incremental IIS 10                                                                                                  | No                              | SI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                          |                                 |            |                                                                                |    |    |                                       |    |    |
| 3. Verifique los servicios del sistema de la directiva "CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL". |                                 | Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                          |                                 |            |                                                                                |    |    |                                       |    |    |

| Comprobación                                  | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |        |
|-----------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                               |                         | <div></div> <p>Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta:<br/><b>Directiva CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL</b> → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema</p> <div></div> <p><b>Nota:</b> Si lo desea puede pulsar sobre el título “Permiso” para ordenar la lista por servicios configurados.</p> |             |        |
| Servicio (Nombre largo)                       | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Servidor                                      | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |
| Registro Remoto                               | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configurado |        |

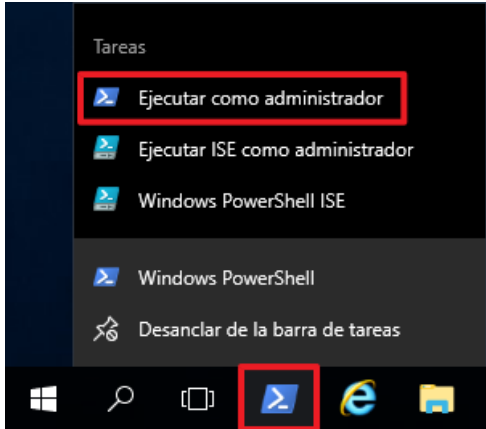
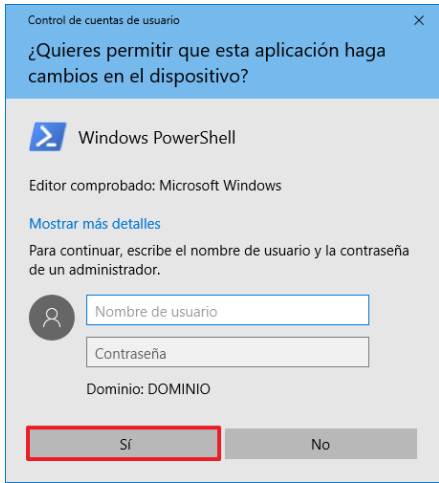
| Comprobación                                                                                                                                       | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Verifique que está creada la directiva "CCN-STIC-598 ENS Incremental Dominio Categoría alta - DL".                                              |        | <p>Ejecute el "Administrador de directivas de grupo" a través de la siguiente ruta:<br/> <b>"Inicio → Herramientas administrativas → Administración de directivas de grupo"</b></p> <p>Despliegue el menú en árbol hasta llegar al contenedor correspondiente al dominio. Verifique que la política "CCN-STIC-598 ENS Incremental Dominio categoría alta - DL" está creada y vinculada en el primer lugar de orden de vínculo.</p>                                                       |
| 5. Verifique la configuración de inscripción automática de certificados en la política "CCN-STIC-598 ENS Incremental Dominio categoría alta - DL". |        | <p>Haga clic derecho sobre la directiva y seleccione "Editar" para ejecutar el "Editor de Administración de directivas de grupo". Verifique que la directiva tiene los siguientes valores en la configuración de inscripción automática. Para ello, navegue hasta:</p> <p><b>Directiva CCN-STIC-598 ENS Incremental Dominio Categoría alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de clave pública</b></p>  |

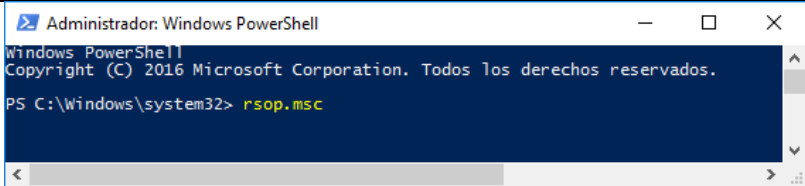
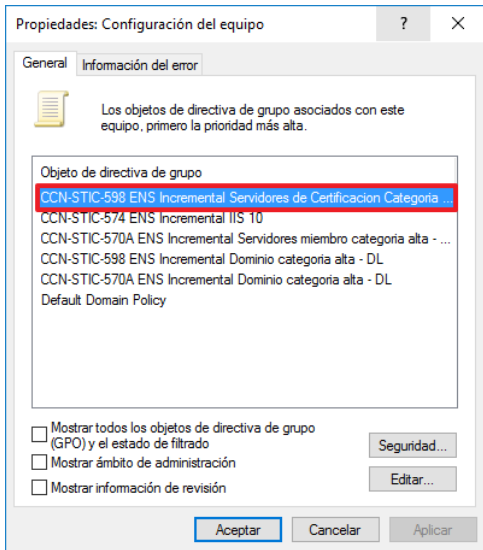
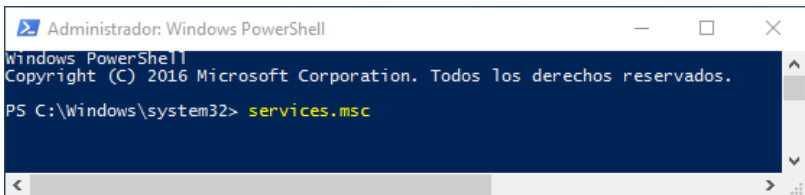
| Comprobación                                                                                               | OK/NOK               | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|------------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------|--------|-------------------------|------------|--|----------------------------------------------------------------------------------------------------|----------------------|--|------------------------------------------------------------|----------------------|--|
|                                                                                                            |                      | <p>Haga doble clic sobre el objeto “Cliente de Servicios de servidor de certificados – Inscripción automática” y compruebe los valores correspondientes a la inscripción automática.</p>                                                                                                                                                                                                         |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
|                                                                                                            |                      | <table border="1"> <thead> <tr> <th>Configuración</th><th>Estado</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Modelo de configuración</td><td>Habilitada</td><td></td></tr> <tr> <td>Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados</td><td>Habilitada (marcada)</td><td></td></tr> <tr> <td>Actualizar certificados que usan plantillas de certificado</td><td>Habilitada (marcada)</td><td></td></tr> </tbody> </table> | Configuración | Estado | OK/NOK | Modelo de configuración | Habilitada |  | Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados | Habilitada (marcada) |  | Actualizar certificados que usan plantillas de certificado | Habilitada (marcada) |  |
| Configuración                                                                                              | Estado               | OK/NOK                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Modelo de configuración                                                                                    | Habilitada           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Renovar certificados expirados, actualizar certificados pendientes y quitar certificados revocados         | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| Actualizar certificados que usan plantillas de certificado                                                 | Habilitada (marcada) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |
| 6. Verifique la correcta aplicación de la política “CCN-STIC-598 Incremental Dominio categoría alta - DL”. |                      | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>                                                                                           |               |        |        |                         |            |  |                                                                                                    |                      |  |                                                            |                      |  |

| Comprobación | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |        | <p>El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Introduzca las credenciales y pulse “Sí” en la ventana de “Control de cuentas de usuario”.</p> <p>Teclee rsop.msc en la consola de comandos que se ha abierto:</p>  <p>A continuación, haga clic derecho sobre “Configuración de equipo” y seleccione “Propiedades” y compruebe que la política “CCN-STIC-598 Incremental Dominio categoría alta - DL” aparece en la lista como muestra la imagen.</p>  |

### 3. COMPROBACIONES EN EL SERVIDOR DE ENTIDAD DE CERTIFICACIÓN

| Comprobación                                                          | OK/NOK | Cómo hacerlo                                                                                                                                      |
|-----------------------------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Inicie sesión en el servidor Entidad de Certificación subordinado. |        | En el servidor Entidad de Certificación subordinada de empresa, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |

| Comprobación                                                                                                                       | OK/NOK | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Verifique la correcta membresía de segregación de roles                                                                         |        | <p>Acceda a la herramienta “Usuarios y equipos de Active Directory” dentro del “Administrador del servidor” y despliegue el nodo “&lt;&lt;su dominio&gt;&gt; → Users”. Ahora, compruebe que los usuarios habilitados para labores de administración de la Entidad Certificadora pertenecen al grupo “Grupo Administración CA”.</p> <p><b>Nota:</b> En este ejemplo se utiliza el nombre “Grupo Administración CA”.</p>                                                                                                                                                                                                                                                                                                                      |
| 3. Verifique la correcta aplicación de la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL”. |        | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:</p>  <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí”.</p>  <p>Teclee “rsop.msc” en la consola de comandos que se ha abierto:</p> |

| Comprobación                                                                                                                                                                   | OK/NOK                  | Cómo hacerlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |             |        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|
|                                                                                                                                                                                |                         | <div></div> <p>Haga clic derecho sobre “Configuración de equipo” en la consola de “Conjunto resultante de directivas” y seleccione “Propiedades”, compruebe que la política “CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL” aparece en la lista como muestra la imagen.</p> <div></div> |             |        |
| 4. Verifique la correcta aplicación de la configuración de servicios del sistema de la política CCN-STIC-598 ENS Incremental Servidores de Certificación Categoría alta - DL”. |                         | <p>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:</p> <div></div> <p>En la consola de “Servicios”, compruebe los siguientes valores.</p>                                                                                                                                                                                                                              |             |        |
| Servicio (Nombre largo)                                                                                                                                                        | Servicio (Nombre corto) | Inicio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Permiso     | OK/NOK |
| Servicios de certificados de Active Directory                                                                                                                                  | CertSvc                 | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Configurado |        |
| Servidor                                                                                                                                                                       | LanmanServer            | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Configurado |        |
| Registro Remoto                                                                                                                                                                | RemoteRegistry          | Automático                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Configurado |        |

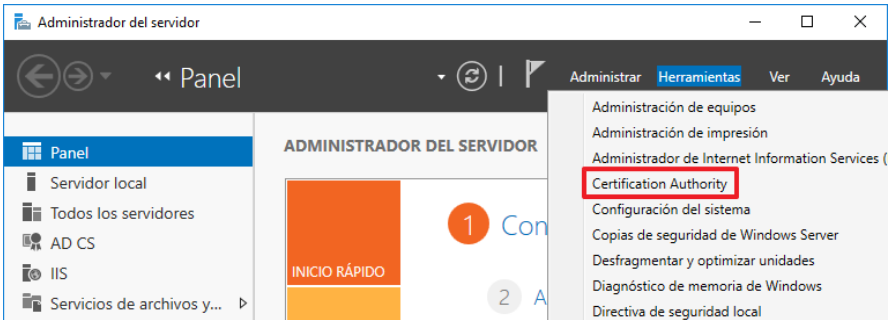
## ANEXO A.5. TAREAS DE ADMINISTRACIÓN DE SERVIDORES DE ENTIDAD DE CERTIFICACIÓN

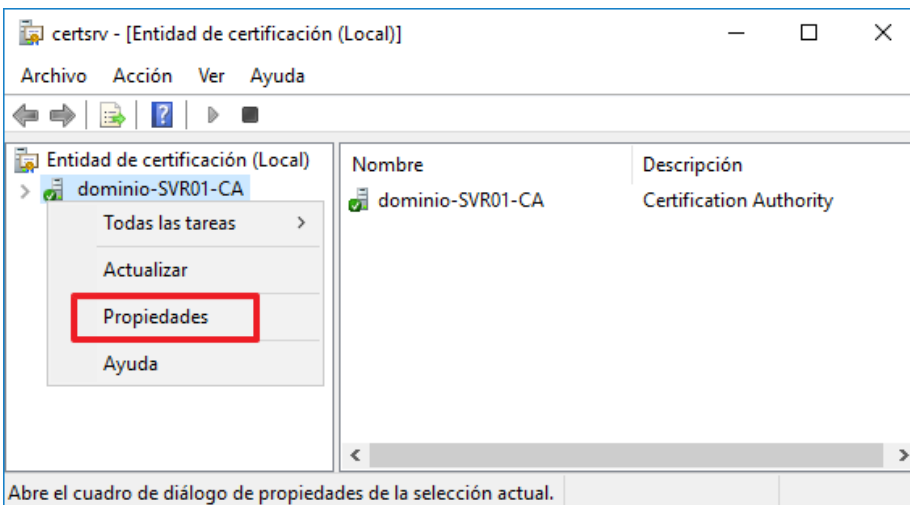
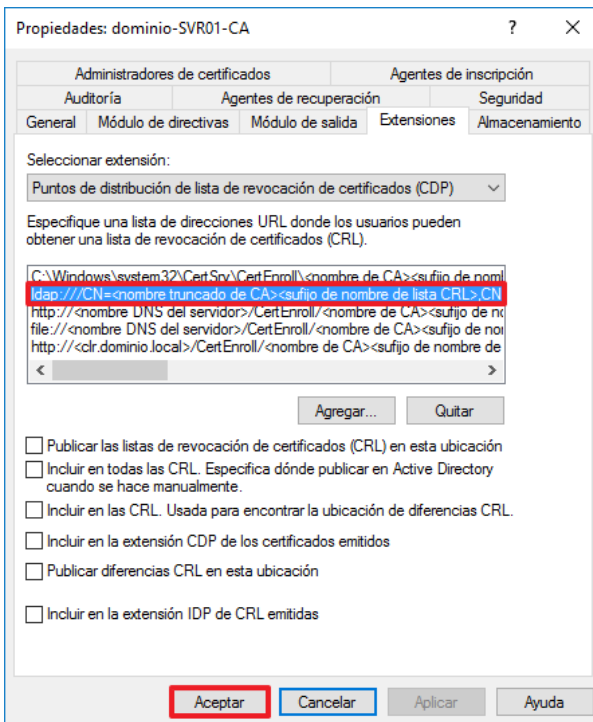
El siguiente anexo describe paso a paso una serie de labores administrativas básicas en el empleo de entidades de certificación y la emisión de certificados solicitados por los equipos clientes de dicha entidad.

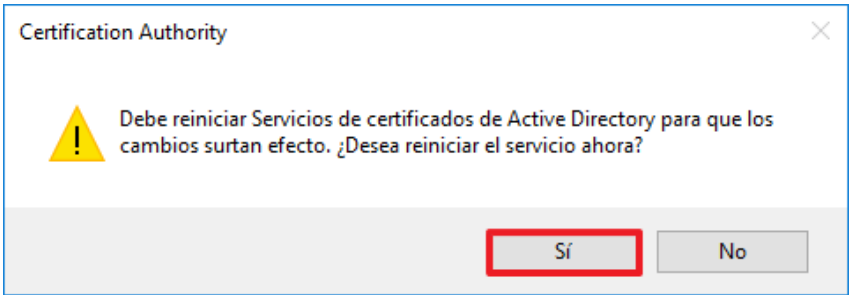
### 1. CONFIGURACIÓN DE PROPIEDADES DE LA ENTIDAD DE CERTIFICACIÓN

En caso de cambiar la política de la empresa con respecto a los puntos de distribución de la lista de revocación de certificados (CRLs), será necesario modificar dichos parámetros en las propiedades de la Entidad de Certificación para, posteriormente, renovar o emitir nuevos certificados actualizados con los nuevos parámetros.

Este apartado indica los pasos a seguir para establecer modificaciones en el servidor Entidad de Certificación, independientemente del tipo de Entidad de Certificación.

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Inicie sesión en el servidor Entidad de Certificación raíz.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                                           |
| 2.   | El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio.                                                                                                                                 |
| 3.   | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | <p>Pulse el botón derecho del ratón sobre la Entidad de Certificación y seleccione “Propiedades”.</p>                                                          |
| 5.   | <p>En la ventana “Propiedades” modifique los parámetros necesarios para alcanzar los objetivos de su entorno y pulse “Aceptar” para guardar los cambios.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                                                                                  |
| 7.   | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                                                                                                     |
| 8.   | Tal y como se ha indicado anteriormente, Una vez modificados los diferentes parámetros de la Entidad de Certificación, para que éstos se reflejen en los certificados ya emitidos, será necesario renovar dichos certificados o emitir nuevos certificados. |

## 2. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN

Los certificados emitidos a través de una Entidad de Certificación tienen un período de validez determinado que, una vez superado, impide que se siga haciendo uso de dichos certificados. Por tanto, cada vez que se supere el espacio de tiempo en el cual los certificados están en vigor, será necesario realizar una renovación del certificado expirado que pertenece a dicha Entidad de Certificación.

Así mismo, existe la posibilidad de que se requiera la renovación del certificado raíz de la Entidad debido a un cambio en las políticas de comportamiento o para evitar su uso por haber sido comprometido de algún modo. Este hecho provocaría la necesidad de cambio del certificado de la Entidad de Certificación tras revocar el que se emitió con anterioridad. Esto es debido a que dicho certificado anterior continúa en vigor y el hecho de que no cumpla con los requisitos o políticas estipulados necesita que este certificado pase a un estado de inutilizable o revocado.

Existen una serie de elementos predeterminados a tener en cuenta según el tipo de certificado que se desea renovar:

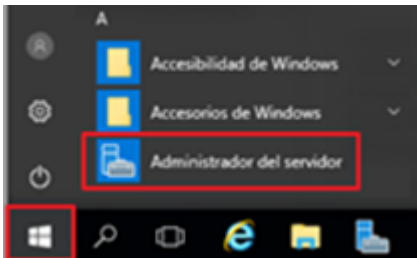
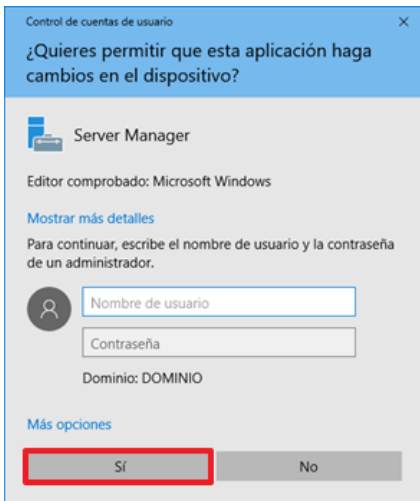
- Para un certificado correspondiente a una Entidad de Certificación raíz, el período de validez se especifica durante la instalación de los Servicios de certificados de Directorio Activo.
- Para un certificado correspondiente a una Entidad de Certificación raíz, el período de validez podrá ser de hasta 5 años y nunca deberá sobrepasar el período de validez de la Entidad de Certificación raíz de la que depende.
- El resto de los certificados tendrán una duración de un máximo de dos años y nunca deberán sobrepasar el período de validez de la Entidad de Certificación que entrega dichos certificados.

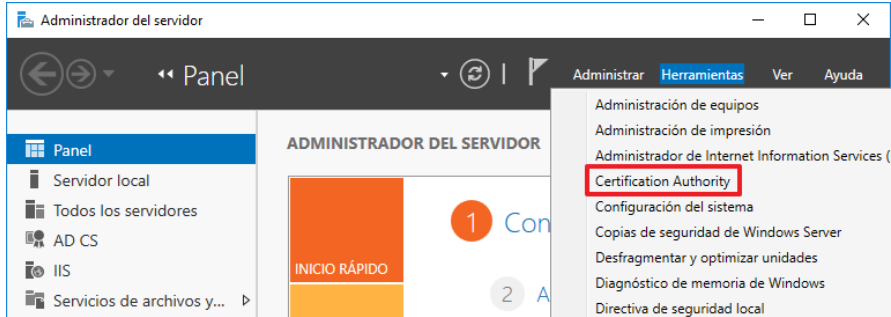
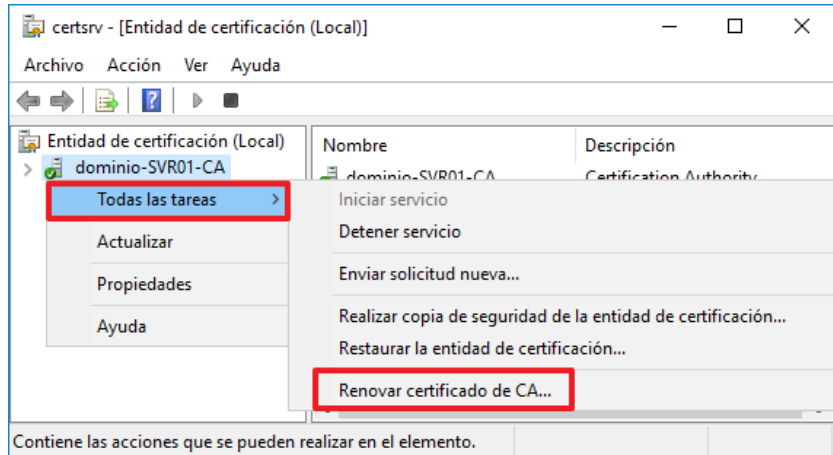
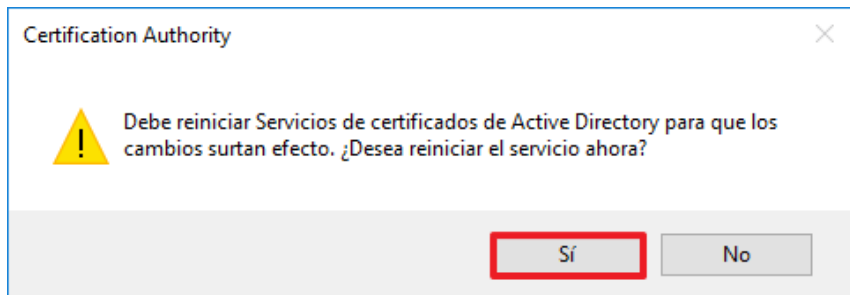
A la hora de realizar la renovación del certificado, el sistema solicitará si se quieren crear nuevas claves pública y privada para el certificado. Si bien es cierto que, con un nivel de cifrado suficiente es difícil que se pueda llegar a romper las claves, es más seguro regenerar las claves porque este procedimiento le otorga al atacante menos tiempo para romper la seguridad, aunque el coste administrativo se ve aumentado.

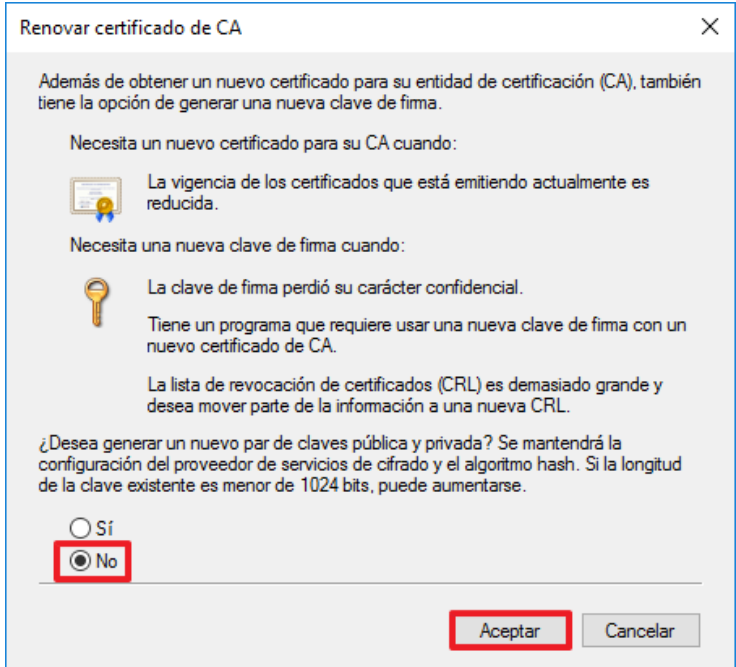
El algoritmo de cifrado con el que se están emitiendo los certificados es muy seguro, esto hace que el conjunto de claves sea prácticamente irrompible, en el entorno que ocupa a esta guía no se volverán a emitir claves privadas y públicas nuevas para evitar tener que emitir de nuevo todos los certificados que comparten confianza con la entidad.

## 2.1. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ

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                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.   | <p>Inicie sesión en el equipo Entidad de Certificación raíz con credenciales de administrador.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                 |
| 10.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>      |
| 11.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio. Introduzca las credenciales y pulse “Sí”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>   |
| 13.  | <p>Sobre el nombre de la Entidad de Certificación, con el botón derecho del ratón seleccione “Todas las tareas → Renovar certificado de CA...”.</p>  |
| 14.  | <p>Pulse “Sí” en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                   |

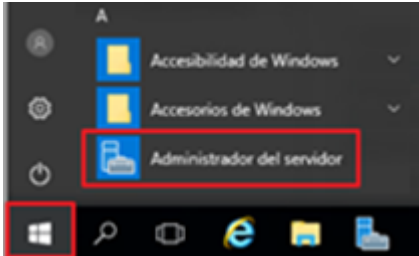
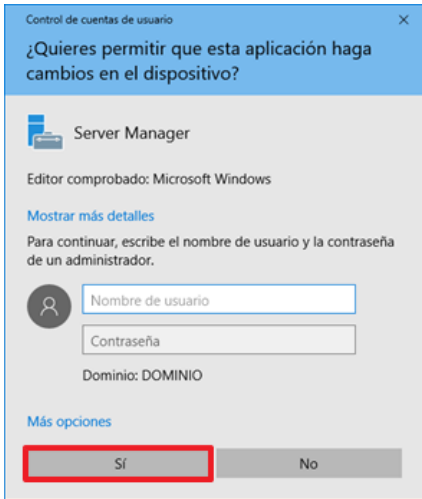
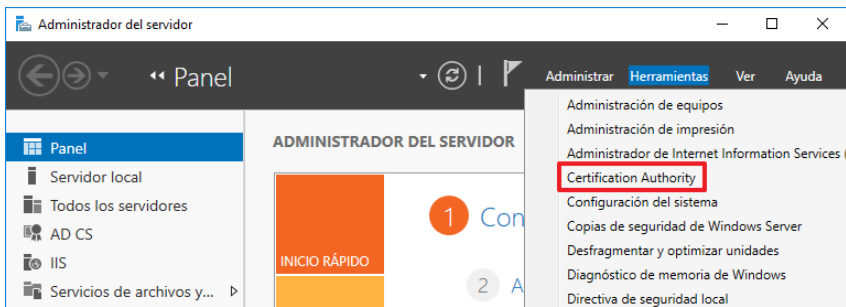
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.  | <p>En la ventana “Renovar certificado de CA” seleccione “No” ante la pregunta de generar nuevas claves y pulse “Aceptar”.</p>  <p><b>Nota:</b> Este proceso comienza en segundo plano y puede tardar unos minutos. No debe cerrar la ventana hasta que finalice el proceso.</p> |

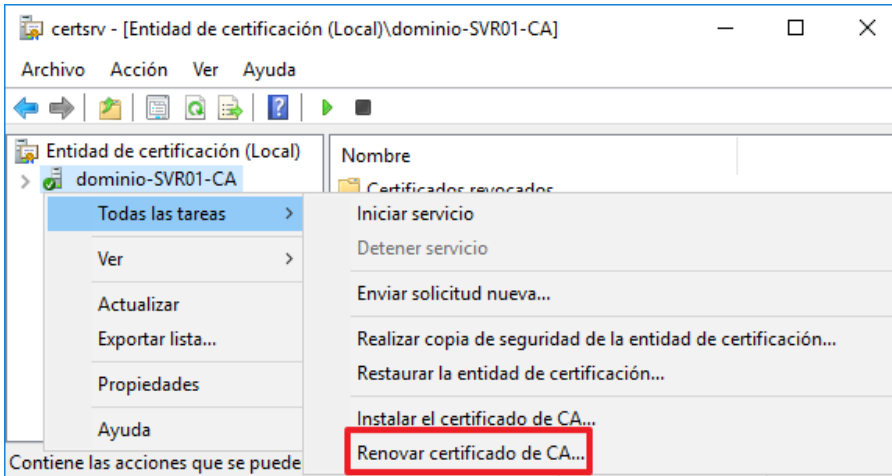
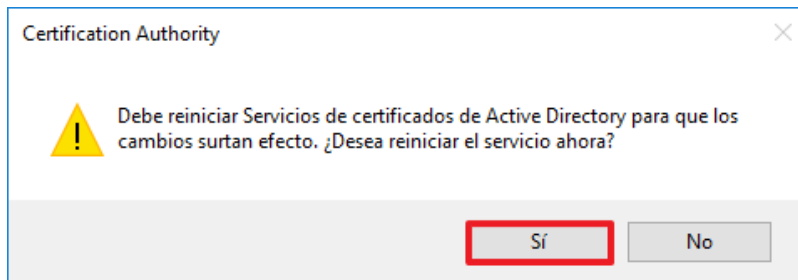
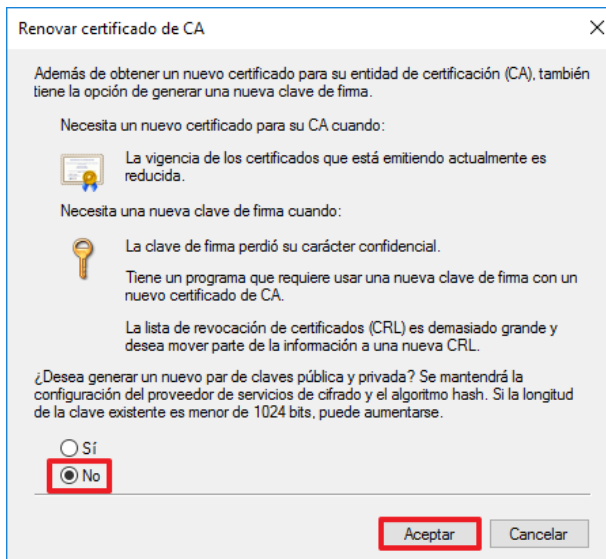
## 2.2. RENOVACIÓN DEL CERTIFICADO RAÍZ DE UNA ENTIDAD DE CERTIFICACIÓN SUBORDINADA

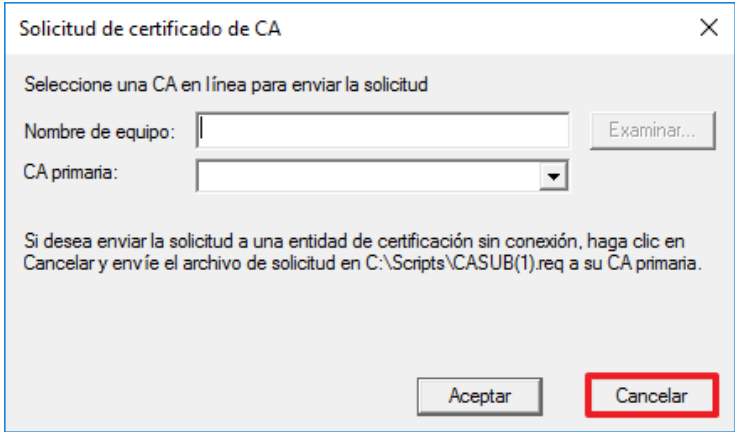
El proceso de renovación de una Entidad de Certificación subordinada, en el escenario contemplado en esta guía, deberá solicitar la firma a la entidad raíz independiente del dominio.

Los pasos que se definen a continuación comprenden el método para renovar el certificado y posteriormente solicitar la firma a través de la entidad raíz.

| Paso | Descripción                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.  | <p>Inicie sesión en el equipo Entidad de Certificación subordinada con credenciales de administrador.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p> |

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 18.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio y pulse “Sí”.</p>                          |
| 19.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.  | <p>Sobre el nombre de la Entidad de Certificación, con el botón derecho del ratón seleccione <b>“Todas las tareas → Renovar el certificado de CA...”</b>.</p>                                                                                                                                          |
| 21.  | <p>Pulse <b>“Sí”</b> en la ventana que solicita confirmación de parada de servicios de certificados.</p>                                                                                                                                                                                              |
| 22.  | <p>En la ventana <b>“Renovar certificado de CA”</b> seleccione <b>“No”</b> ante la pregunta de generar nuevas claves y pulse <b>“Aceptar”</b>.</p>  <p><b>Nota:</b> Este proceso comienza en segundo plano y puede tardar unos minutos. No debe cerrar la ventana hasta que finalice el proceso.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23.  | <p>En la ventana “Solicitud de certificado de CA”, pulse “Cancelar”, ya que la entidad raíz no es accesible.</p>  <p><b>Nota:</b> La nueva solicitud de certificado se alojará en la ruta indicada en el mensaje que figura en la zona inferior de la ventana “Solicitud de certificado de CA”; en el ejemplo, “C:\Scripts”.</p> |
| 24.  | Extraiga el fichero de solicitud (en el ejemplo, “CASUB(1).req”) para utilizarlo en el servidor independiente de la Entidad de Certificación raíz.                                                                                                                                                                                                                                                                 |

### 3. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS

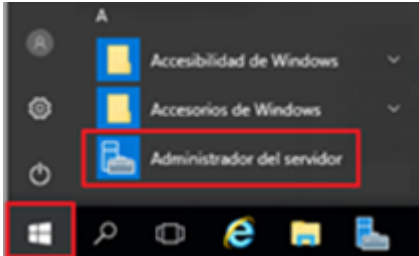
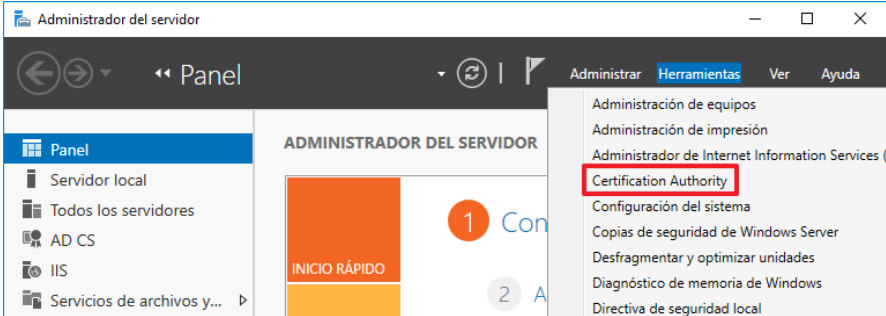
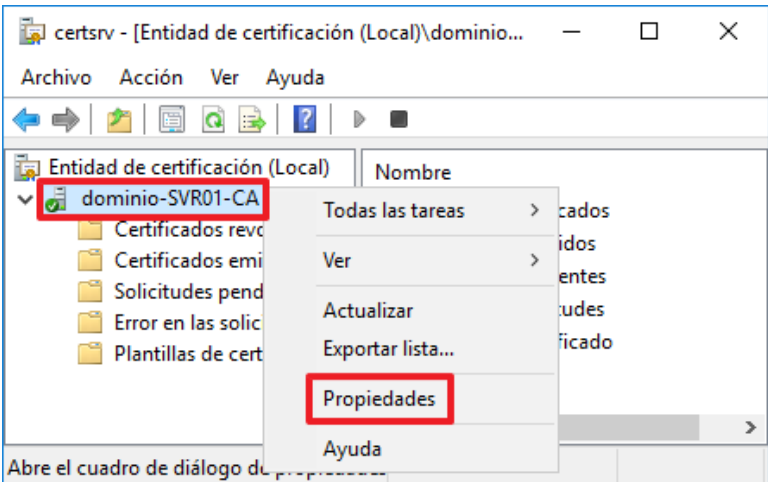
Una lista de revocación es un archivo que mantiene almacenada la lista de los certificados que han sido revocados y que, por tanto, ya no están disponibles para hacer uso de ellos.

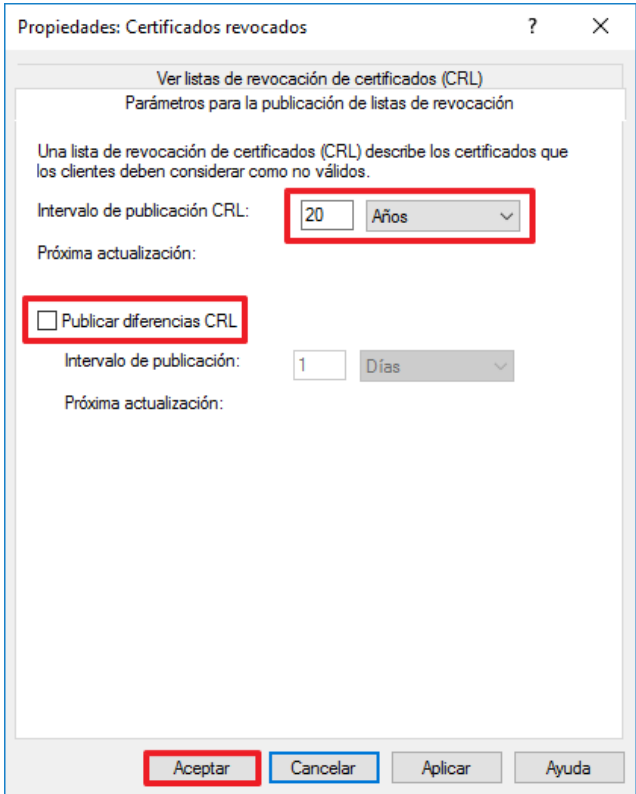
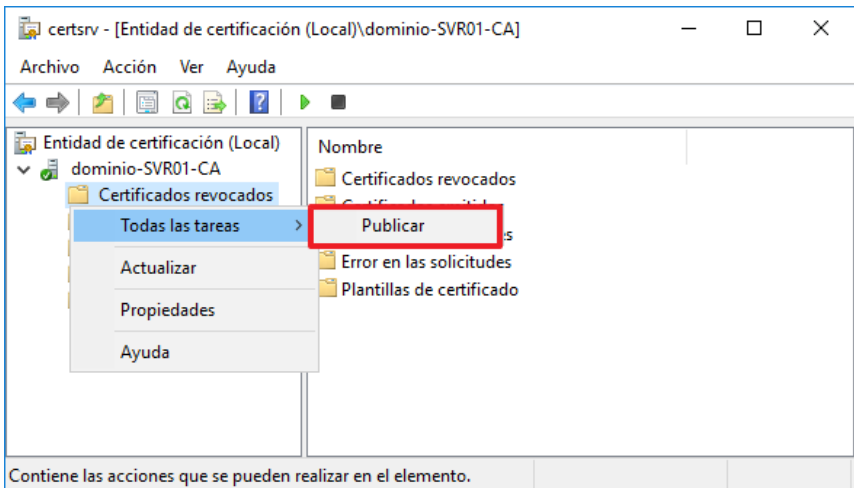
El siguiente apartado enumera los pasos necesarios para generar listas de revocación de certificados (CRLs) y publicarlas tanto en el caso de entornos con Entidad de Certificación raíz de empresa como en entornos de servidor independiente Entidad de Certificación raíz y Entidad de Certificación subordinada de empresa.

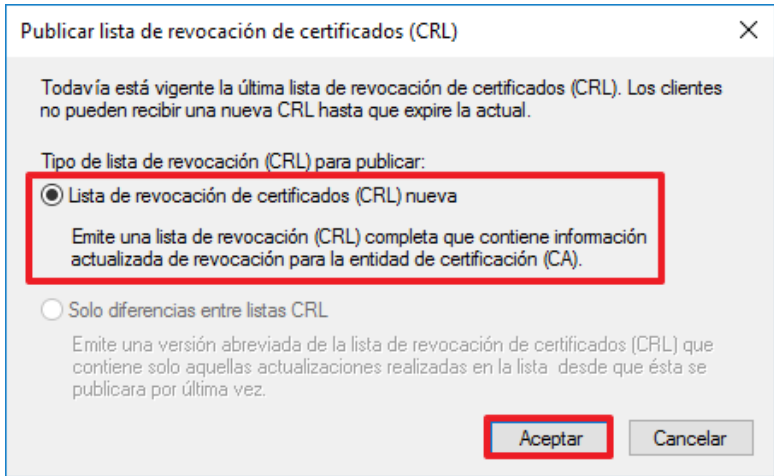
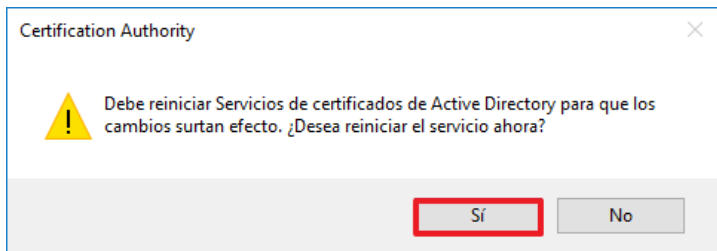
#### 3.1. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (CRL) MEDIANTE UNA ENTIDAD DE CERTIFICACIÓN RAÍZ DE EMPRESA

Las siguientes configuraciones se realizarán en el servidor de la Entidad de Certificación raíz de empresa.

| Paso | Descripción                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25.  | <p>Inicie sesión en el servidor Entidad de Certificación raíz de empresa.</p> <p><b>Nota:</b> Debe iniciar sesión con una cuenta que sea Administrador del Dominio.</p> |

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 27.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del dominio y pulse “Sí”.</p>                                                                                                             |
| 28.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>   |
| 29.  | <p>Para configurar las CRLs, pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>           |

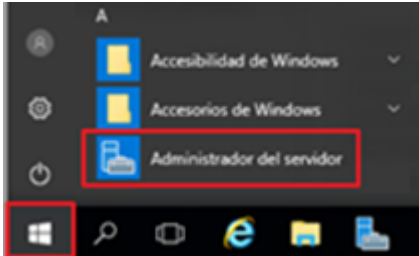
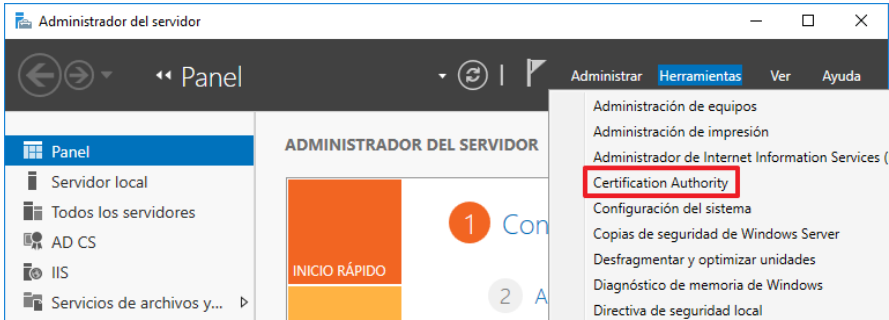
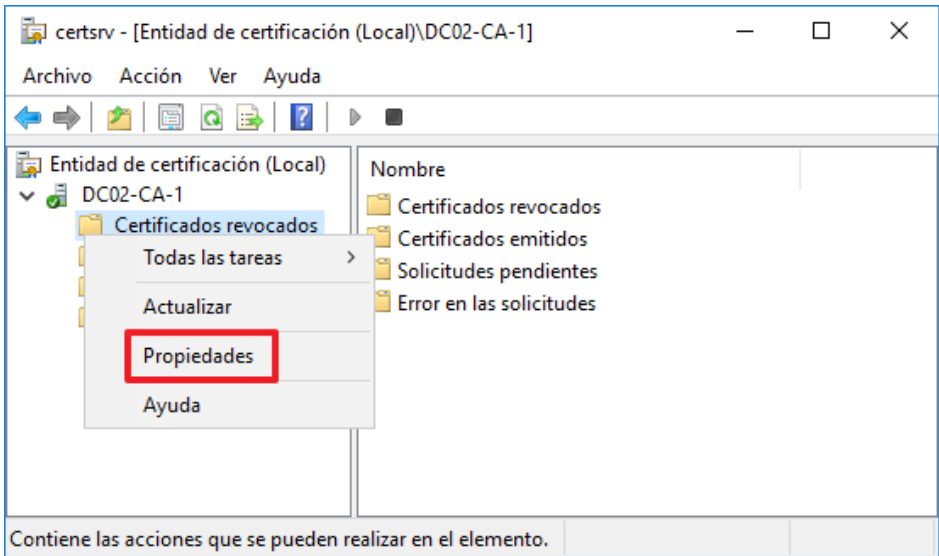
| Paso | Descripción                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30.  | <p>Modifique el “Intervalo de publicación CRL” y deshabilite la publicación de diferencias CRL. Es posible también la consulta de las listas de revocación mediante la pestaña “Ver listas de revocación de certificados (CRL)”. Pulse “Aceptar”.</p>  |
| 31.  | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                                           |

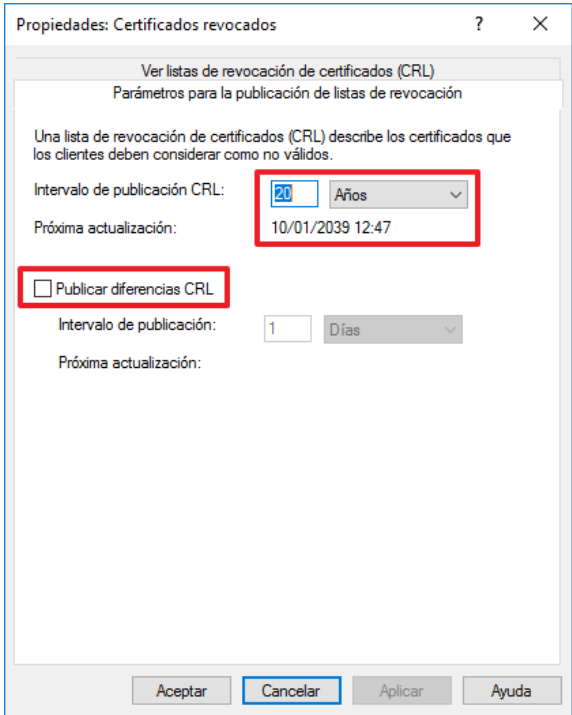
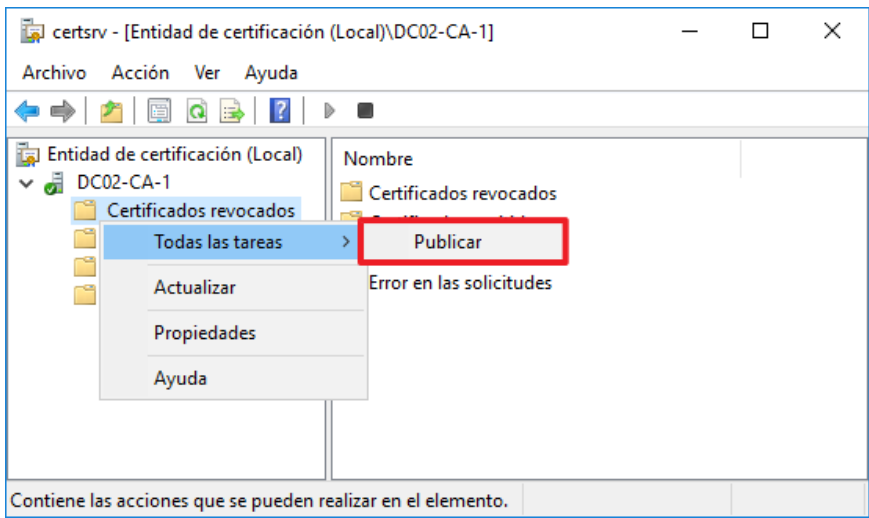
| Paso | Descripción                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 32.  | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>  |
| 33.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                    |
| 34.  | Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.                                                                                                        |

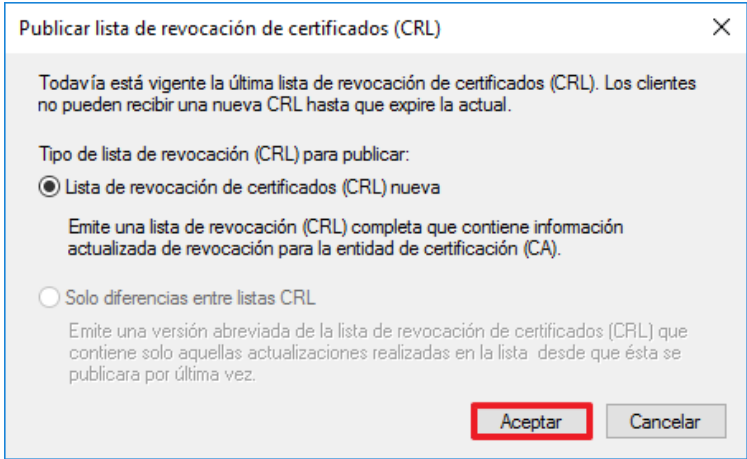
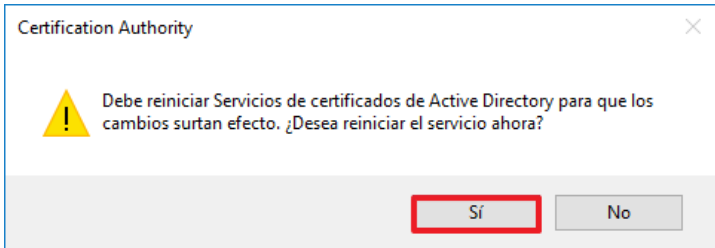
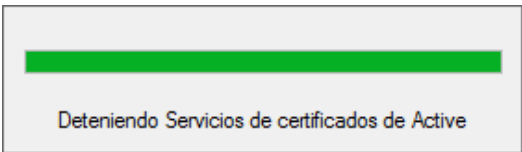
### 3.2. GENERACIÓN Y PUBLICACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (CRL) MEDIANTE UNA ENTIDAD DE CERTIFICACIÓN SUBORDINADA A UNA ENTIDAD DE CERTIFICACIÓN RAÍZ INDEPENDIENTE

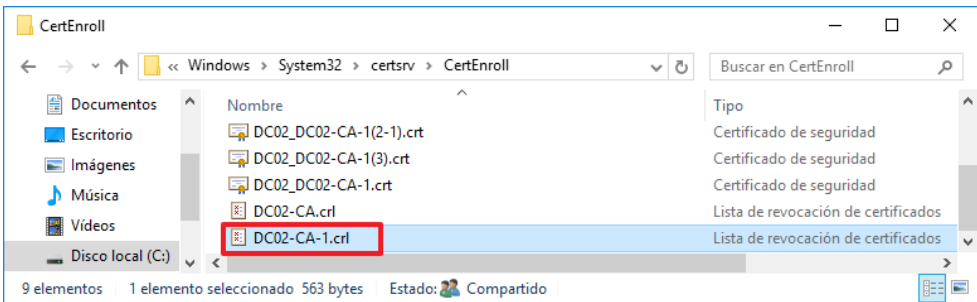
Las siguientes configuraciones se realizarán a través de una certificación raíz independiente.

| Paso | Descripción                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 35.  | <p>Inicie sesión en el equipo Entidad de Certificación raíz independiente.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p> |

| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 36.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 37.  | <p>El control de cuentas de usuario le solicitará las credenciales de un usuario administrador del equipo.</p>                                                                                                                           |
| 38.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>   |
| 39.  | <p>Para configurar las CRLs, pulse el botón derecho del ratón sobre el contenedor “Certificados Revocados” y seleccione “Propiedades”.</p>           |

| Paso | Descripción                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 40.  | <p>Modifique el “Intervalo de publicación CRL” y deshabilite la publicación de diferencias CRL. Es posible también la consulta de las listas de revocación mediante la pestaña “Ver listas de revocación de certificados (CRL)”.</p>  |
| 41.  | <p>En los “Servicios de certificados de Active Directory”, haga clic derecho de nuevo sobre “Certificados revocados” y seleccione <b>“Todas las tareas → Publicar”</b>.</p>                                                          |

| Paso | Descripción                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 42.  | <p>Mantenga seleccionada la opción “Lista de revocación de certificados (CRL) nueva” y pulse “Aceptar”.</p>  |
| 43.  | <p>El sistema reiniciará los “Servicios de certificados”. Pulse “Sí” para continuar.</p>                    |
| 44.  | <p>Tras unos segundos, se reiniciarán los “Servicios de certificados”.</p>                                 |
| 45.  | <p>Pulse “Aceptar” para cerrar la ventana de “Propiedades” de la Entidad de Certificación.</p>                                                                                                 |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46.  | <p>A continuación, copie el fichero con extensión “.crl” que se ha generado en la ruta “%SYSTEMROOT%\System32\CertSrv\CertEnroll” a un dispositivo externo para posteriormente copiarlo en el servidor Entidad de Certificación subordinada de empresa.</p>  <p><b>Nota:</b> Para realizar copias de una máquina a otra y teniendo en cuenta que no son accesibles entre ellas, se deberá utilizar un dispositivo externo tipo disco duro o pendrive USB tanto si se trata de una máquina física como de una máquina virtual con acceso a dispositivos externos de almacenamiento tipo USB. En el caso de Hyper-V se podrán emplear dispositivos virtuales de almacenamiento.</p> |

#### 4. GENERACIÓN DE PLANTILLAS DE CERTIFICADO

Del mismo modo que existen numerosos tipos de certificados, existen numerosos tipos de plantillas de certificado. El servicio de Entidad de Certificación del directorio activo incluye una serie de plantillas predefinidas, que suelen ser las solicitadas más habitualmente como podrían ser las plantillas de autenticación de cliente (para autenticación de sesión, correo, etc.), plantillas de autenticación de un equipo o servidor o plantillas para autenticar un sitio web...

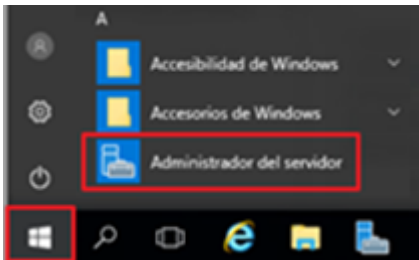
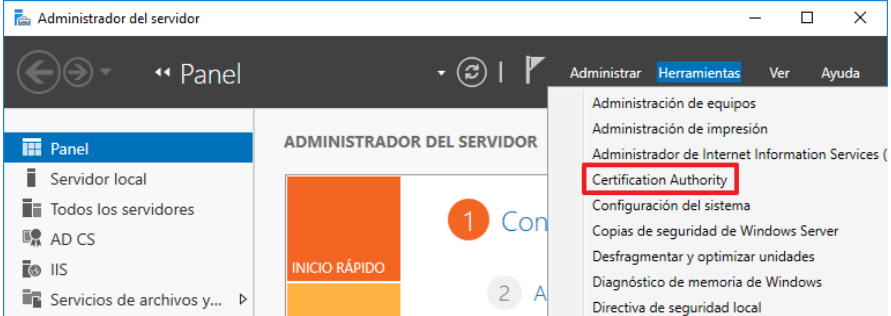
Estas plantillas pregeneradas se pueden utilizar para la emisión de certificados sin realizar sobre ellas ningún tipo de modificación, siempre y cuando el propósito coincida con los parámetros del certificado. Así mismo, estas plantillas se utilizarán como base para crear una plantilla de certificado personalizada mediante la cual se pueden establecer de forma manual parámetros y características que se adecuen totalmente a la necesidad o propósito del certificado a solicitar.

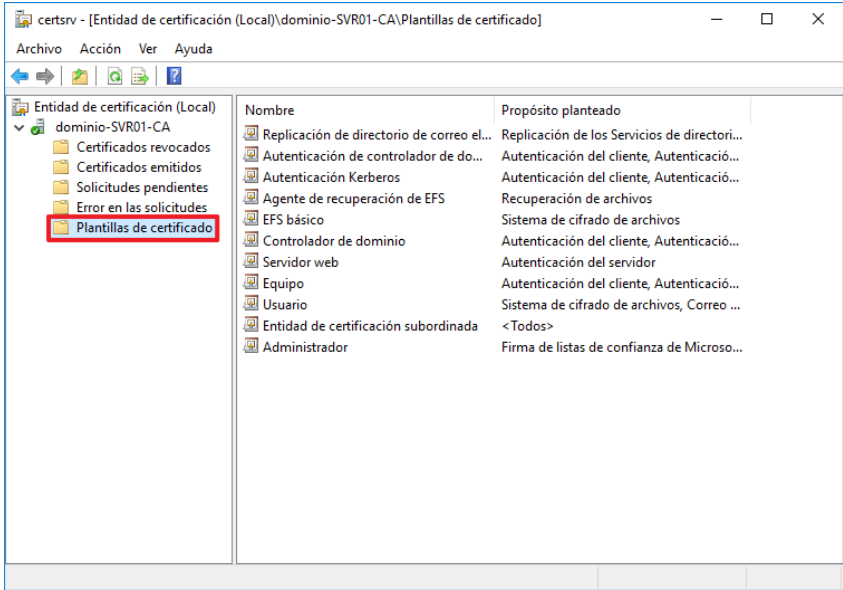
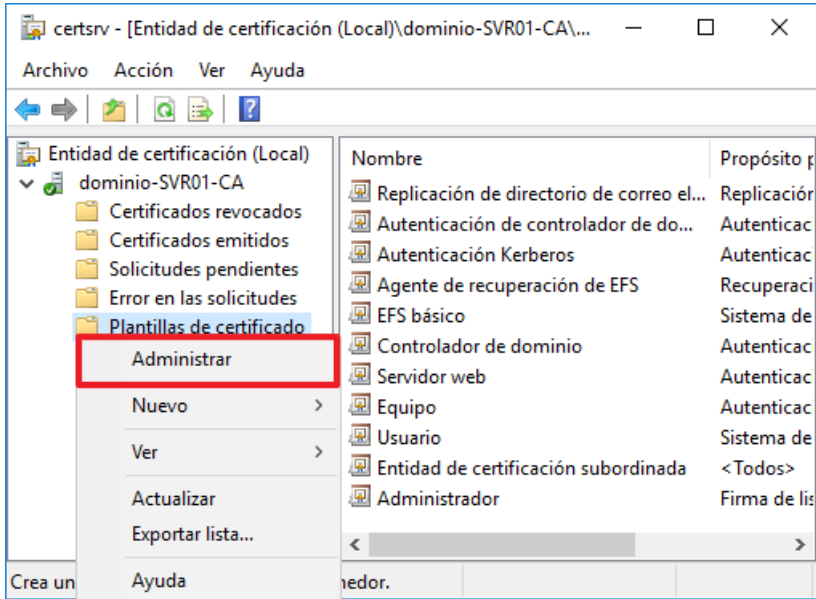
Esta sección define los pasos a seguir para generar plantillas a través de una plantilla base y se realizarán a través de una Entidad de Certificación raíz de empresa o de una Entidad de Certificación subordinada de empresa que permita que sean accesibles para los clientes que vayan a realizar la solicitud.

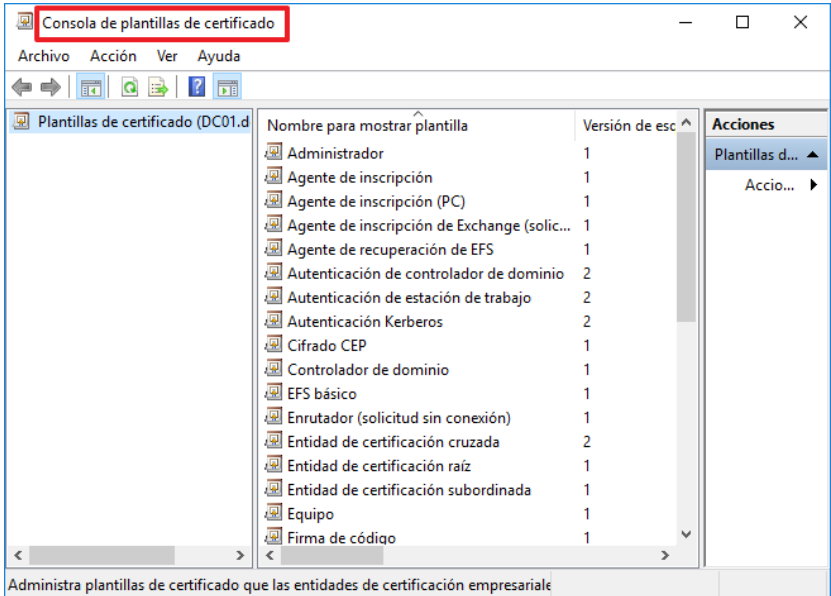
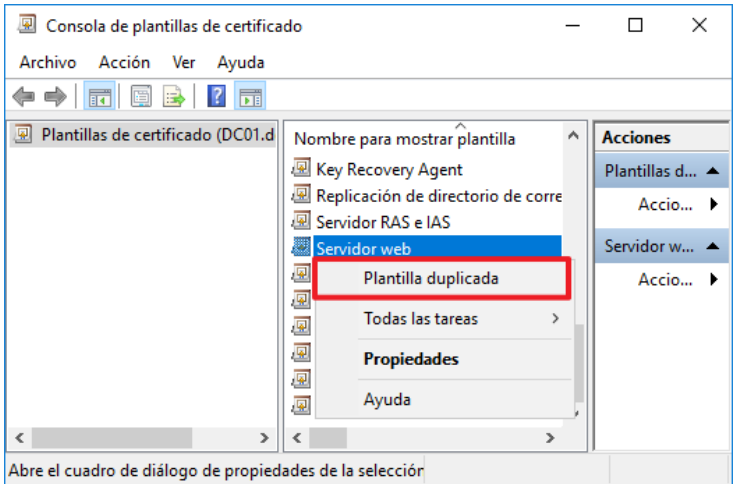
Cabe mencionar, que una Entidad de Certificación Independiente no posee la característica de plantillas de certificado.

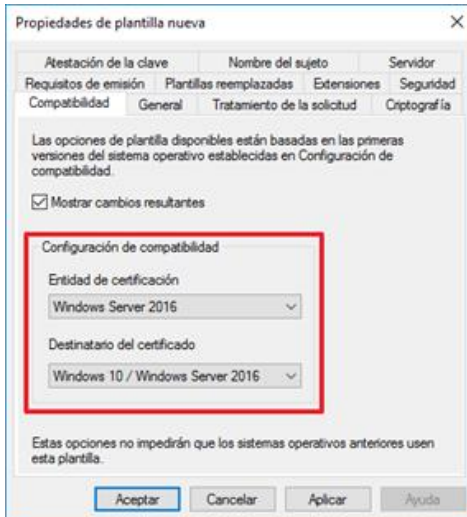
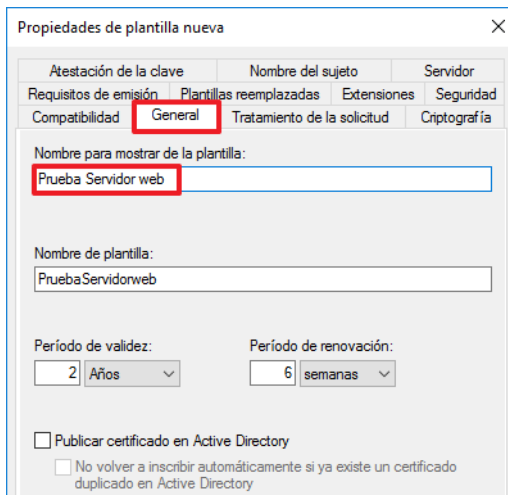
## 4.1. CREACIÓN DE PLANTILLAS DE CERTIFICADO

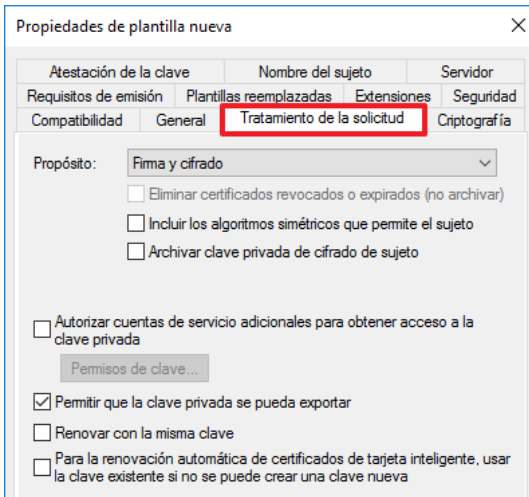
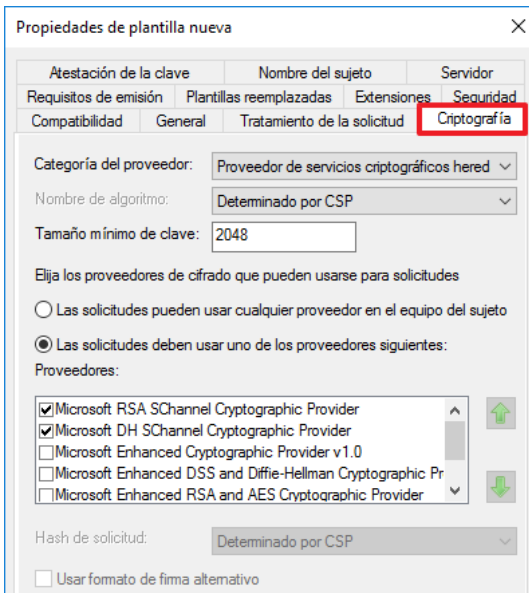
Este apartado define los pasos para crear una plantilla de certificado a partir de una plantilla base.

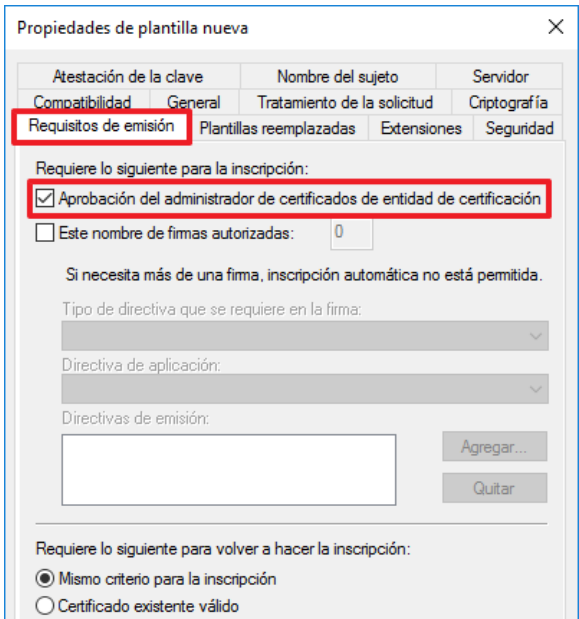
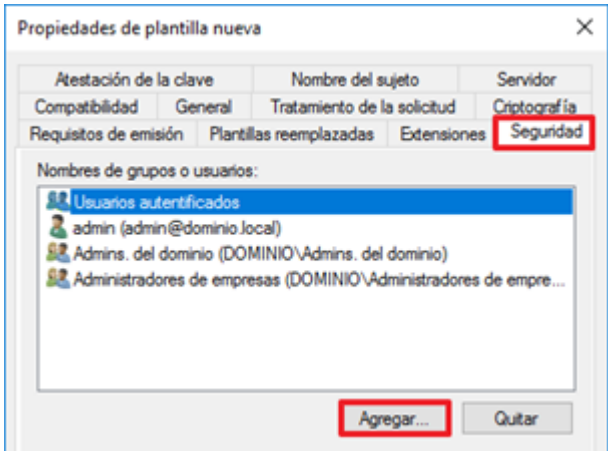
| Paso | Descripción                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 47.  | <p>Inicie sesión en el servidor Entidad de Certificación raíz o subordinada de empresa que no sea independiente.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                         |
| 48.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 49.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                             |
| 50.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>  |

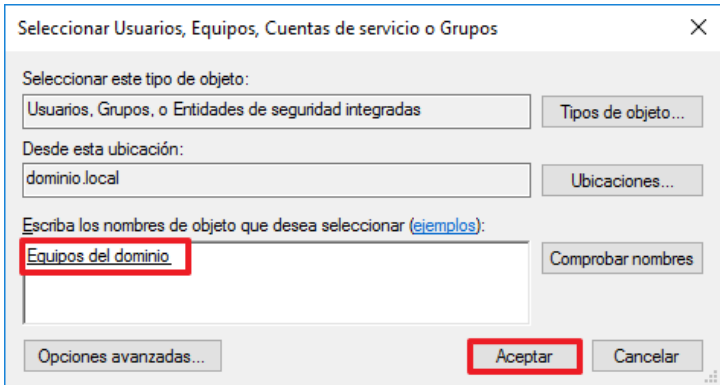
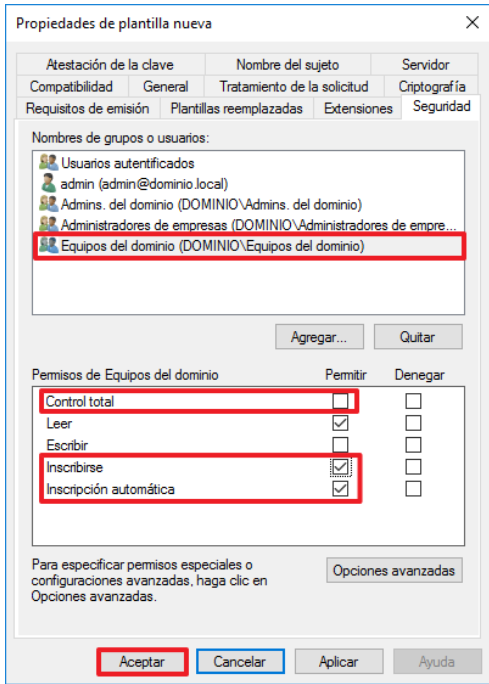
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 51.  | <p>Sitúese sobre el contenedor de “Plantillas de certificado”.</p>  <p><b>Nota:</b> La lista de plantillas que aparece en el menú derecho contiene las plantillas de certificado que están disponibles para su solicitud. Existe un repositorio con más tipos de plantillas de certificados que se pueden parametrizar para posteriormente publicar. Solamente las plantillas que aparecen en esta lista estarán accesibles para que los clientes realicen la solicitud del certificado.</p> |
| 52.  | <p>Sitúese sobre el contenedor “Plantillas de certificado”, pulse el botón derecho del ratón sobre él y seleccione “Administrar” para acceder al resto de plantillas de certificado.</p>                                                                                                                                                                                                                                                                                                   |

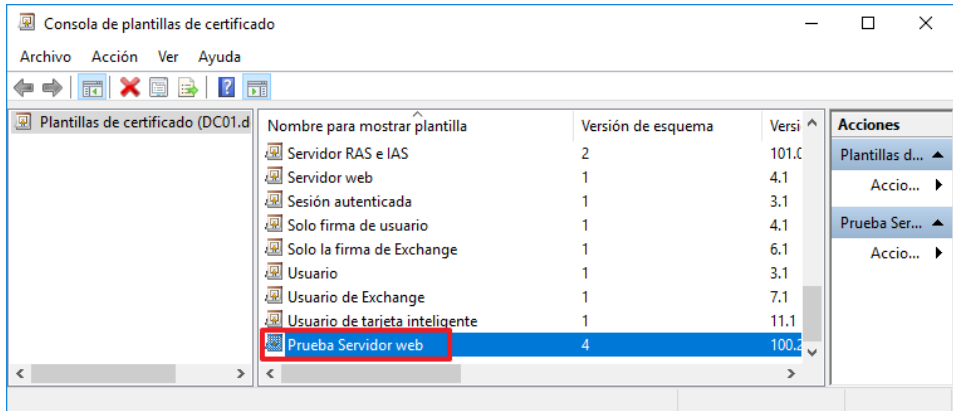
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 53.  | <p>A continuación, se abrirá la “Consola de plantillas de certificado” que mostrará la lista completa de plantillas que se podrán usar como base para la creación de la plantilla de certificados personalizada.</p>  <p><b>Nota:</b> En caso de no necesitar la personalización de la plantilla, y si solamente requiere que una plantilla de esta lista aparezca en el contenedor de plantillas de certificado para que sea accesible a solicitudes, consulte el apartado 4.2.PUBLICACIÓN DE UNA PLANTILLA DE CERTIFICADOS EN LA ENTIDAD DE CERTIFICACIÓN</p> |
| 54.  | <p>Una plantilla base no debe ser modificada debido a que se perdería la parametrización por defecto de dicha plantilla. Por tanto, se duplicará una plantilla para personalizar tanto sus parámetros como el nombre de la plantilla. Para ello, en la “Consola de plantillas de certificado” seleccione una plantilla y pulsando el botón derecho del ratón sobre ella seleccione “Plantilla Duplicada”.</p>  <p><b>Nota:</b> En el ejemplo se realizará un duplicado de la plantilla “Servidor web”.</p>                                                     |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 55.  | <p>Es posible establecer la configuración de compatibilidad separándolo por Entidad de Certificación y destinatario de certificado.</p>  <p><b>Nota:</b> La configuración de compatibilidad se configurará en base al entorno en el que esté basado la entidad certificadora.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 56.  | <p>Se abrirá la ventana de “Propiedades de plantilla nueva” donde se podrá definir los diferentes parámetros para adecuar la plantilla al tipo de certificado necesario. En la pestaña “General” se puede establecer un nombre para la plantilla, así como definir el período de validez o la posibilidad de publicar el certificado en el directorio activo.</p>  <p><b>Nota:</b> En el ejemplo se mantienen los períodos y se cambia el nombre a “Prueba Servidor Web”. Nótese que a menos que se modifique, el campo “Nombre de plantilla” omite los espacios. Este hecho se deberá tener en cuenta en caso de utilizar herramientas de comandos como “certutil.exe”, ya que, si se invoca la plantilla con el “Nombre para mostrar de la plantilla”, dará error. El período de validez máximo que se puede establecer en una plantilla de certificado es de dos años. Sin embargo, si se modifica la entrada de registro tal como se ha hecho en el apartado anterior, sería posible establecer un periodo mayor, hasta alcanzar el número definido en dicha entrada.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57.  | <p>En la pestaña “Tratamiento de la solicitud” se puede especificar el propósito del certificado, tanto si servirá para firmar un sitio web como para cifrar contenidos. Del mismo modo se puede definir el comportamiento de cara al cifrado y permitir la exportación de la clave privada (la exportación de la clave privada es necesaria cuando se usa el certificado en un servicio que no puede comunicarse con el directorio activo).</p>  <p><b>Nota:</b> En el ejemplo se marcará la opción de “Permitir que la clave privada se pueda exportar”.</p> |
| 58.  | <p>En la pestaña de “Criptografía” se podrá definir el algoritmo, tamaño de clave, proveedor de cifrado y hash de la solicitud.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 59.  | <p>En la pestaña “Requisitos de emisión”, es posible definir si el administrador de la Entidad de Certificación debe aprobar la publicación del certificado solicitado mediante la opción “Aprobación del administrador de certificados de Entidad de Certificación”. Seleccionando esta opción, ningún solicitante recibirá el certificado, a menos que el administrador gestione la emisión, independientemente de los permisos de inscripción o inscripción automática que tenga el solicitante.</p>  <p><b>Nota:</b> En el ejemplo, se marcará esta opción.</p> |
| 60.  | <p>En la pestaña “Seguridad”, se puede definir qué usuarios tendrán permiso para operar sobre los certificados, en caso de que se quisiera que el equipo de ejemplo, fuera capaz de recibir el certificado tras su solicitud y que esta recepción se recibiera de forma automática (sin que el administrador tuviera la obligación de administrar la entrega), se debe añadir el grupo “Equipos del dominio” y darle los permisos que le permitan las opciones “Inscribirse” e “Inscripción automática”. Para ello, pulse el botón “Agregar”.</p>                  |

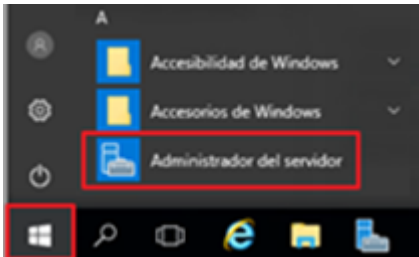
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 61.  | <p>Escriba “Equipos del dominio” en el campo de texto y pulse “Aceptar”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 62.  | <p>Sitúese sobre el grupo añadido recientemente “Equipos del dominio” y marque las dos opciones “Inscribirse” e “Inscripción automática”. Pulse “Aceptar” para cerrar la ventana de “Propiedades”.</p>  <p><b>Nota:</b> En el ejemplo se marcan las opciones “Inscribirse” e “Inscripción automática” para el grupo de directorio activo “Equipos del dominio”. En este caso particular, al haber marcado en el paso 13 la opción “Aprobación del administrador de certificados de Entidad de Certificación”, aunque, por permisos, los equipos del dominio deben poder recibir el certificado de forma automática, requerirán por parte del administrador la entrega del certificado tras la solicitud.</p> |

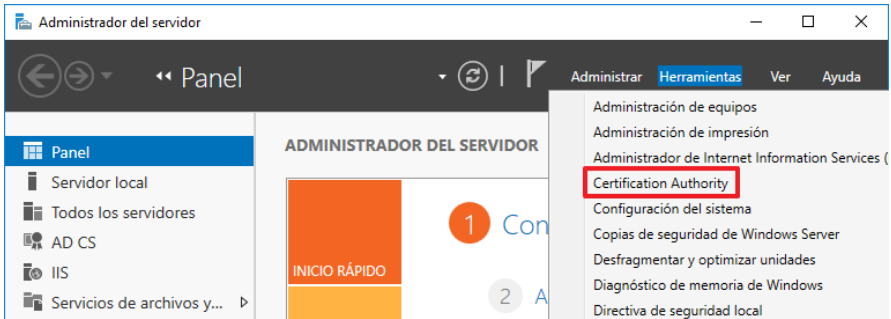
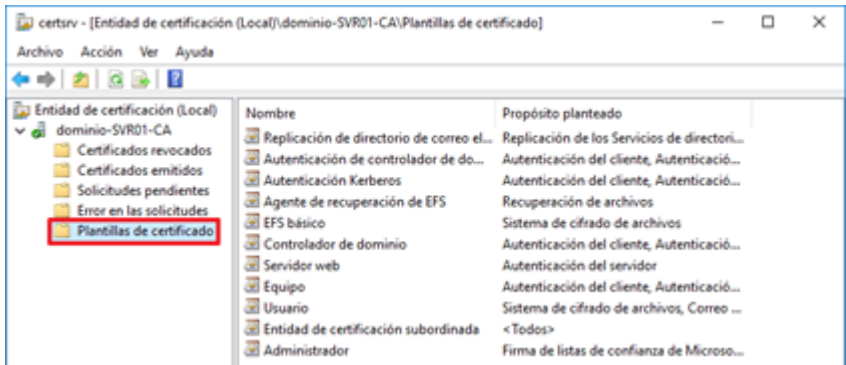
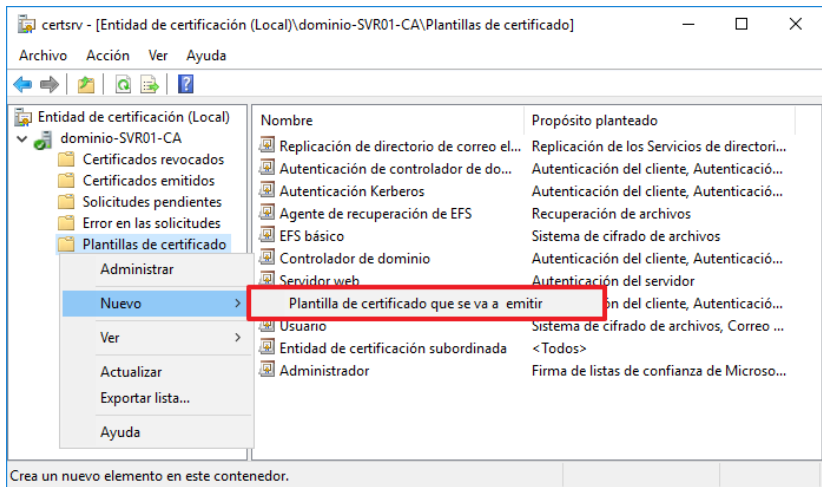
| Paso                           | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------|-------|--------------------|---|-------|--------------|---|-----|--------------------|---|-----|-----------------------|---|-----|---------------------------|---|-----|---------|---|-----|---------------------|---|-----|--------------------------------|---|------|---------------------|---|-------|
| 63.                            | <p>Compruebe que la nueva plantilla aparece en la “Consola de plantillas de certificado”.</p>  <table><thead><tr><th>Nombre para mostrar plantilla</th><th>Versión de esquema</th><th>Versi</th></tr></thead><tbody><tr><td>Servidor RAS e IAS</td><td>2</td><td>101.0</td></tr><tr><td>Servidor web</td><td>1</td><td>4.1</td></tr><tr><td>Sesión autenticada</td><td>1</td><td>3.1</td></tr><tr><td>Solo firma de usuario</td><td>1</td><td>4.1</td></tr><tr><td>Solo la firma de Exchange</td><td>1</td><td>6.1</td></tr><tr><td>Usuario</td><td>1</td><td>3.1</td></tr><tr><td>Usuario de Exchange</td><td>1</td><td>7.1</td></tr><tr><td>Usuario de tarjeta inteligente</td><td>1</td><td>11.1</td></tr><tr><td>Prueba Servidor web</td><td>4</td><td>100.0</td></tr></tbody></table> | Nombre para mostrar plantilla | Versión de esquema | Versi | Servidor RAS e IAS | 2 | 101.0 | Servidor web | 1 | 4.1 | Sesión autenticada | 1 | 3.1 | Solo firma de usuario | 1 | 4.1 | Solo la firma de Exchange | 1 | 6.1 | Usuario | 1 | 3.1 | Usuario de Exchange | 1 | 7.1 | Usuario de tarjeta inteligente | 1 | 11.1 | Prueba Servidor web | 4 | 100.0 |
| Nombre para mostrar plantilla  | Versión de esquema                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Versi                         |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Servidor RAS e IAS             | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 101.0                         |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Servidor web                   | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 4.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Sesión autenticada             | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 3.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Solo firma de usuario          | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 4.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Solo la firma de Exchange      | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 6.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Usuario                        | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 3.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Usuario de Exchange            | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 7.1                           |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Usuario de tarjeta inteligente | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 11.1                          |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |
| Prueba Servidor web            | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 100.0                         |                    |       |                    |   |       |              |   |     |                    |   |     |                       |   |     |                           |   |     |         |   |     |                     |   |     |                                |   |      |                     |   |       |

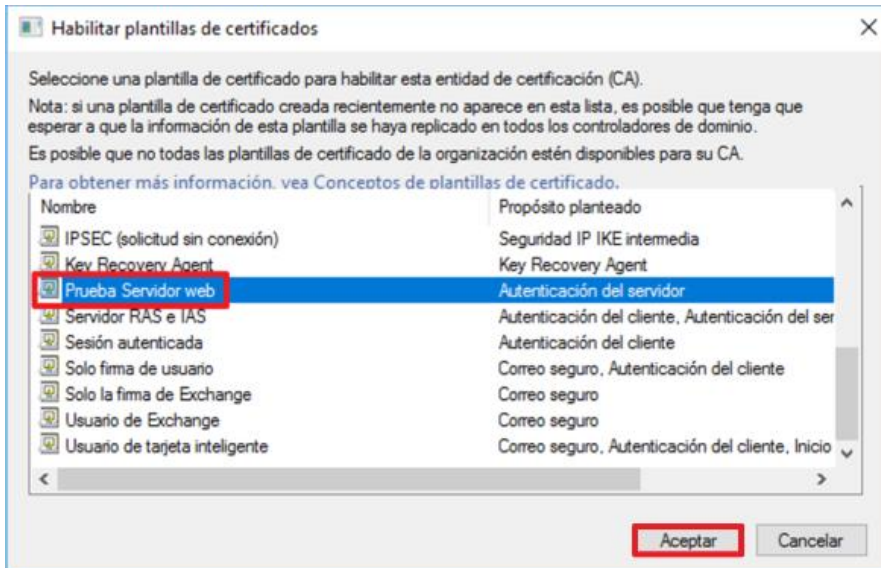
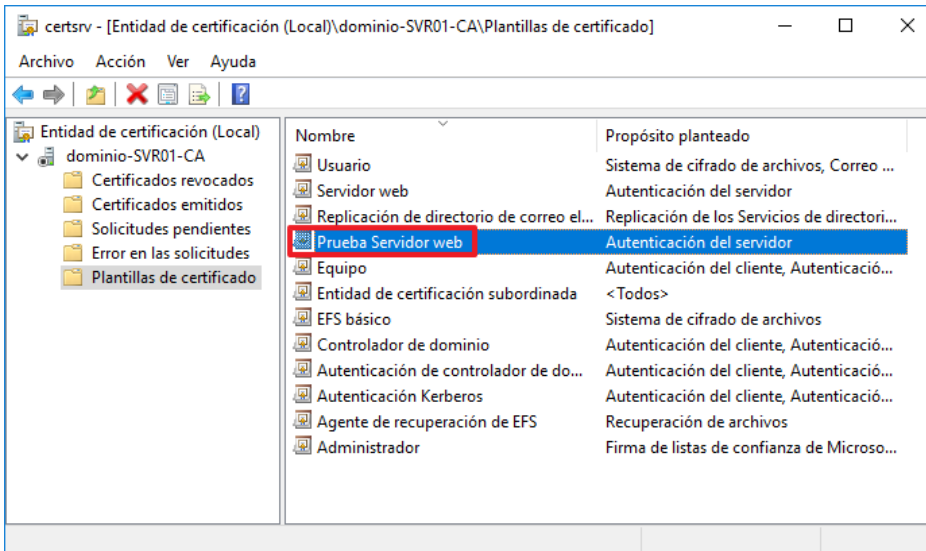
La plantilla aún no está disponible para poder solicitarla. Para poder utilizar la plantilla deberá completar el apartado siguiente “4.2.PUBLICACIÓN DE UNA PLANTILLA DE CERTIFICADOS EN LA ENTIDAD DE CERTIFICACIÓN”.

## 4.2. PUBLICACIÓN DE UNA PLANTILLA DE CERTIFICADOS EN LA ENTIDAD DE CERTIFICACIÓN

Este apartado define los pasos para publicar en la Entidad de Certificación la plantilla creada en el apartado anterior para que sea accesible a solicitudes de certificado.

| Paso | Descripción                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64.  | <p>Inicie sesión en el servidor Entidad de Certificación raíz o subordinada de empresa.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                    |
| 65.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 66.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                               |

| Paso | Descripción                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 67.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                                                        |
| 68.  | <p>Sitúese sobre el contenedor de “Plantillas de certificado”.</p>  <p><b>Nota:</b> En el ejemplo, la Entidad de Certificación es de tipo subordinada y recibe el nombre de “dominio-SRV01-CA”.</p>                       |
| 69.  | <p>Sitúese sobre el contenedor “Plantillas de certificado”, pulse el botón derecho del ratón y seleccione “Nuevo → Plantilla de certificado que se va a emitir” para acceder al resto de plantillas de certificado.</p>  |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 70.  | <p>En “Habilitar plantillas de certificado”, seleccione la plantilla de certificado que desee publicar a través de la Entidad de Certificación para que sea accesible desde los clientes solicitantes. A continuación, pulse “Aceptar”.</p>  <p><b>Nota:</b> En el ejemplo se publica en la Entidad de Certificación” la plantilla creada en el paso anterior “Prueba Servidor Web”.</p> |
| 71.  | <p>Compruebe que la plantilla aparece en el contenedor “Plantillas de certificado” de la Entidad de Certificación. En este momento, la plantilla será accesible para solicitar un certificado a través de ella.</p>                                                                                                                                                                    |

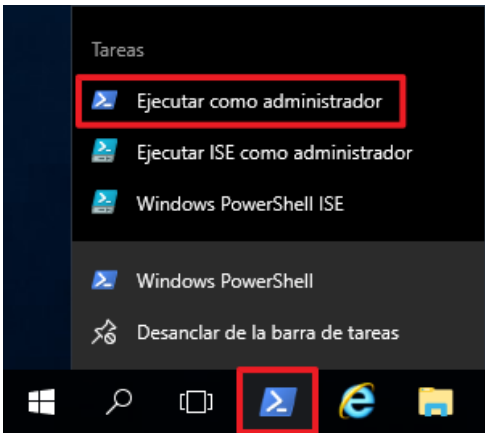
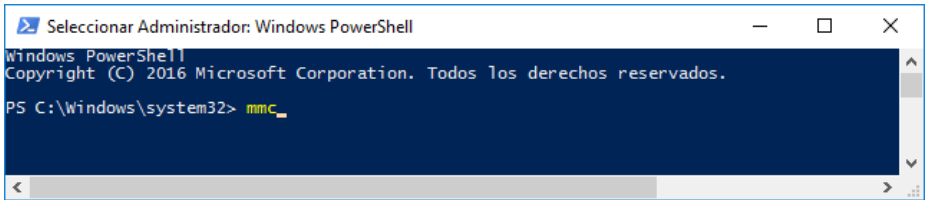
## 5. PROCEDIMIENTOS DE SOLICITUD Y ADMINISTRACIÓN DE CERTIFICADOS

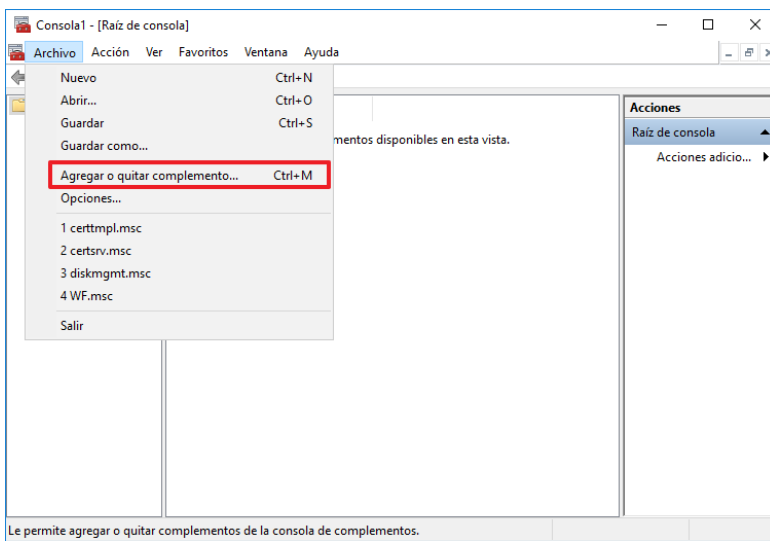
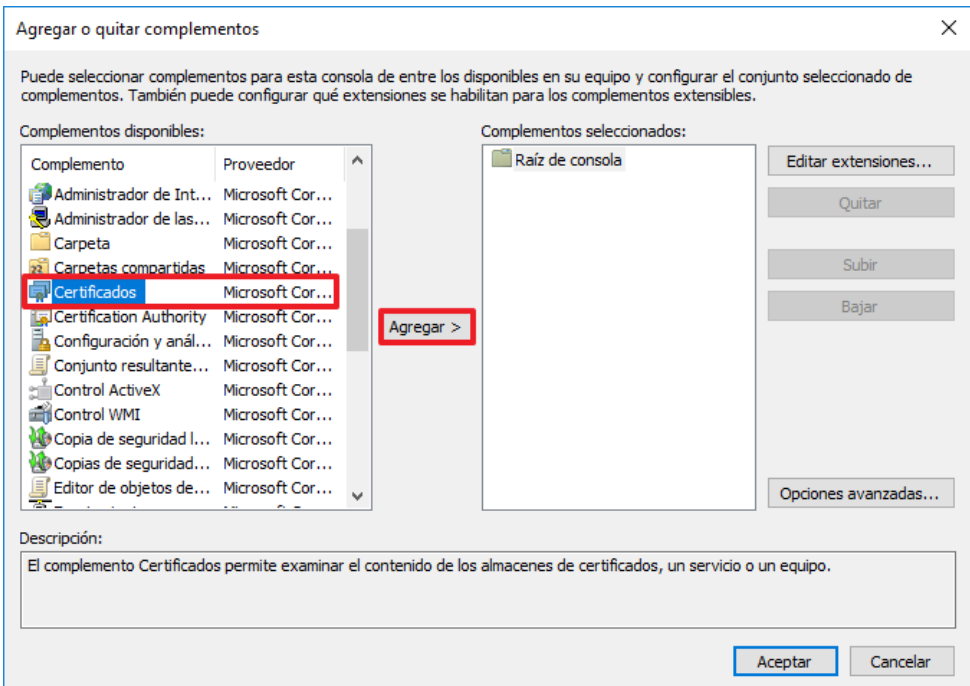
La presente sección define los pasos para realizar diversas operaciones con certificados.

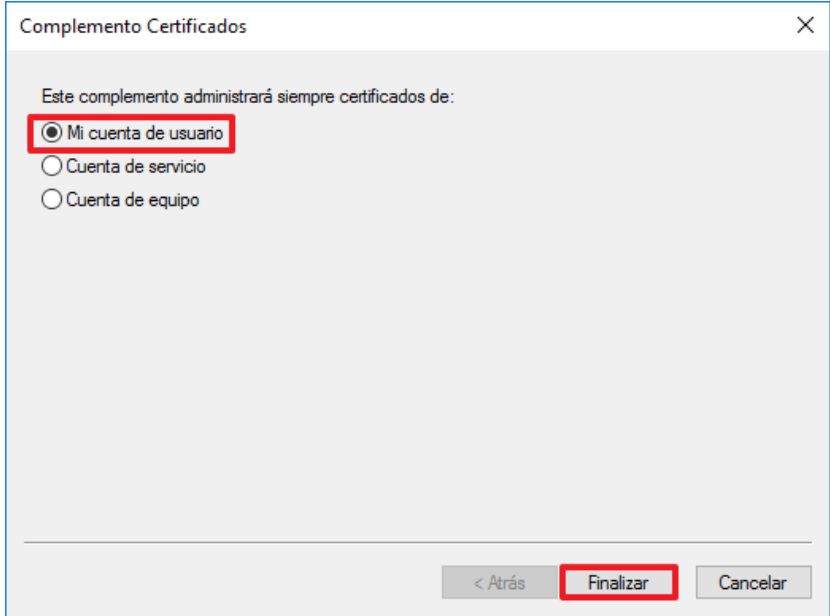
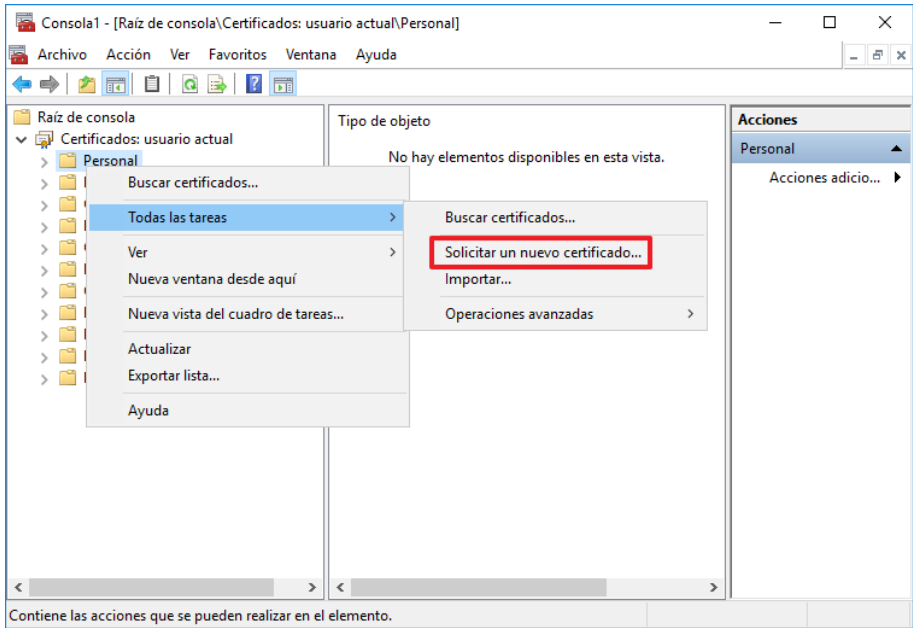
### 5.1. SOLICITUD DE CERTIFICADOS

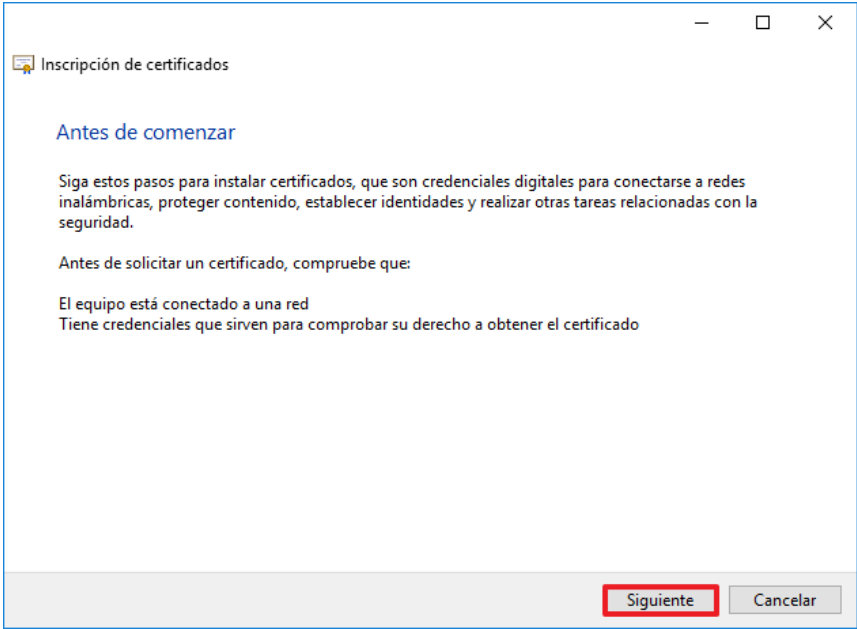
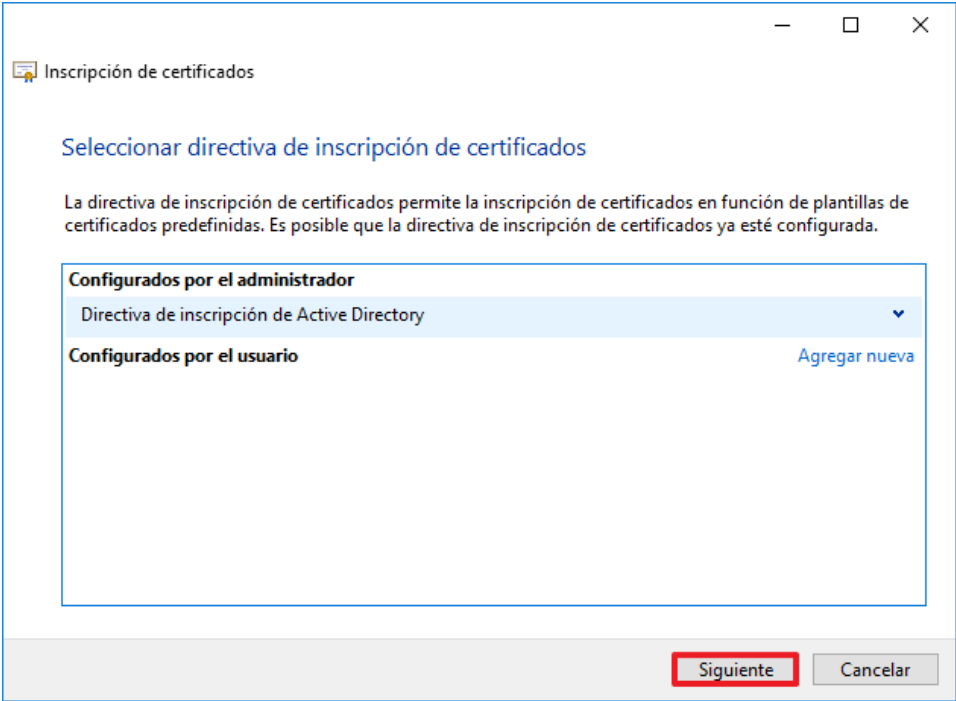
#### 5.1.1. DESDE LA CONSOLA MMC

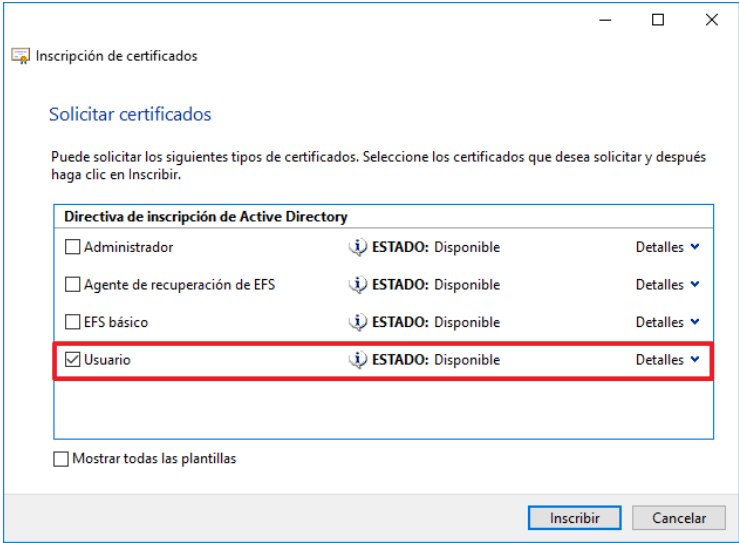
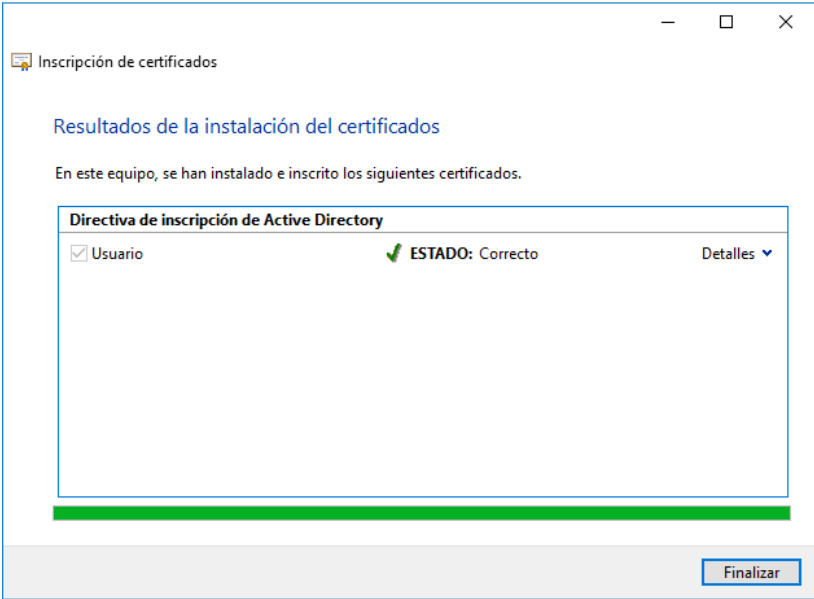
Esta sección define los pasos a seguir para solicitar un certificado, a través de un equipo cliente de la Entidad de Certificación y mediante la consola de “Certificados” de Administración de Microsoft o MMC. En el ejemplo, se solicitará un certificado a partir de la plantilla de autenticación de usuario y la solicitud se hará desde un servidor que actuará como cliente de la entidad.

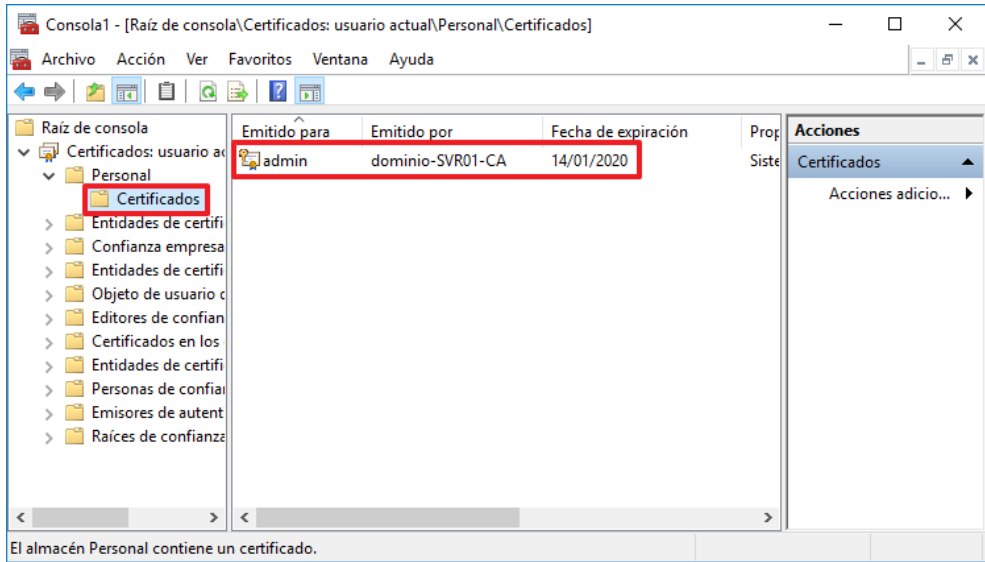
| Paso | Descripción                                                                                                                                                                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 72.  | <p>Inicie sesión en el servidor que actúa como cliente solicitante del servidor Entidad de Certificación.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración</p>                                                                                                                           |
| 73.  | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador".</p>  |
| 74.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                                                                                                                       |
| 75.  | <p>Teclee “mmc” en la consola de comandos y pulse “Enter”.</p>                                                                                                                                                                                 |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 76.  | <p>En la consola seleccione <b>“Archivo → Agregar o quitar complemento...”</b>.</p>  <p>The screenshot shows the 'Consola1 - [Raíz de consola]' window. The 'Archivo' menu is open, and 'Agregar o quitar complemento...' is highlighted with a red box. Other menu items include 'Nuevo', 'Abrir...', 'Guardar', 'Guardar como...', 'Opciones...', and a list of certificates (1 certtmpl.msc, 2 certsrv.msc, 3 diskmgmt.msc, 4 WF.msc). The 'Acciones' pane on the right shows 'Raíz de consola' and 'Acciones adicionales'.</p>                                                                                                                                                             |
| 77.  | <p>Seleccione <b>“Certificados”</b> de la columna <b>“Complementos disponibles”</b> y pulse <b>“Agregar &gt;”</b>.</p>  <p>The screenshot shows the 'Agregar o quitar complementos' dialog box. The 'Complementos disponibles:' list on the left has 'Certificados' selected and highlighted with a red box. The 'Complementos seleccionados:' list on the right contains 'Raíz de consola'. The 'Agregar &gt;' button is highlighted with a red box. The 'Descripción:' field at the bottom states: 'El complemento Certificados permite examinar el contenido de los almacenes de certificados, un servicio o un equipo.' Buttons for 'Aceptar' and 'Cancelar' are at the bottom right.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 78.  | <p>Según el tipo de certificado, se deberá seleccionar el tipo de cuenta de la que se quiere abrir la consola de certificados. Esta elección dependerá del tipo de certificado que se quiera solicitar. Pulse “Finalizar” para continuar.</p>  <p><b>Nota:</b> En el ejemplo se selecciona “Mi cuenta de usuario”, ya que se solicita un certificado de usuario de autenticación del cliente.</p> |
| 79.  | <p>Pulse “Aceptar” para abrir la consola de certificados y despliegue el menú en árbol situado a la izquierda hasta llegar al contenedor “Personal” mediante la siguiente ruta: <b>“Raíz de consola → Certificados: usuario actual → Personal”</b><br/>Pulse con el botón derecho del ratón sobre “Personal” y seleccione <b>“Todas las tareas → Solicitar un nuevo certificado...”</b>.</p>     |

| Paso | Descripción                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80.  | <p>Se abrirá el asistente de “Inscripción de certificados”. En la ventana “Antes de comenzar” pulse “Siguiente”.</p>  |
| 81.  | <p>En “Seleccionar directiva de inscripción de certificados”, mantenga la configuración y pulse “Siguiente”.</p>     |

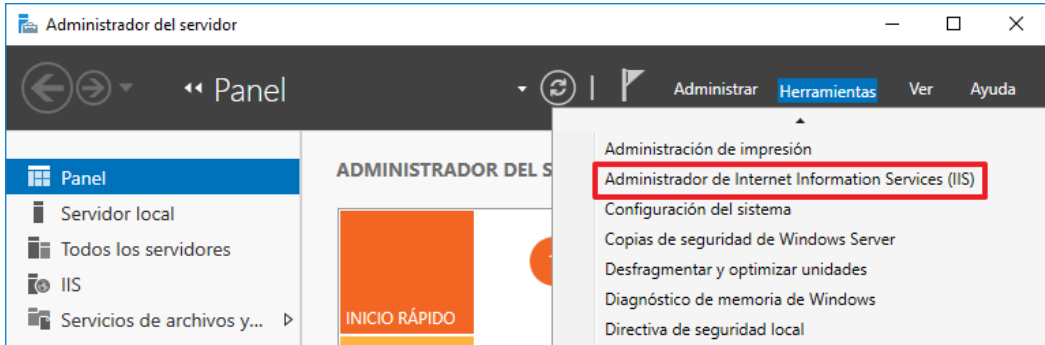
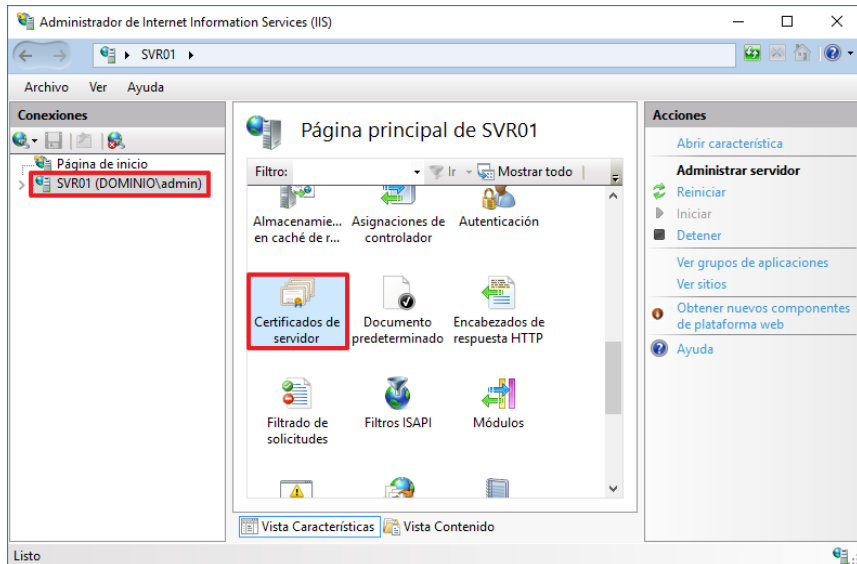
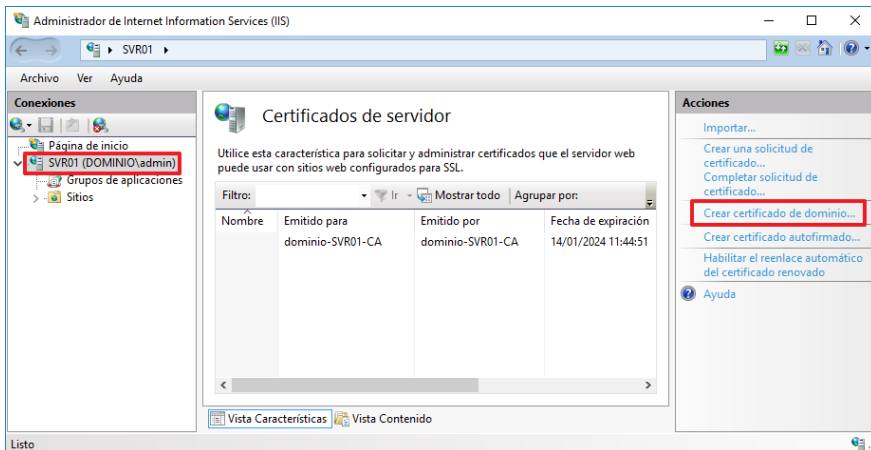
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 82.  | <p>Seleccione posteriormente “Usuario” y pulse sobre el botón “Inscribir”.</p>                                                                                                                                                                                                                                                                                                                         |
| 83.  | <p>El certificado se inscribirá automáticamente debido a que el usuario tenía permisos de “Inscripción automática” en la plantilla.</p>  <p><b>Nota:</b> En caso de que el usuario no tuviera los permisos mencionados, sería necesario realizar una serie de pasos adicionales en la Entidad de Certificación. Estos pasos serán descritos en el apartado siguiente: “Emisión de certificados”.</p> |

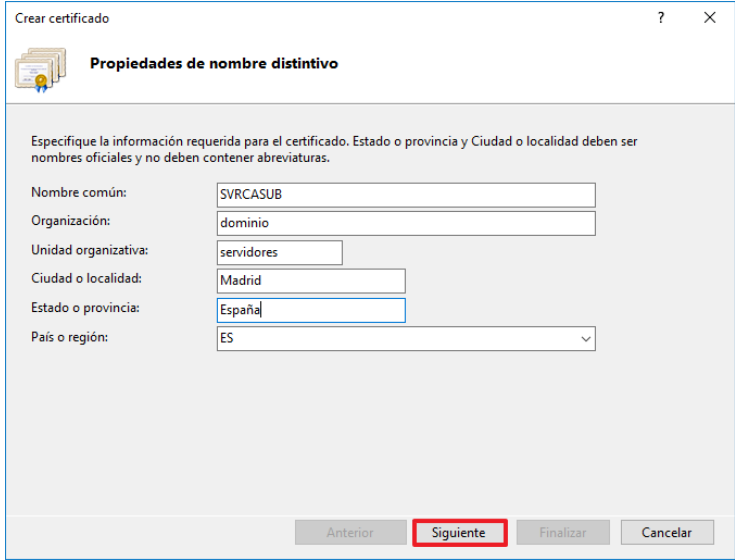
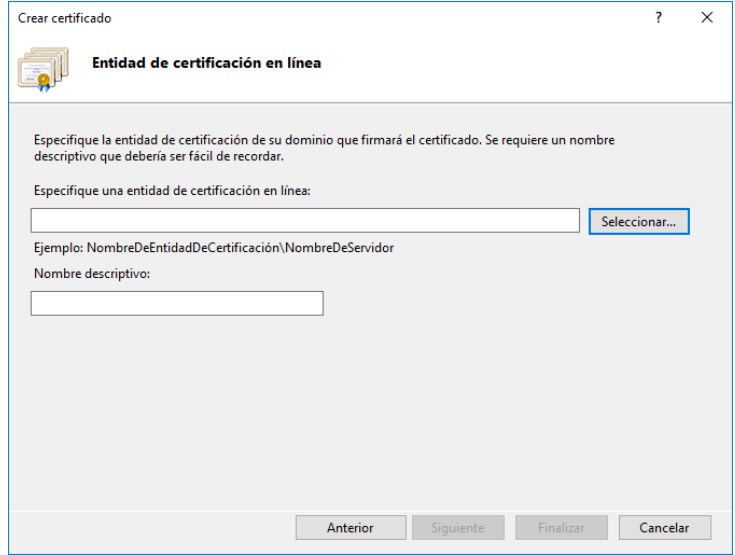
| Paso         | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |             |                     |       |                  |            |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------|---------------------|-------|------------------|------------|
| 84.          | <p>Navegue hasta el contenedor “Certificados” mediante la siguiente ruta:<br/>“Raíz de consola → Certificados: usuario actual → Personal → Certificados”<br/>Compruebe que se ha emitido el certificado para el usuario y se ha hecho desde la entidad raíz de empresa o subordinada de empresa.</p>  <table><tr><th>Emitido para</th><th>Emitido por</th><th>Fecha de expiración</th></tr><tr><td>admin</td><td>dominio-SVR01-CA</td><td>14/01/2020</td></tr></table> | Emitido para        | Emitido por | Fecha de expiración | admin | dominio-SVR01-CA | 14/01/2020 |
| Emitido para | Emitido por                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Fecha de expiración |             |                     |       |                  |            |
| admin        | dominio-SVR01-CA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 14/01/2020          |             |                     |       |                  |            |

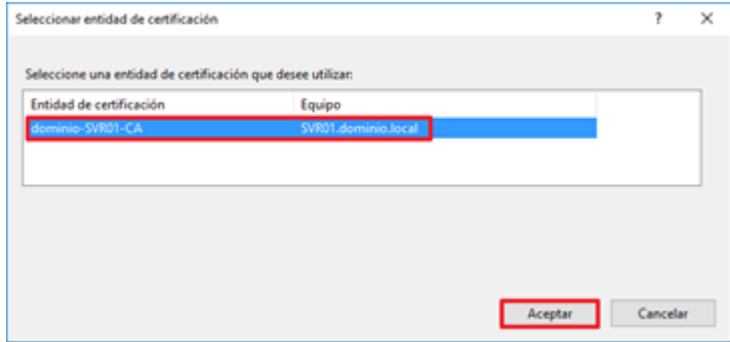
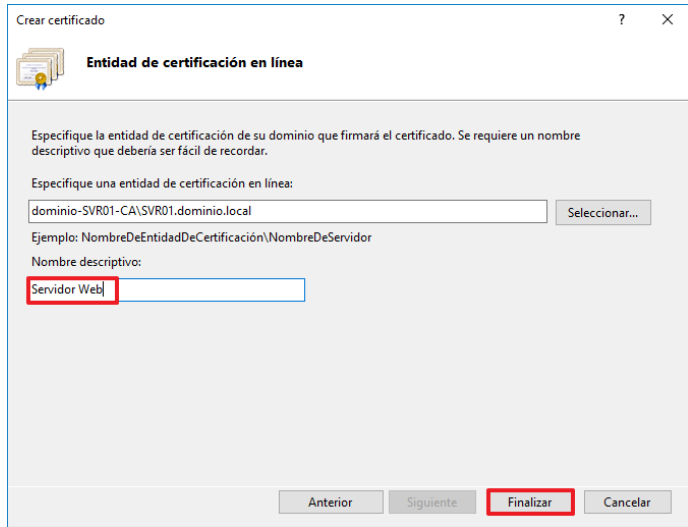
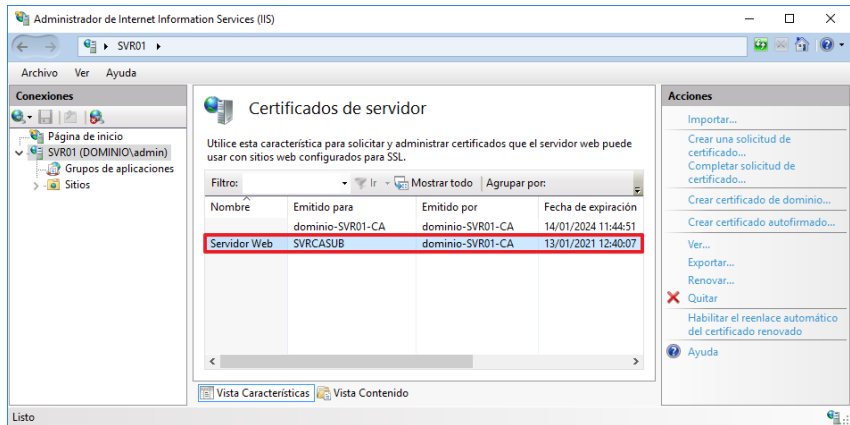
### 5.1.2. DESDE EL SERVICIO DE INTERNET INFORMATION SERVICES (IIS)

Esta sección define los pasos a seguir para solicitar un certificado, a través de un equipo cliente de la Entidad de Certificación y mediante el servicio de Internet Information Services o IIS. En el ejemplo, se solicitará un certificado de servidor de internet desde la consola de administración de IIS del servidor Entidad de Certificación, aunque estos pasos también son válidos en servidores miembros del dominio que tengan los servicios de Internet Information Services instalado.

| Paso | Descripción                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 85.  | <p>Inicie sesión en el servidor que actúa como cliente solicitante del servidor Entidad de Certificación.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administrador de dominio.</p>                                                     |
| 86.  | <p>Ejecute la consola administrativa “Administrador de Internet Information Services (IIS)”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 87.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí”.</p>                                                                                  |

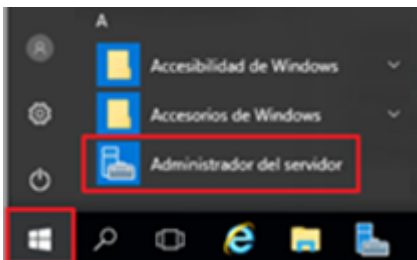
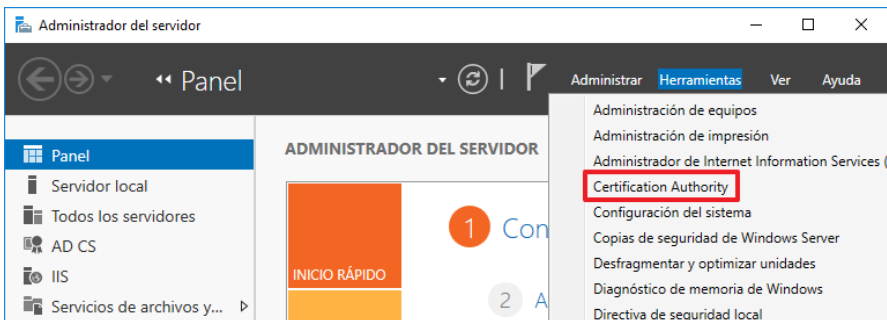
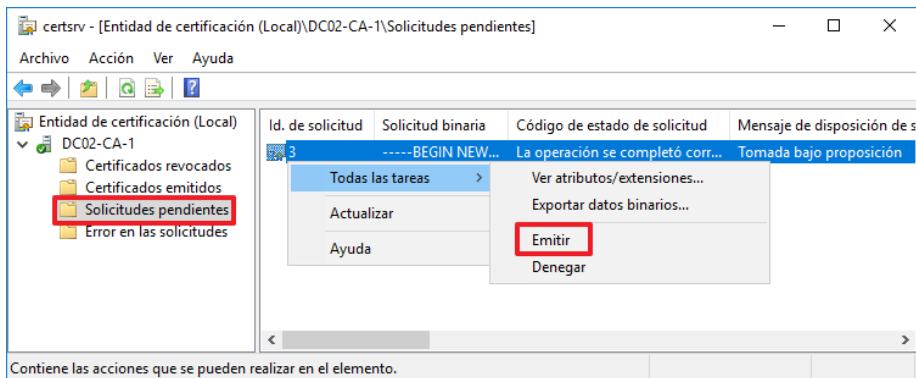
| Paso | Descripción                                                                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88.  | <p>Navegue hasta el “Administrador de Internet Information Services (IIS)” mediante la ruta <b>“Administrador del servidor → Herramientas → Administrador de Internet Information Services (IIS)”</b>.</p>   |
| 89.  | <p>En el “Administrador de Internet Information Services” seleccione en el panel izquierdo el nombre de la Entidad de Certificación y, en “Vista Características” localice “Certificados de Servidor”.</p>  |
| 90.  | <p>Pulse doble clic sobre certificados de servidor y en el menú “Acciones” situado a la derecha seleccione “Crear certificado de dominio...”.</p>                                                          |

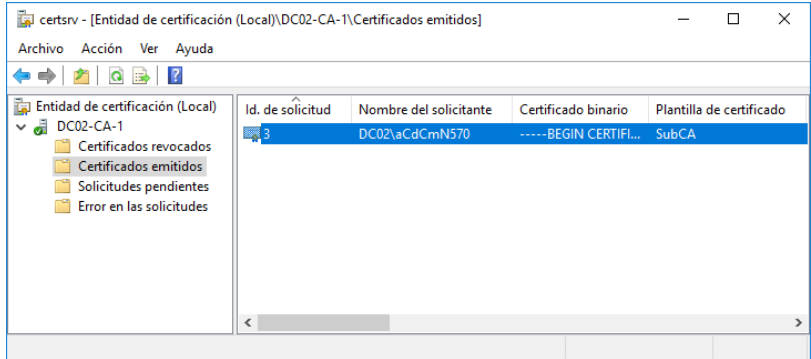
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 91.  | <p>En el “Asistente para solicitar certificados” se podrán establecer los diferentes parámetros según las necesidades. Una vez establecidos estos parámetros pulse “Siguiente”.</p>  <p><b>Nota:</b> Los datos introducidos que refleja la captura son a modo de ejemplo.</p> |
| 92.  | <p>En “Especifique una Entidad de Certificación en línea:” pulse “Seleccionar”.</p>                                                                                                                                                                                         |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93.  | <p>Seleccione la Entidad de Certificación que emitirá el certificado y pulse “Aceptar”.</p>                                                                                                                                                                          |
| 94.  | <p>Proporcione un nombre descriptivo y pulse “Finalizar”.</p>                                                                                                                                                                                                       |
| 95.  | <p>Compruebe que el certificado aparece en la lista.</p>  <p><b>Nota:</b> En este caso, el certificado se inscribe de forma automática. El siguiente paso describe los pasos a seguir en caso de que un certificado solicitado no se inscriba automáticamente.</p> |

## 5.2. EMISIÓN DE SOLICITUDES PENDIENTES DE CERTIFICADOS

Esta sección define una serie de pasos para emitir y distribuir los certificados solicitados a través de una Entidad de Certificación de empresa, independientemente de que ésta sea raíz o subordinada.

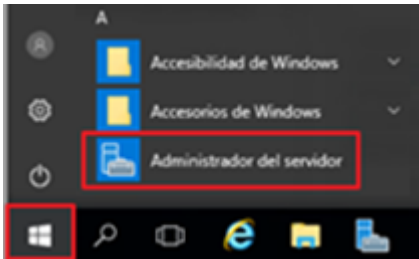
| Paso | Descripción                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 96.  | <p>Inicie sesión en el servidor Entidad de Certificación raíz de empresa.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                                                                    |
| 97.  | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                                      |
| 98.  | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                                                                 |
| 99.  | <p>En el “Administrador del servidor” despliegue el menú superior derecho “Herramientas” y a continuación seleccione “Certification Authority”.</p>                                      |
| 100. | <p>Sitúese en el contenedor “Solicitudes pendientes” y sobre la solicitud de certificado que aparece pulse con el botón derecho del ratón y seleccione “Todas las tareas → Emitir”.</p>  |

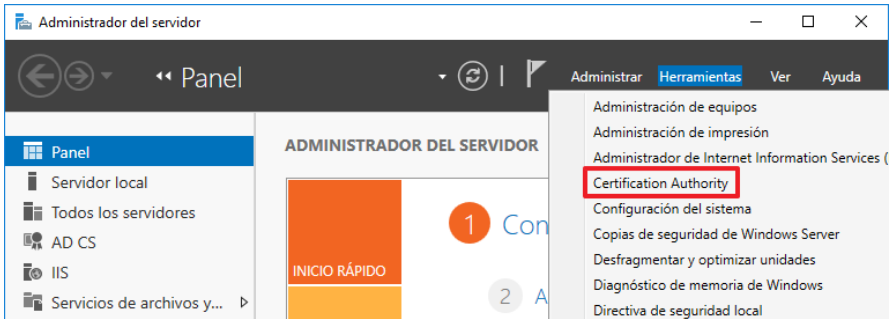
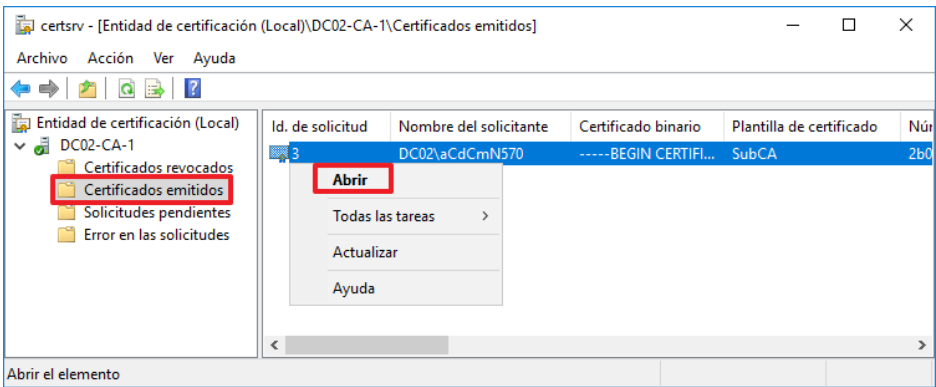
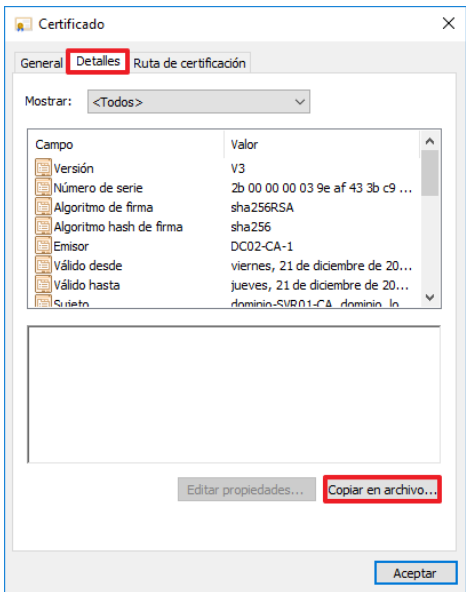
| Paso | Descripción                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 101. | <p>Sitúese sobre el contenedor “Certificados emitidos”. Podrá comprobar que el certificado recién emitido aparece en la lista y será distribuido al cliente solicitante.</p>  |

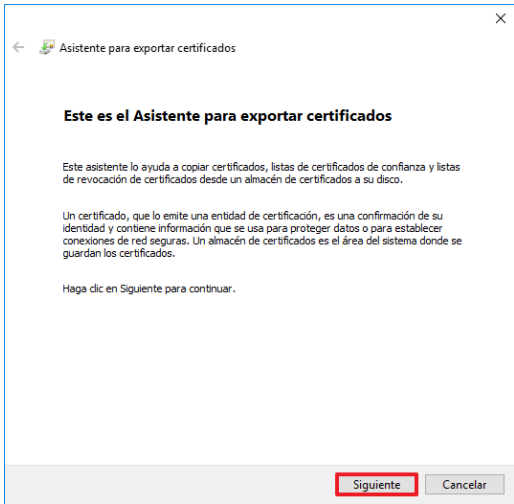
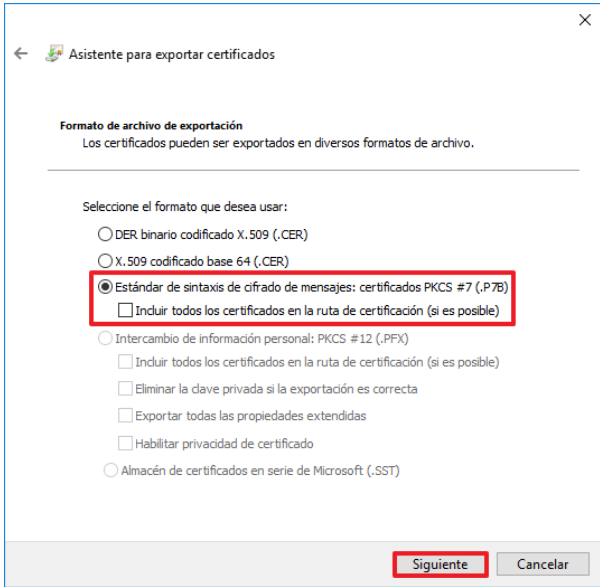
### 5.3. EXPORTACIÓN DE CERTIFICADOS

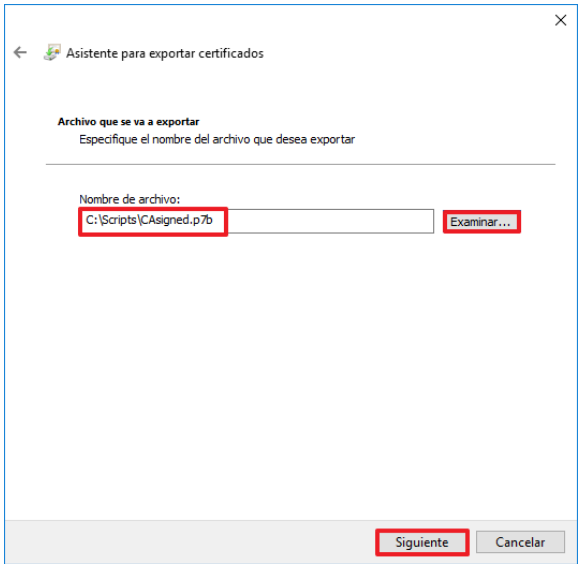
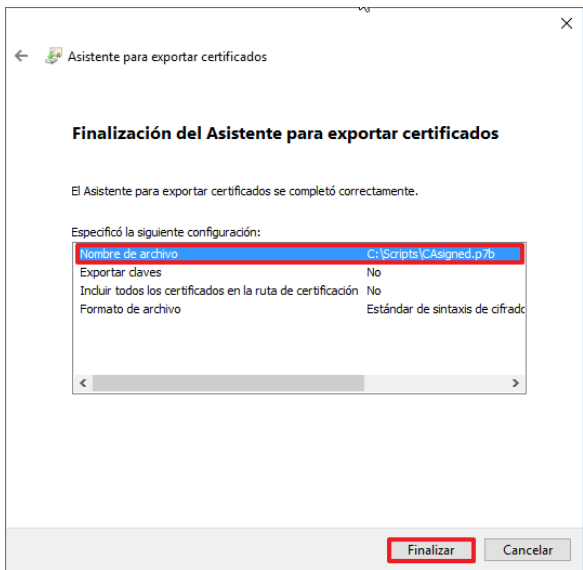
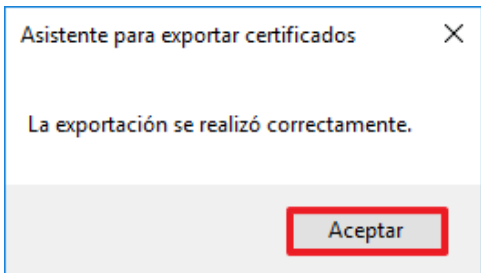
Para poder llevar certificados a un entorno que no puede acceder a la Entidad de Certificación, existe la opción de exportar el certificado para importarlo desde el cliente que no tiene acceso a la Entidad de Certificación o que no es compatible con el Directorio Activo.

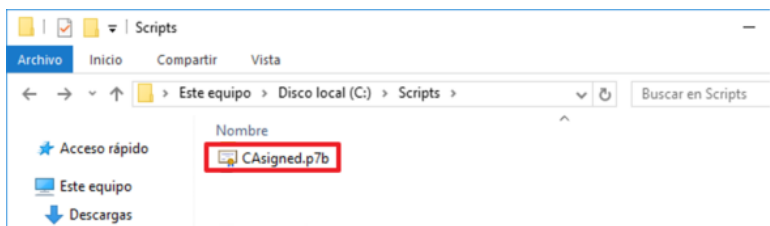
Estos pasos se pueden realizar tanto desde la Entidad de Certificación como desde la consola de certificados del cliente al que se le ha emitido el certificado. En el siguiente ejemplo, se va a realizar la exportación de un certificado a través de la Entidad de Certificación que lo emitió.

| Paso | Descripción                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 102. | <p>Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado con credenciales de administración.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>              |
| 103. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 104. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                               |

| Paso | Descripción                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 105. | <p>En el menú situado a la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                 |
| 106. | <p>Vaya a la carpeta certificados emitidos, seleccione, en el apartado central, el certificado que desea exportar con el botón derecho del ratón y seleccione la opción “Abrir”.</p>  |
| 107. | <p>Una vez abierta la ventana “Certificado”, diríjase a la pestaña “Detalles” y pulse sobre “Copiar en archivo...”.</p>                                                              |

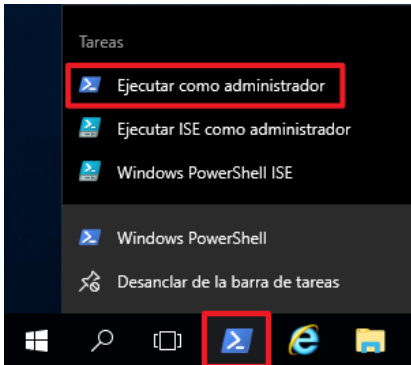
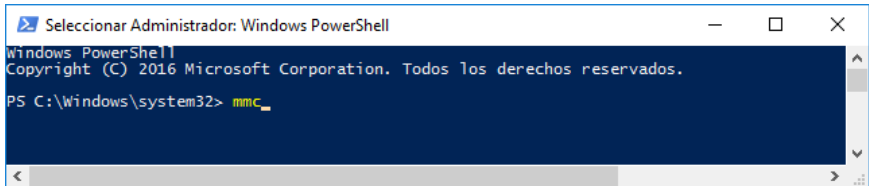
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 108. | <p>En el “Asistente para exportación de certificados” pulse “Siguiente”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 109. | <p>En “Formato de archivo de exportación” seleccione “Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)” y pulse “Siguiente”.</p>  <p><b>Nota:</b> El certificado se exportará sin la clave privada, ya que para el propósito no es necesario. Incluso cuando es posible exportar la clave privada, si el propósito del certificado no lo requiere, es más seguro evitar exportar el certificado con su clave privada. En el caso de que sí fuera necesaria la exportación de la clave privada (un servicio ajeno a Windows no compatible con el Directorio Activo, por ejemplo), el sistema solicitará el establecimiento de una contraseña (necesaria en la posterior importación).</p> |

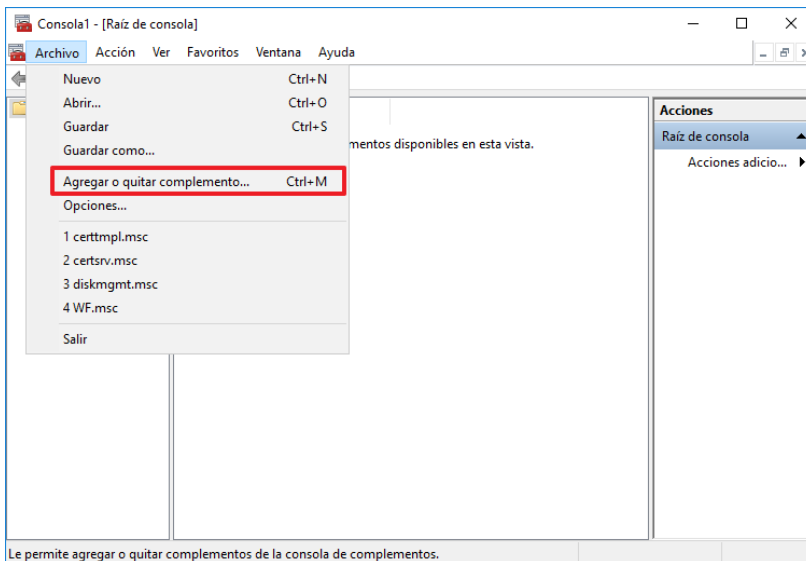
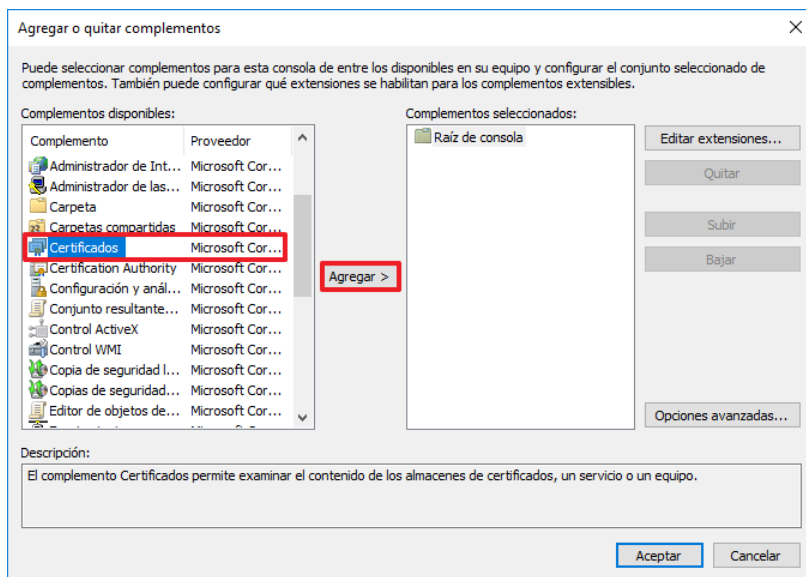
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 110. | <p>En “Archivo que se va a exportar” pulse examinar para establecer la ubicación y el nombre del archivo que se va a exportar. Pulse “Siguiente” continuar</p>  <p><b>Nota:</b> En el ejemplo se ubica el fichero en “C:\Scripts” y se denomina CAsigned.P7B”.</p> |
| 111. | <p>Pulse “Finalizar” para salir del asistente.</p>                                                                                                                                                                                                               |
| 112. | <p>Pulse “Aceptar” en el mensaje que confirma que la exportación se ha realizado correctamente.</p>                                                                                                                                                              |

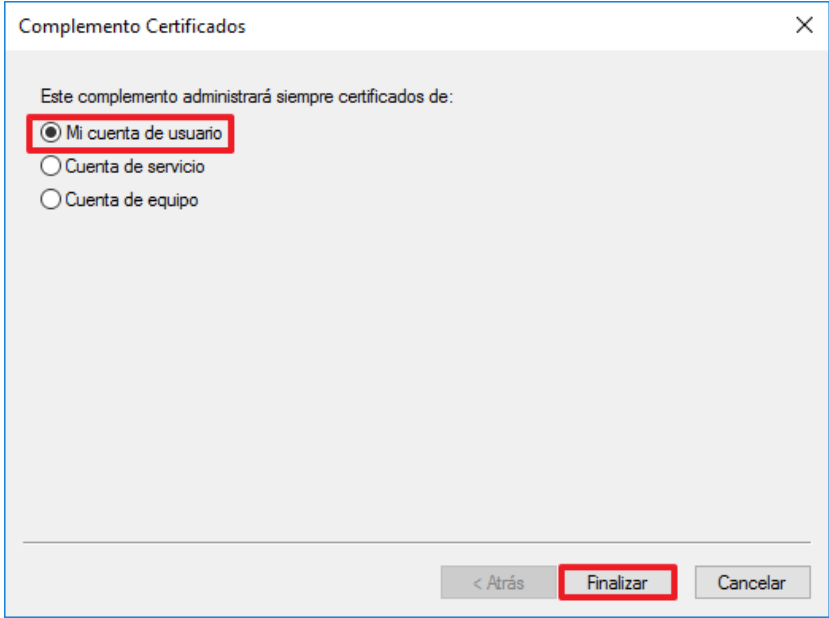
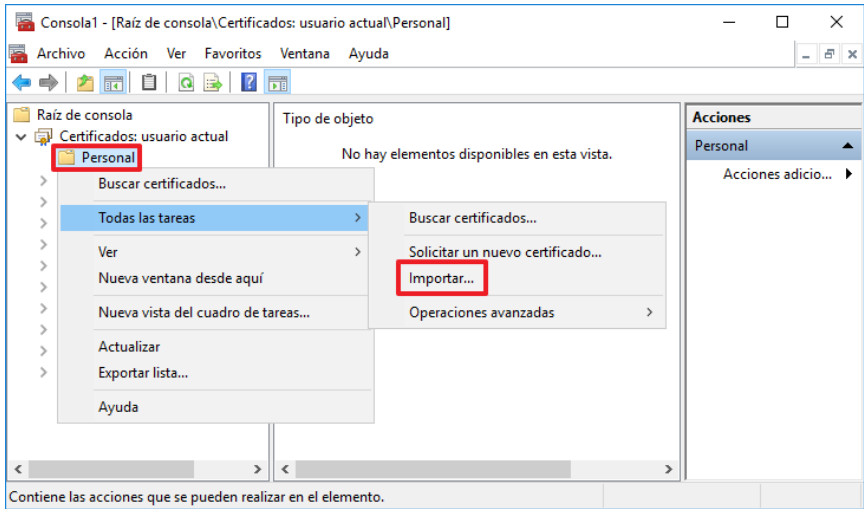
| Paso | Descripción                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 113. | <p>En la ruta correspondiente podrá encontrar el certificado exportado.</p>  |

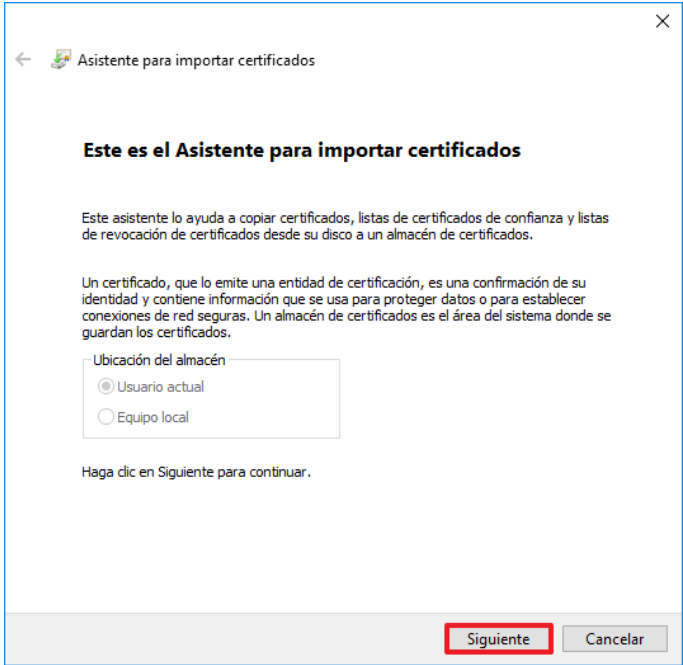
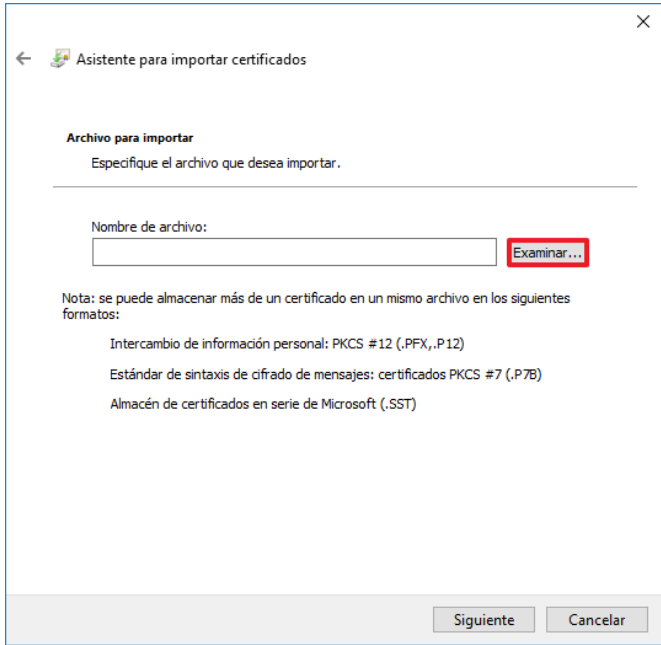
## 5.4. IMPORTACIÓN DE CERTIFICADOS

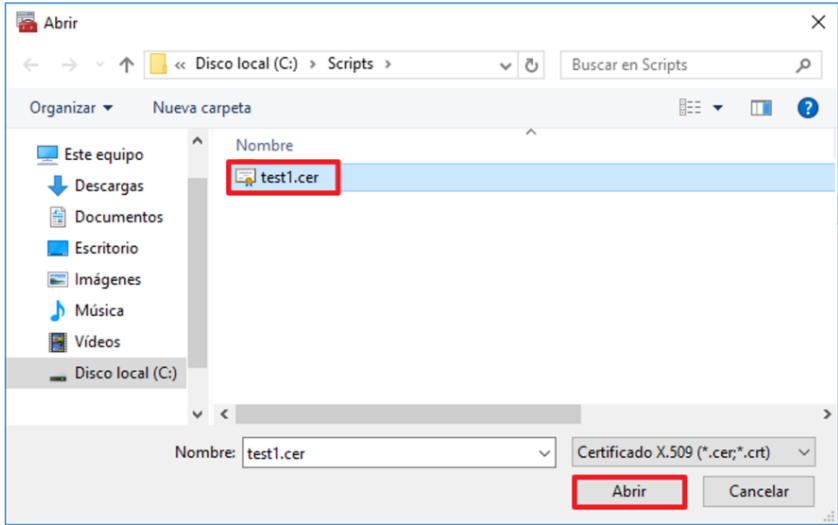
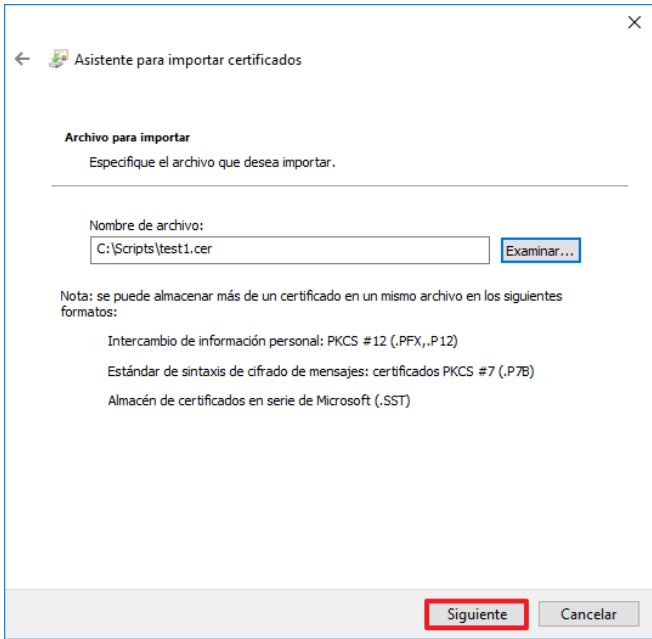
En este apartado se definen los pasos para importar un certificado que se había exportado previamente.

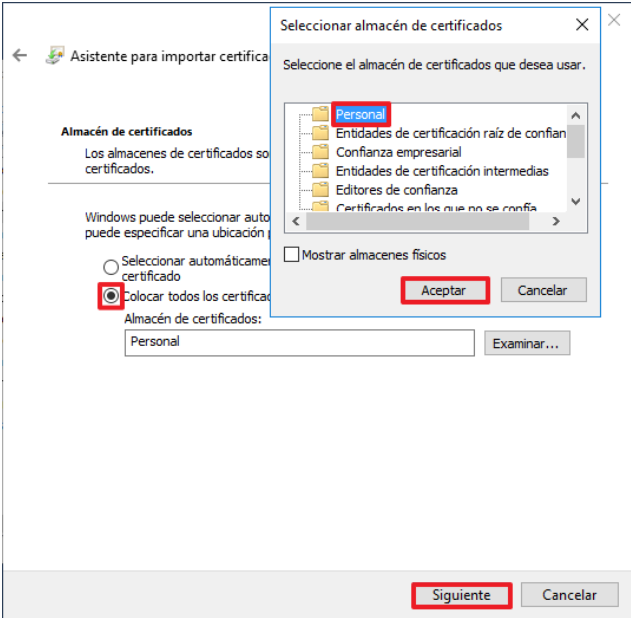
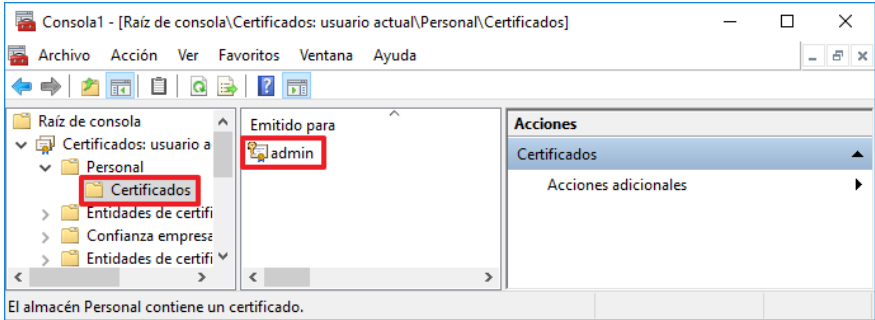
| Paso | Descripción                                                                                                                                                                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 114. | <p>Inicie sesión en el servidor que actúa como cliente solicitante del servidor Entidad de Certificación.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                                                                                          |
| 115. | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador".</p>  |
| 116. | <p>El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí".</p>                                                                                                                                                       |
| 117. | <p>Teclee "mmc" en la consola de comandos y pulse "Enter".</p>                                                                                                                                                                                 |

| Paso | Descripción                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 118. | <p>En la consola seleccione <b>“Archivo → Agregar o quitar complemento...”</b>.</p>  <p>Le permite agregar o quitar complementos de la consola de complementos.</p> |
| 119. | <p>Seleccione <b>“Certificados”</b> en la columna <b>“Complementos disponibles”</b> y pulse <b>“Agregar &gt;”</b></p>                                             |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 120. | <p>Según el tipo de certificado, se deberá seleccionar el tipo de cuenta de la que se quiere abrir la consola de certificados. Esta elección dependerá del tipo de certificado que se quiera solicitar. Pulse “Finalizar” para continuar.</p>  <p><b>Nota:</b> En el ejemplo se selecciona “Mi cuenta de usuario”, ya que se solicita un certificado de usuario de autenticación del cliente.</p> |
| 121. | <p>Pulse “Aceptar” para abrir la consola de certificados y despliegue el menú en árbol situado a la izquierda hasta llegar al contenedor “Personal” mediante la siguiente ruta: <b>“Raíz de consola → Certificados: usuario actual → Personal”</b>. Pulse con el botón derecho del ratón sobre “Personal” y seleccione <b>“Todas las tareas → Importar...”</b>.</p>                              |

| Paso | Descripción                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 122. | <p>Se abrirá el “Asistente para la importación de certificados”. En la ventana inicial del asistente pulse “Siguiente”.</p>  |
| 123. | <p>En la ventana “Archivo para importar” pulse el botón “Examinar...”.</p>                                                  |

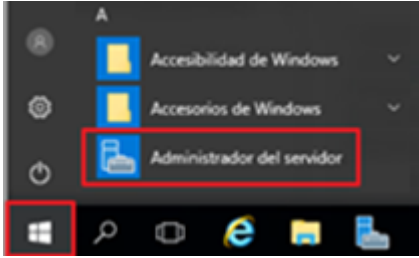
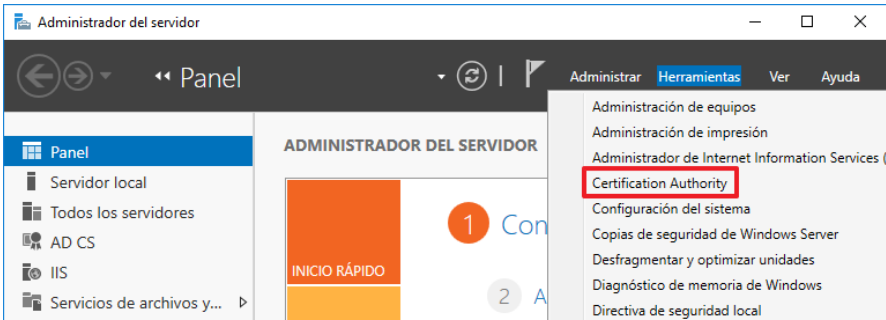
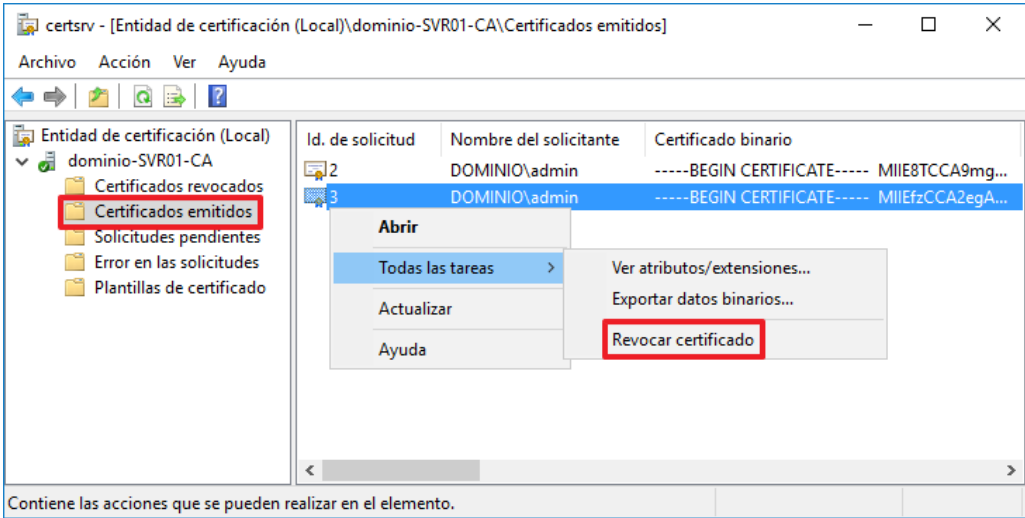
| Paso | Descripción                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------|
| 124. | <p>Localice el certificado y pulse “Abrir”.</p>  |
| 125. | <p>Pulse “Siguiente” para continuar.</p>        |

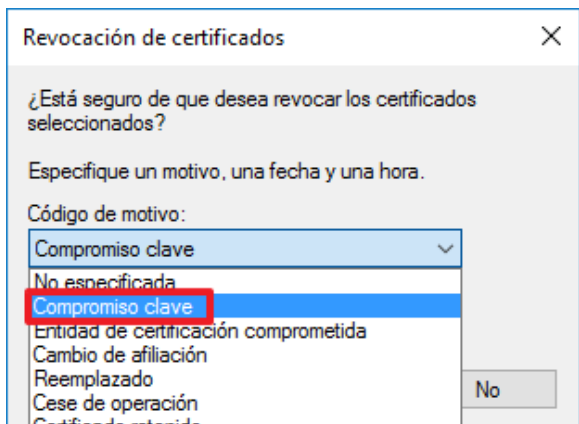
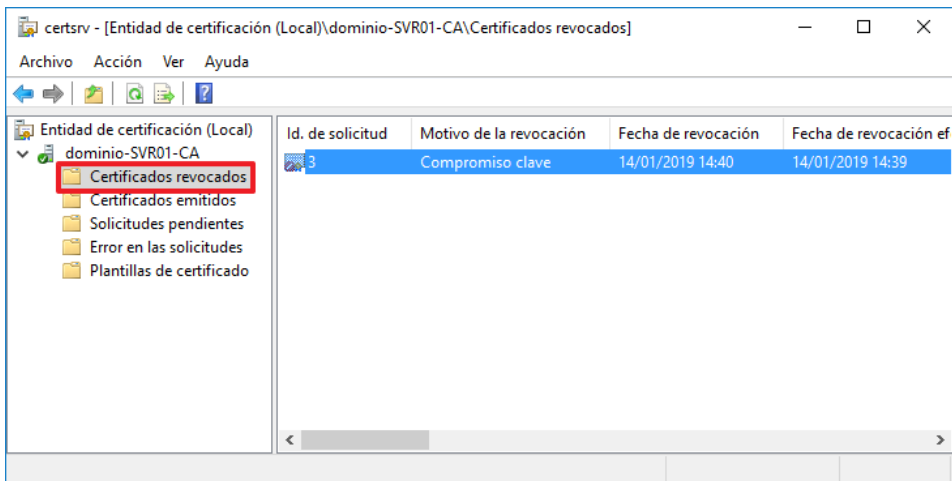
| Paso | Descripción                                                                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 126. | <p>En “Almacén de certificados” seleccione “Colocar todos los certificados en el siguiente almacén” y pulse “Examinar”. Seleccione “Personal” de la lista y pulse “Aceptar”.</p>                                                  |
| 127. | Pulse “Siguiente” para continuar.                                                                                                                                                                                                                                                                                   |
| 128. | Pulse “Finalizar” para cerrar el asistente.                                                                                                                                                                                                                                                                         |
| 129. | <p>Navegue hasta el contenedor “Certificados” mediante la siguiente ruta: <b>“Raíz de consola → Certificados: usuario actual → Personal → Certificados”</b>. Compruebe que se ha importado el certificado para el usuario.</p>  |

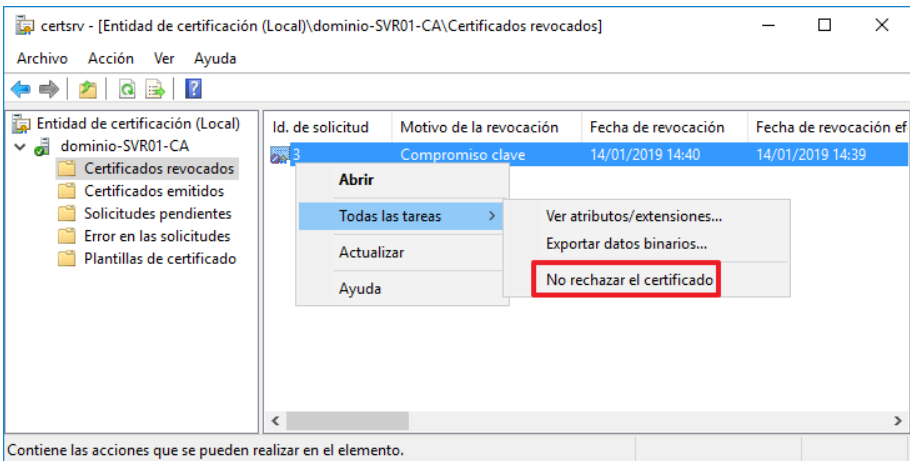
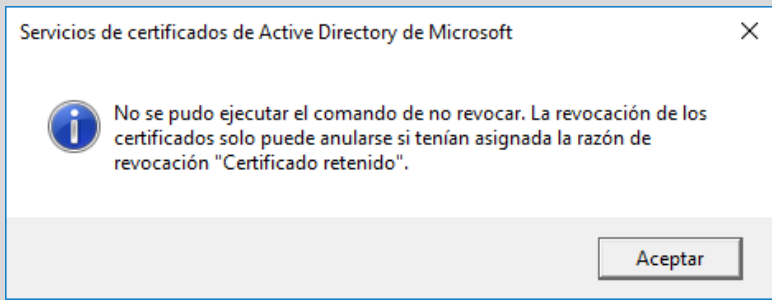
## 5.5. REVOCACIÓN DE CERTIFICADOS

Existen una serie de motivos para revocar un certificado, entre ellos podría estar el hecho de que la clave o la Entidad de Certificación que lo emitió hayan sido comprometidas, que el certificado ya no sea válido o haya sido sustituido por otro certificado, o bien que el cliente de dicho certificado ya no vaya a hacer uso del mismo.

Esta sección define los pasos para revocar un certificado, por alguno de los motivos expuestos, a través de un servidor Entidad de Certificación de empresa e independientemente de que sea una entidad raíz o subordinada.

| Paso | Descripción                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 130. | <p>Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                                                                         |
| 131. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>                                                            |
| 132. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                                                                                       |
| 133. | <p>En el menú situado a la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                                                          |
| 134. | <p>Vaya a la carpeta “Certificados emitidos”, seleccione, en el apartado central, el certificado que desea revocar con el botón derecho del ratón, y seleccione “Todas las tareas → Revocar certificado”.</p>  |

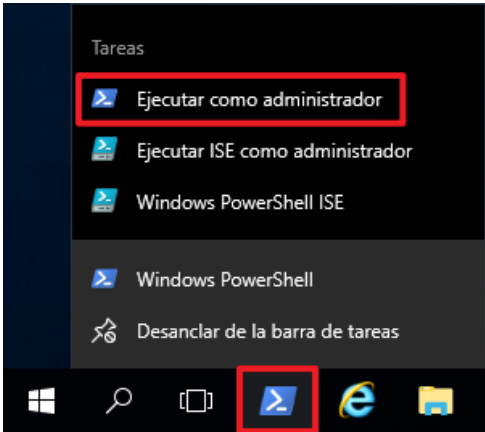
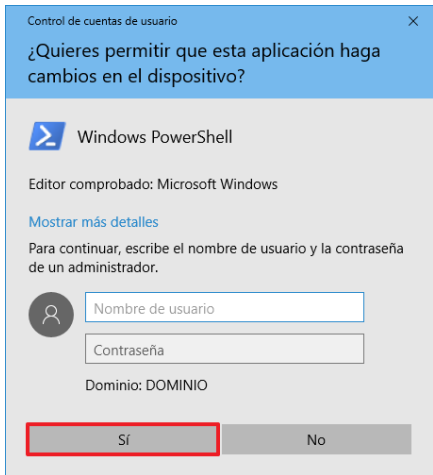
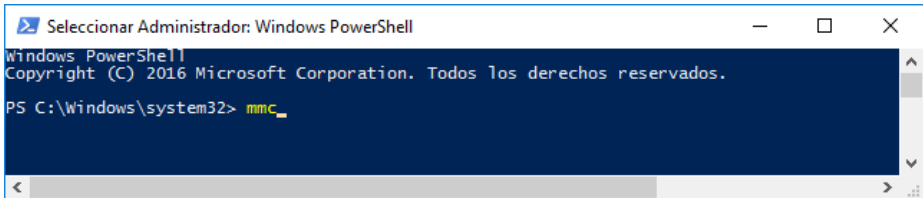
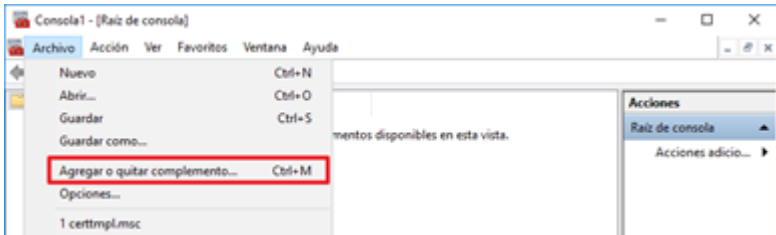
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 135. | <p>En la ventana de “Revocación de certificados” despliegue “Código de motivo:” y escoja la razón por la que se revocará el certificado.</p> <div></div> <p><b>Nota:</b> En el ejemplo se ha seleccionado “Compromiso de la clave” como razón de revocación.</p> |
| 136. | <p>Pulse “Sí” para cerrar la ventana de “Revocación de certificados”.</p>                                                                                                                                                                                                                                                                          |
| 137. | <p>Sitúese sobre el contenedor “Certificados revocados” para comprobar que el certificado recientemente revocado aparece en la lista.</p> <div></div>                                                                                                          |

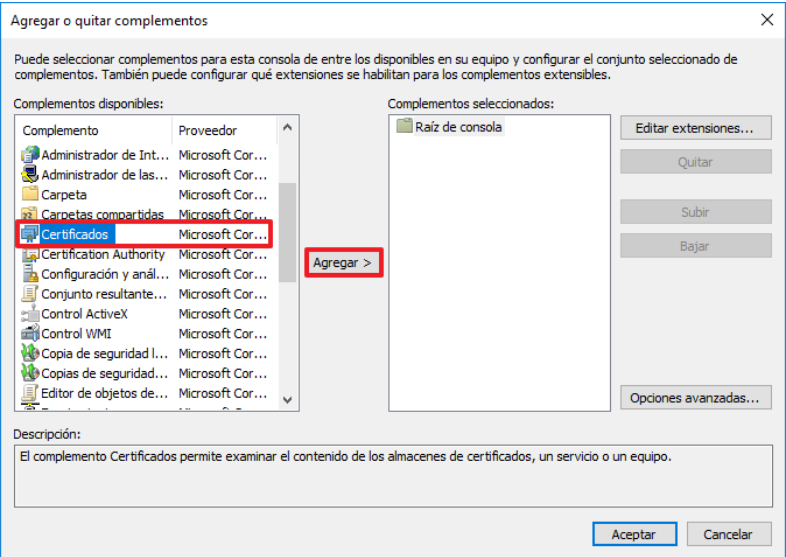
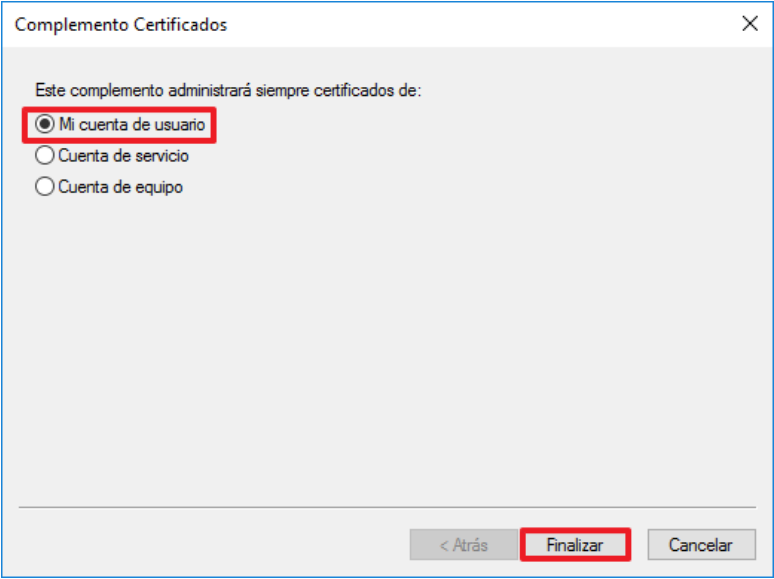
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 138. | <p>La revocación de un certificado no es reversible, a menos que la razón de revocación seleccionada haya sido “Certificado retenido”. Si fuera este el caso, sería posible deshacer la revocación pulsando sobre el certificado con el botón derecho del ratón y seleccionando <b>“Todas las tareas → No rechazar el certificado”</b>.</p>  <p><b>Nota:</b> En caso de haber escogido cualquier otro motivo de revocación (como en el ejemplo), al intentar deshacer la revocación aparecerá el siguiente mensaje:</p>  |

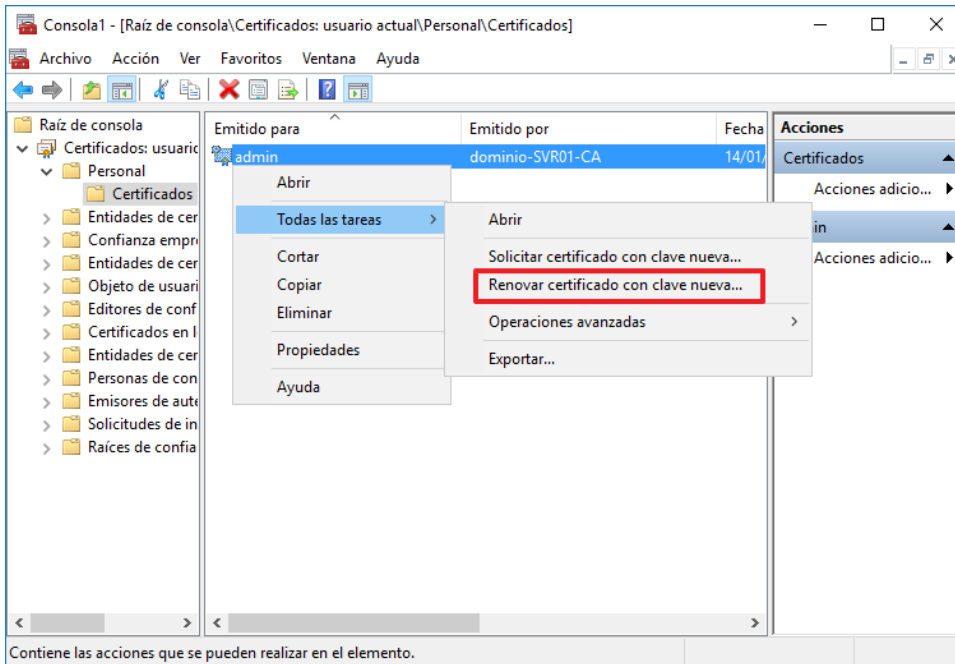
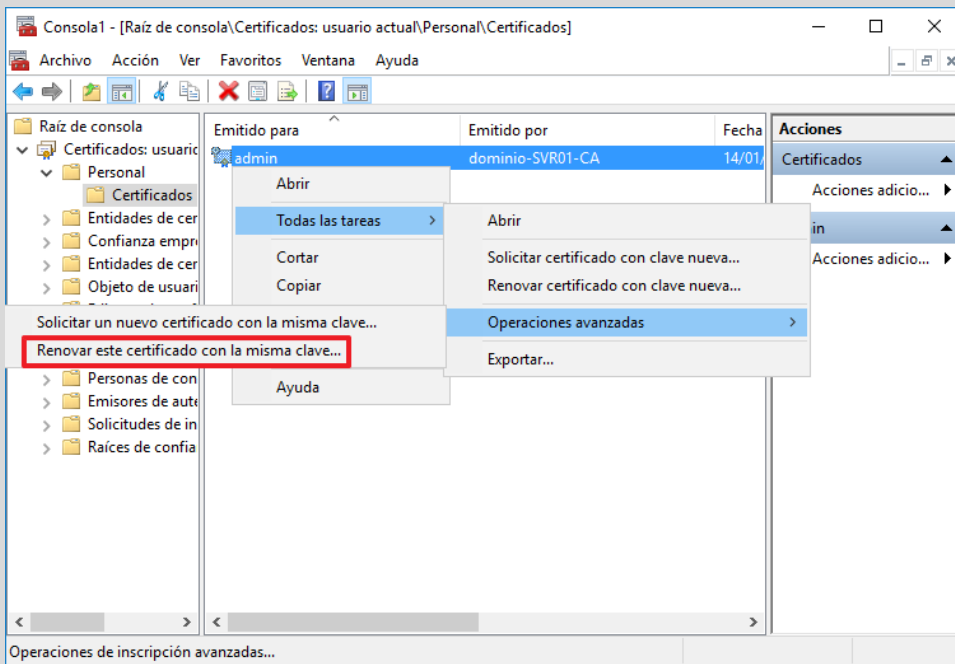
## 5.6. RENOVACIÓN DE CERTIFICADOS

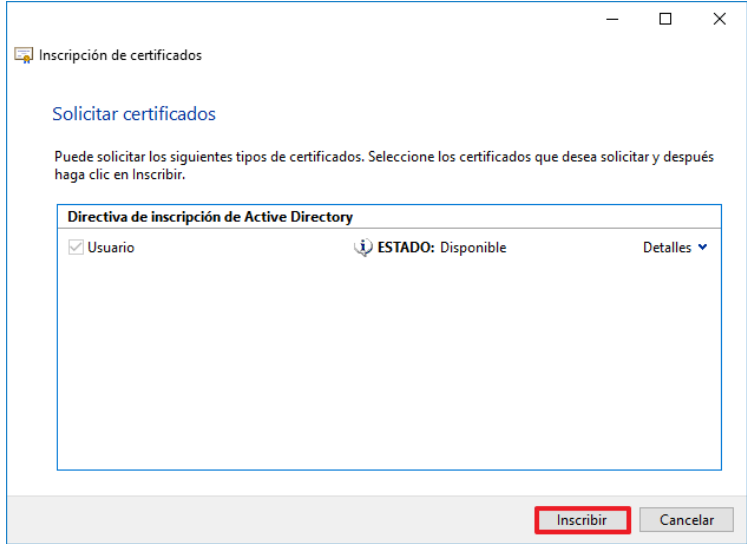
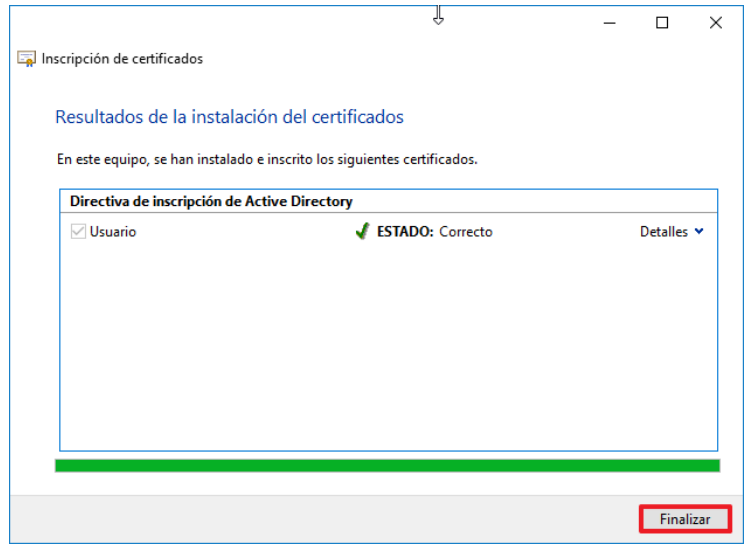
Cuando un certificado expira es posible renovarlo siempre que esté disponible la misma plantilla en el servidor de Entidad de Certificación. Los siguientes pasos recogen el procedimiento para que un cliente solicite un certificado de renovación del que ha expirado. El proceso es similar a la solicitud de un nuevo certificado con la salvedad de que no permitirá elegir otra plantilla que la escogida para la emisión del certificado anterior y que permitirá escoger entre renovar el certificado con clave nueva o utilizar la misma clave para el nuevo certificado.

| Paso | Descripción                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 139. | <p>Inicie sesión en el servidor que actúa como cliente solicitante del servidor Entidad de Certificación.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 140. | <p>Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador".</p>  |
| 141. | <p>El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí".</p>                                                                  |
| 142. | <p>Teclee "mmc" en la consola de comandos y pulse "Enter".</p>                                                                                                                                                                               |
| 143. | <p>En la consola seleccione "Archivo → Agregar o quitar complemento...".</p>                                                                                                                                                                 |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 144. | <p>Seleccione “Certificados” de la columna “Complementos disponibles” y pulse “Agregar &gt;”</p>                                                                                                                                                                                                                                                                                                    |
| 145. | <p>Según el tipo de certificado, se deberá seleccionar el tipo de cuenta de la que se quiere abrir la consola de certificados. Esta elección dependerá del tipo de certificado que se quiera solicitar. Pulse “Finalizar” para continuar.</p>  <p><b>Nota:</b> En el ejemplo se selecciona “Mi cuenta de usuario”, ya que se solicita un certificado de usuario de autenticación del cliente.</p> |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 146. | <p>Pulse “Aceptar” para abrir la consola de certificados y despliegue el menú en árbol situado a la izquierda hasta llegar al contenedor “<b>Personal</b>” mediante la siguiente ruta: “<b>Raíz de consola → Certificados: usuario actual → Personal</b>”.</p> <p>Pulse con el botón derecho del ratón sobre el certificado y seleccione “<b>Todas las tareas → Renovar certificado con clave nueva...</b>”.</p>  <p><b>Nota:</b> En caso de querer conservar la misma clave sería posible a través del menú superior, manteniendo seleccionado el certificado y haciendo clic sobre “<b>Acción → Todas las tareas → Operaciones avanzadas → Renovar certificado con la misma clave</b>”.</p>  |

| Paso | Descripción                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 147. | Se abrirá el “Asistente para la inscripción de certificados”. En la ventana inicial del asistente pulse “Siguiente”.                                                  |
| 148. | <p>En la ventana “Solicitar certificados” pulse el botón “Inscribir”.</p>           |
| 149. | <p>En “Resultados de la instalación del certificado” seleccione “Finalizar”.</p>  |

## 6. COPIA DE SEGURIDAD Y RESTAURACIÓN DE UNA ENTIDAD DE CERTIFICACIÓN

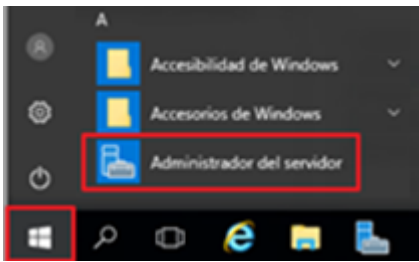
Con el objeto de prevenir que una corrupción de la base de datos o algún otro tipo incidencia relacionado con la información contenida en la Entidad de Certificación, que conlleve la pérdida del servicio se recomienda la realización de una copia de seguridad preventiva. Ésta se realizará tanto de la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

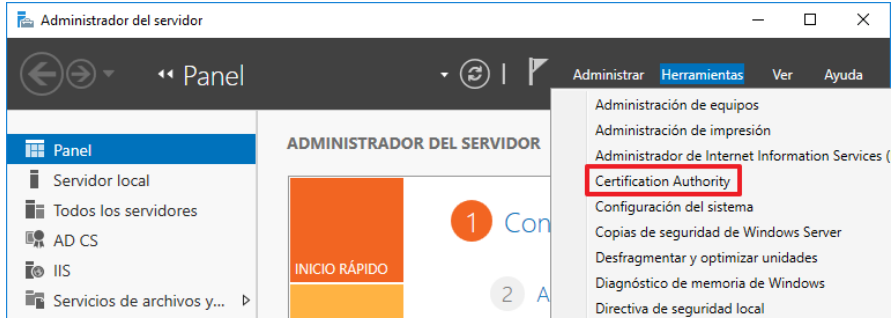
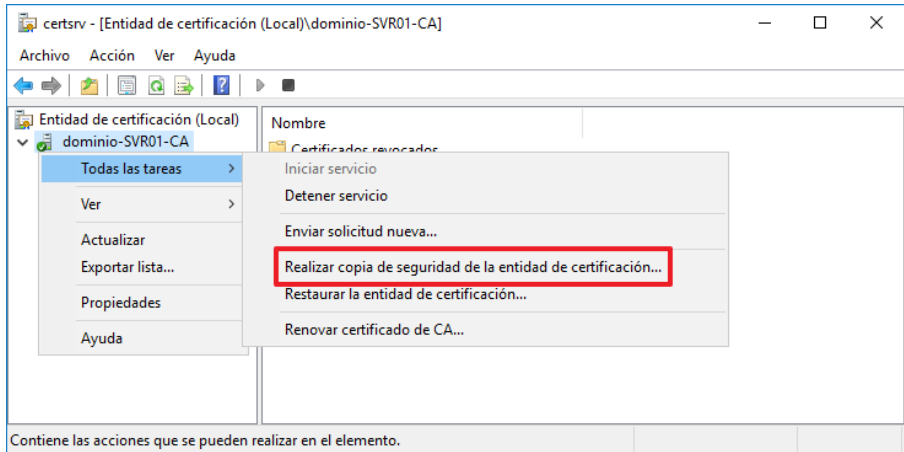
Los procedimientos operacionales del servicio permiten la recuperación tanto de la base de datos como del fichero de registro sobre el mismo servidor o sobre otro diferente. La sección siguiente describe el proceso para generar una copia de seguridad de la Entidad de Certificación, así como la restauración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

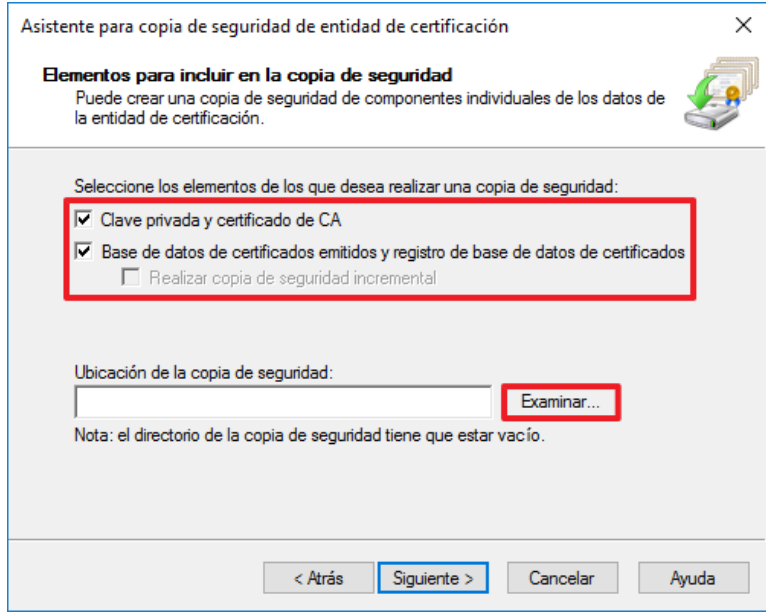
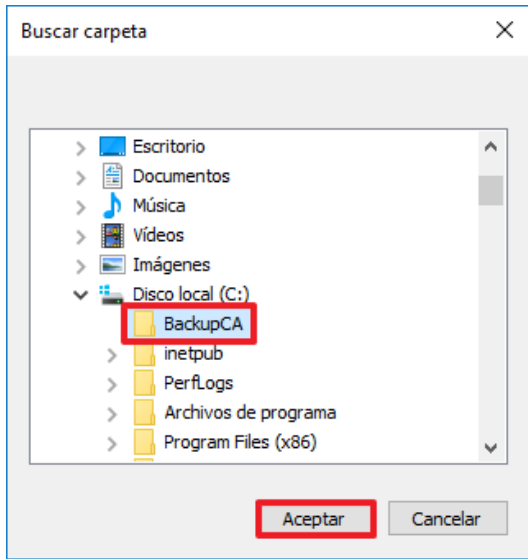
Estas copias de seguridad poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. Por ende, dichas copias de seguridad deberán estar cifradas para garantizar la confidencialidad de las claves utilizadas, y ser almacenadas en dispositivos externos cifrados salvaguardados en cajas blindadas.

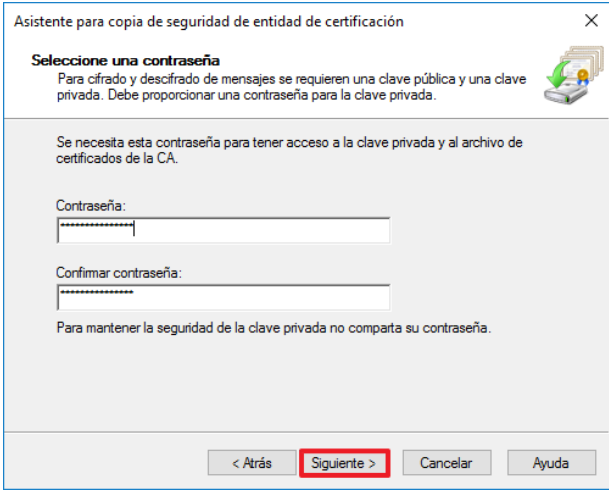
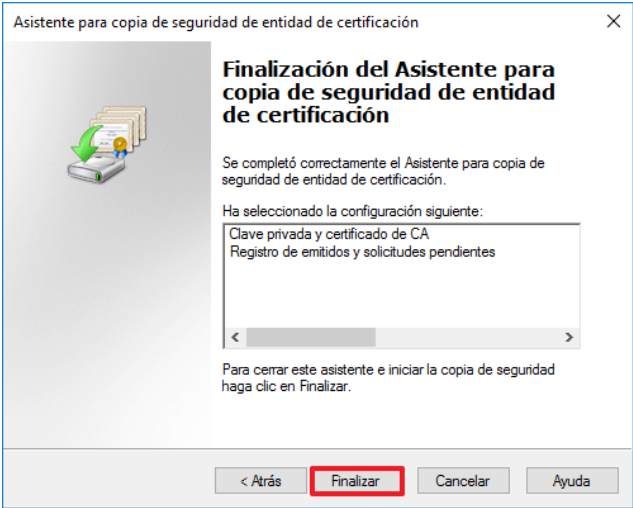
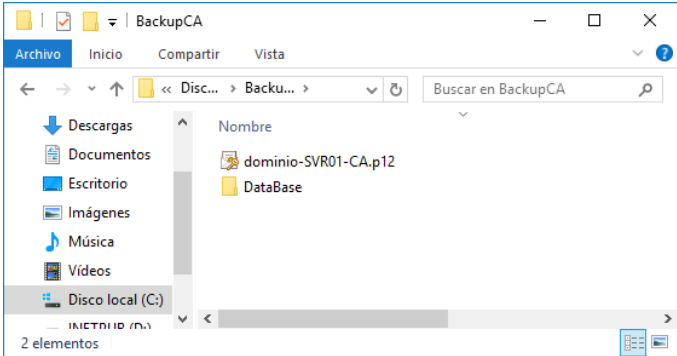
### 6.1. COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN

Esta sección recoge los pasos a seguir para realizar una copia de seguridad de una Entidad de Certificación y los pasos a seguir para restaurar desde dicha copia de seguridad. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma.

| Paso | Descripción                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 150. | <p>Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                 |
| 151. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 152. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                               |

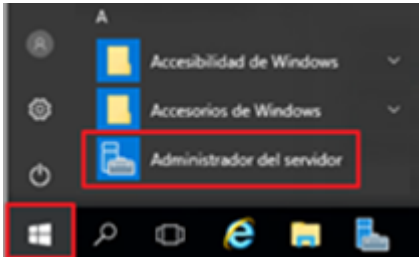
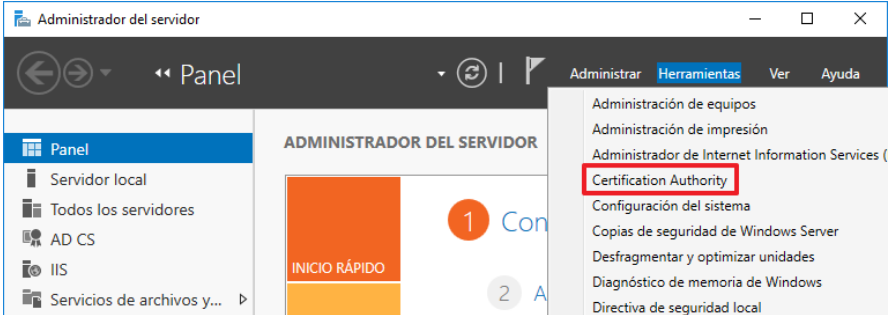
| Paso | Descripción                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 153. | <p>En el menú situado a la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                                              |
| 154. | <p>Pulse el botón derecho del ratón sobre la Entidad de Certificación y seleccione <b>“Todas las tareas → Realizar copia de seguridad de la Entidad de Certificación...”</b>.</p>  |
| 155. | <p>En el “Asistente para copia de seguridad de Entidad de Certificación” pulse “Siguiente &gt;” para continuar.</p>                                                                                                                                                   |

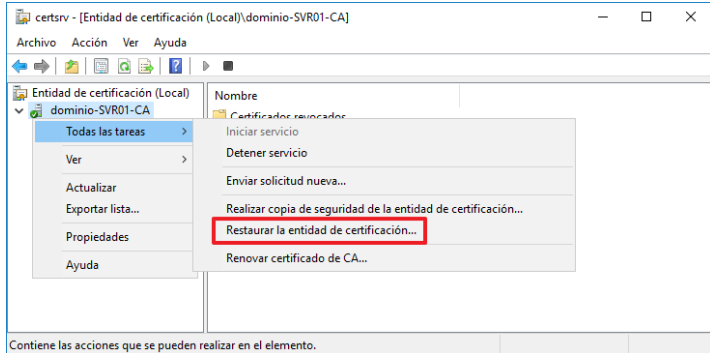
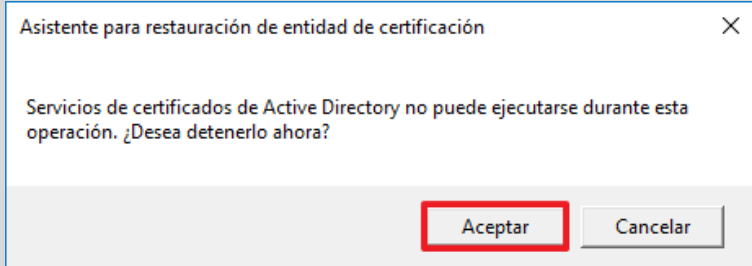
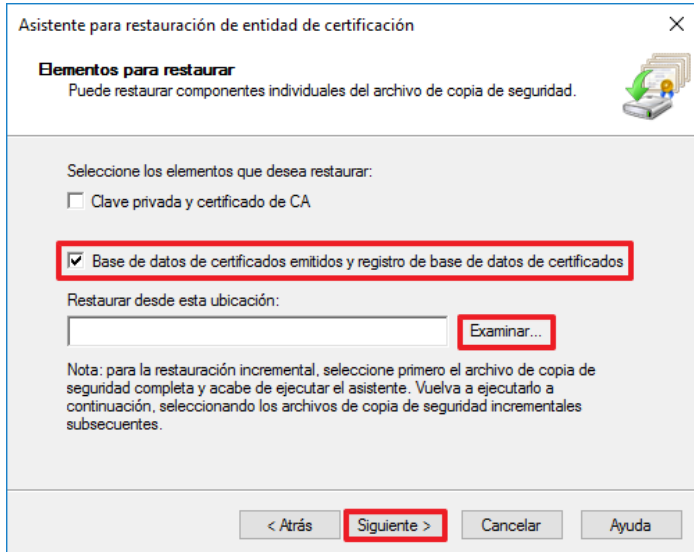
| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 156. | <p>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.</p>  <p><b>Nota:</b> En el ejemplo no es posible seleccionar una copia incremental de la base de datos porque no existe ninguna copia completa anterior.</p> |
| 157. | <p>Seleccione un directorio vacío para realizar la copia de seguridad y pulse “Aceptar”.</p>  <p><b>Nota:</b> En el ejemplo se ha utilizado “C:\BackupCA”</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 158. | <p>Pulse “Siguiente &gt;” para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

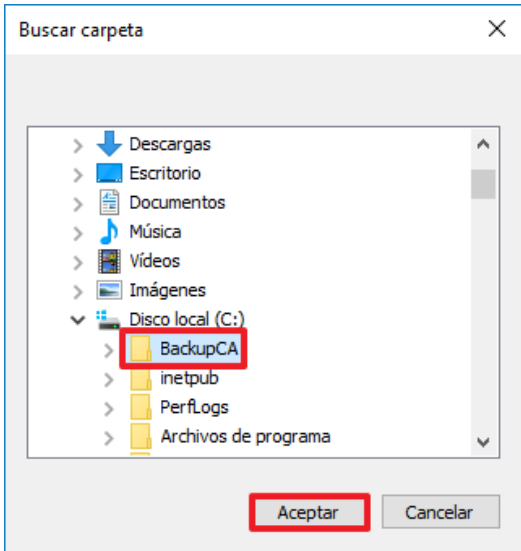
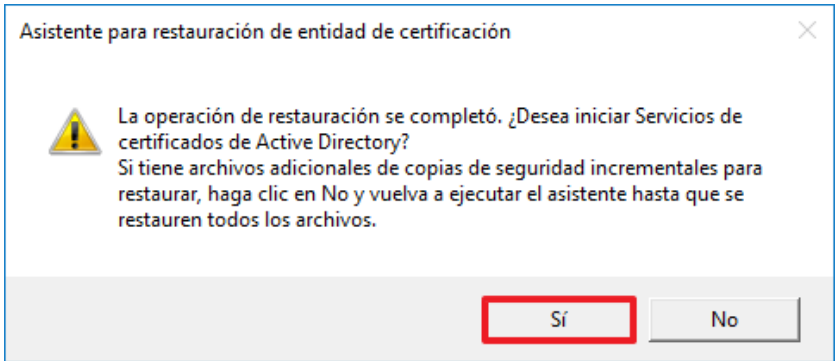
| Paso | Descripción                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 159. | <p>Establezca una contraseña escribiéndola por duplicado en los campos correspondientes y pulse “Siguiente &gt;”</p>  |
| 160. | <p>Pulse “Finalizar” para cerrar el asistente.</p>                                                                   |
| 161. | <p>En la carpeta podrá encontrar tanto el certificado de la CA como los ficheros de la base de datos.</p>           |

## 6.2. RESTAURACIÓN DE COPIA DE SEGURIDAD DE UNA ENTIDAD DE CERTIFICACIÓN

La siguiente tabla recoge los pasos a seguir para restaurar una copia de seguridad de una Entidad de Certificación. Estos pasos se realizarán a través de una Entidad de Certificación, independientemente del tipo de la misma.

| Paso | Descripción                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 162. | <p>Inicie sesión en la Entidad de Certificación sobre la que va a exportar el certificado.</p> <p><b>Nota:</b> Deberá iniciar sesión con una cuenta con privilegios de administración.</p>                                                |
| 163. | <p>Ejecute la consola administrativa “Certification Authority”. Para ello ejecute el “Administrador del servidor” desde el icono correspondiente.</p>  |
| 164. | <p>El “Control de cuentas de usuarios” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí”.</p>                                                              |
| 165. | <p>En el menú situado a la derecha, haga clic sobre “Herramientas” y pulse sobre “Certification Authority” en el menú desplegable.</p>                |

| Paso | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 166. | <p>Pulse el botón derecho del ratón sobre la Entidad de Certificación y seleccione <b>“Todas las tareas → Restaurar la Entidad de Certificación...”</b>.</p>  <p><b>Nota:</b> Si el servicio de Entidad de Certificación está en funcionamiento, se le solicitará detenerlo. En este caso pulse <b>“Aceptar”</b> para permitir al sistema detener el servicio de Entidad de Certificación de Directorio Activo.</p>  |
| 167. | <p>En el <b>“Asistente para copia de seguridad de Entidad de Certificación”</b> pulse <b>“Siguiente &gt;”</b> para continuar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 168. | <p>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 <b>“Base de datos de certificados emitidos y registro de base de datos de certificados”</b>. Pulse <b>“Examinar”</b> para continuar.</p>                                                                                                                                                                         |

| Paso | Descripción                                                                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 169. | <p>Localice la carpeta que contiene la base de datos y pulse “Aceptar”.</p>  <p><b>Nota:</b> En el ejemplo se ha utilizado “C:\BackupCA”</p> |
| 170. | Pulse “Siguiente >” para continuar.                                                                                                                                                                                            |
| 171. | Pulse “Finalizar” para cerrar el asistente.                                                                                                                                                                                    |
| 172. | <p>Ante el mensaje que indica que la operación se completó y que se iniciará el servicio de nuevo pulse “Sí”.</p>                          |