CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 573

IMPLEMENTACIÓN DEL ENS EN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.11.29 15:32:52 +01'00'

NIPO: 083-19-035-6
Fecha de Edición: noviembre de 2018

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

PRÓLOGO

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

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

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

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

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

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

noviembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE UN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD EN UN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN SERVIDOR DE FICHEROS

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación del Servidor de ficheros 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 usó 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 Servidor de ficheros 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 el Servidor de ficheros, 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 (ficheros, directorios y recursos compartidos) 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 determinar aquellos recursos que serán compartidos y cuáles serán accesibles para los usuarios.

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.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj134043(v=ws.11)

https://docs.microsoft.com/es-es/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview

https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control

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.

Así mismo es interesante que los usuarios que pertenezcan a los grupos que administran el Servidor de ficheros sean usuarios que no pertenezcan al grupo de administradores del dominio ni sean cuentas locales de administración.

Además, deben añadirse varias cuentas para administrar el Servidor de ficheros y sus recursos (mínimo dos) para evitar que toda la responsabilidad recaiga sobre una sola cuenta.

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 el Servidor de ficheros 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 de interés, no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.

Para el cumplimiento de 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.

Se establecerán mecanismos de cuota de disco para evitar el uso de los recursos que ofrece el Servidor de ficheros a los usuarios, al mismo tiempo que se filtran los archivos que se pueden alojar en el mismo, con el objetivo de prevenir código dañino, exceso de ficheros, etc.

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.

El Servidor de ficheros, 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 auditoria desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

Adicionalmente el Servidor de ficheros dispone de mecanismo que permiten emitir informes sobre todo aquello que se almacena, modifica o elimina en él pudiendo realizar seguimientos y acciones correspondientes.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN WINDOWS SERVER 2016 COMO SERVIDOR DE FICHEROS

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-573, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-573, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-573, adaptándolos a la organización.
OP. EXP. 2	Configuración de seguridad	Implementación de GPO a través de plantillas facilitadas en la presente guía. Configuraciones adicionales de seguridad descritas a través de la presente guía.
OP. EXP. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-573, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-573, adaptándolos a la organización. Revisión e implementación de guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

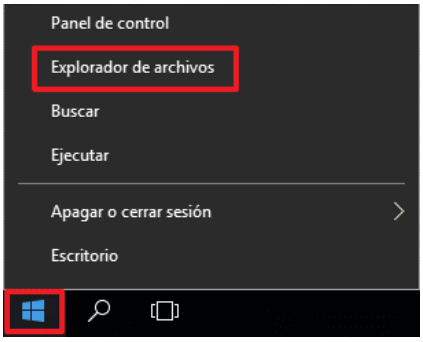
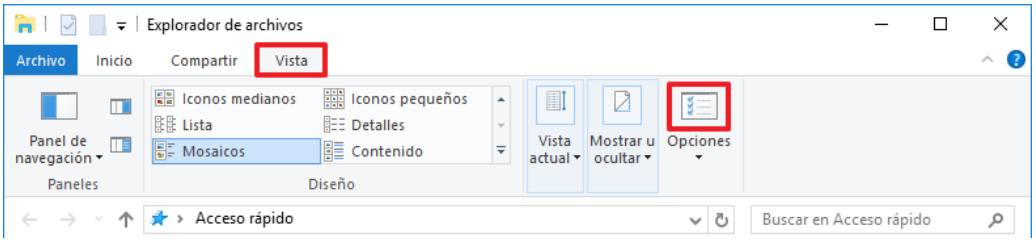
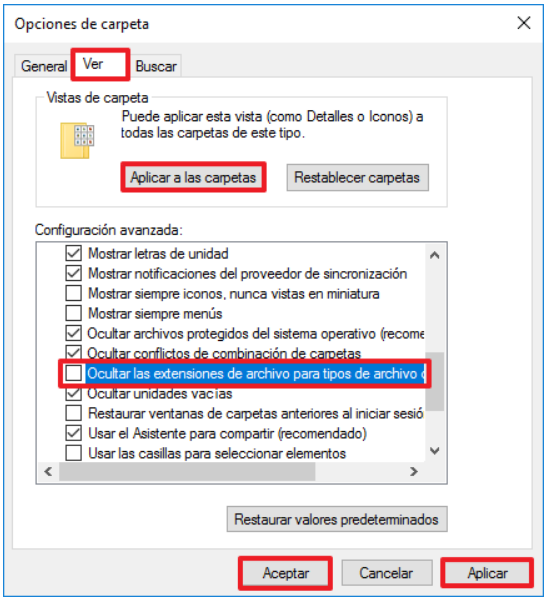
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen Servidores de ficheros con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría 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.

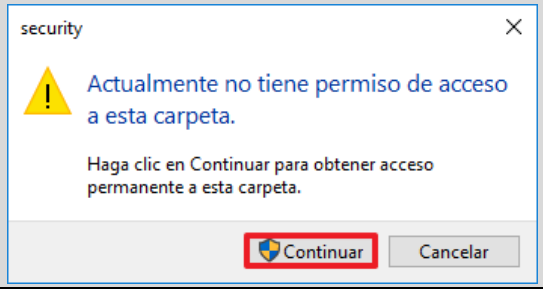
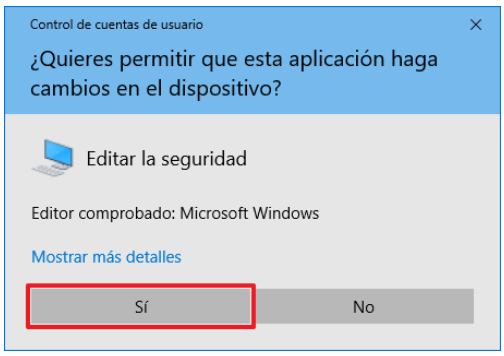
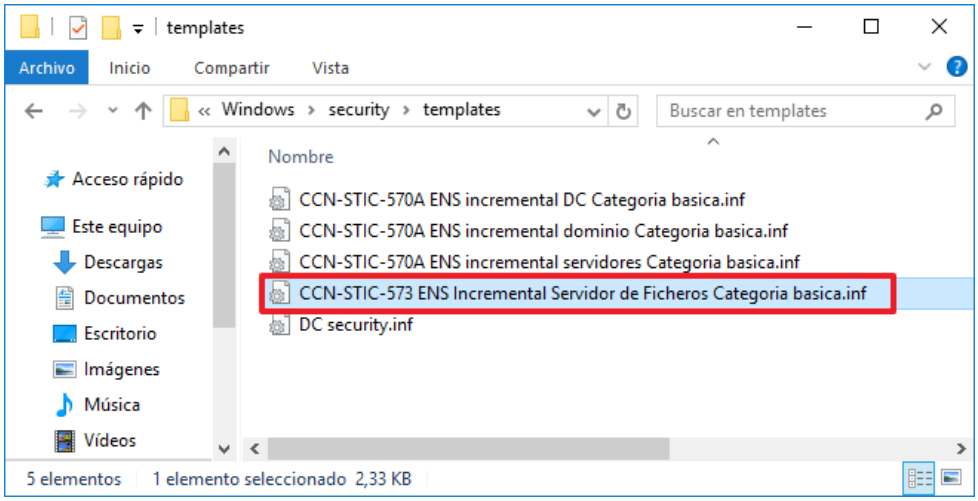
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

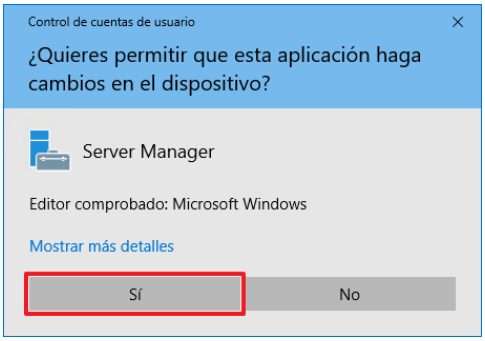
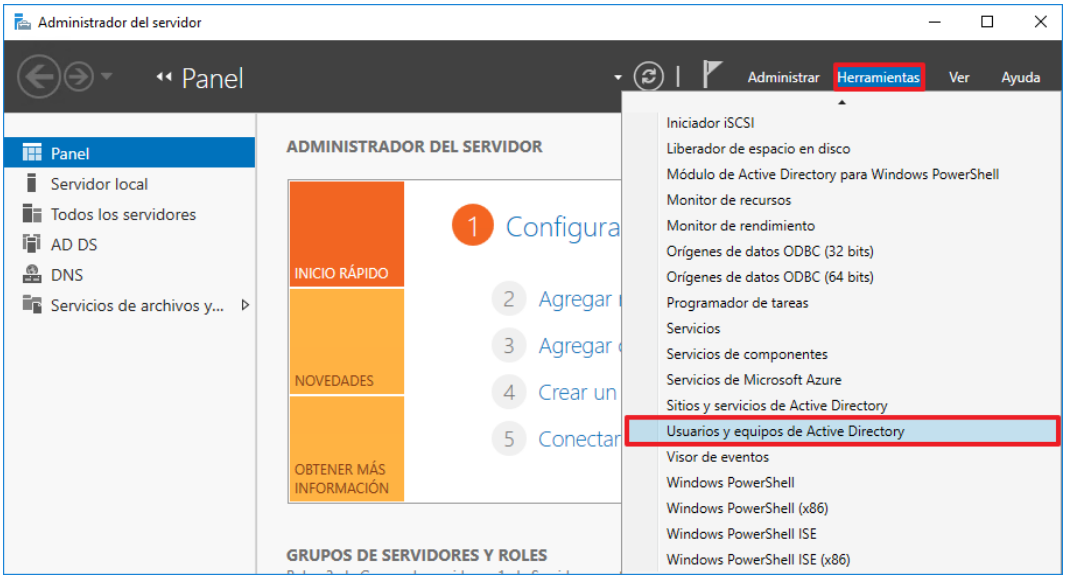
1. PREPARACIÓN DEL DOMINIO

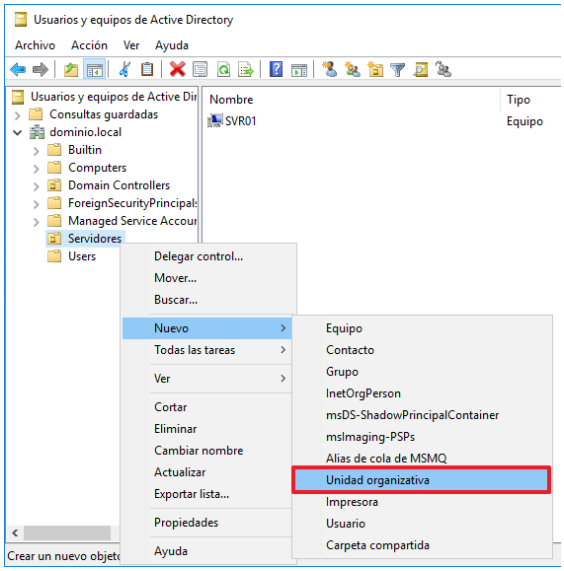
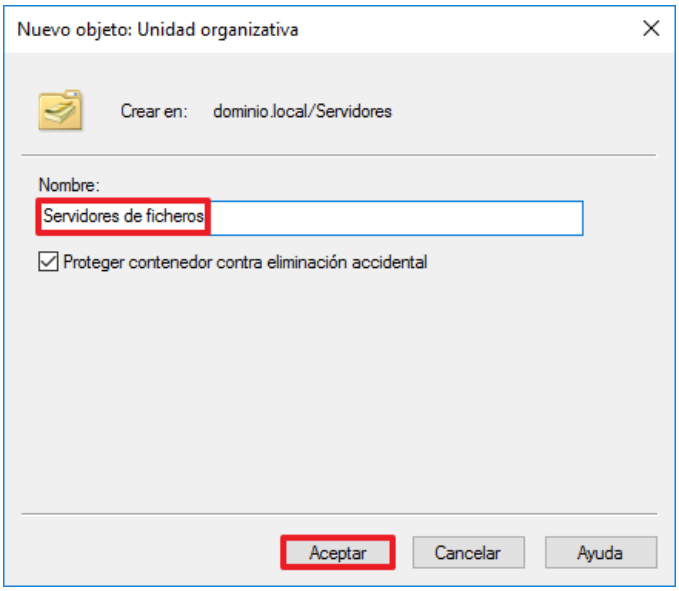
Los pasos que se describen a continuación se realizarán sobre un equipo Controlador de Dominio del dominio al que va a pertenecer el Servidor de ficheros que se está asegurando.

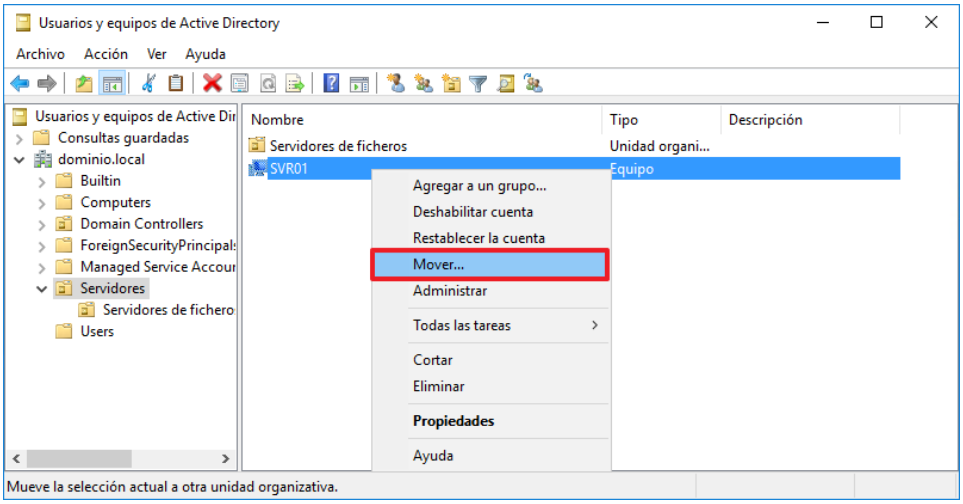
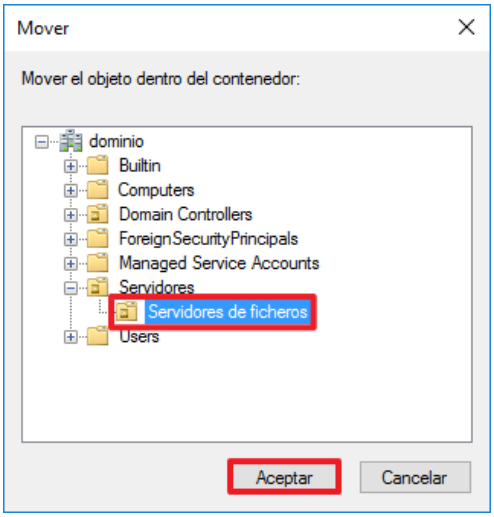
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

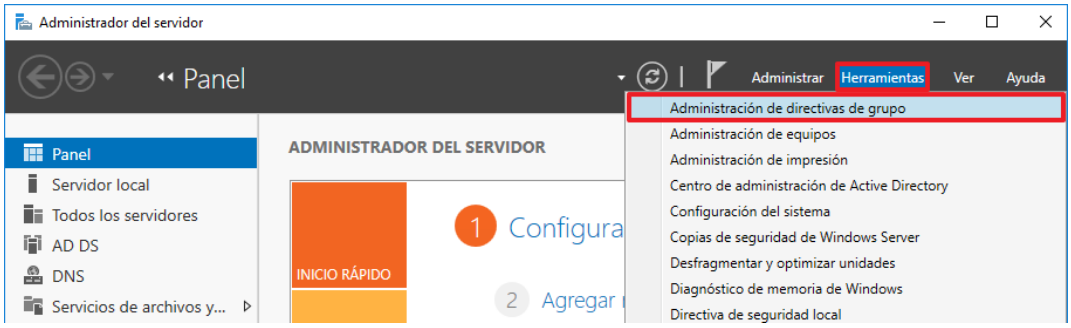
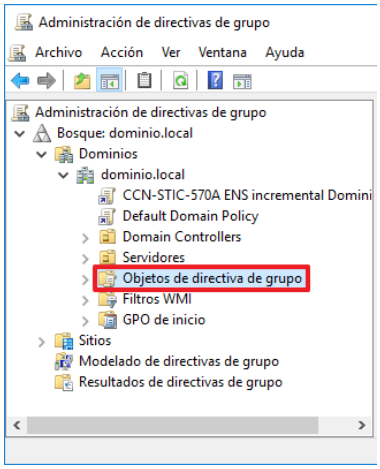
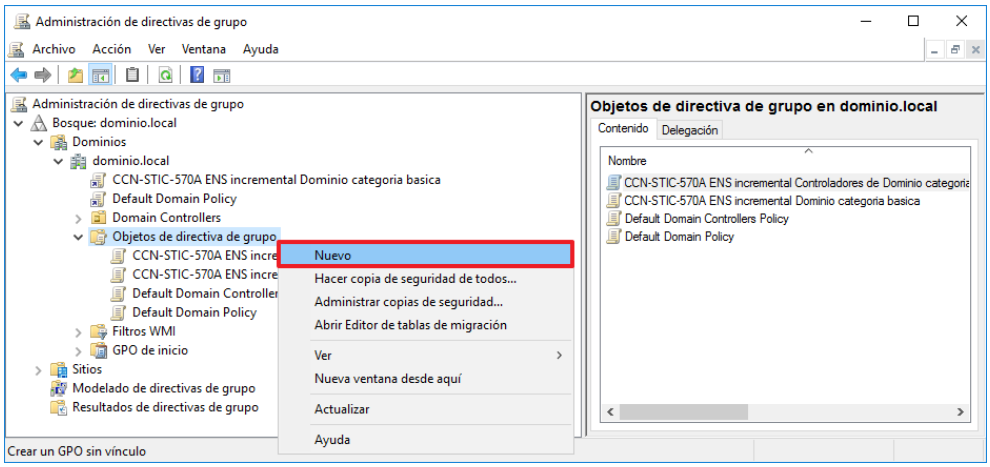
Paso	Descripción
4.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
6.	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”. 

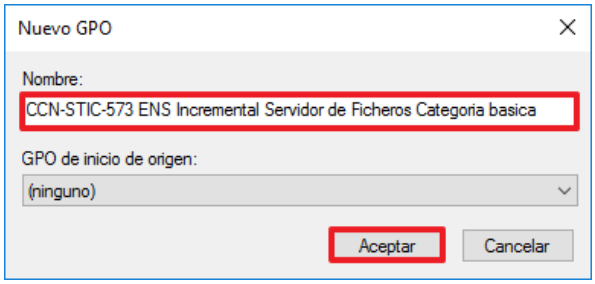
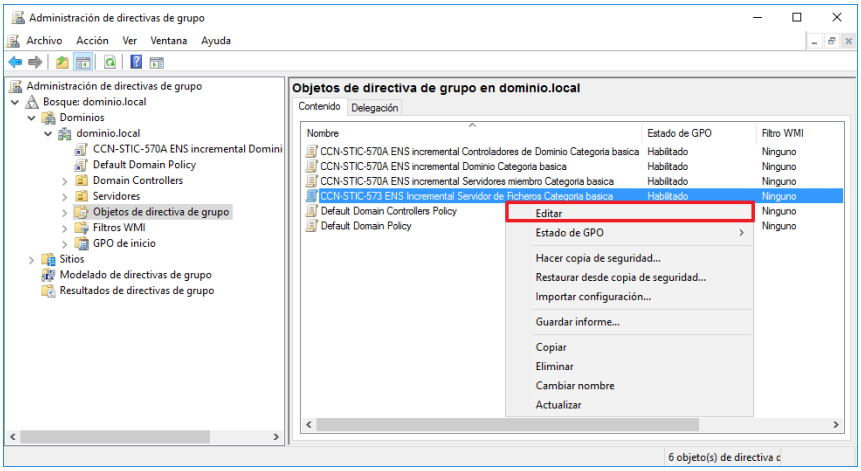
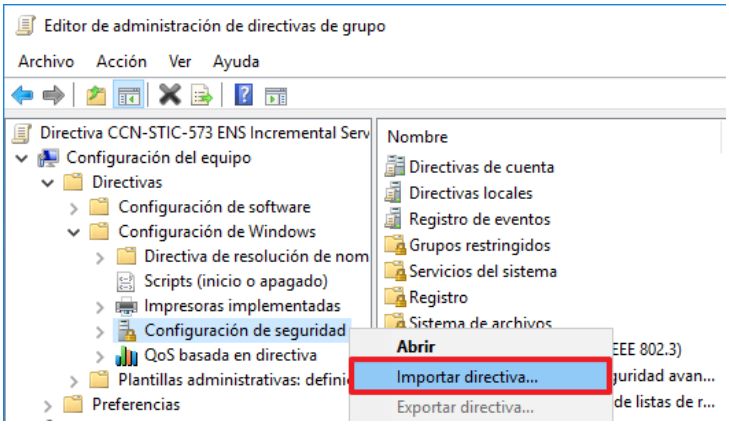
Paso	Descripción
7.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 
8.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
9.	Copie el fichero “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
10.	A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 

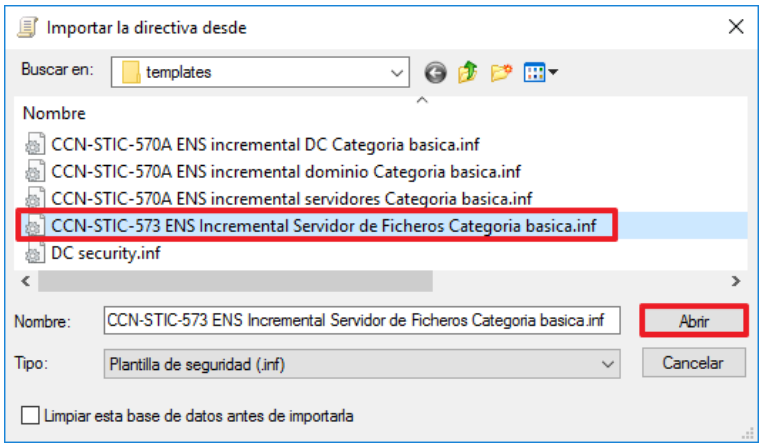
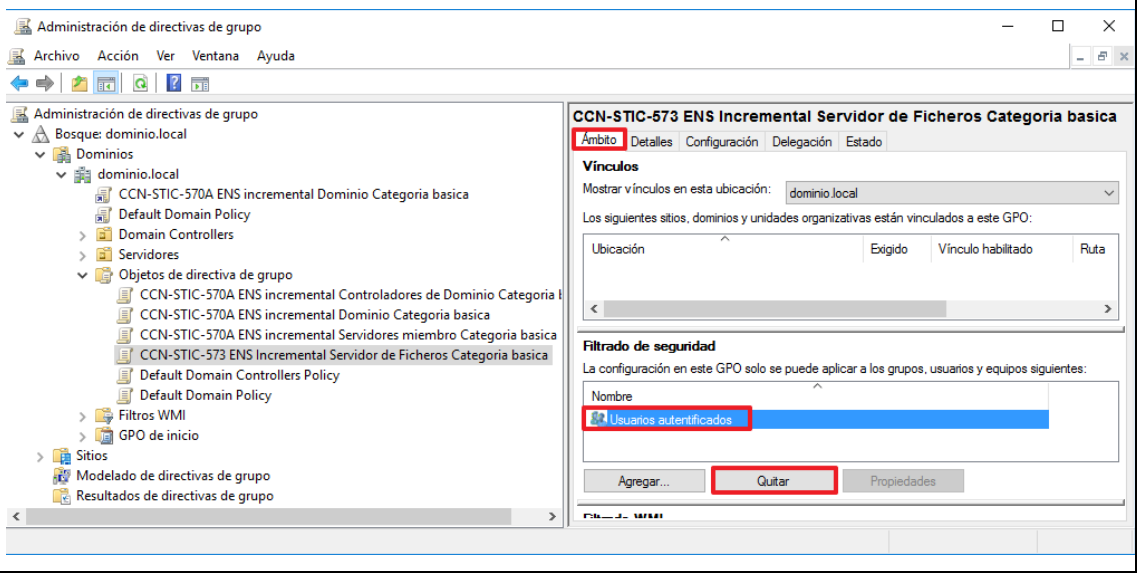
Paso	Descripción
11.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
12.	A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor”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

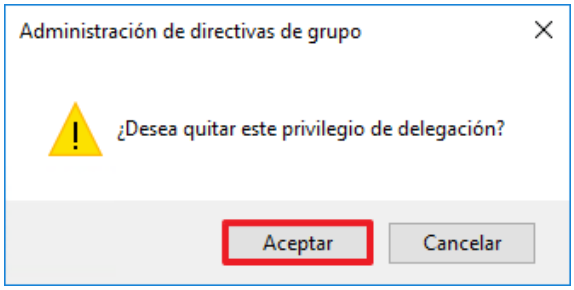
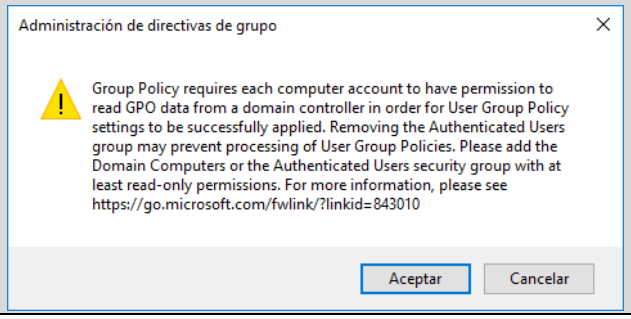
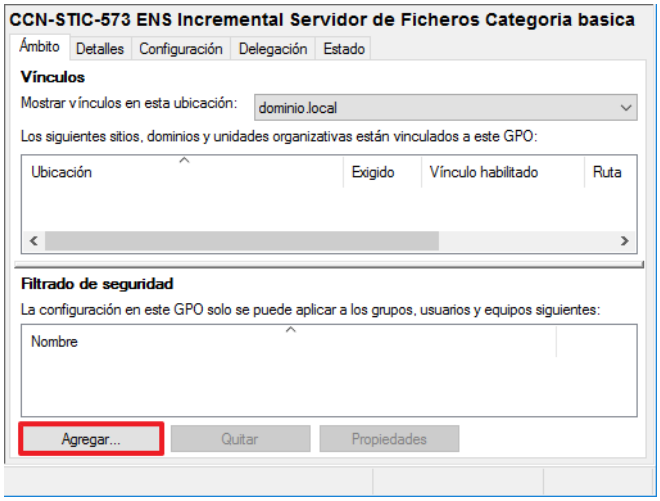
Paso	Descripción
13.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> →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

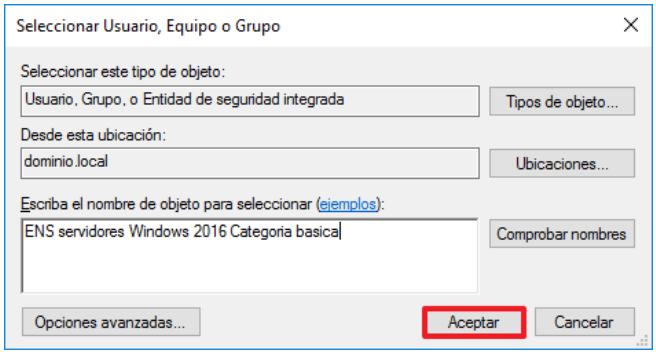
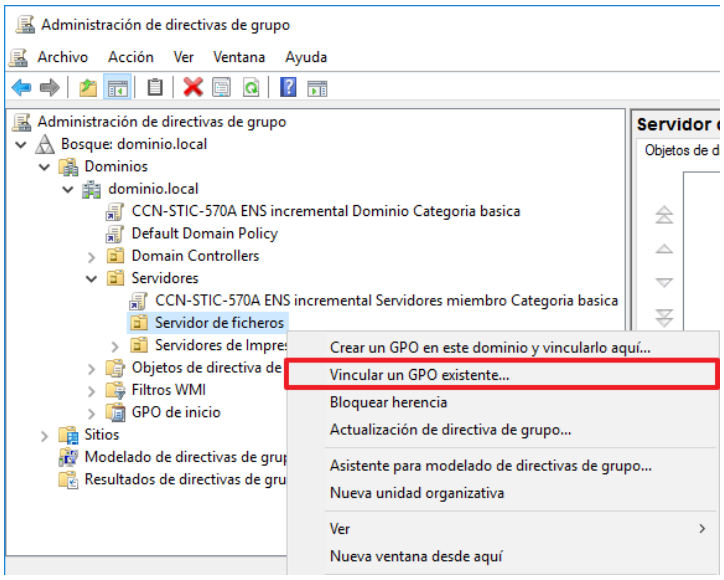
Paso	Descripción
15.	Una vez creada la nueva unidad organizativa, deberá mover los servidores de ficheros a la unidad organizativa “Servidores de ficheros”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva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

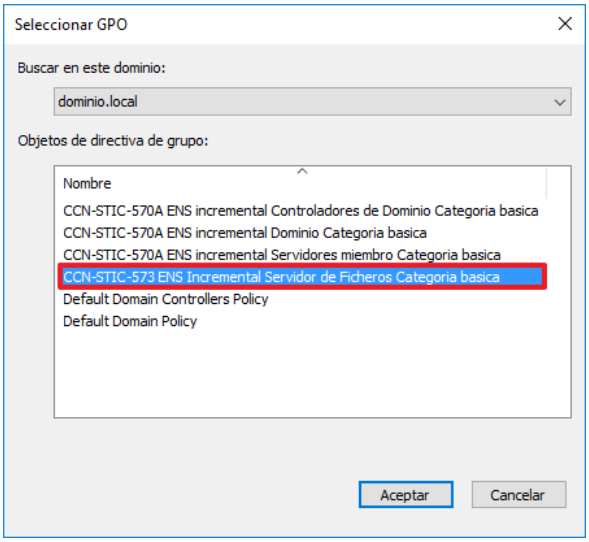
Paso	Descripción
19.	Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón “Herramientas > Administración de directivas de grupo”. 
20.	Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en **“Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”**. 
21.	Pulse con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción del menú contextual “Nuevo”. 

Paso	Descripción
22.	Establezca para la nueva GPO el nombre “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoría básica” y pulse “Aceptar”. 
23.	A continuación, pulse con el botón derecho sobre la GPO recién creada y seleccione la opción del menú contextual “Editar”. 
24.	Ubíquese sobre el nodo **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción del menú contextual “Importar directiva…”. 

Paso	Descripción
26.	Seleccione la plantilla de seguridad “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica.inf” ubicada en “C:\Windows\Security\Templates”. Pulse sobre el botón “Abrir” para continuar. 
27.	Cierre el “Editor de administración de directivas de grupo”.
28.	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 autentificados”. Pulse sobre el botón “Quitar”. 

Paso	Descripción
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.  **Nota:** Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”. 
30.	A continuación, pulse sobre el botón “Agregar…”. 

Paso	Descripción
31.	Agregue los grupos de usuarios que contengan los equipos con el rol “Servidor de ficheros” y pulse “Aceptar” para finalizar.  **Nota:** Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria basica” que contiene el servidor con el rol “Servidor de ficheros”.
32.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de ficheros”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de ficheros”.
33.	Seleccione con el botón derecho la unidad organizativa y pulse sobre la opción del menú contextual “Vincular GPO existente…”. 

Paso	Descripción
34.	A continuación, localice la GPO configurada anteriormente, "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoría básica", y pulse "Aceptar". 
35.	Cierre la consola "Administración de directivas de grupo" y elimine la carpeta "C:\Scripts".

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

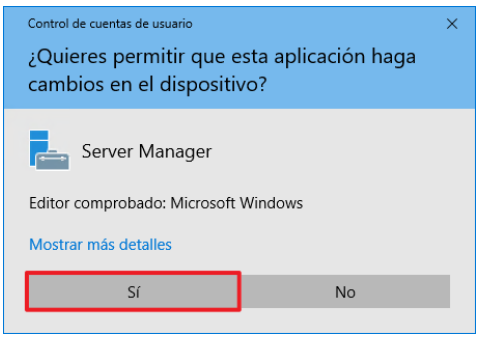
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, 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.

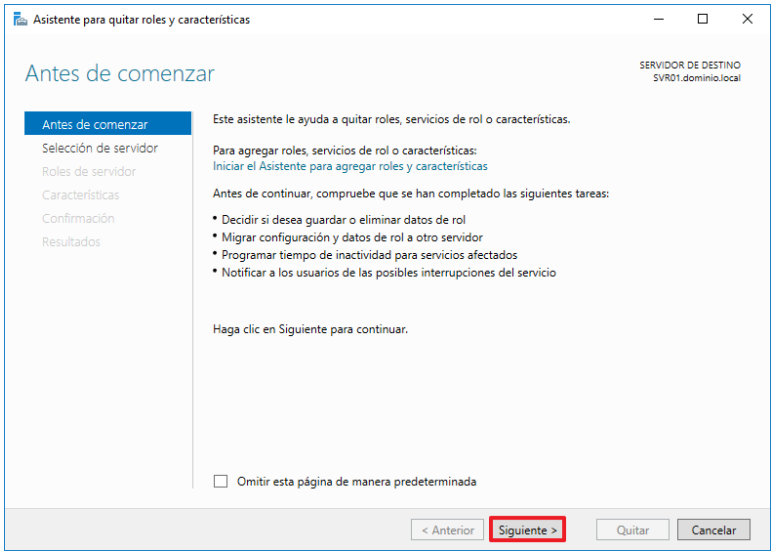
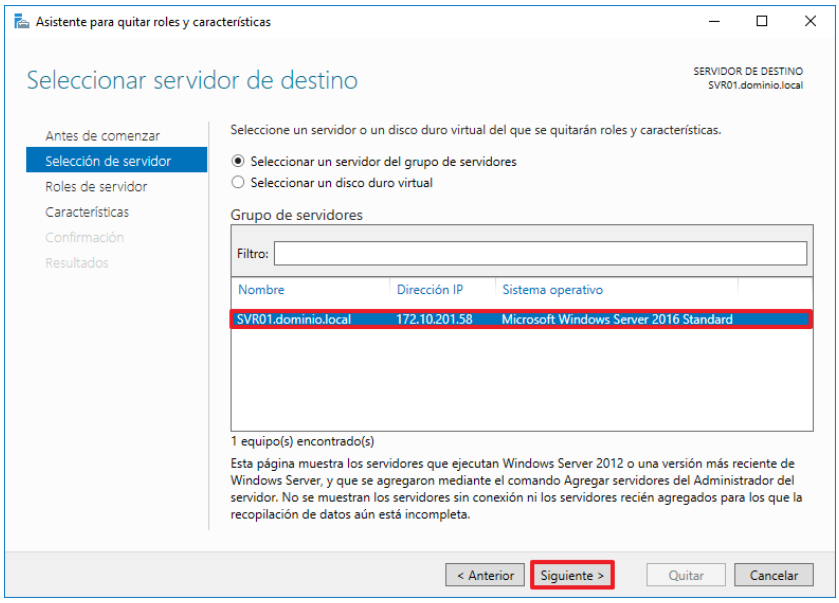
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

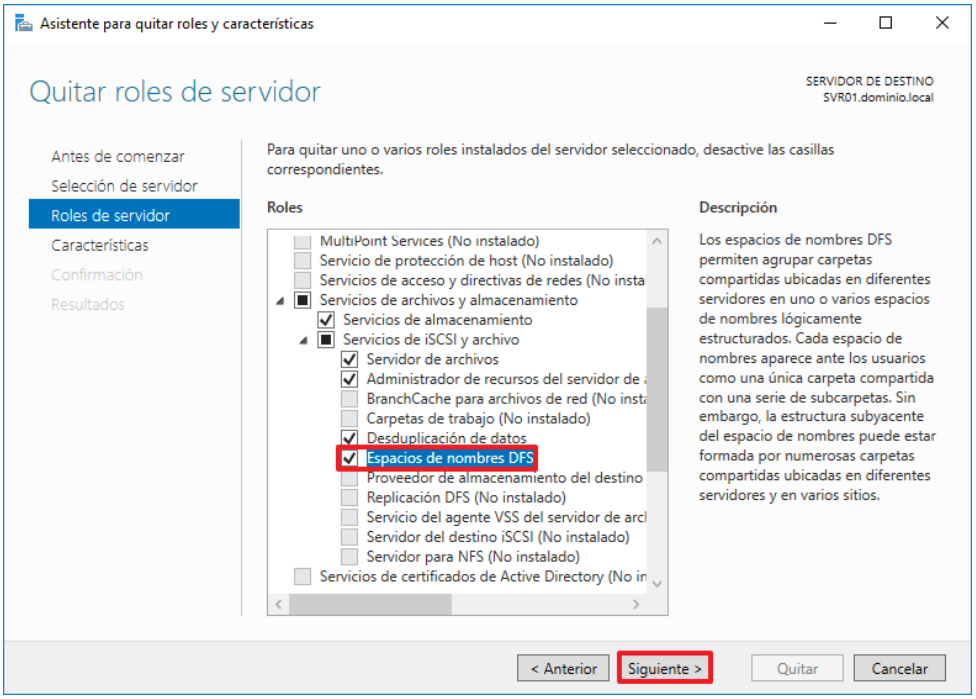
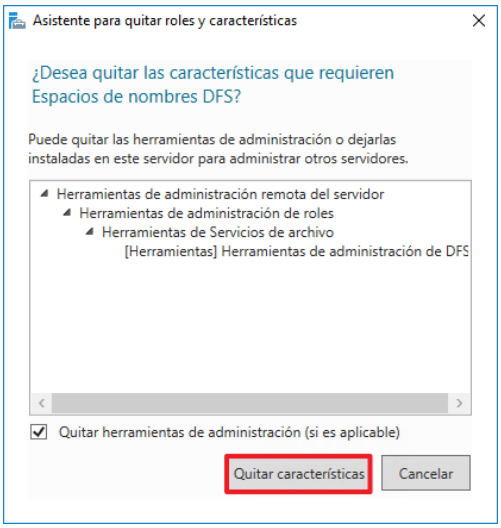
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

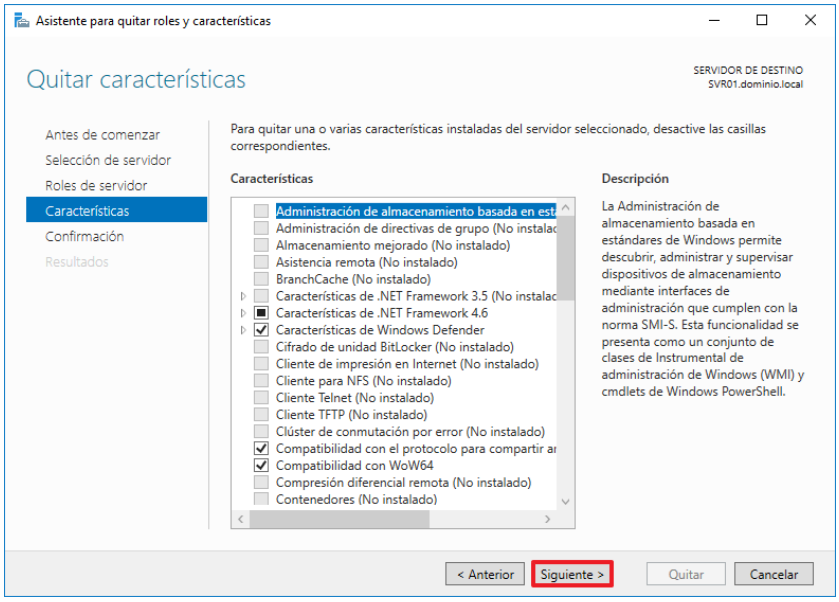
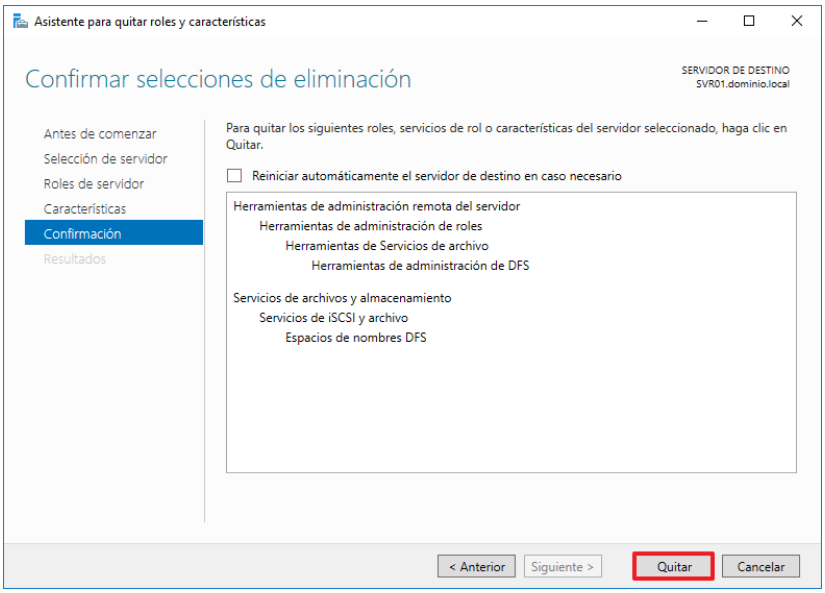
Uno de los aspectos que marca el ENS, desde su requisito de la categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

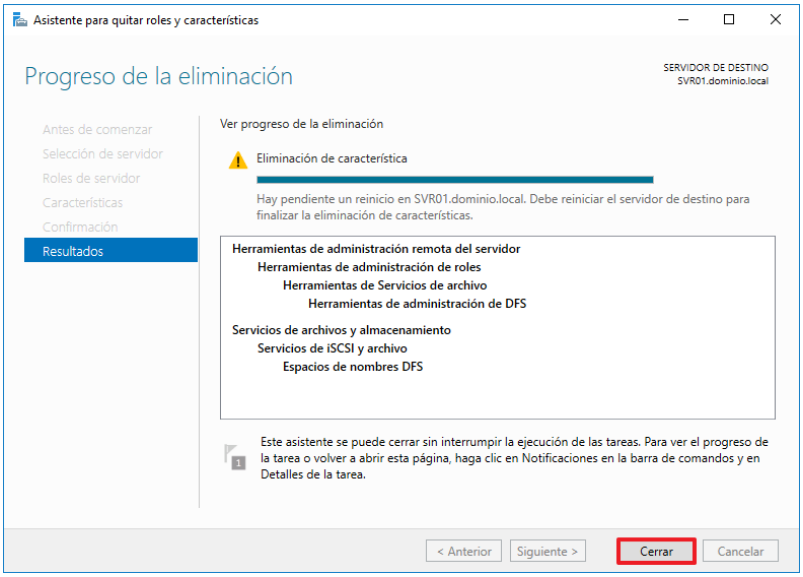
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de ficheros.

Paso	Descripción
36.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.
37.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
38.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
39.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Quitar roles y funciones". 

Paso	Descripción
40.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
41.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

Paso	Descripción
42.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Espacios de nombres DFS”.
43.	En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.  **Nota:** En este ejemplo se eliminan las características que dependen del rol.

Paso	Descripción
44.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
45.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

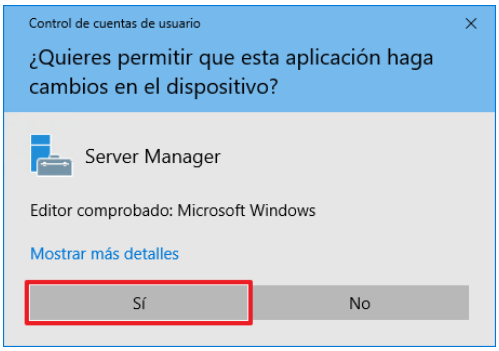
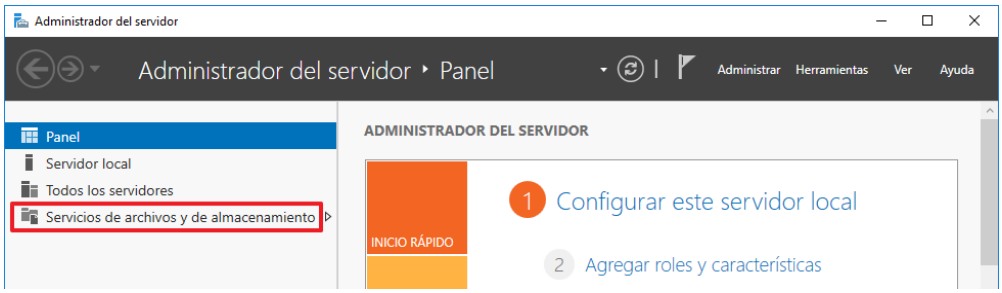
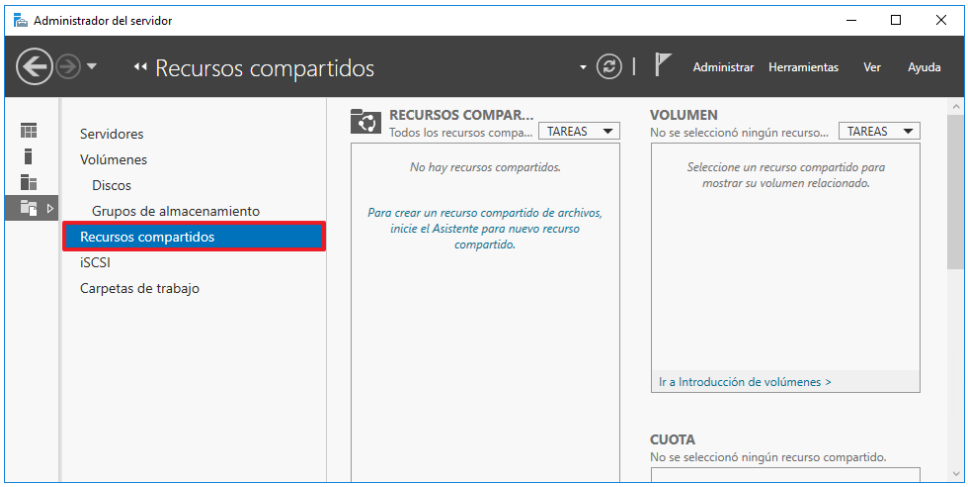
Paso	Descripción
46.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar. 
47.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.

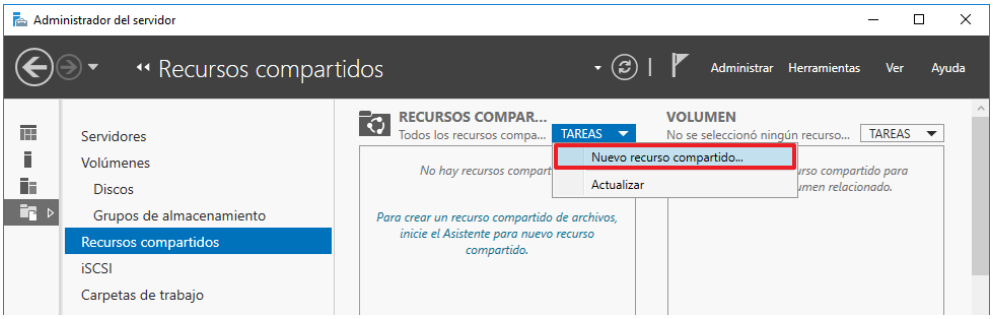
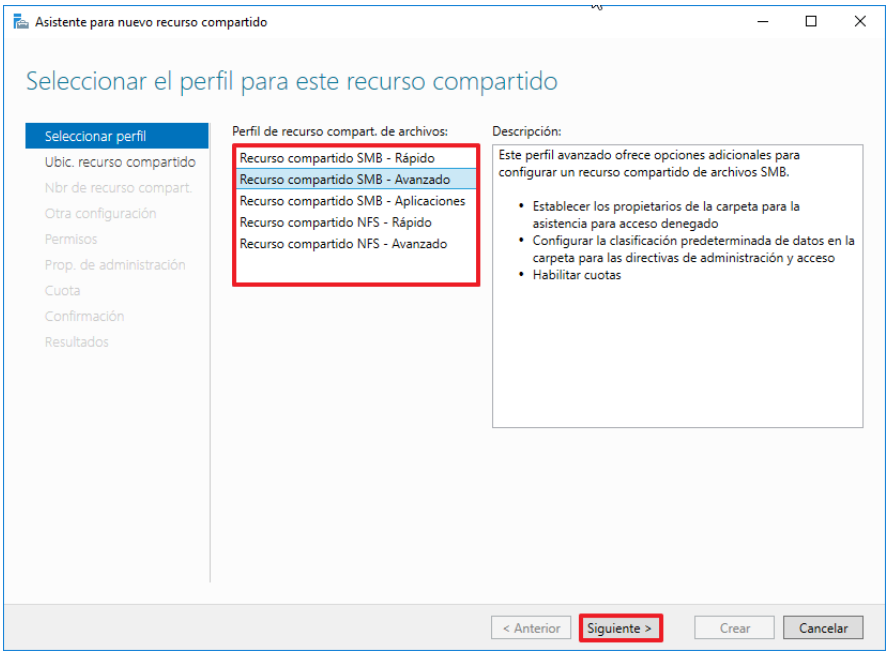
2.2. COMPARTICIÓN DE RECURSOS

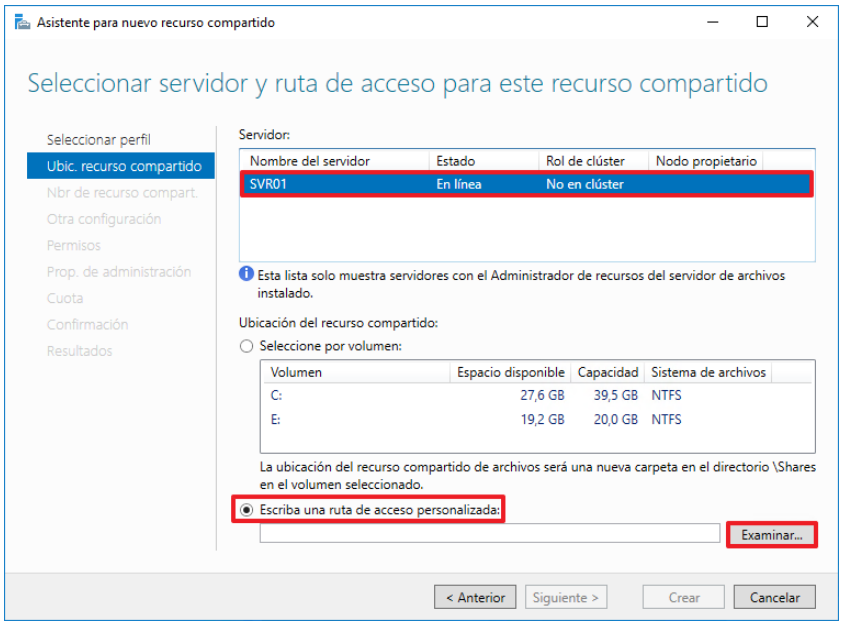
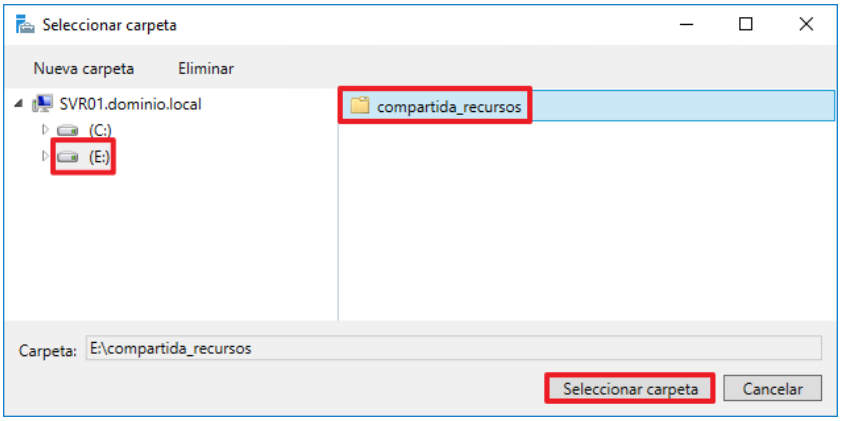
Es importante determinar que recursos se comparten en el Servidor de ficheros. Dependiendo de que recursos se compartan pueden generarse accesos indeseados, es por ello que tal y como indica el ENS es recomendable que los recursos que se comparten en el Servidor de ficheros estén alojados en otra ubicación de disco diferente a la del sistema operativo y que ésta solo se utilice para el alojamiento de recursos, evitando con ello exponer más información de la estrictamente necesaria.

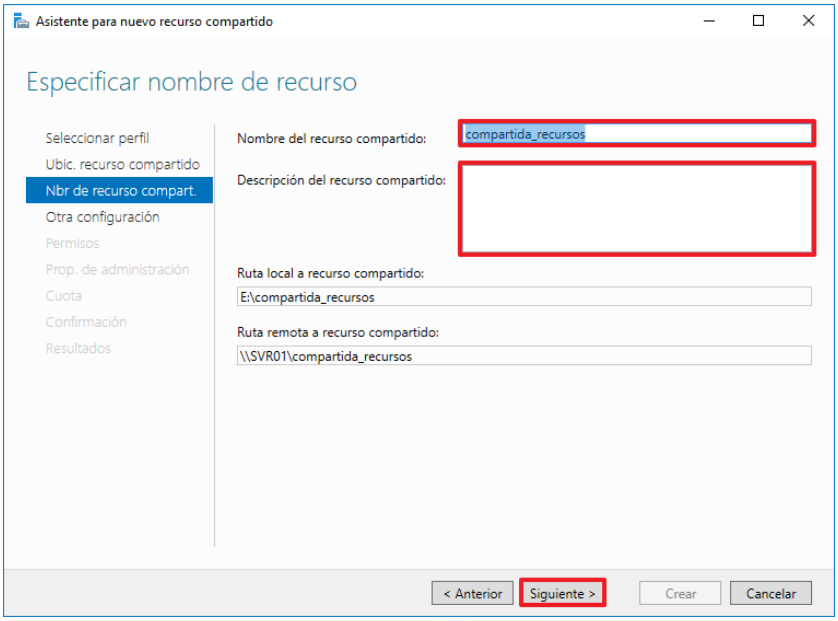
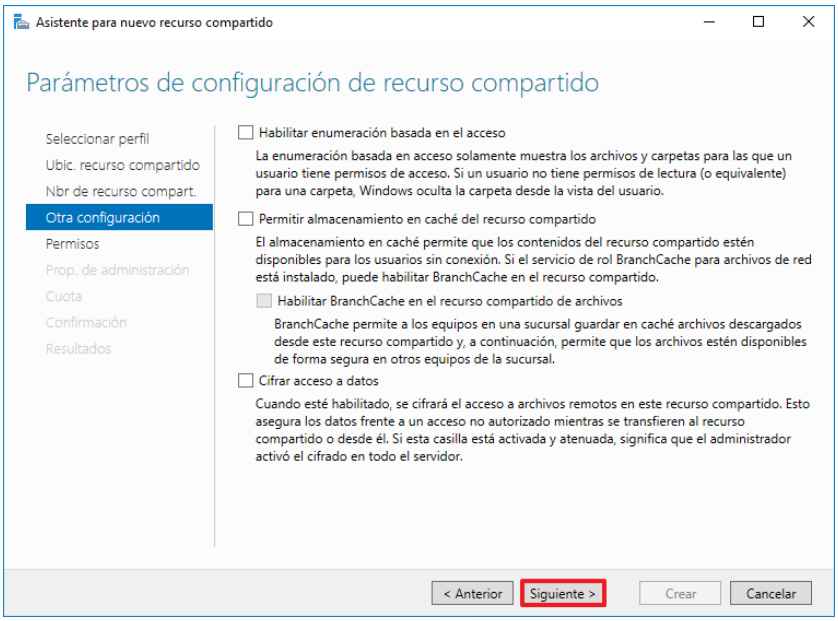
En este apartado se determinará la gestión de los recursos que son compartidos a través del Servidor de ficheros.

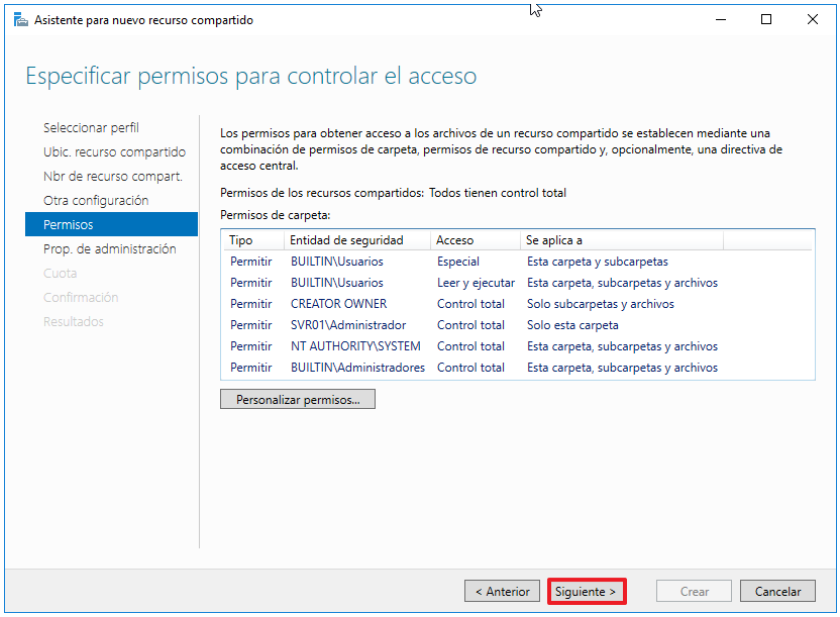
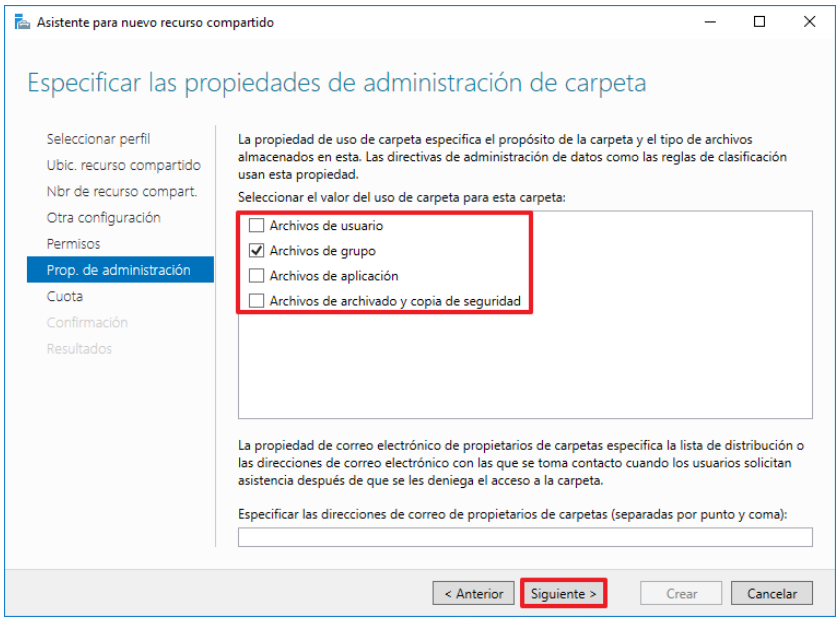
Paso	Descripción
48.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros. 

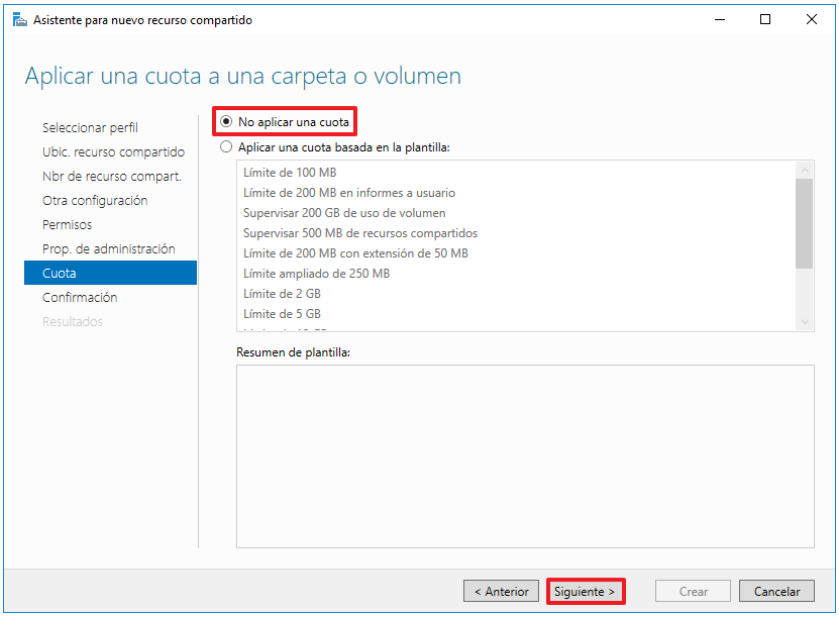
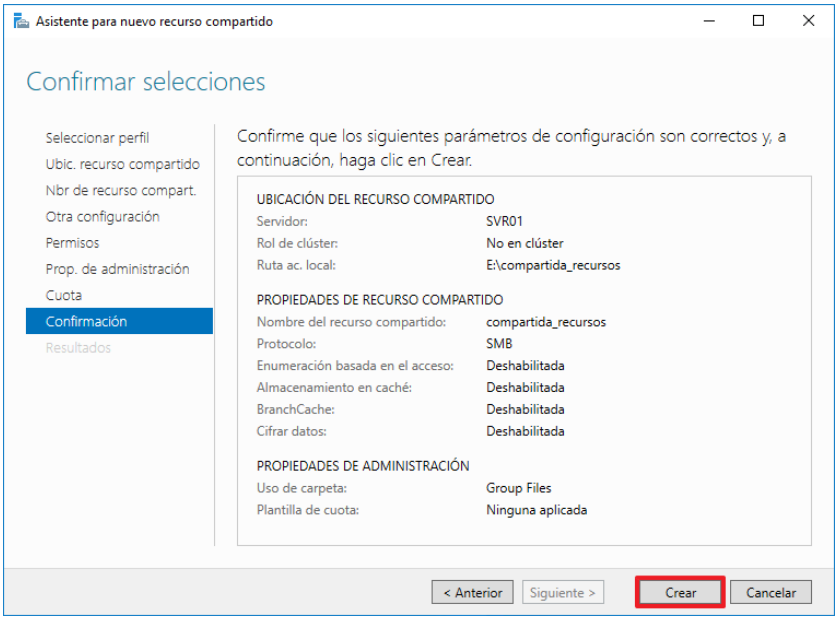
Paso	Descripción
49.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
50.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
51.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
52.	Seleccione la sección “Recursos compartidos”. 

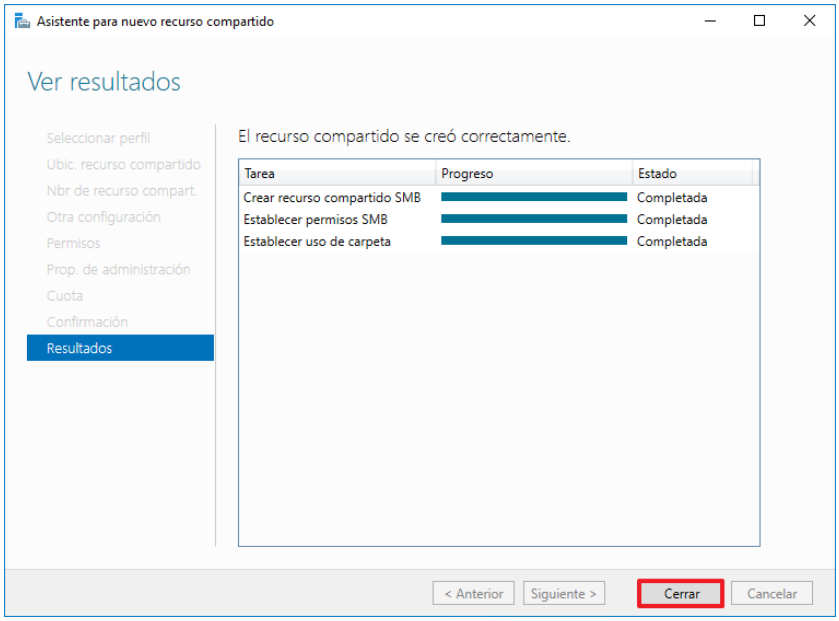
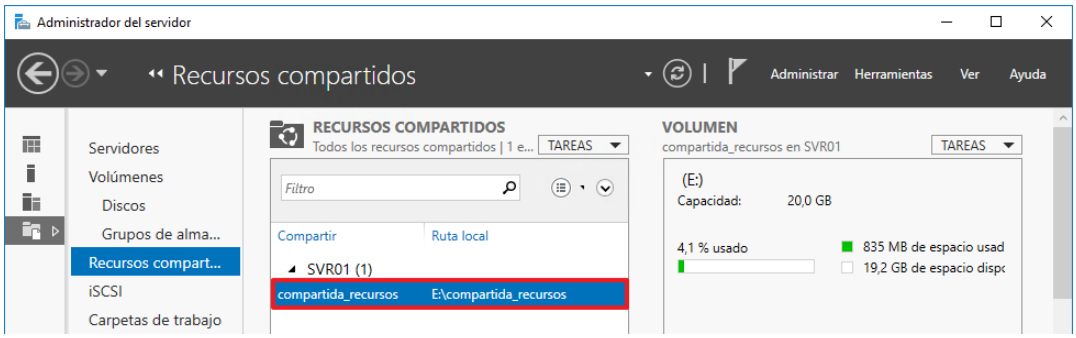
Paso	Descripción
53.	En el apartado “Recursos compartidos” pulse sobre el desplegable “TAREAS” y seleccione la opción “Nuevo recurso compartido…”. 
54.	Se iniciará el asistente para añadir un nuevo recurso compartido. En el apartado “Seleccionar perfil” seleccione un perfil de recurso compartido de archivos y pulse “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la opción “Recurso compartido SMB – Avanzado”.

Paso	Descripción
55.	Seleccione el servidor sobre el que desea crear el recurso compartido. A continuación seleccione la opción “Escriba una ruta de acceso personalizada:” y pulse sobre el botón “Examinar…”. 
56.	Ante la ventana emergente navegue y seleccione el recurso que desea compartir. Pulse sobre “Seleccionar carpeta” para continuar.  **Nota:** Para este ejemplo se comparte un directorio creado previamente denominado “compartida_recursos” en una ubicación dedicada a recursos compartidos denominada “Datos (E:)”. Ajuste esta configuración a las necesidades de su organización.
57.	A continuación, pulse sobre “Siguiente >” para continuar con el asistente.

Paso	Descripción
58.	En el apartado “Nbr. De recurso compart.” Establezca un nombre para el recurso y una descripción del mismo si lo desea. Pulse sobre “Siguiente >”.  **Nota:** En este ejemplo se mantiene el nombre del recurso seleccionado en el apartado anterior del asistente.
59.	En el apartado “Otra configuración” seleccione los parametros de configuración de recurso compartido que precise y pulse “Siguiente >”.  **Nota:** Para este ejemplo no se ha seleccionado ninguna configuración adicional.

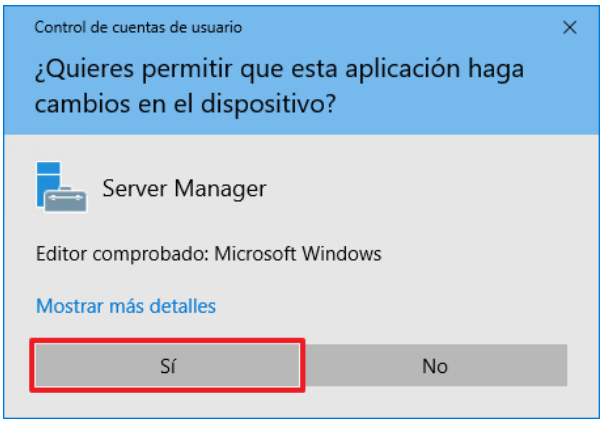
Paso	Descripción
60.	Pulse “Siguiente >” en el apartado “Permisos”.  **Nota:** Los permisos de acceso a los archivos del recurso compartido se configurarán posteriormente.
61.	Seleccione en el apartado “Prop. De administración” una categorización para el recurso compartido si lo desea y pulse el botón “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la categorización “Archivos de grupo”. Adapte esta configuración a su entorno.

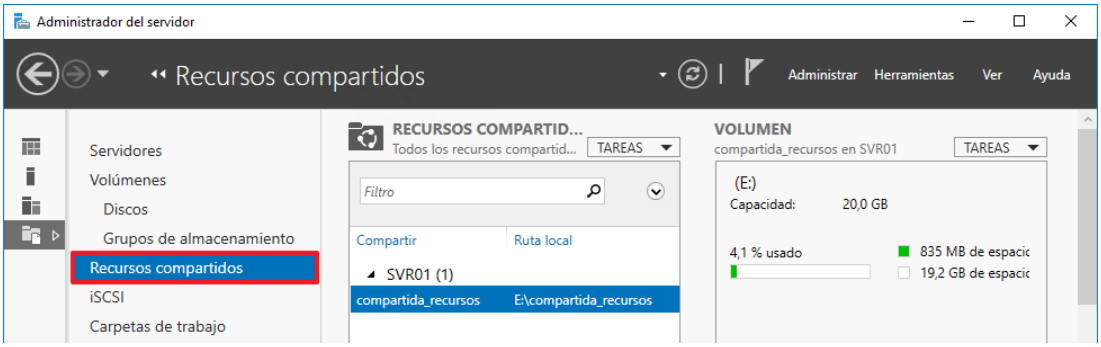
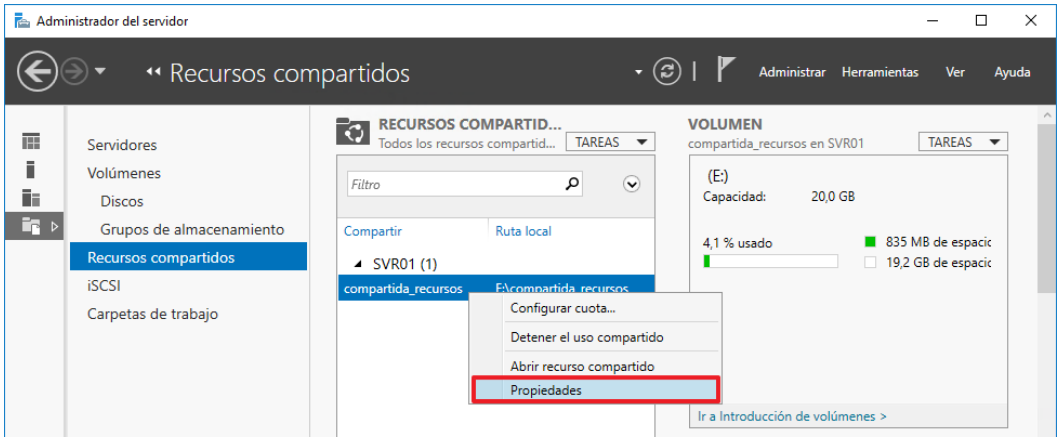
Paso	Descripción
62.	Pulse “Siguiente >” en el apartado “Cuota”.  **Nota:** En este ejemplo se deja marcado la opción por defecto “No aplicar una cuota”.
63.	En el apartado “Confirmación” pulse sobre el botón “Crear”. 

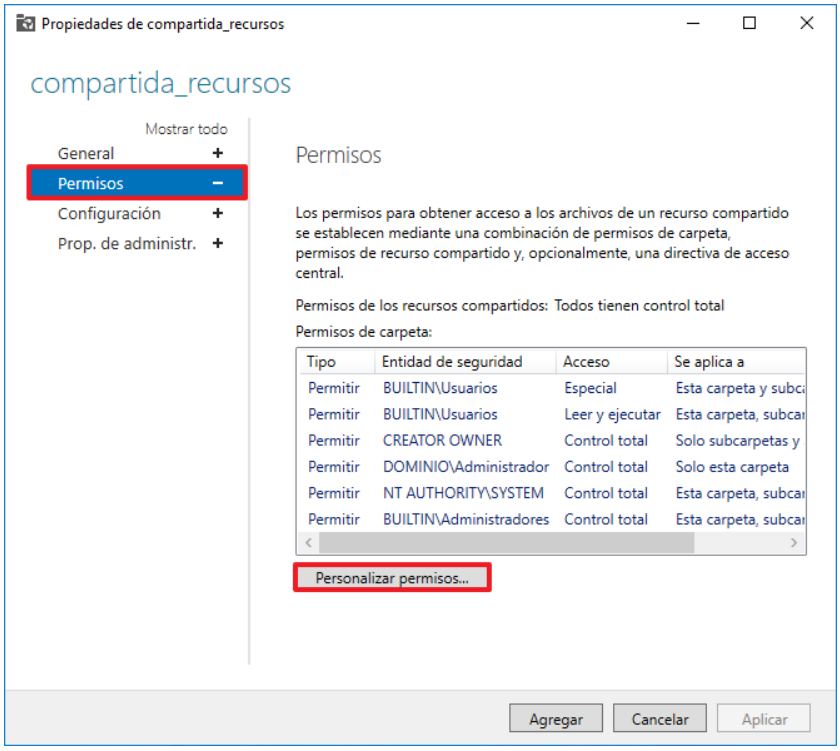
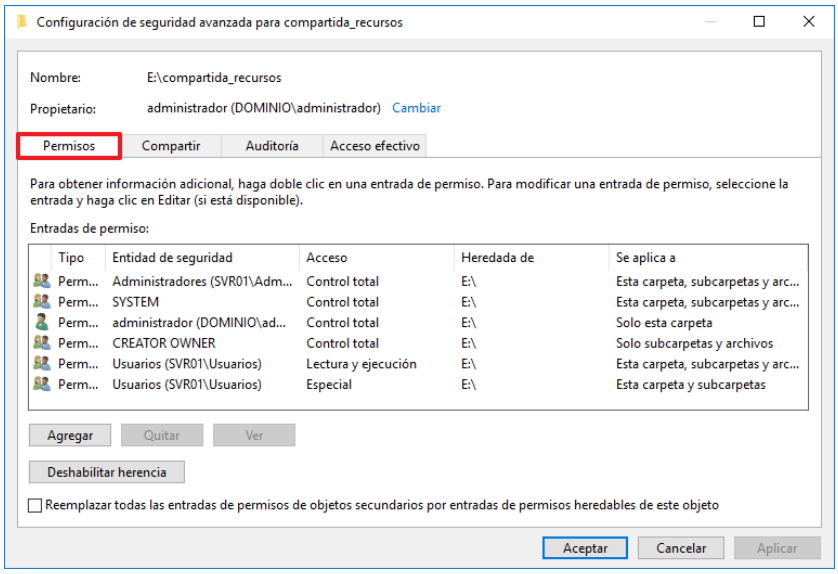
Paso	Descripción
64.	En el apartado “Resultados” se mostrará el proceso de creación del recurso. Cuando finalice pulse sobre “Cerrar”. 
65.	Podrá comprobar desde el “Administrador del servidor” el recurso que se acaba de compartir. 

2.3. SEGURIDAD SOBRE LOS RECURSOS COMPARTIDOS

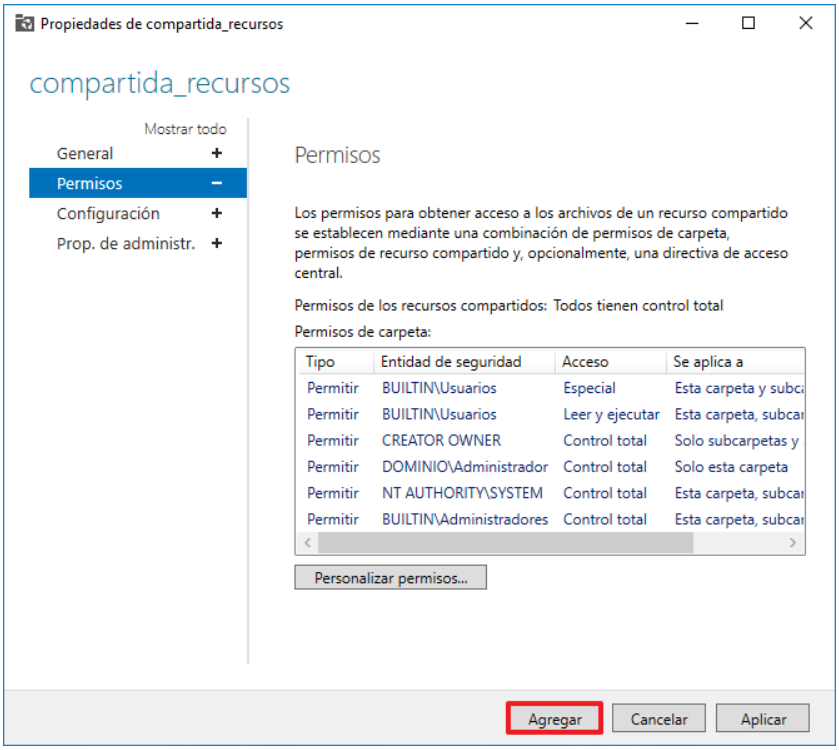
En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos compartidos del servidor de ficheros, según lo establecido por el ENS en la categoría básica del marco operacional para con ello, limitar y controlar el acceso a recursos compartidos con información sensible de ser sustraída.

Paso	Descripción
66.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.
67.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
68.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
69.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
70.	Seleccione la sección “Recursos compartidos”. 
71.	Seleccione con el botón derecho el recurso sobre el que desea modificar los permisos y pulse la opción “Propiedades”.  **Nota:** En este ejemplo se editan las propiedades del recurso denominado “compartida_recursos”.

Paso	Descripción
72.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos…”. 
73.	A continuación, en la pestaña “Permisos” edite los permisos que desee para el recurso compartido.  **Nota:** Tenga en consideración que deberá eliminar por seguridad el grupo “Todos” de cualquier recurso que este compartido.

Paso	Descripción
74.	Para finalizar, pulse sobre “Aceptar” y después sobre el botón “Agregar” para hacer efectivos los cambios.



ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA SERVIDORES DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

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 el punto de la guía “ANEXO A.2.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT 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 Microsoft Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

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

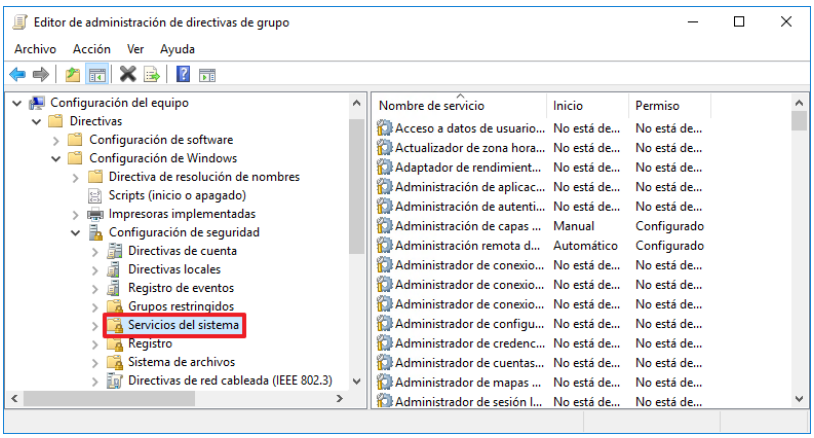
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de ficheros, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el controlador de dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

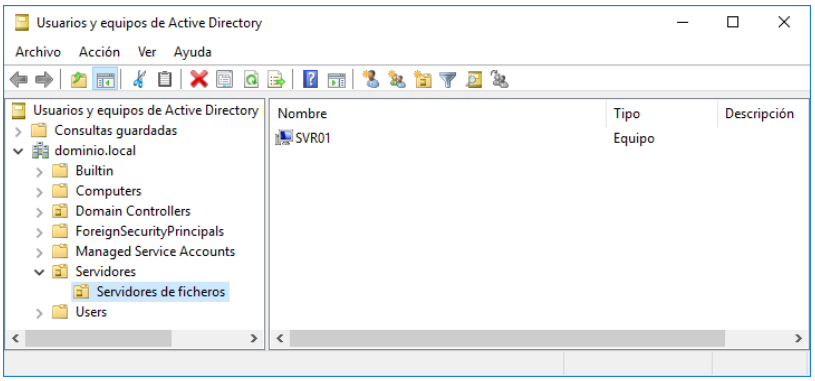
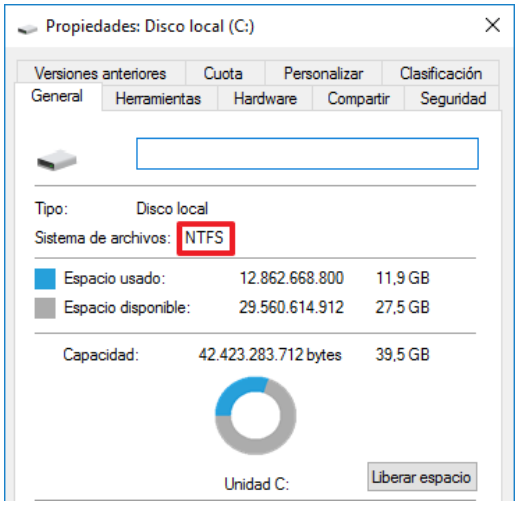
b) En el servidor de ficheros:
   i. Administrador de Windows (explorer.exe).
   ii. Servicios (services.msc).
   iii. Administrador de recursos del servidor de archivos (fsrm.msc).
   iv. Carpetas compartidas (fsmgmt.msc).

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.
2. Verifique que está creada la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica		Utilice el Administrador de directivas de grupo (**Inicio → Herramientas administrativas → Administración de directivas de grupo**) y despliegue el menú hasta llegar a las unidades organizativas que contienen los Servidores de ficheros. Verifique que está creada la política "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica". **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros".

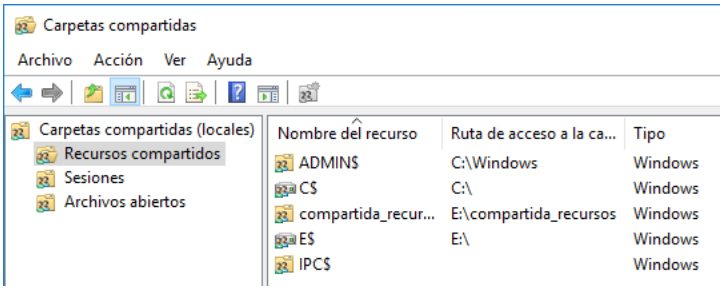
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica" tiene los siguientes valores de servicios de sistema dentro de: **Directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema.** 

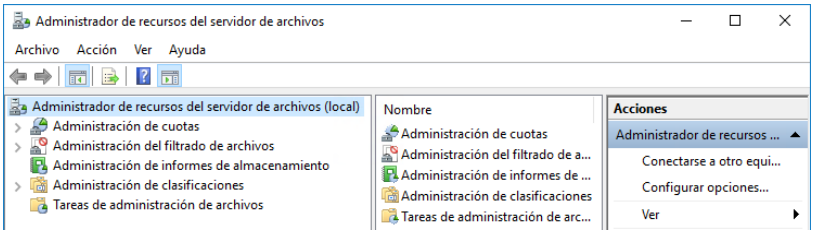
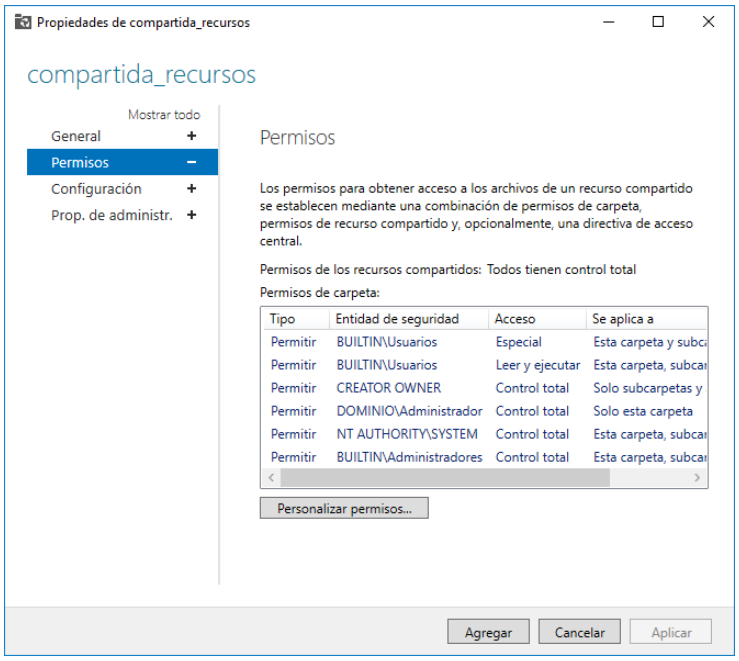
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permisos	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que los servidores de ficheros están dentro de las Unidades Organizativas correspondientes		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Ficheros. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de ficheros que se están asegurando. **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros". 
5. Inicie sesión en un Servidor de ficheros		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.
6. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos**, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que los servicios del sistema relacionados con el servidor de ficheros están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permisos	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

8. Verifique que la instalación del servidor de ficheros se ha realizado correctamente.		Utilizando la herramienta de administración de ficheros (ejecutando "fsmgmt.msc" desde, botón derecho sobre **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique que la instalación del servidor de ficheros se ha realizado correctamente.		Utilizando la herramienta de administración de ficheros (ejecutando "fsrm.msc" desde, botón derecho sobre **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 
10. Verifique que los recursos compartidos poseen los permisos adecuados para los diferentes usuarios.		Desde el Administrador del servidor acceda al apartado **"Servicios de archivos y almacenamiento → Recursos compartidos"**. Haga clic derecho sobre uno de los recursos compartidos y seleccione "Propiedades". Acceda a la sección "Permisos" y verifique los permisos que posee el recurso. 

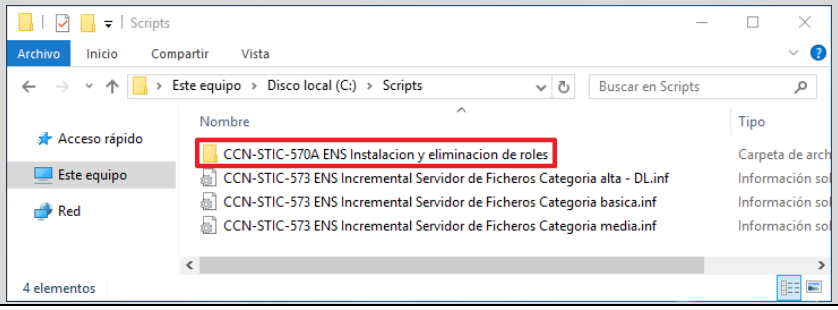
ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN EN 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 empleen Servidores de ficheros 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 la categoría 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.

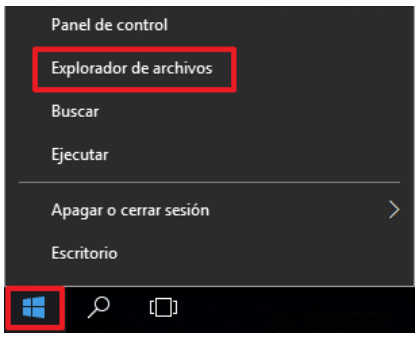
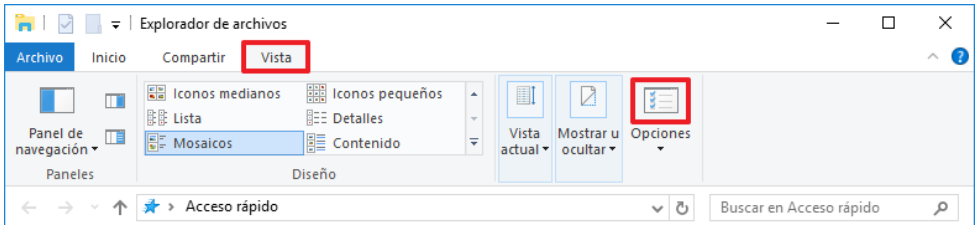
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

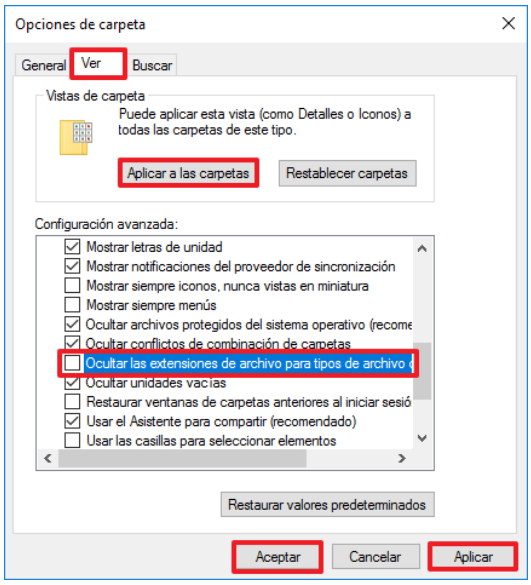
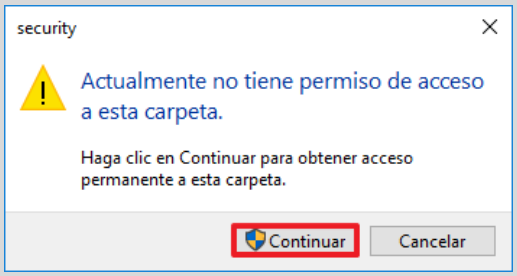
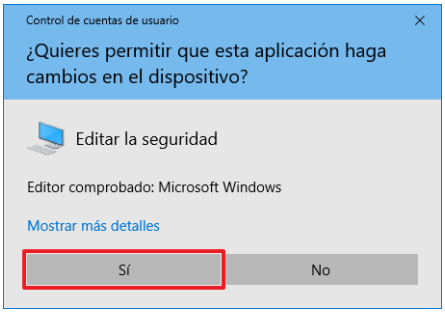
Nota: Si instala el Servidor de ficheros por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada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

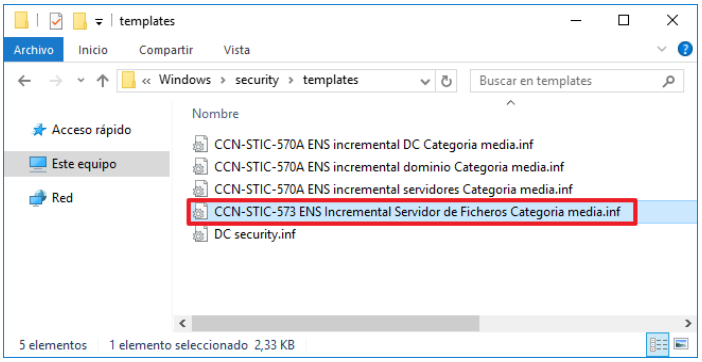
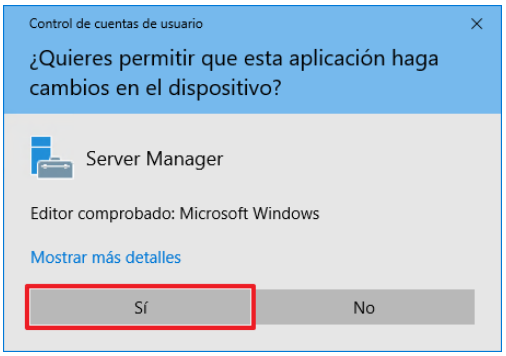


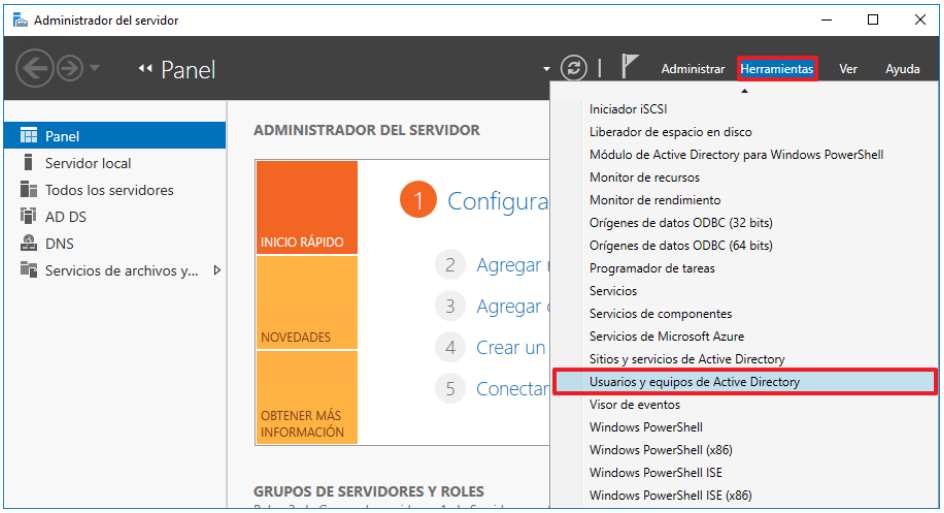
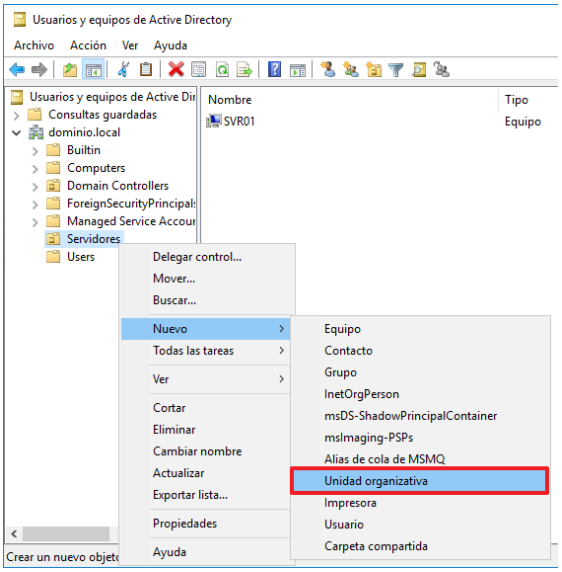
1. PREPARACIÓN DEL DOMINIO

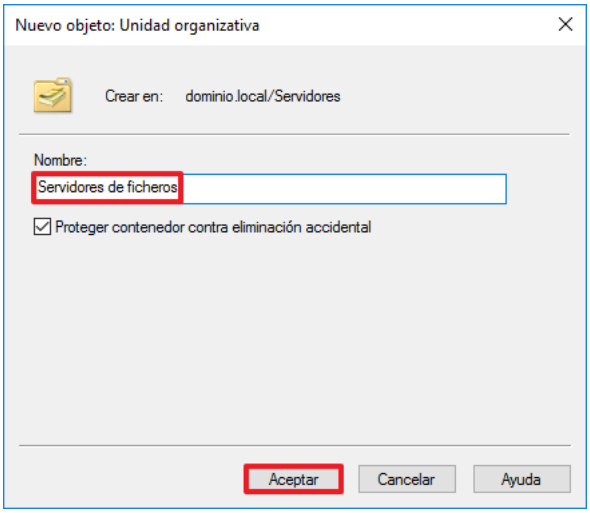
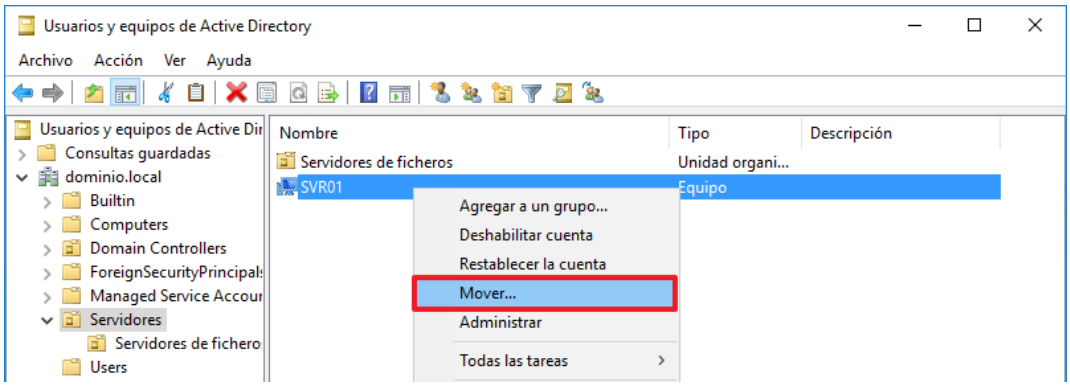
Los pasos que se describen a continuación se realizarán sobre un equipo Controlador de Dominio del dominio al que va a pertenecer el Servidor de ficheros que se está asegurando.

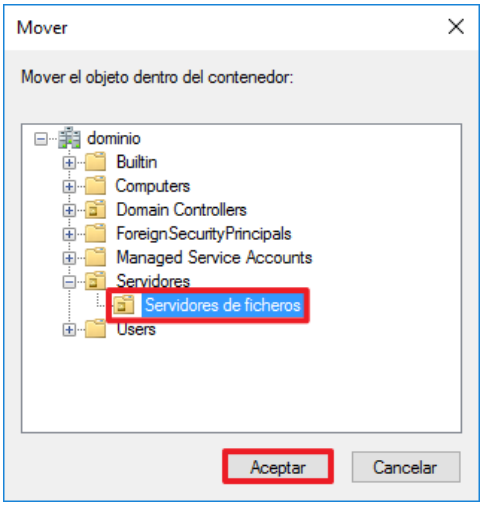
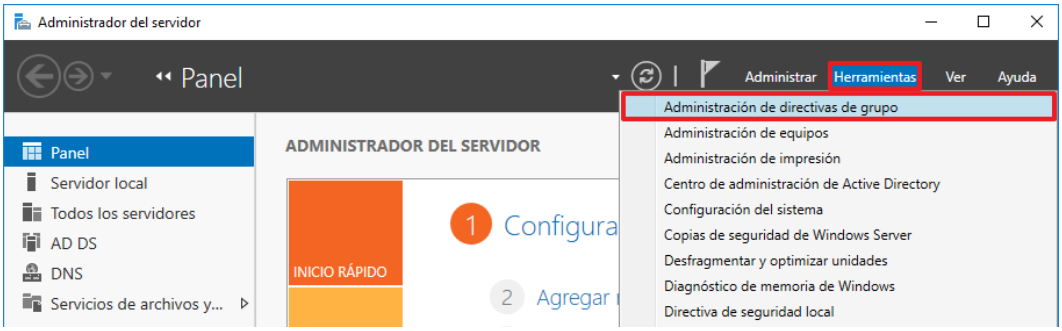
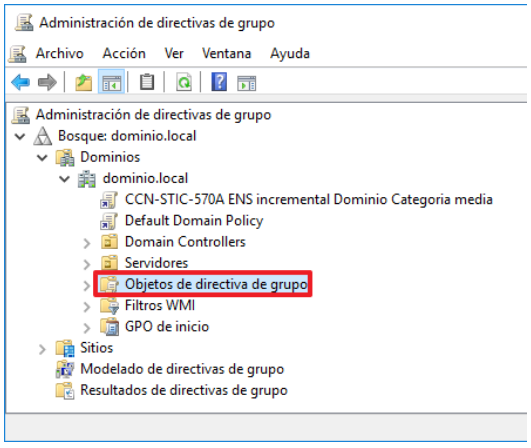
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	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”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

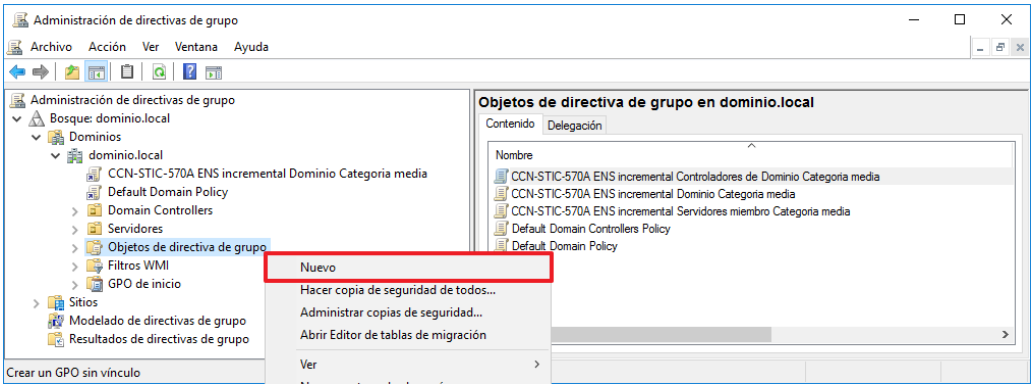
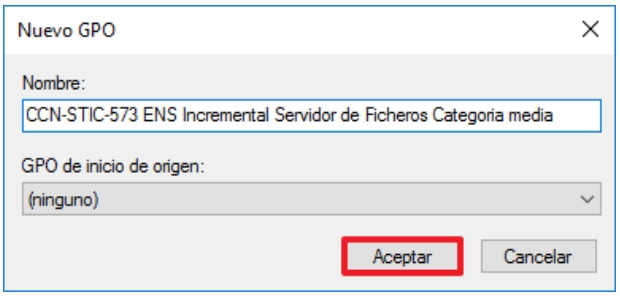
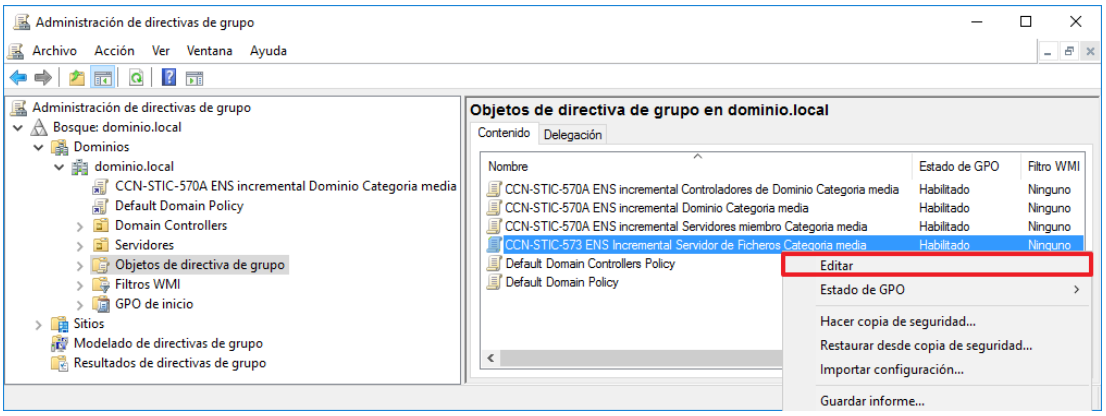
Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 
8.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 

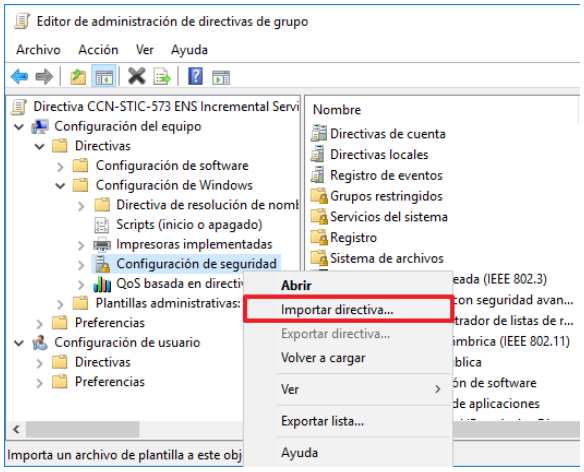
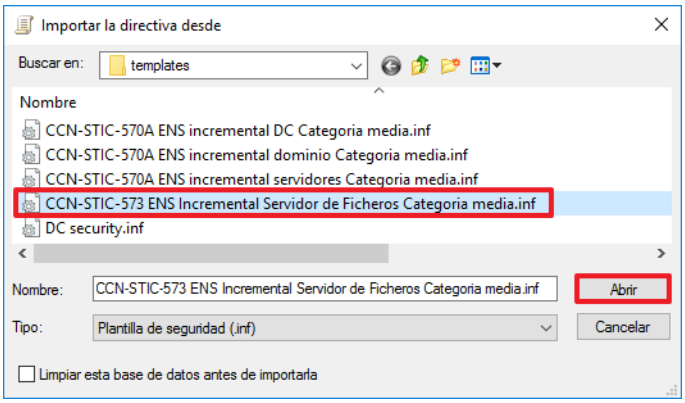
Paso	Descripción
9.	Copie el fichero “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
10.	A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
11.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

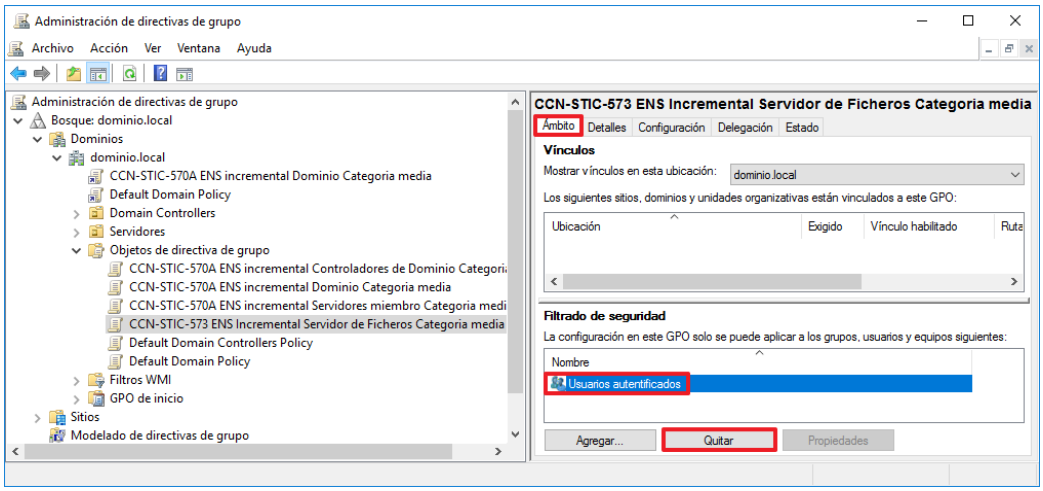
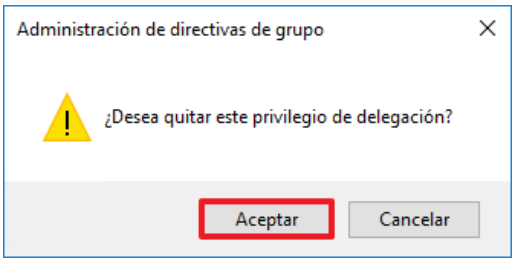
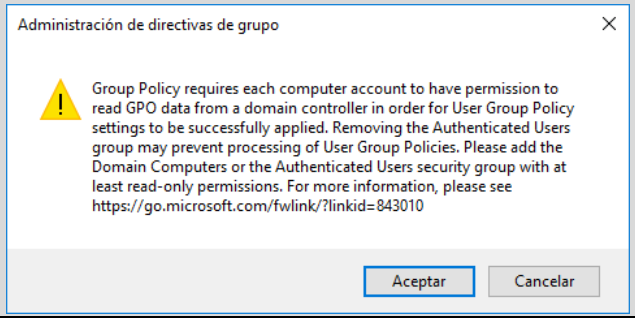
Paso	Descripción
12.	A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”** 
13.	En la consola, cree una nueva 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 **“<<dominio>> → <<unidad organizativa>>”**, y desplegando el menú contextual con el botón derecho, seleccione la opción **“Nuevo → Unidad organizativa”**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local/Servidores”.

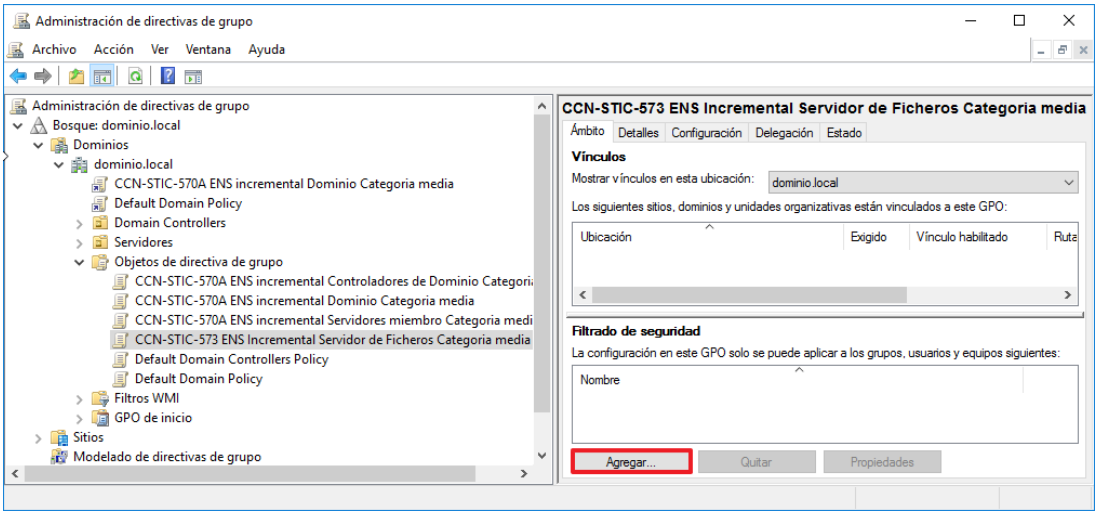
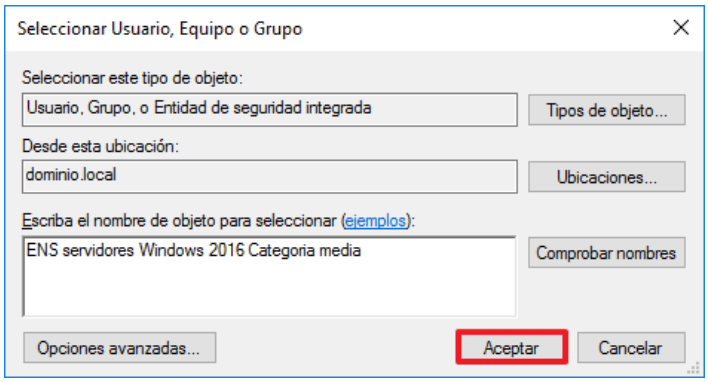
Paso	Descripción
14.	Introduzca el nombre “Servidores de ficheros” tal y como se muestra en la imagen y pulse sobre “Aceptar”. 
15.	Una vez creada la nueva unidad organizativa, deberá mover los servidores de ficheros a la unidad organizativa “Servidores de ficheros”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa. 

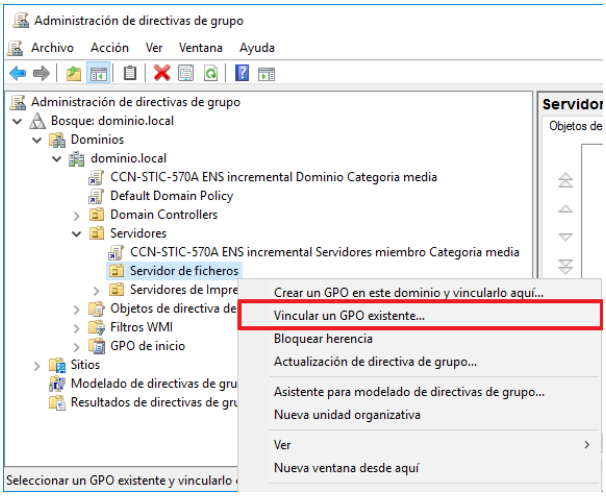
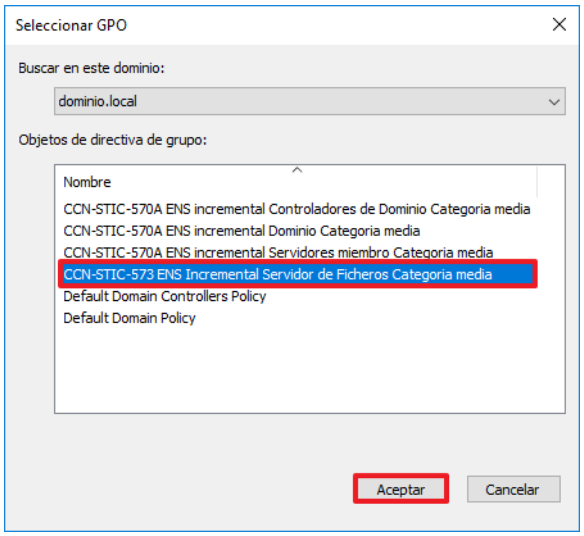
Paso	Descripción
16.	A continuación, seleccione la unidad organizativa “Servidores de ficheros” y pulse sobre “Aceptar”. 
17.	Cierre la herramienta de “Usuarios y equipos de Active Directory”.
18.	A continuación, abra el “Administrador del servidor”.
19.	Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón “**Herramientas → Administración de directivas de grupo**”. 
20.	Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en **“Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”**. 

Paso	Descripción
21.	Pulse con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción del menú contextual “Nuevo”. 
22.	Establezca para la nueva GPO el nombre “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media” y pulse “Aceptar”. 
23.	A continuación, pulse con el botón derecho sobre la GPO recién creada y seleccione la opción del menú contextual “Editar”. 
24.	Ubíquese sobre el nodo **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.

Paso	Descripción
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción del menú contextual “Importar directiva…”. 
26.	Seleccione la plantilla de seguridad “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media.inf” ubicada en “C:\Windows\Security\Templates”. Pulse sobre el botón “Abrir” para continuar. 
27.	Cierre el “Editor de administración de directivas de grupo”.

Paso	Descripción
28.	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 autentificados”. Pulse sobre el botón “Quitar”. 
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.  **Nota:** Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”. 

Paso	Descripción
30.	A continuación, pulse sobre el botón “Agregar…”. 
31.	Agregue los grupos de usuarios que contengan los equipos con el rol “Servidor de ficheros” y pulse “Aceptar” para finalizar.  **Nota:** Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria media” que contiene el servidor con el rol “Servidor de ficheros”.
32.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de ficheros”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de ficheros”.

Paso	Descripción
33.	Seleccione con el botón derecho la unidad organizativa y pulse sobre la opción del menú contextual “Vincular GPO existente…”. 
34.	A continuación, localice la GPO configurada anteriormente, “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media”, y pulse “Aceptar”. 
35.	Cierre la consola “Administración de directivas de grupo” y elimine la carpeta “C:\Scripts”.

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.

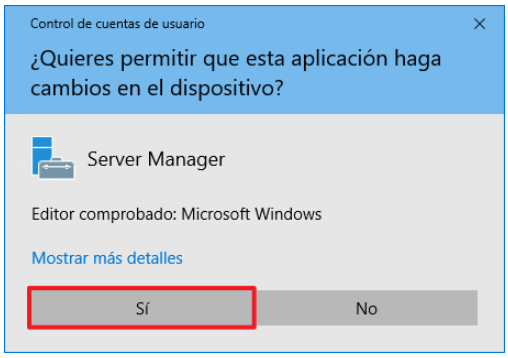
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

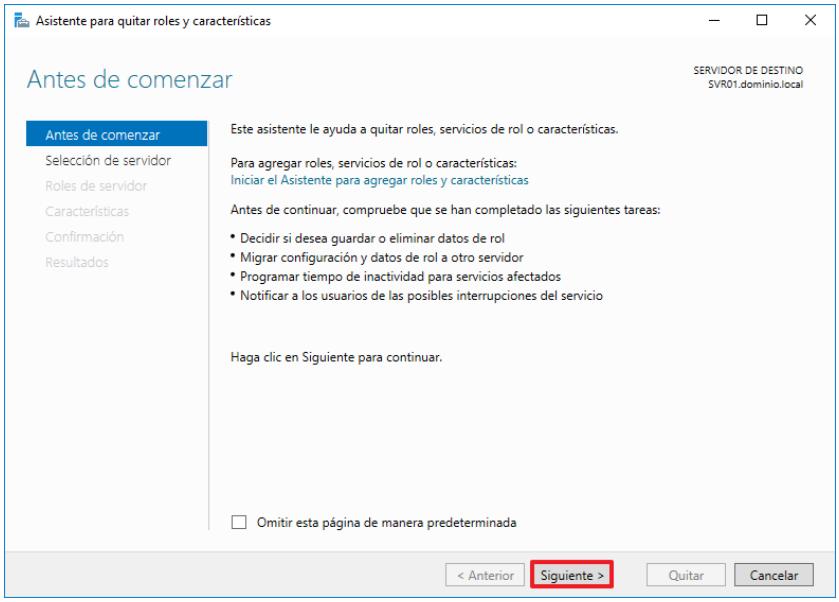
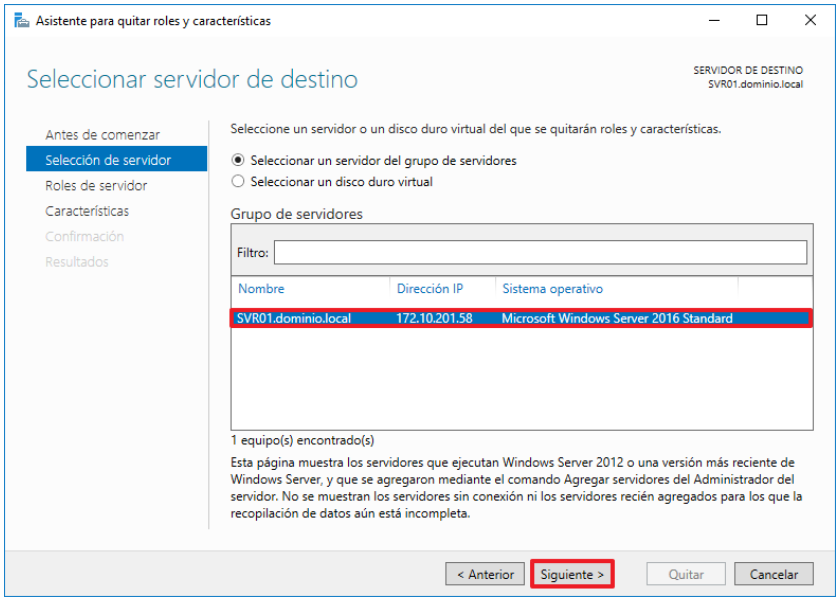
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

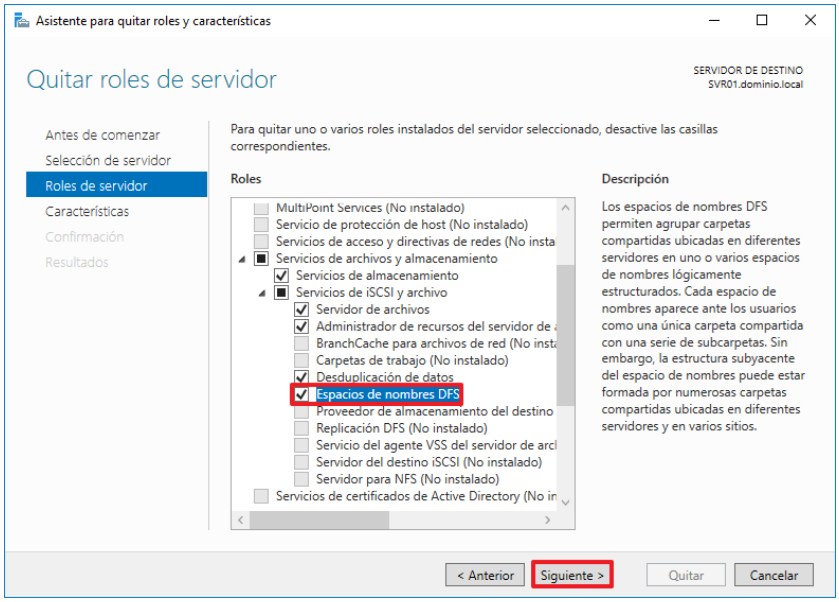
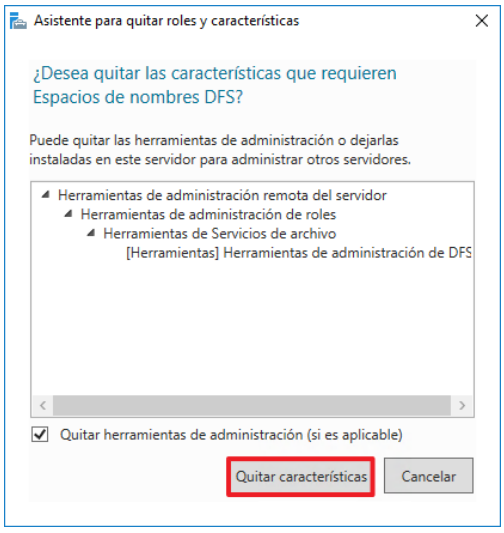
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de ficheros.

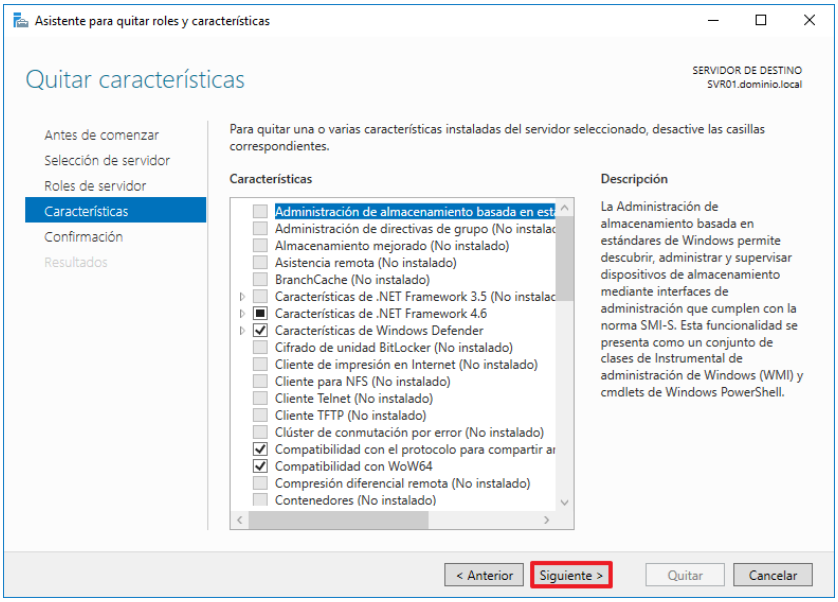
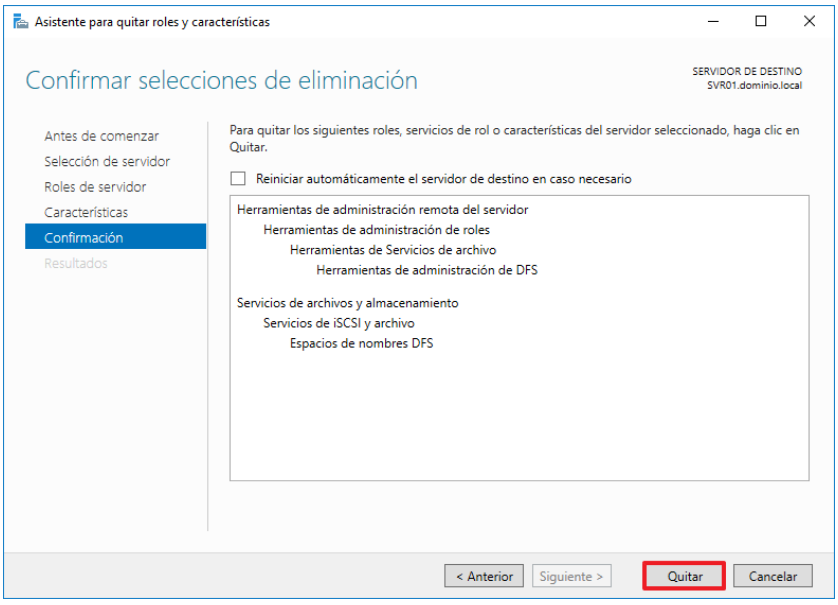
Nota: Para continuar con el siguiente paso a paso deberá realizar previamente el "ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR MIEMBRO O CONTROLADOR DE DOMINIO QUE LES SEA DE APLICACIÓN LA CATEGORIA MEDIA O ALTA DEL ENS" de la guía "CCN-STIC-570A - Implementación del ENS en Microsoft Windows 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.

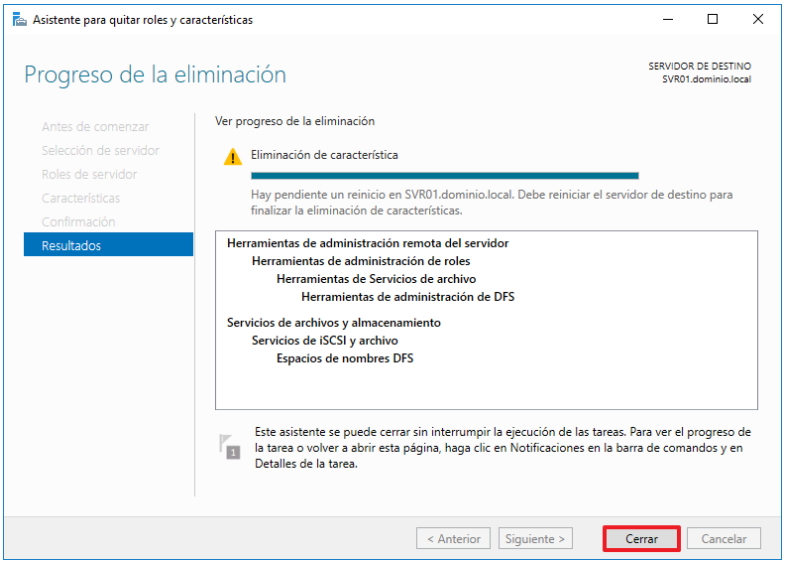
Paso	Descripción
36.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
37.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
38.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
39.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 

Paso	Descripción
40.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
41.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

Paso	Descripción
42.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Espacios de nombres DFS”.
43.	En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.  **Nota:** En este ejemplo se eliminan las características que dependen del rol.

Paso	Descripción
44.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
45.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

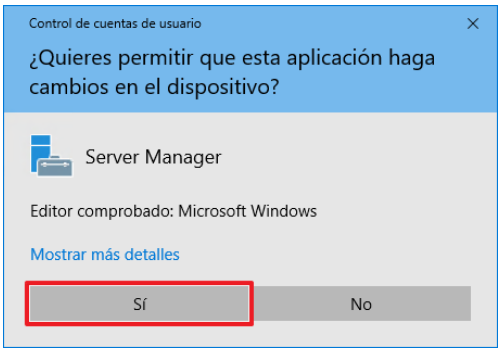
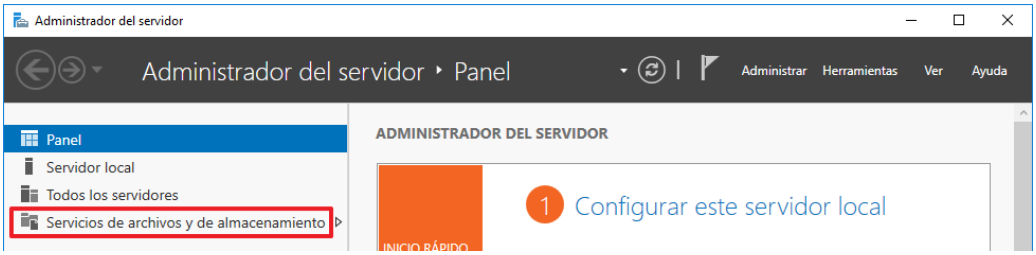
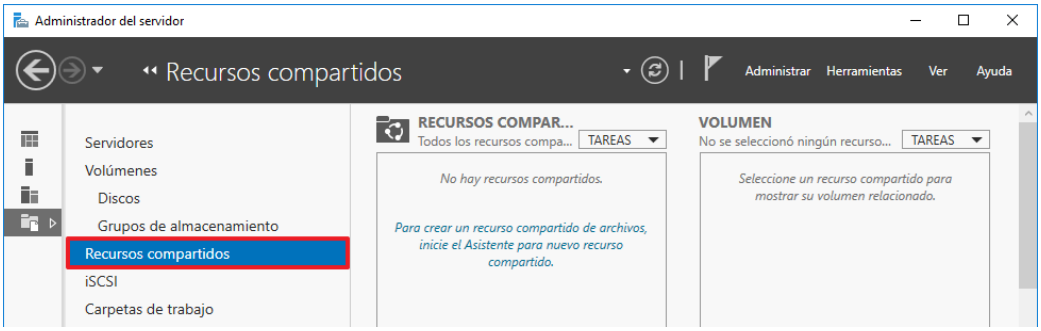
Paso	Descripción
46.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar. 
47.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
48.	A continuación, deberá desvincular la GPO creada anteriormente para eliminar un rol.

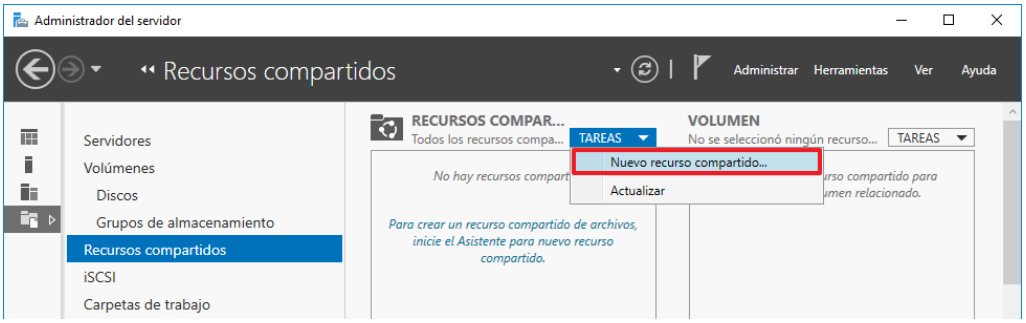
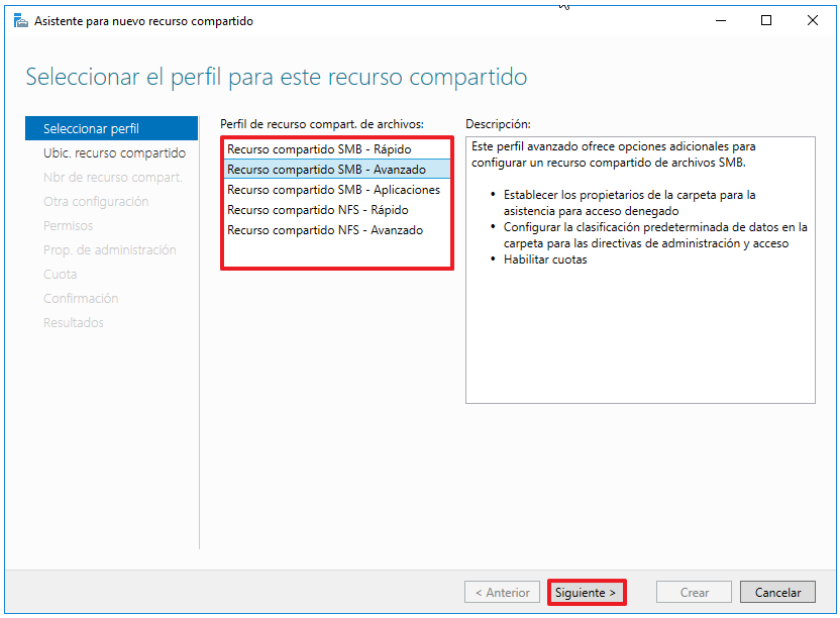
2.2. COMPARTICIÓN DE RECURSOS

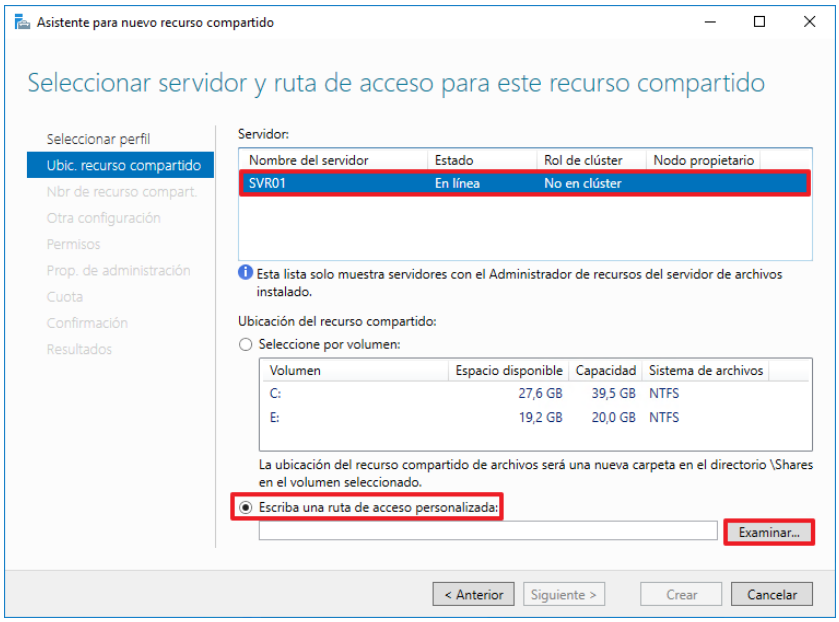
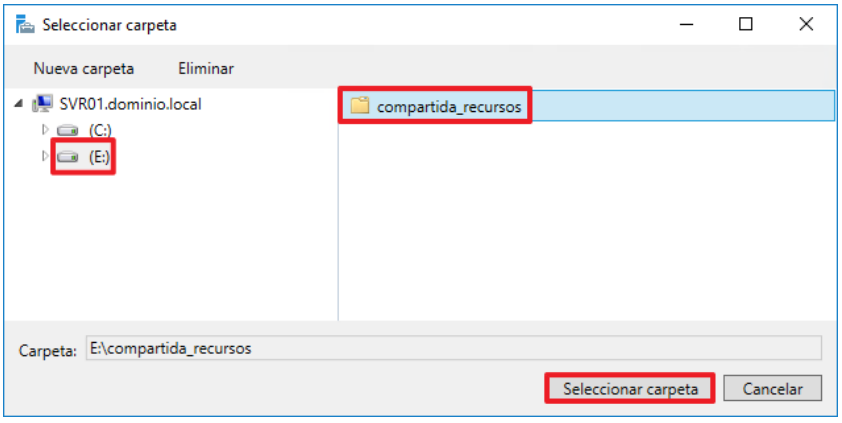
Es importante determinar que recursos se comparten en el Servidor de ficheros. Dependiendo de que recursos se compartan pueden generarse accesos indeseados, es por ello que tal y como indica el ENS es recomendable que los recursos que se comparten en el Servidor de ficheros estén alojados en otra ubicación de disco diferente a la del sistema operativo y que ésta solo se utilice para el alojamiento de recursos, evitando con ello exponer más información de la estrictamente necesaria.

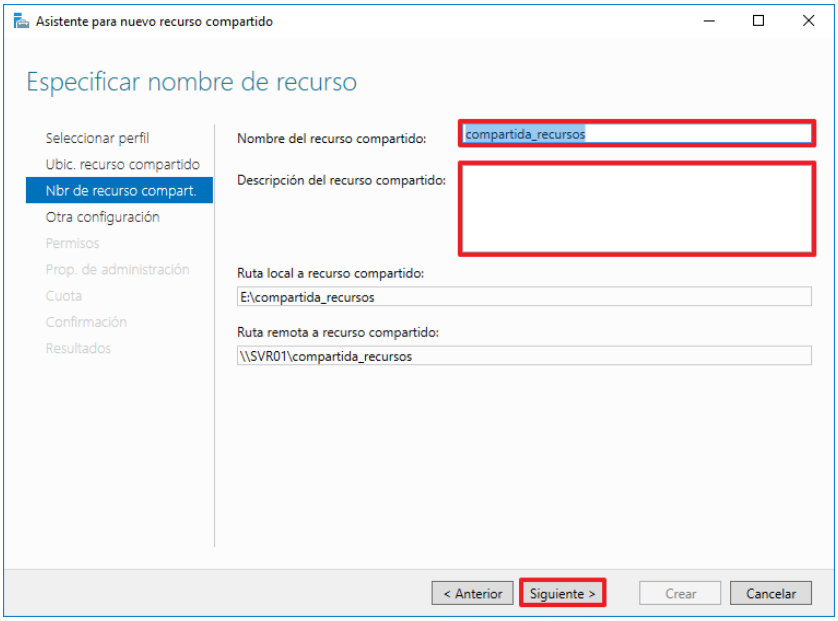
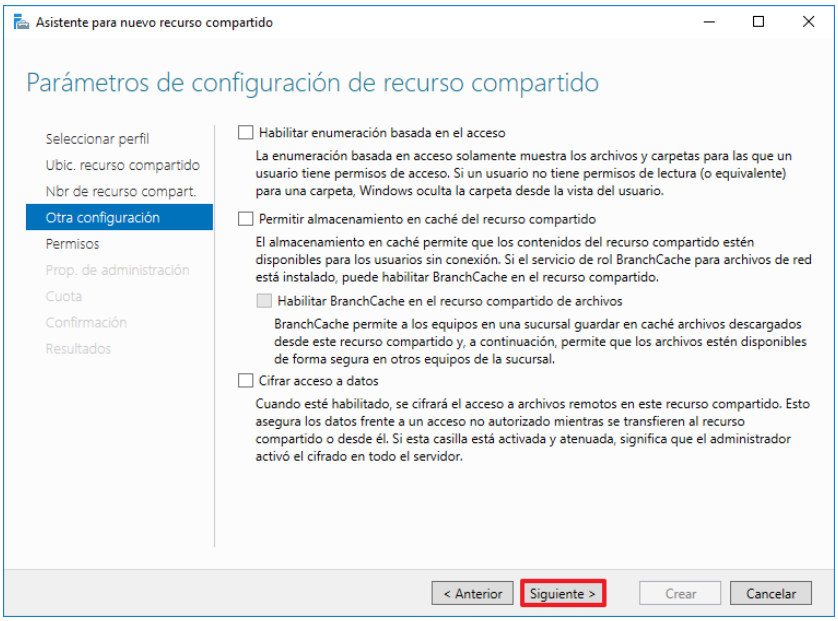
En este apartado se determinará la gestión de los recursos que son compartidos a través del Servidor de ficheros.

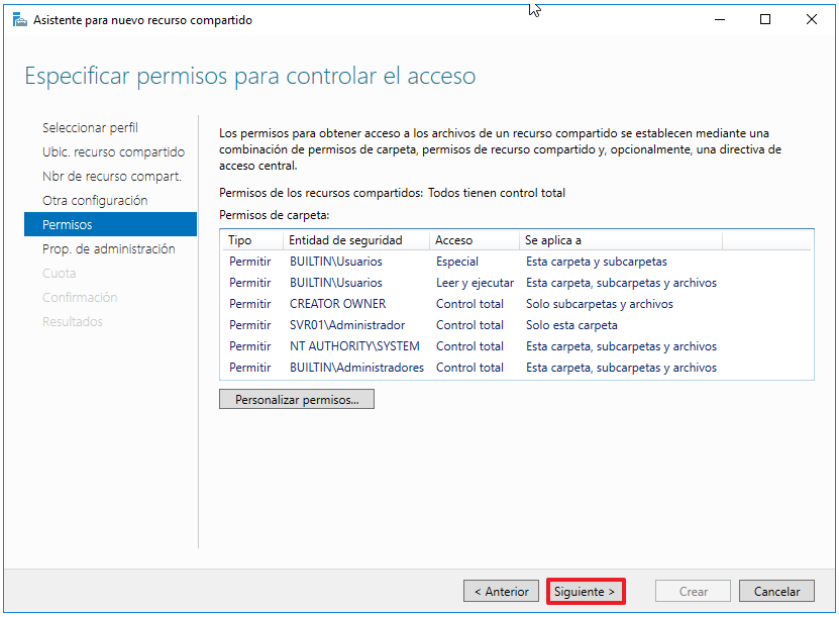
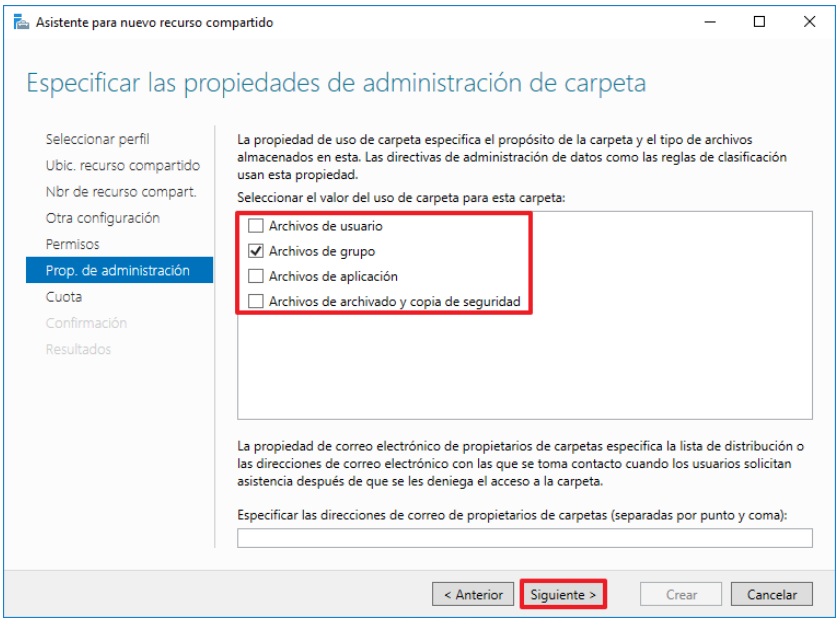
Paso	Descripción
49.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

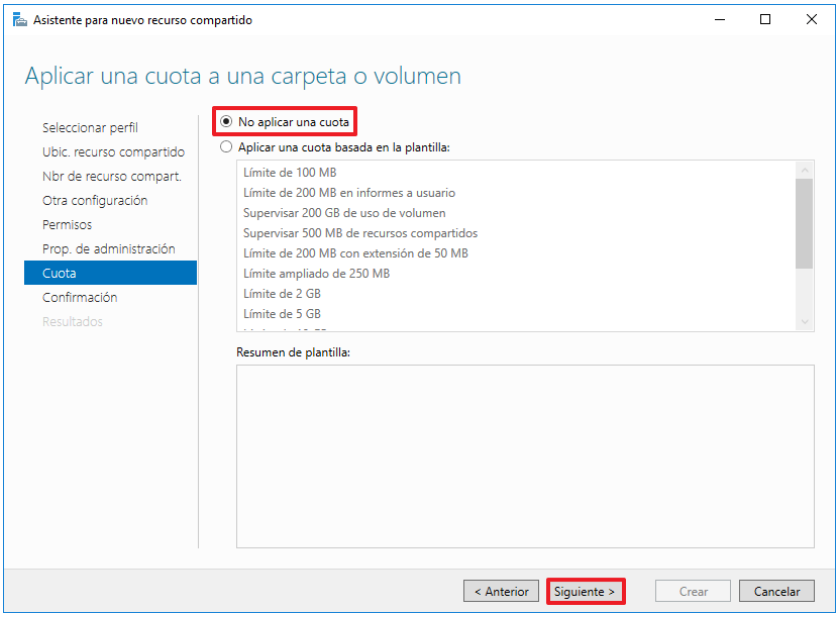
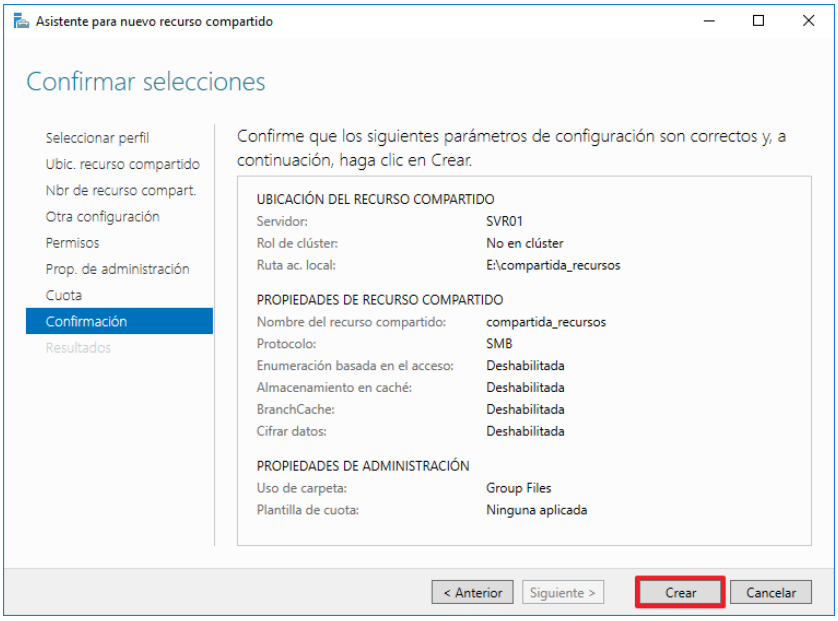
Paso	Descripción
50.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
51.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
52.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
53.	Seleccione la sección “Recursos compartidos”. 

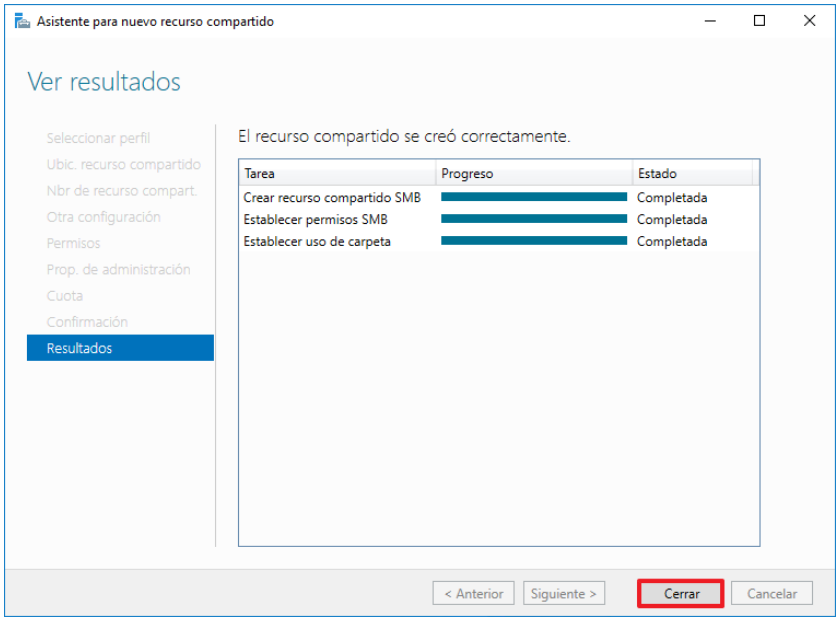
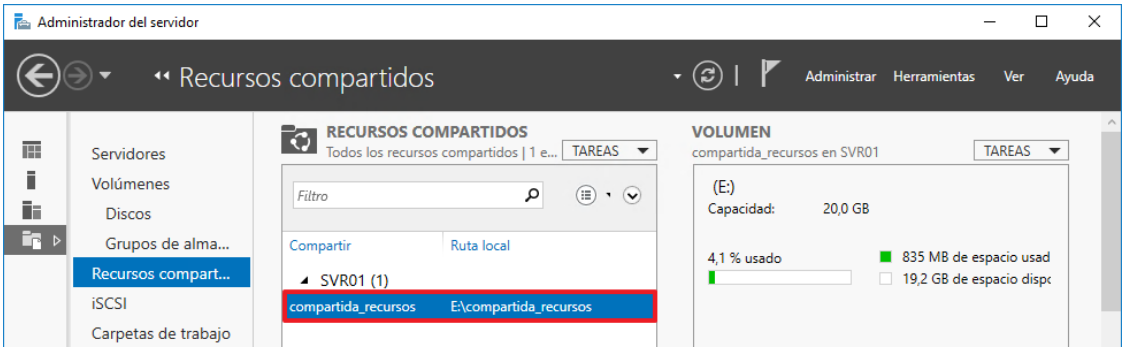
Paso	Descripción
54.	En el apartado “Recursos compartidos” pulse sobre el desplegable “TAREAS” y seleccione la opción “Nuevo recurso compartido…”. 
55.	Se iniciará el asistente para añadir un nuevo recurso compartido. En el apartado “Seleccionar perfil” seleccione un perfil de recurso compartido de archivos y pulse “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la opción “Recurso compartido SMB – Avanzado”.

Paso	Descripción
56.	Seleccione el servidor sobre el que desea crear el recurso compartido. A continuación seleccione la opción “Escriba una ruta de acceso personalizada:” y pulse sobre el botón “Examinar…”. 
57.	Ante la ventana emergente navegue y seleccione el recurso que desea compartir. Pulse sobre “Seleccionar carpeta” para continuar.  **Nota:** Para este ejemplo se comparte un directorio creado previamente denominado “compartida_recursos” en una ubicación dedicada a recursos compartidos denominada “Datos (E:)”. Ajuste esta configuración a las necesidades de su organización.
58.	A continuación, pulse sobre “Siguiente >” para continuar con el asistente.

Paso	Descripción
59.	En el apartado “Nbr. De recurso compart.” Establezca un nombre para el recurso y una descripción del mismo si lo desea. Pulse sobre “Siguiente >”.  **Nota:** En este ejemplo se mantiene el nombre del recurso seleccionado en el apartado anterior del asistente.
60.	En el apartado “Otra configuración” seleccione los parametros de configuración de recurso compartido que precise y pulse “Siguiente >”.  **Nota:** Para este ejemplo no se ha seleccionado ninguna configuración adicional.

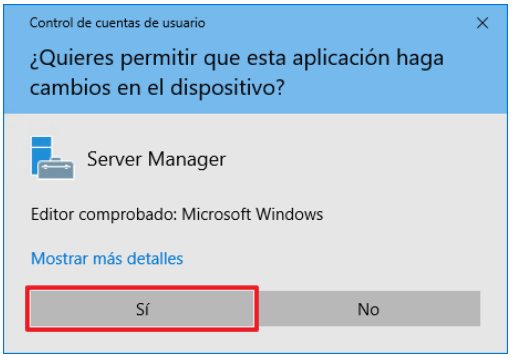
Paso	Descripción
61.	Pulse “Siguiente >” en el apartado “Permisos”.  **Nota:** Los permisos de acceso a los archivos del recurso compartido se configurarán posteriormente.
62.	Seleccione en el apartado “Prop. De administración” una categorización para el recurso compartido si lo desea y pulse el botón “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la categorización “Archivos de grupo”. Adapte esta configuración a su entorno.

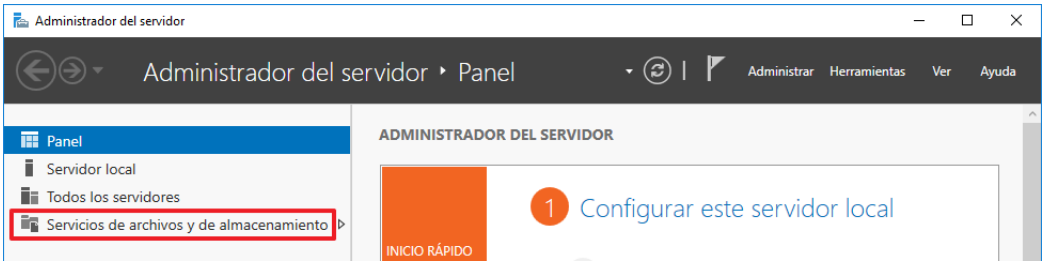
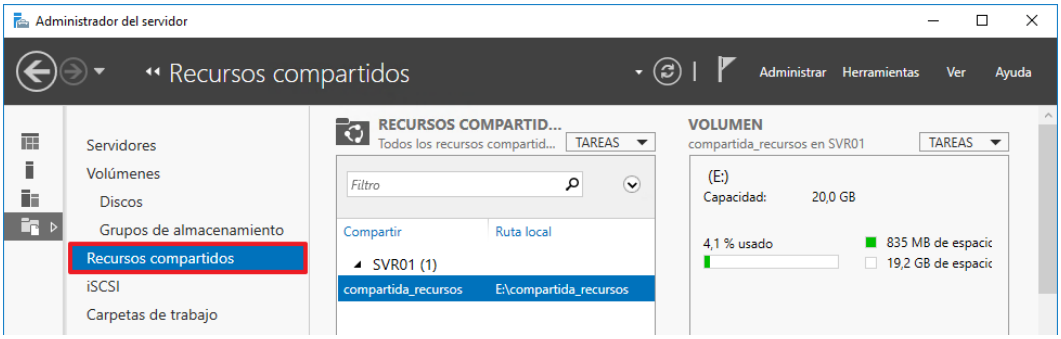
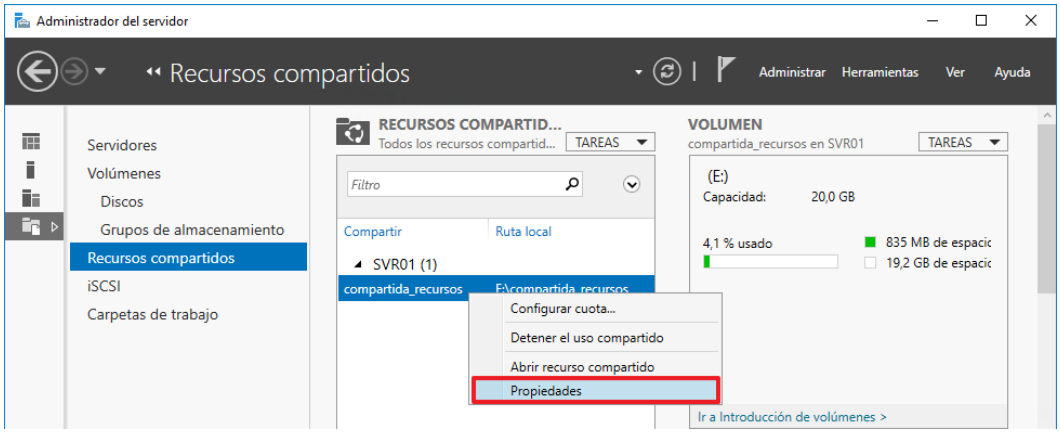
Paso	Descripción
63.	Pulse “Siguiente >” en el apartado “Cuota”.  **Nota:** En este ejemplo se deja marcado la opción por defecto “No aplicar una cuota”.
64.	En el apartado “Confirmación” pulse sobre el botón “Crear”. 

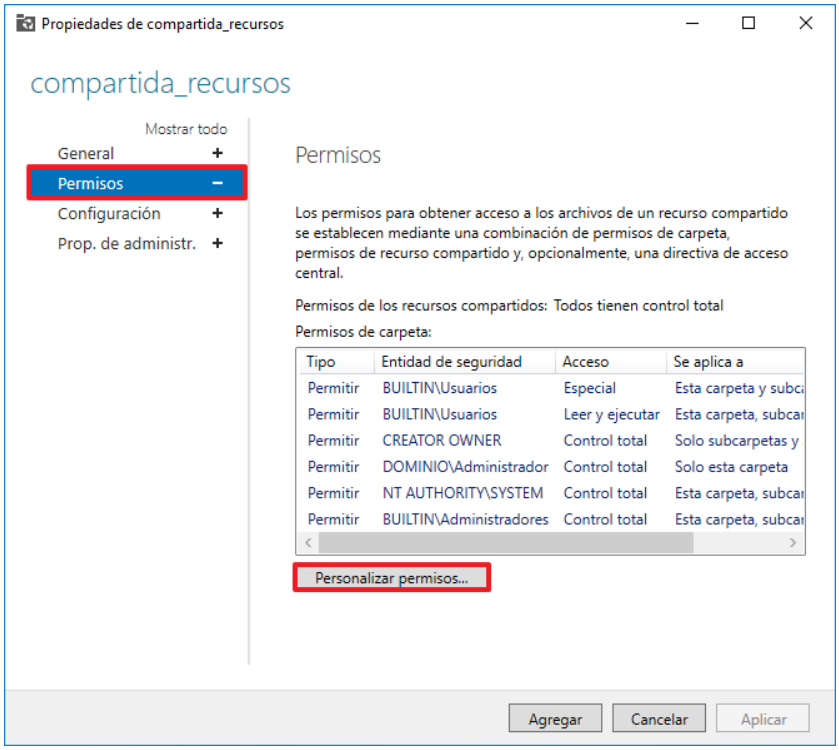
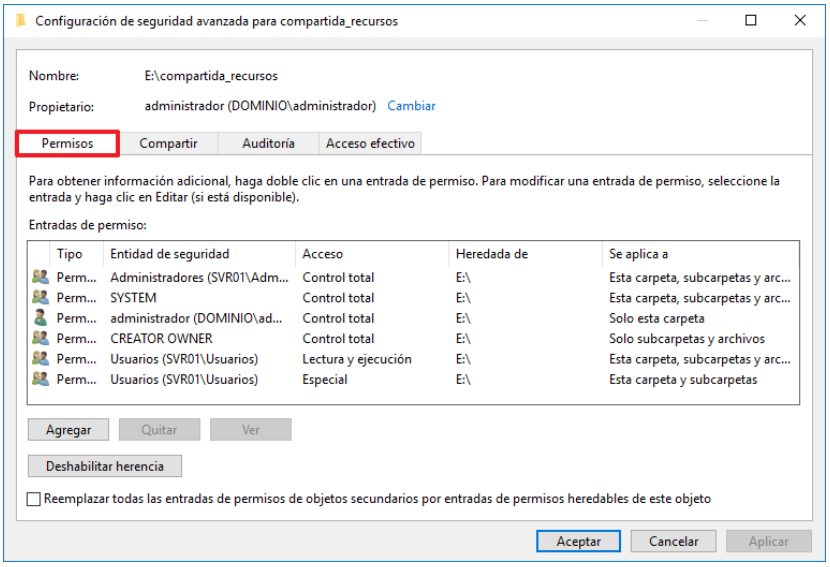
Paso	Descripción
65.	En el apartado “Resultados” se mostrará el proceso de creación del recurso. Cuando finalice pulse sobre “Cerrar”. 
66.	Podrá comprobar desde el “Administrador del servidor” el recurso que se acaba de compartir. 

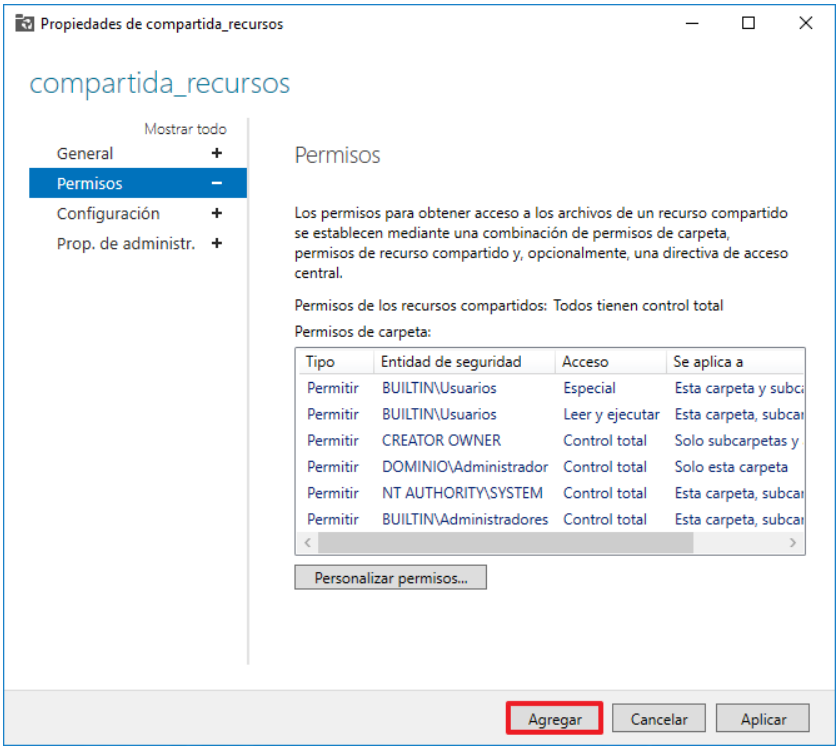
2.3. SEGURIDAD SOBRE LOS RECURSOS COMPARTIDOS

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos del Servidor de ficheros según el marco operacional de categoría media establecida por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

Paso	Descripción
67.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
68.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
69.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
70.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
71.	Seleccione la sección “Recursos compartidos”. 
72.	Seleccione con el botón derecho el recurso sobre el que desea modificar los permisos y pulse la opción “Propiedades”.  **Nota:** En este ejemplo se editan las propiedades del recurso denominado “compartida_recursos”.

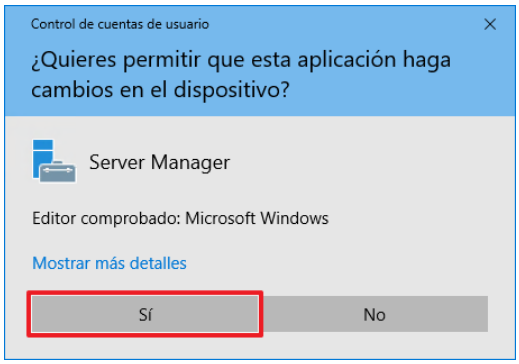
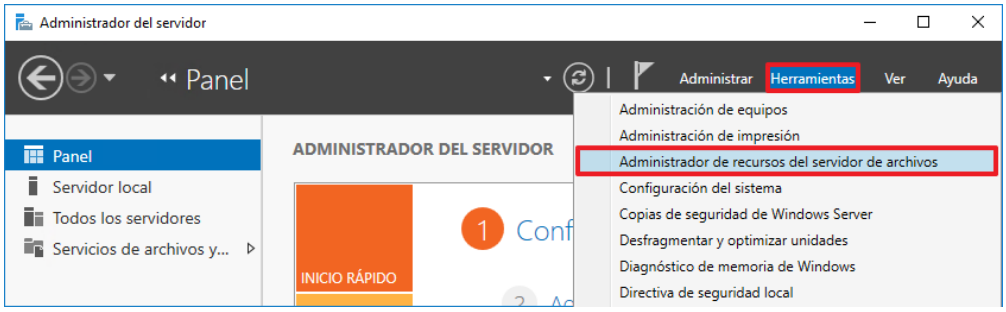
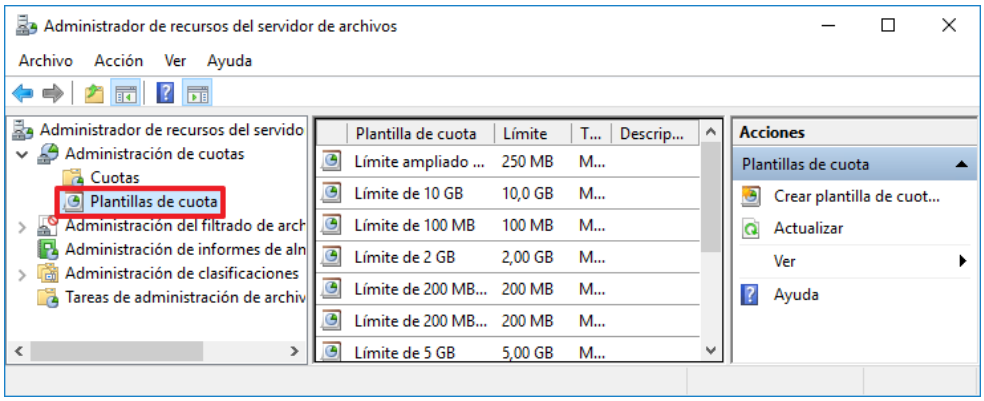
Paso	Descripción
73.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos…”. 
74.	A continuación, en la pestaña “Permisos” edite los permisos que desee para el recurso compartido.  **Nota:** Tenga en consideración que deberá eliminar por seguridad el grupo “Todos” de cualquier recurso que este compartido.

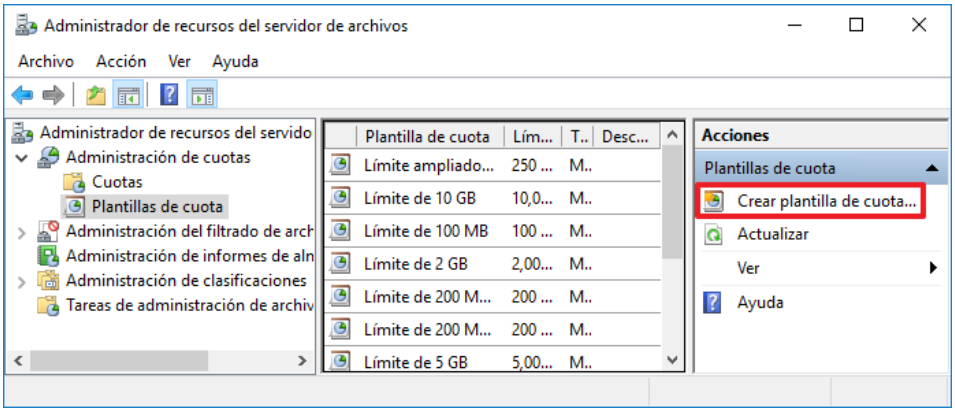
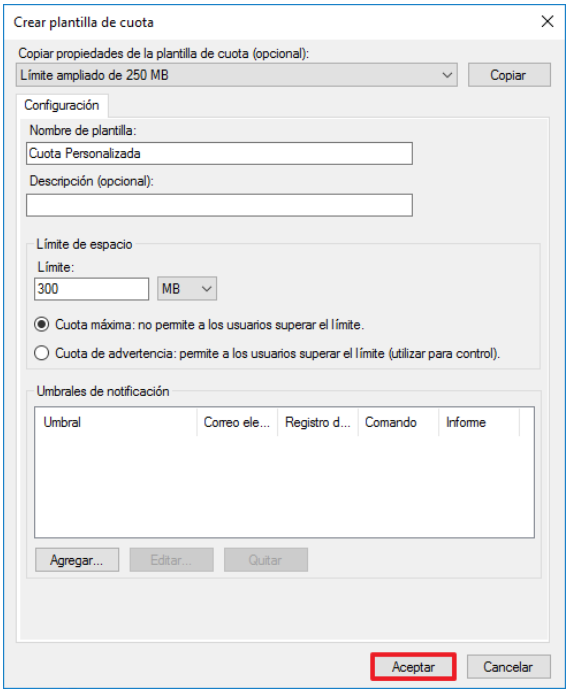
Paso	Descripción
75.	Para finalizar, pulse sobre “Aceptar” y después sobre el botón “Agregar” para hacer efectivos los cambios. 

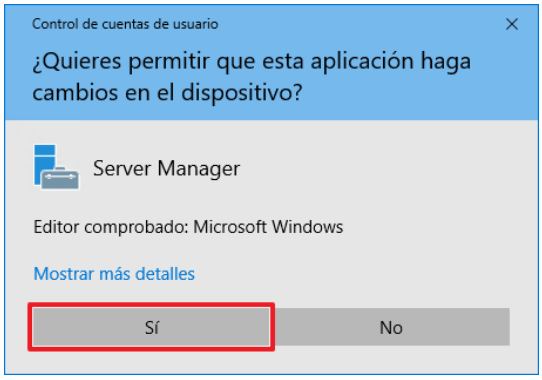
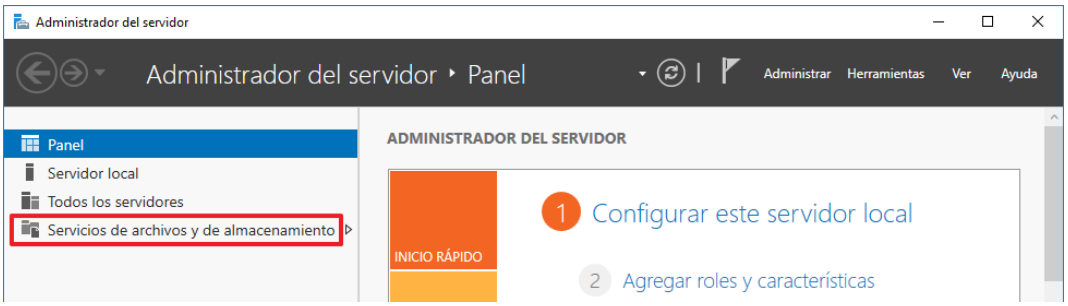
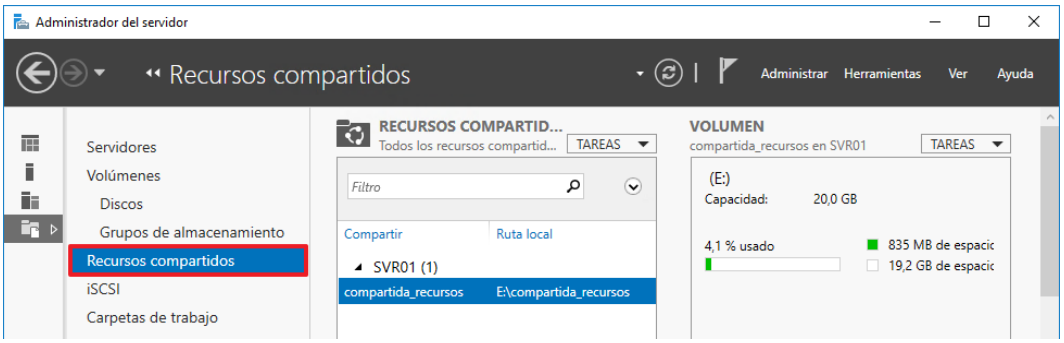
2.4. CUOTAS DE DISCO

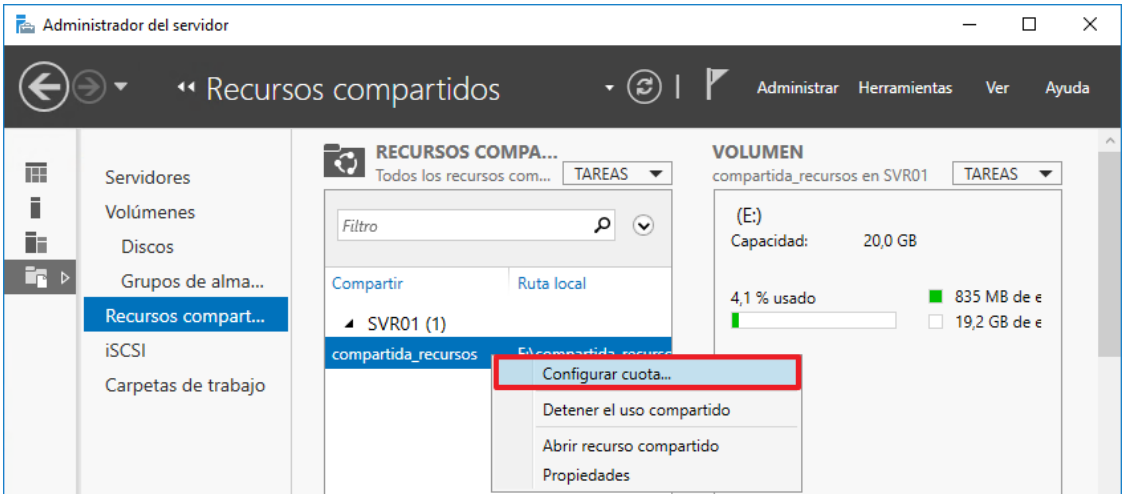
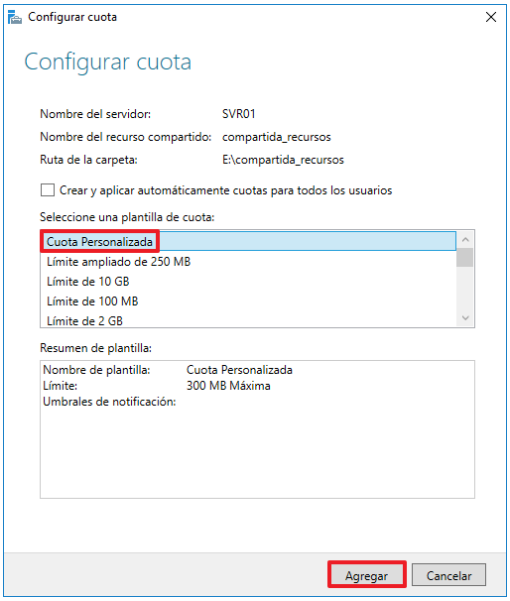
Con la aplicación del ENS para la categoría media sobre el “Servidor de ficheros” será necesario configurar las cuotas de disco para prevenir un uso excesivo de los recursos y el sistema pueda reaccionar frente a los incidentes que se puedan provocar.

Paso	Descripción
76.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
77.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
78.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
79.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
80.	Expanda el nodo **“Plantillas de cuota” desde la ruta “Administrador de recursos del servidor de archivos (local) → Administración de cuotas → Plantillas de cuota”** tal y como se muestra a continuación. 

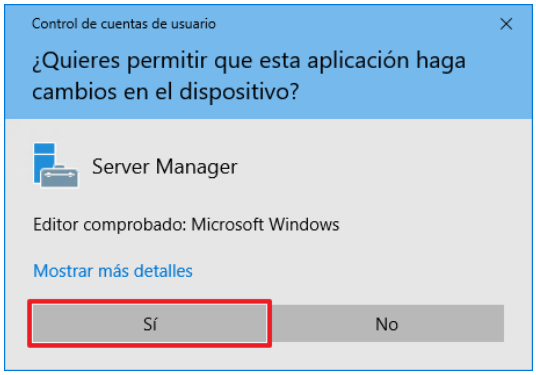
Paso	Descripción
81.	En el panel “Acciones” seleccione “Crear plantilla de cuota…”. 
82.	En la nueva ventana emergente, establezca la configuración deseada para la cuota y pulse “Aceptar” para finalizar la creación de la cuota.  **Nota:** En este ejemplo se utiliza el nombre “Cuota Personalizada” y se da un valor límite de 300MB.
83.	A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 

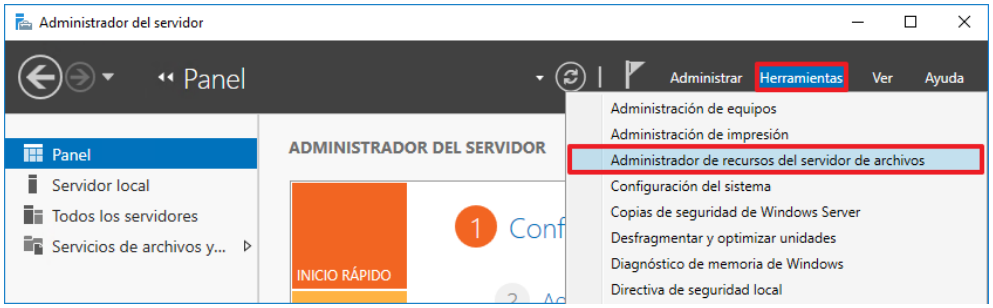
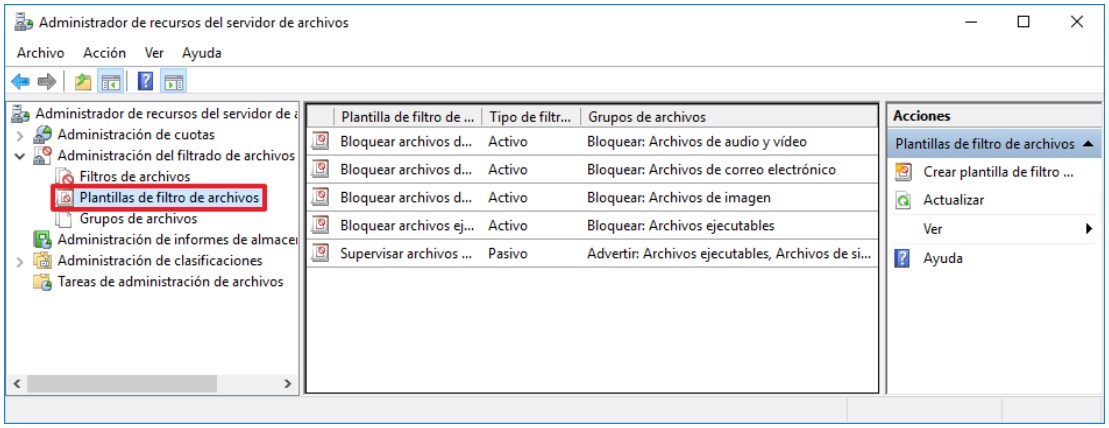
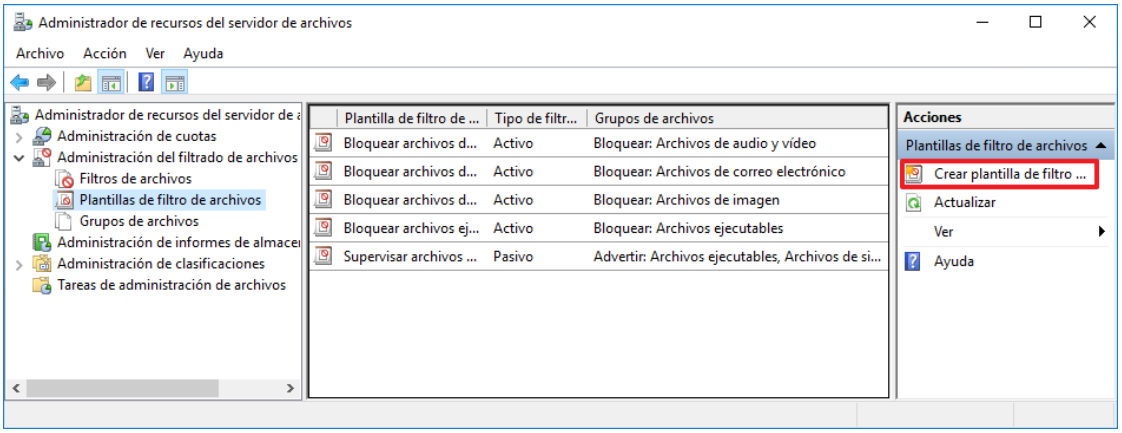
Paso	Descripción
84.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
85.	Pulse sobre “Servicios de archivos y de almacenamiento”. 
86.	Seleccione la sección “Recursos compartidos”. 

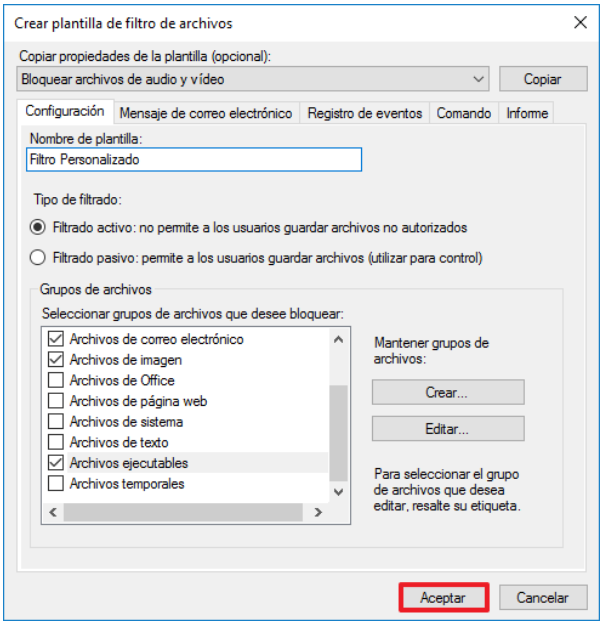
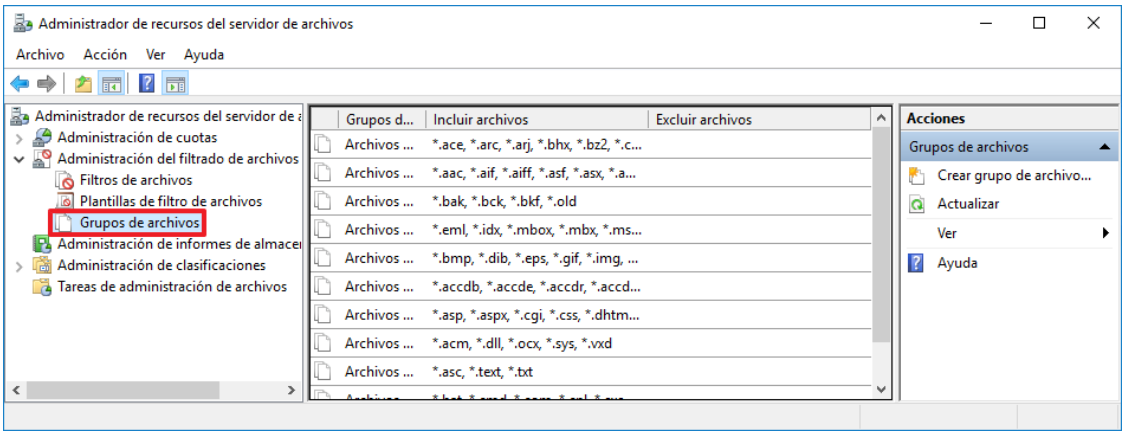
Paso	Descripción
87.	Seleccione con el botón derecho el recurso sobre el que desea aplicar la cuota configurada anteriormente y pulse la opción “Configurar cuota…”. 
88.	En la nueva ventana emergente seleccione una cuota creada por defecto por el sistema o una cuota creada específicamente para el recurso compartido. Pulse “Agregar” para finalizar.  **Nota:** En este ejemplo se aplica la cuota denominada “Cuota Personalizada”, creada anteriormente. Si no aparece la cuota creada anteriormente reinicie el “Administrador del servidor”.

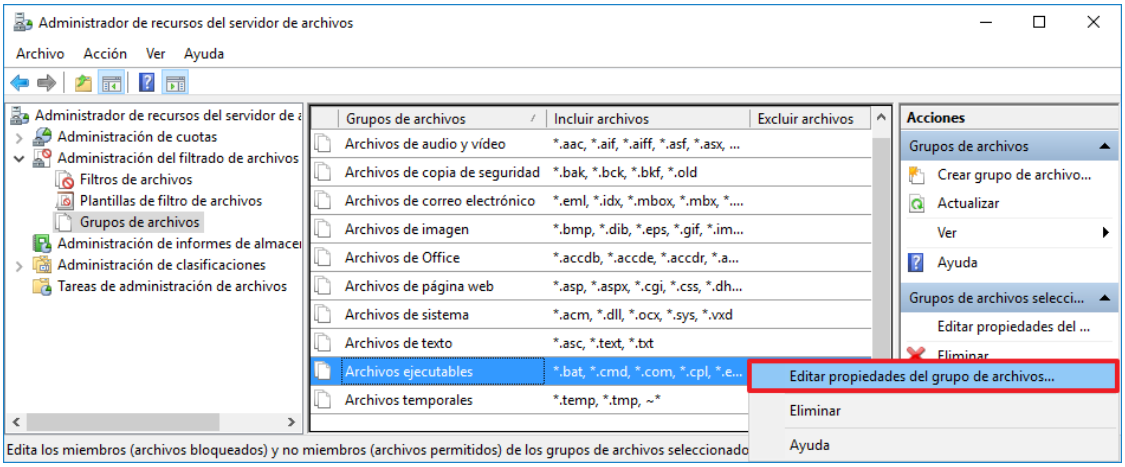
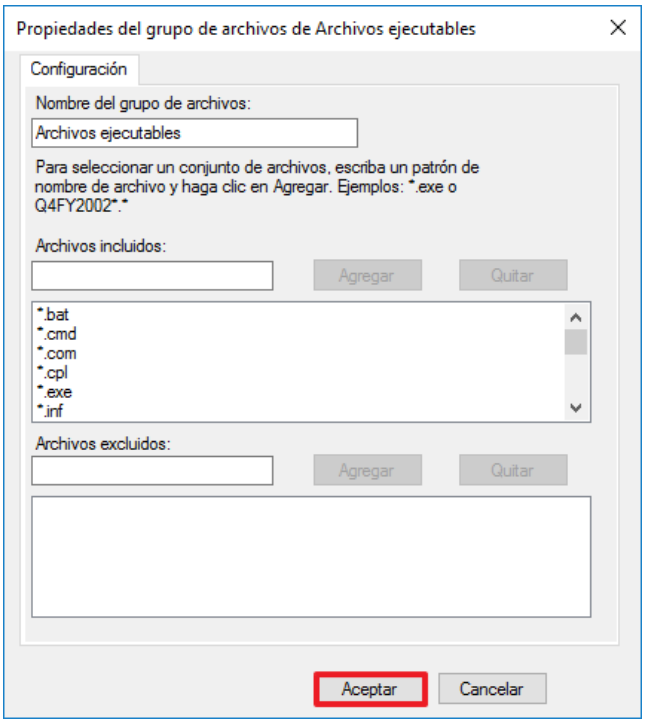
2.5. FILTRADO DE ARCHIVOS

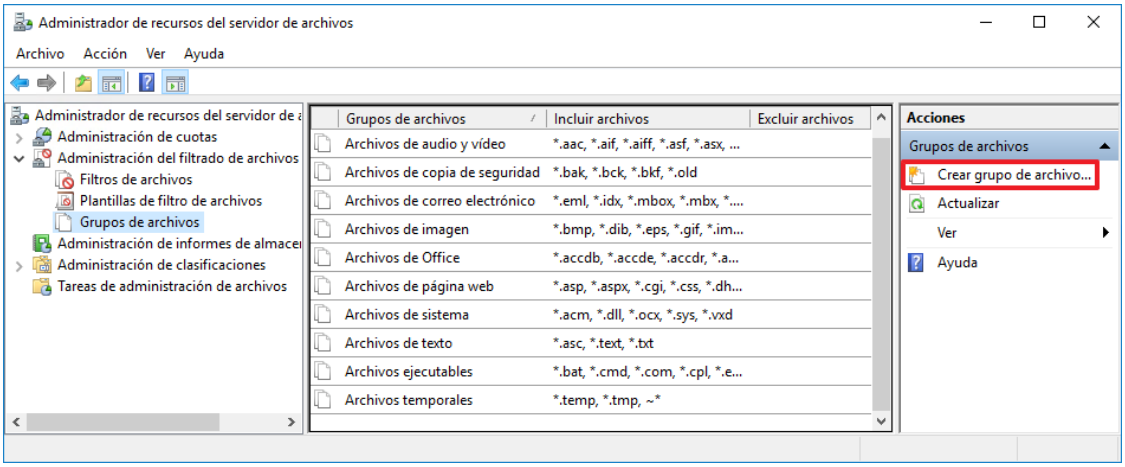
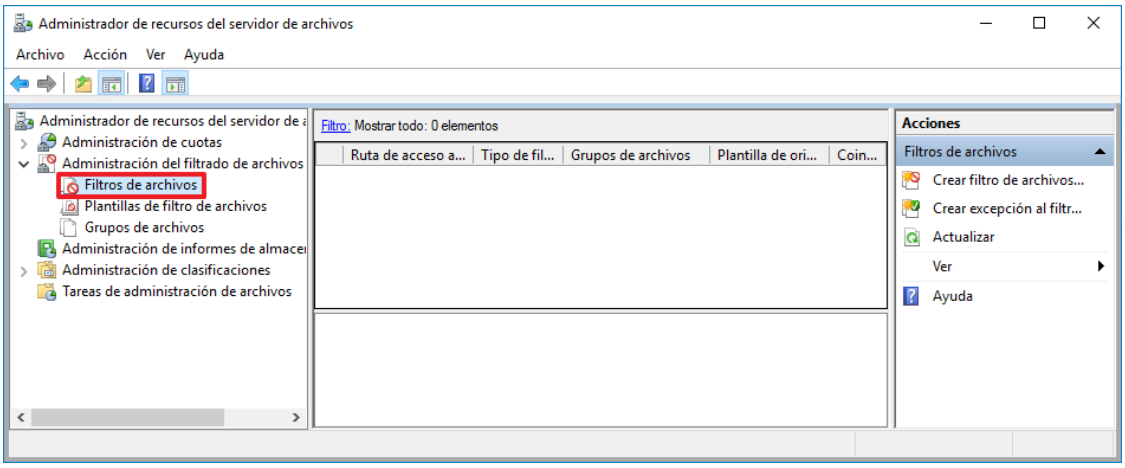
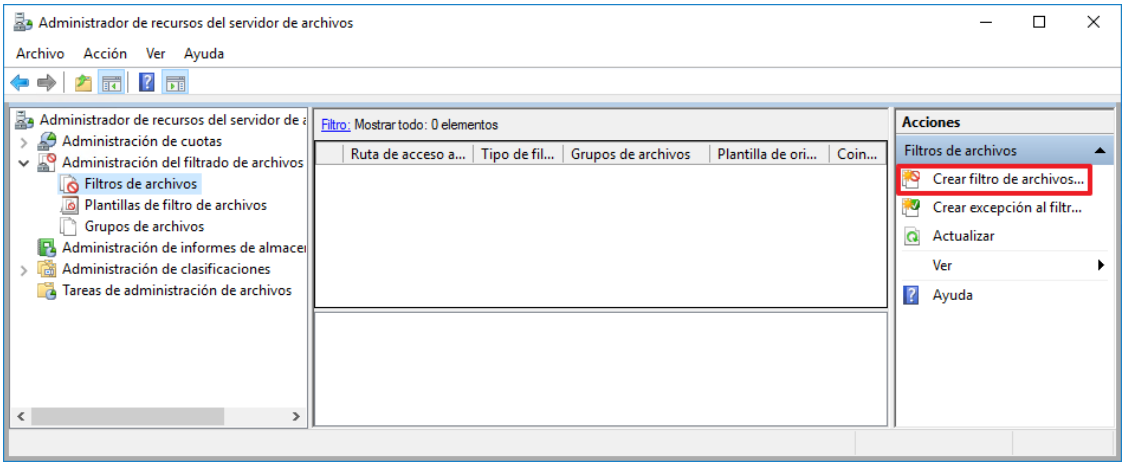
Según lo establecido en el marco operacional para equipos "Servidor de ficheros" que les sea de aplicación la categoría media de ENS, será necesario configurar el filtrado de archivos para prevenir la introducción en éste de archivos indeseados o que puedan poner en riesgo la seguridad del sistema.

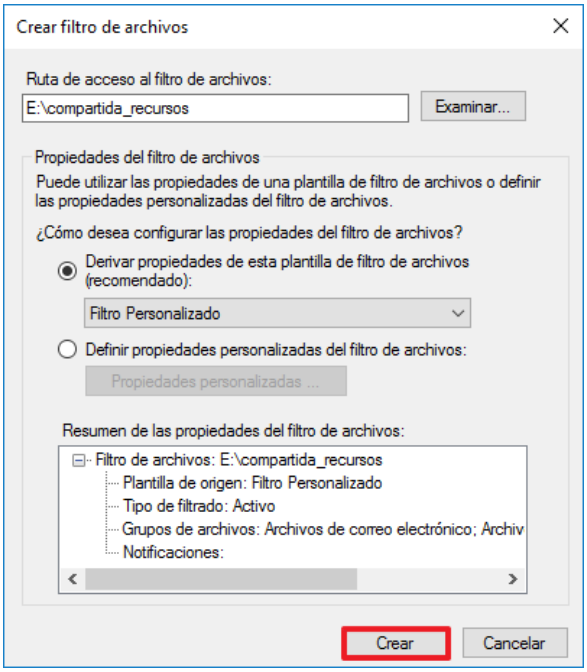
Paso	Descripción
89.	Inicie sesión en el servidor miembro donde tenga instalado el rol "Servidor de ficheros".  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
90.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
91.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
92.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
93.	Expanda el nodo “Plantillas de filtro de archivos” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Plantillas de filtro de archivos”** tal y como se muestra a continuación. 
94.	En el panel “Acciones” seleccione “Crear plantilla de filtro”. 

Paso	Descripción
95.	Ajuste y establezca la configuración para realizar un filtro adecuado que evite comprometer la seguridad del sistema. Pulse “Aceptar” para finalizar.  **Nota:** En este ejemplo se crea un filtro denominado “Filtro Personalizado” que bloquea archivos de correo electrónico, archivos de imagen y archivos ejecutables.
96.	Expanda el nodo “Grupos de archivos” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Grupos de archivos”** tal y como se muestra a continuación. 

Paso	Descripción
97.	Seleccione cualquier grupo de archivos con el botón derecho y pulse sobre la opción del menú contextual “Editar propiedades del grupo de archivos…”.  **Nota:** Para este ejemplo se edita el grupo de archivos “Archivos ejecutables”.
98.	En la ventana emergente configure los tipos de archivos que se bloquean y cuales están excluidos. Pulse “Aceptar” para finalizar. 

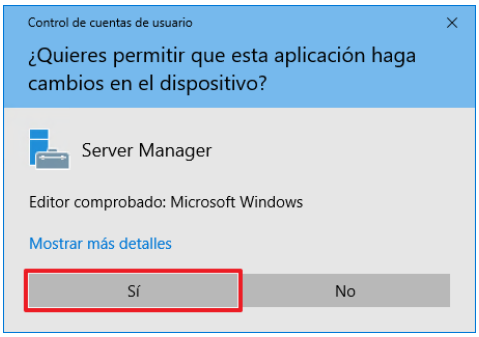
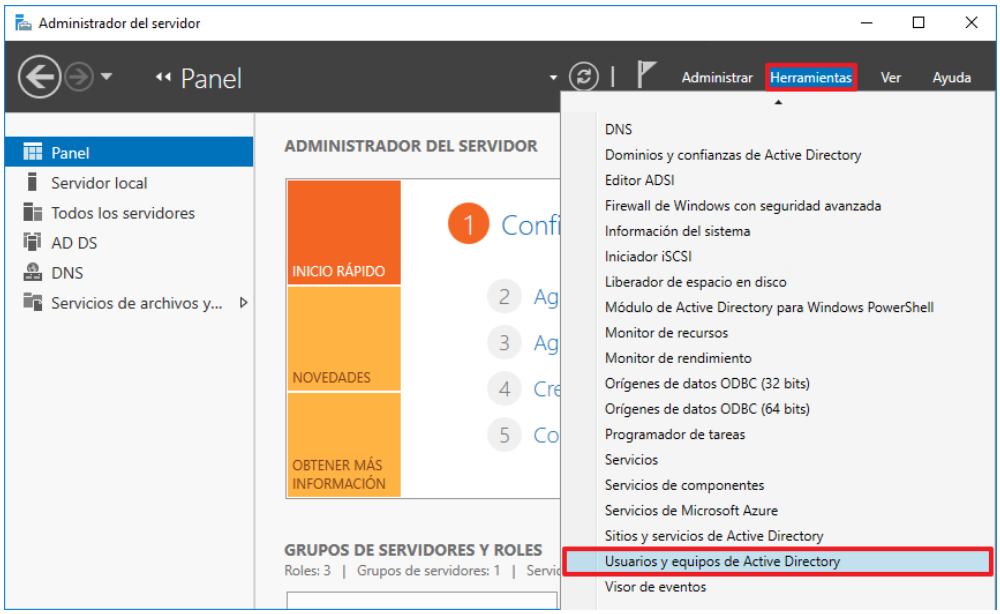
Paso	Descripción
99.	Además, es posible crear un grupo personalizado de archivos para bloquear o excluir seleccionando la opción “Crear grupo de archivos…” en el panel “Acciones”. 
100.	Expanda el nodo “Filtros de archivos” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Filtros de archivos”** tal y como se muestra a continuación. 
101.	En el panel “Acciones” seleccione “Crear filtro de archivos…”. 

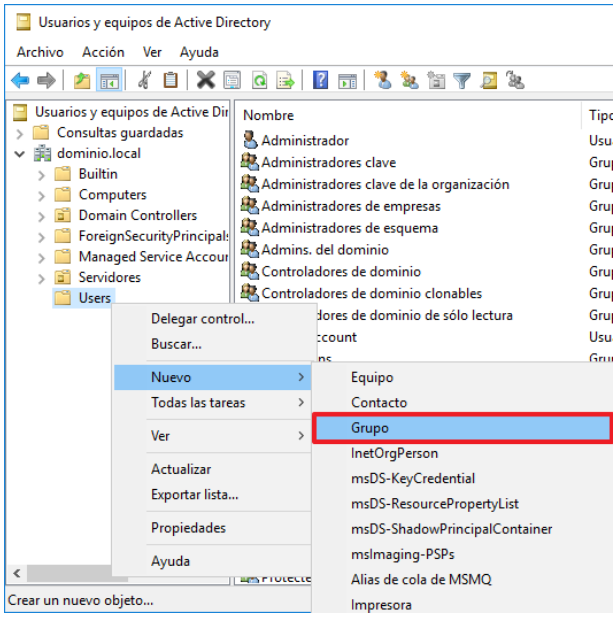
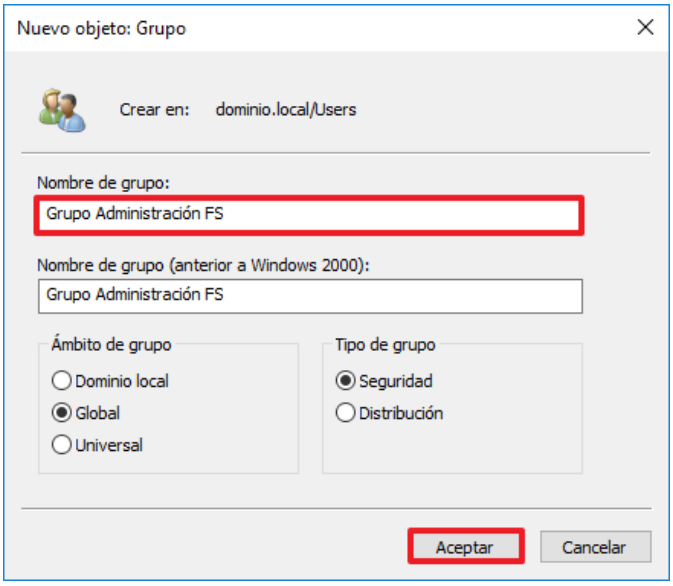
Paso	Descripción
102.	En la ventana emergente seleccione el recurso sobre el que desea aplicar un filtro de archivos y escoja el filtro a aplicar. Pulse “Crear” para finalizar.  **Nota:** Para este ejemplo se ha utilizado el recurso ubicado en “E:\Compartida_Recursos” y se le ha aplicado el filtro creado anteriormente denominado “Filtro Personalizado”.

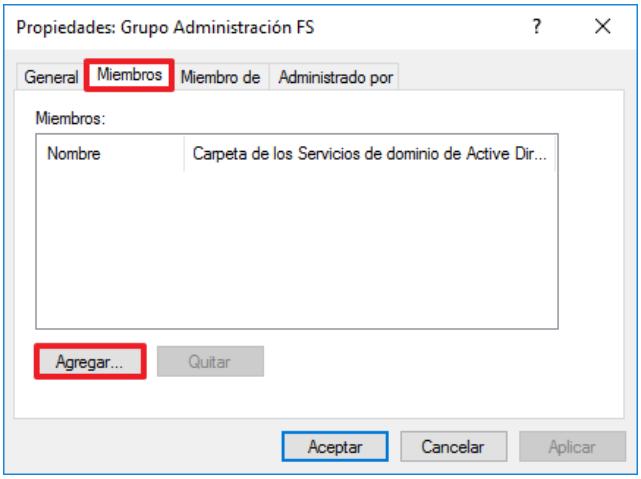
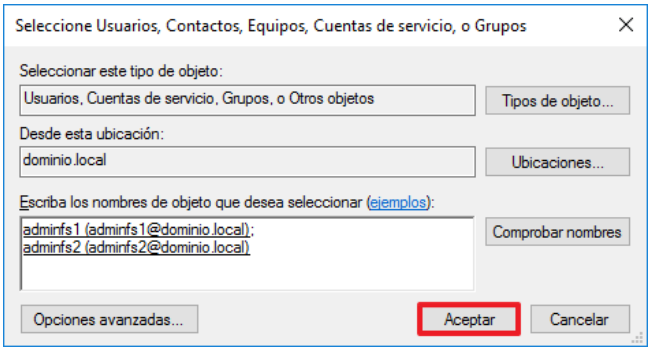
2.6. SEGREGACIÓN DE ROLES

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

Paso	Descripción
103.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

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

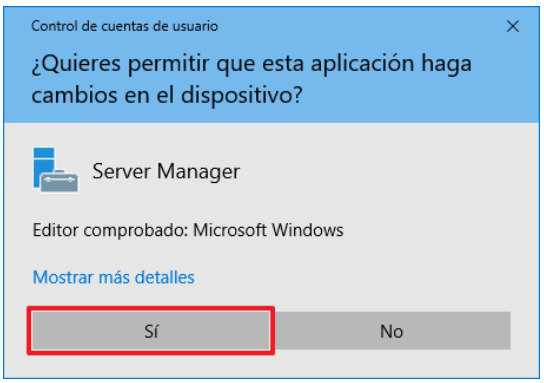
Paso	Descripción
107.	Despliegue el nodo **"<su dominio> → Users"**. Pulse con el botón derecho sobre "Users" y seleccione la opción del menú contextual **"Nuevo → Grupo"**. 
108.	Establezca el nombre de grupo deseado para su organización y pulse "Aceptar".  **Nota:** En este ejemplo se utiliza el nombre "Grupo Administración FS".

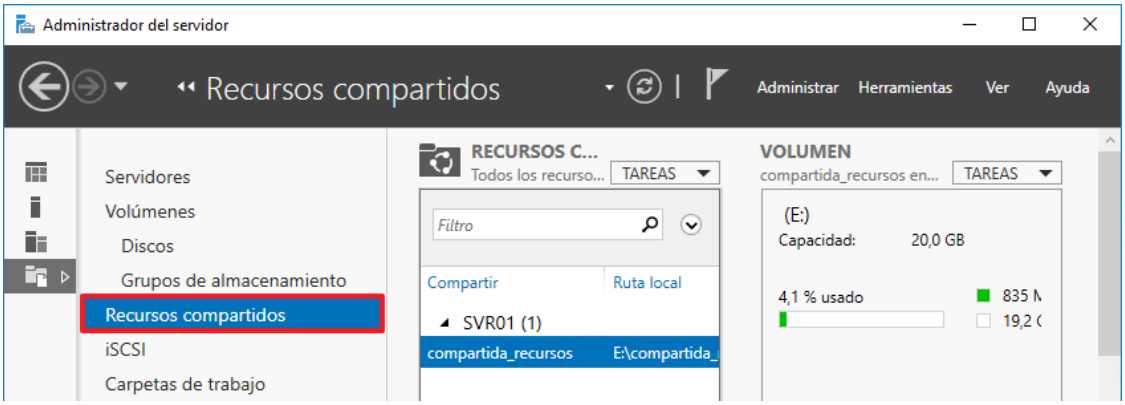
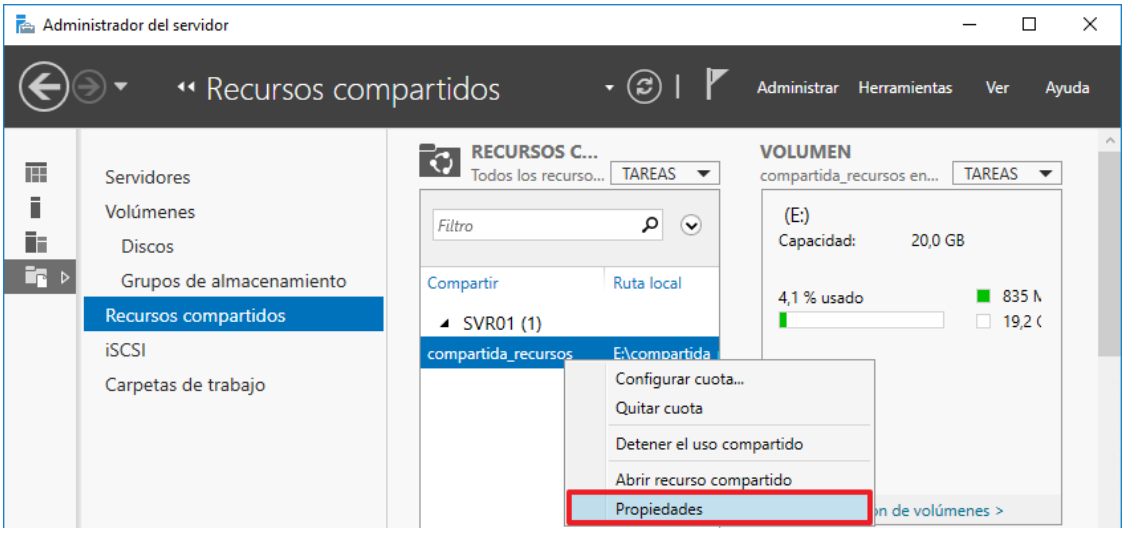
Paso	Descripción
109.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar…” para añadir usuarios al grupo. 
110.	Añada los usuarios que desee al grupo y pulse “Aceptar”.  **Nota:** En este ejemplo se añaden los usuarios “adminfs1” y “adminfs2” utilizados para la creación de esta guía.”

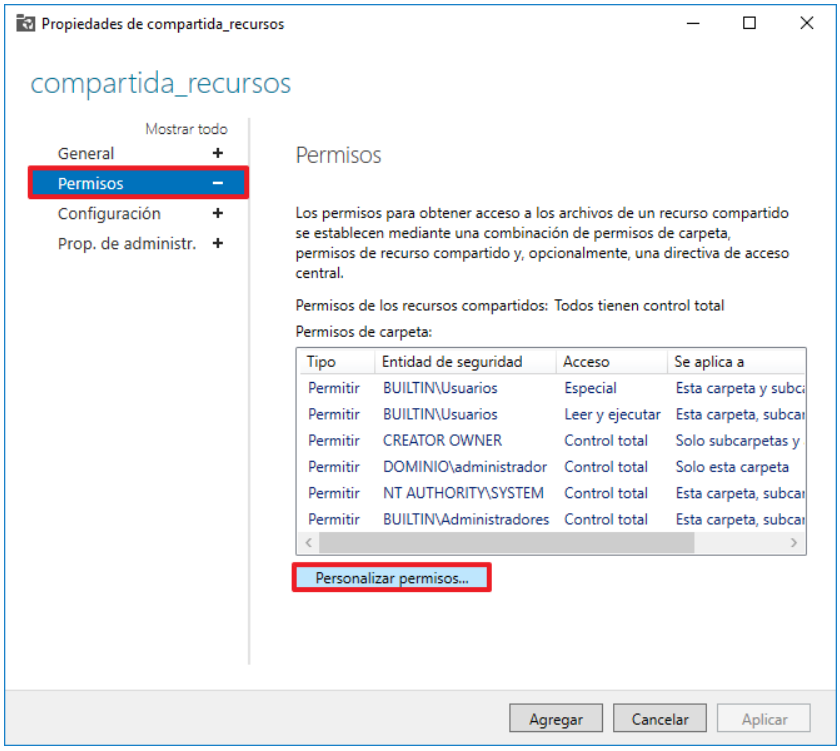
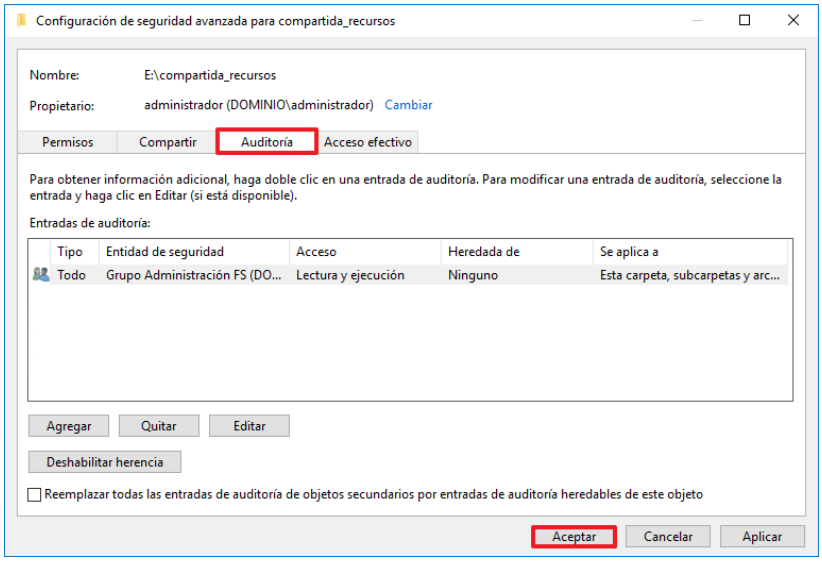
2.7. AUDITORIA DE ARCHIVOS

Con la aplicación del ENS para la categoría media sobre el Servidor de ficheros quedará registrado el uso de los recursos compartidos del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información, con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

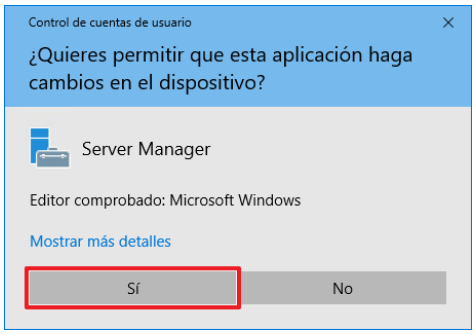
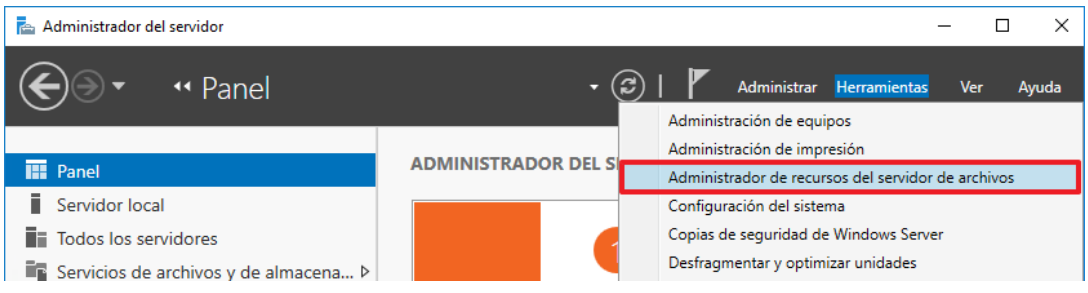
Paso	Descripción
111.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
112.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
113.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

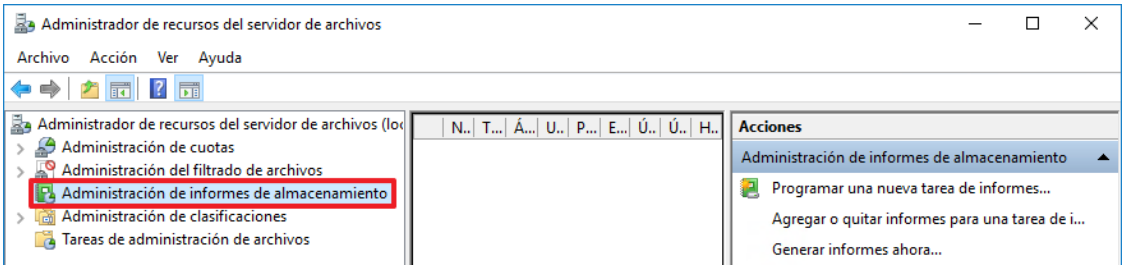
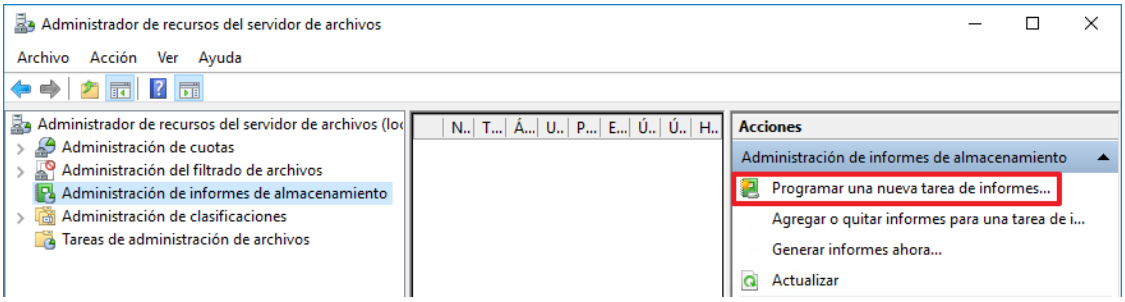
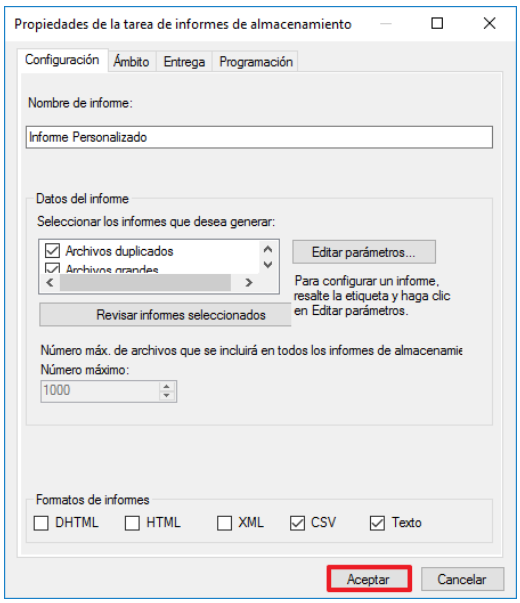
Paso	Descripción
114.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
115.	Seleccione la sección “Recursos compartidos”. 
116.	Seleccione con el botón derecho el recurso sobre el que desea gestionar la auditoría y pulse la opción “Propiedades”.  **Nota:** En este ejemplo se selecciona el recurso compartido creado anteriormente “compartida_recursos”.

Paso	Descripción
117.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos…”. 
118.	Acceda a la pestaña “Auditoría” y configure ésta acorde a las necesidades de su organización. Pulse “Aceptar” y después en la ventana de propiedades del recurso compartido pulse “Agregar” para finalizar el proceso.  **Nota:** En este ejemplo se añade el grupo denominado “Grupo Administración FS”.

2.8. INFORMES DE ALMACENAMIENTO

Con la aplicación del ENS para la categoría media sobre el Servidor de ficheros será necesario configurar los informes de almacenamiento con el objetivo de tener un control sobre los ficheros que están alojados en el sistema y así evitar poner en riesgo la seguridad de éste.

Paso	Descripción
119.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
120.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
121.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
122.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 

Paso	Descripción
123.	Expanda el nodo “Administración de informes de almacenamiento” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración de informes de almacenamiento”** tal y como se muestra a continuación. 
124.	En el panel “Acciones” seleccione “Programar una nueva tarea de informes…”. 
125.	Determine en la ventana emergente la configuración deseada para los informes de almacenamiento sobre un recurso.  **Nota:** En este ejemplo se ha configurado un informe con el nombre “Informe Personalizado” para el recurso denominado “compartida_recursos”.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA SERVIDORES DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

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 el punto de la guía "ANEXO A.3.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN EN 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 Windows 2016 con implementación de seguridad de categoría media del ENS.

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

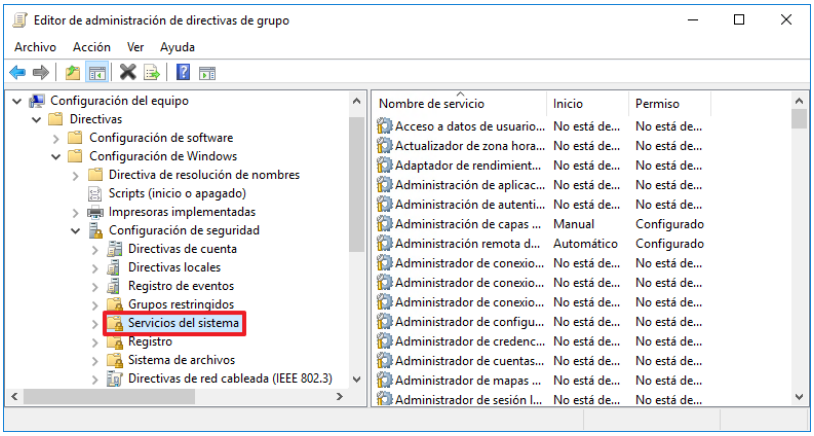
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de ficheros, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el controlador de dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

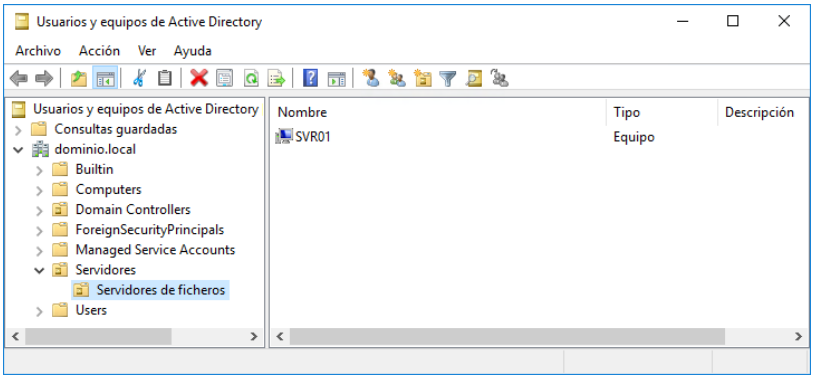
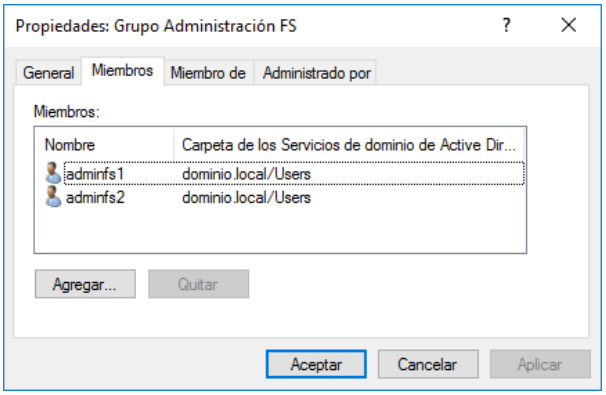
b) En el servidor de ficheros:
   i. Administrador de Windows (explorer.exe).
   ii. Servicios (services.msc).
   iii. Administrador de recursos del servidor de archivos (fsrm.msc).
   iv. Carpetas compartidas (fsmgmt.msc).

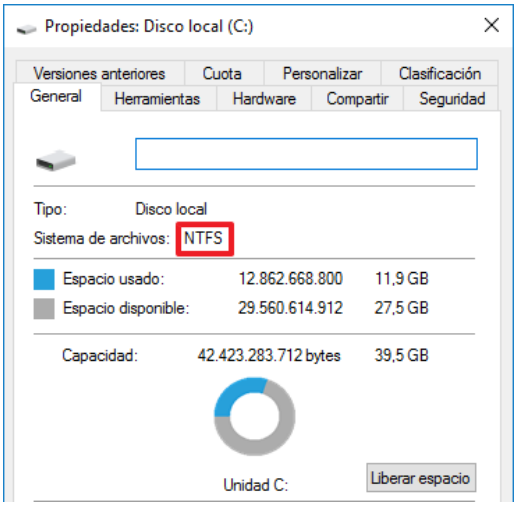
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

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.

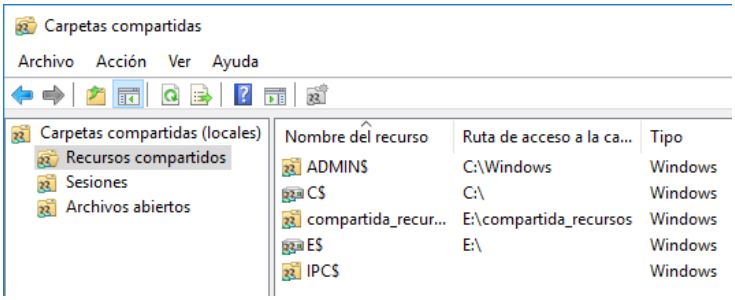
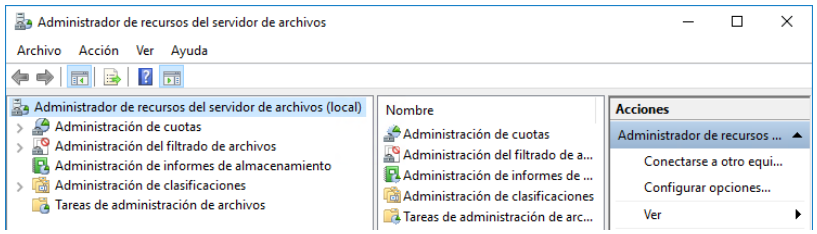
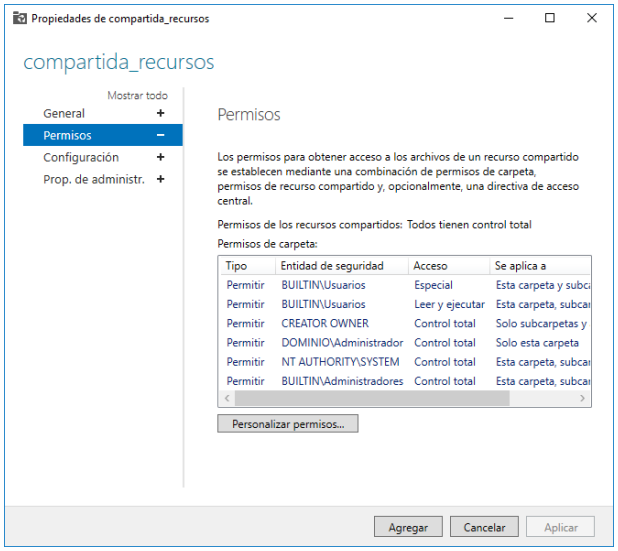
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media		Utilice el Administrador de directivas de grupo (**Inicio → Herramientas administrativas → Administración de directivas de grupo**) y despliegue el menú hasta llegar a las unidades organizativas que contienen los Servidores de ficheros. Verifique que está creada la política "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media". **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros".
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-573 ENS Incremental Servidor de Ficheros CategorIa media" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

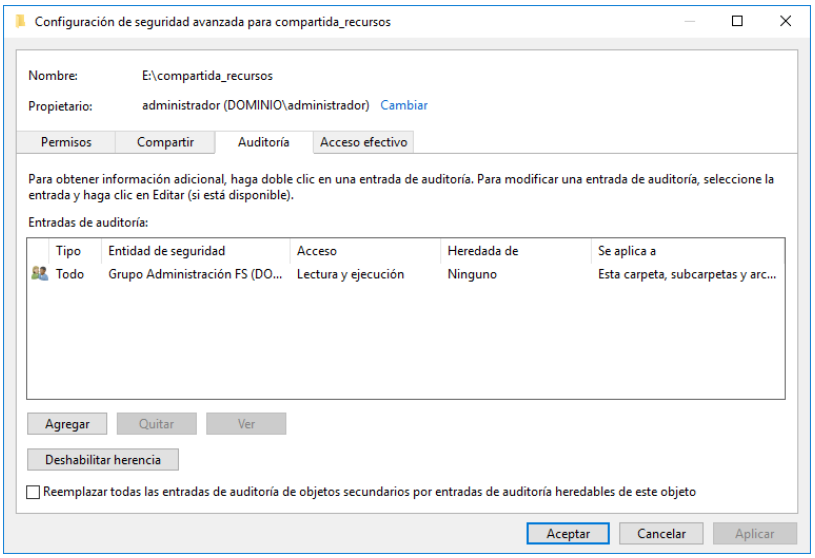
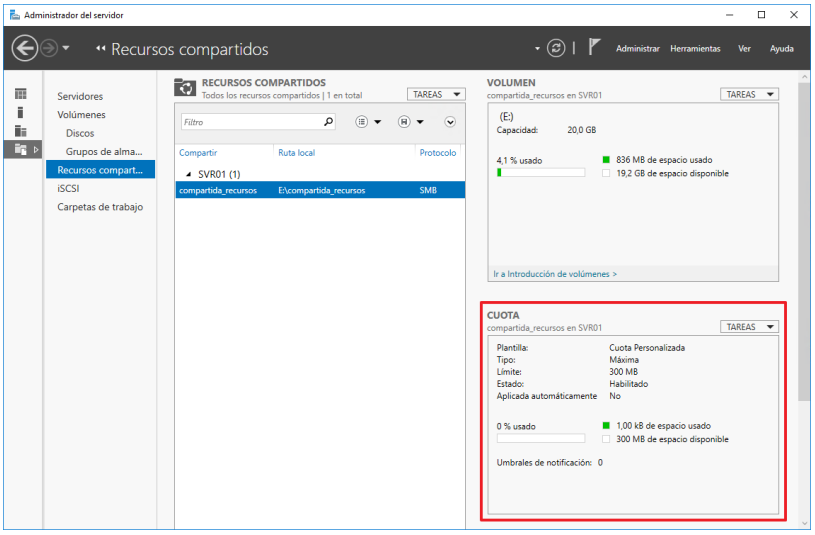
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

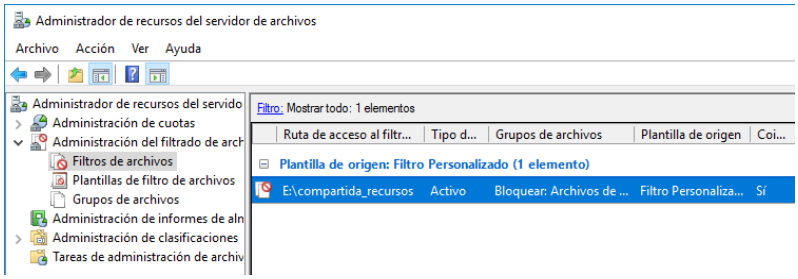
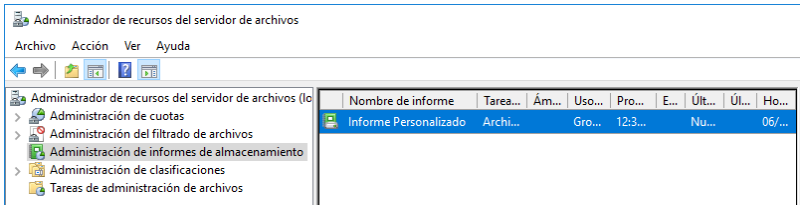
Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que los servidores de ficheros están dentro de las Unidades Organizativas correspondientes		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Ficheros. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de ficheros que se están asegurando.  **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros".
5. Verifique que existen grupos para administrar los recursos compartidos del Servidor de ficheros.		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y compruebe que existen grupos con usuarios para asignar posteriormente a los recursos compartidos con los permisos adecuados.  **Nota:** Para la creación de esta guía se utiliza el grupo "Grupo Administración FS" con los usuarios "adminsfs1" y "adminsfs2".
6. Inicie sesión en un Servidor de ficheros		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos**, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 
8. Verifique que los servicios del sistema relacionados con el servidor de ficheros están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique que la instalación del servidor de ficheros se ha realizado correctamente.		Utilizando la herramienta de administración de ficheros (ejecutando "fsmgmt.msc" desde, botón derecho sobre **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 
10. Verifique que la instalación del servidor de ficheros se ha realizado correctamente		Utilizando la herramienta de administración de ficheros (ejecutando "fsrm.msc" desde, botón derecho sobre **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 
11. Verifique que los recursos compartidos poseen los permisos adecuados para los diferentes usuarios.		Desde el Administrador del servidor acceda al apartado **"Servicios de archivos y almacenamiento → Recursos compartidos"**. Haga clic derecho sobre uno de los recursos compartidos y seleccione "Propiedades". Acceda a la sección "Permisos" y verifique los permisos que posee el recurso. 

Comprobación	OK/NOK	Cómo hacerlo
12.Verifique que los recursos poseen una auditoría configurada.		En la sección "Permisos", pulse sobre "Personalizar permisos…". Acceda a la pestaña auditoría y verifique su configuración.  **Nota:** Para la realización de esta guía se activa la auditoría para el grupo denominado "Grupo Administración FS".
13.Verifique que los recursos compartidos poseen las cuotas de disco adecuadas.		Desde el Administrador del servidor acceda al apartado **"Servicios de archivos y almacenamiento → Recursos compartidos"**. Seleccione cualquier recurso y observe el aparatado "Cuota" para comprobar cuál de las disponibles tiene aplicada cada recurso.  **Nota:** Para la realización de esta guía se aplica la cuota denominada "Cuota Personalizada" sobre "E:\compartida_recursos".

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que los recursos compartidos poseen el filtrado de archivos adecuado.		Utilizando la herramienta de administración de ficheros (ejecutando "fsrm.msc" desde, botón derecho sobre **Inicio → Ejecutar…**) verifique en el nodo **"Administración del filtrado de archivos → Filtros de archivos"** que existen filtros aplicados a los recursos compartidos.  **Nota:** Para la realización de esta guía se aplica un filtro sobre el recurso denominado "compartida_recursos".
15. Verifique que se han configurado informes de almacenamiento para los recursos compartidos.		Utilizando la misma herramienta verifique en el nodo **"Administración de informes de almacenamiento"** que están configurados los informes para los distintos recursos.  **Nota:** Para la realización de esta guía se crea un informe para el recuso denominado "compartida_recursos".

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

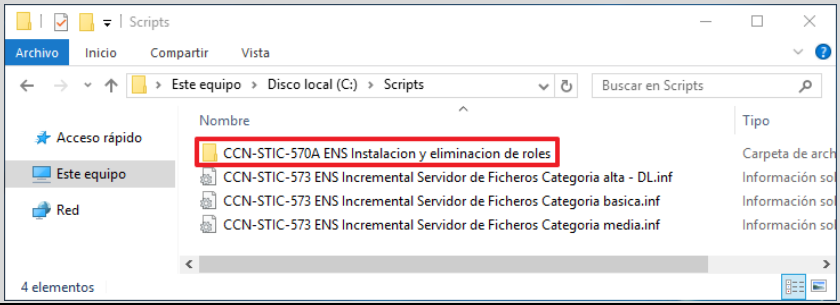
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen Servidores de ficheros con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría 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 alta, 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 usó 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.

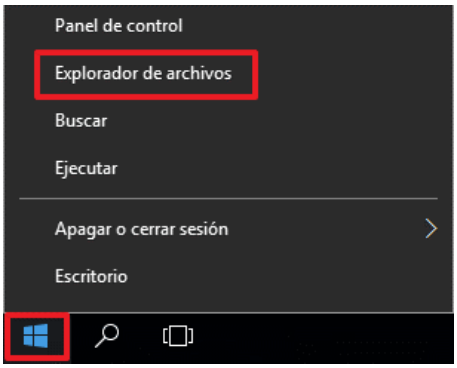
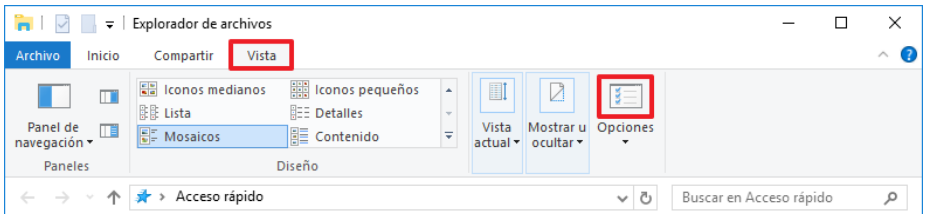
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

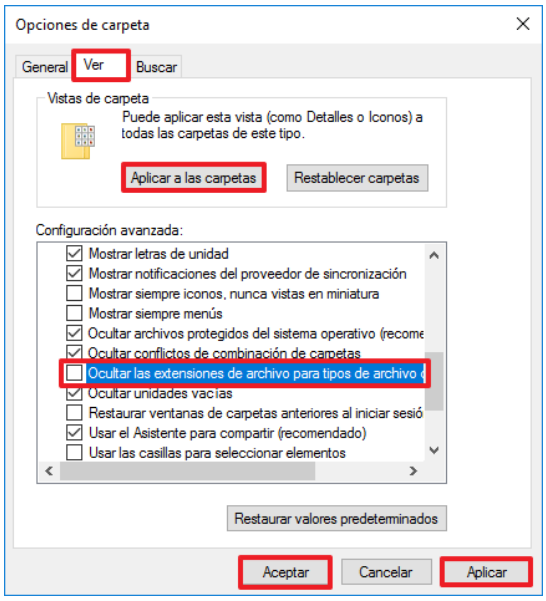
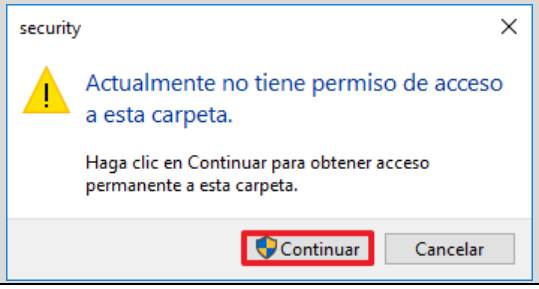
Nota: Si instala el Servidor de ficheros por primera vez con la guía “CCN-STIC-570A – Implementación del ENS en Windows Server 2016” aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada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

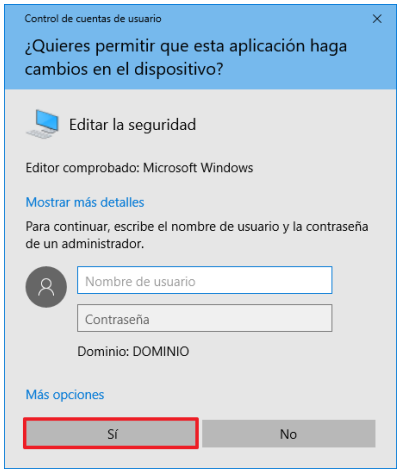
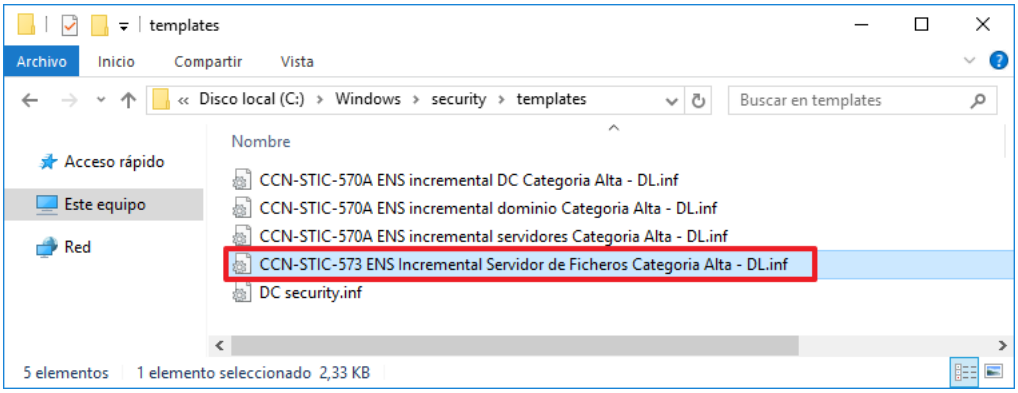


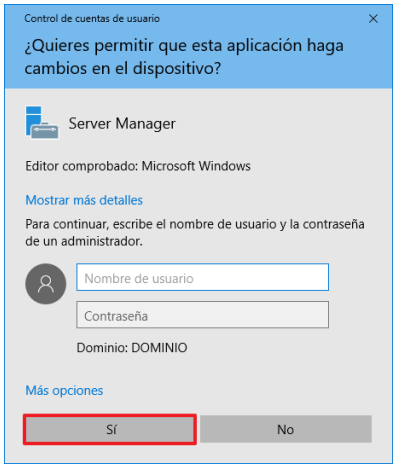
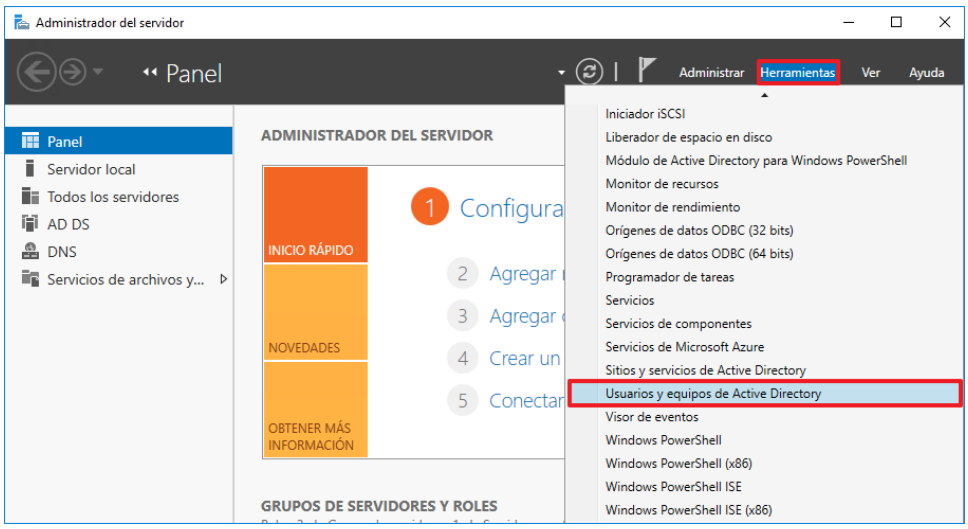
1. PREPARACIÓN DEL DOMINIO

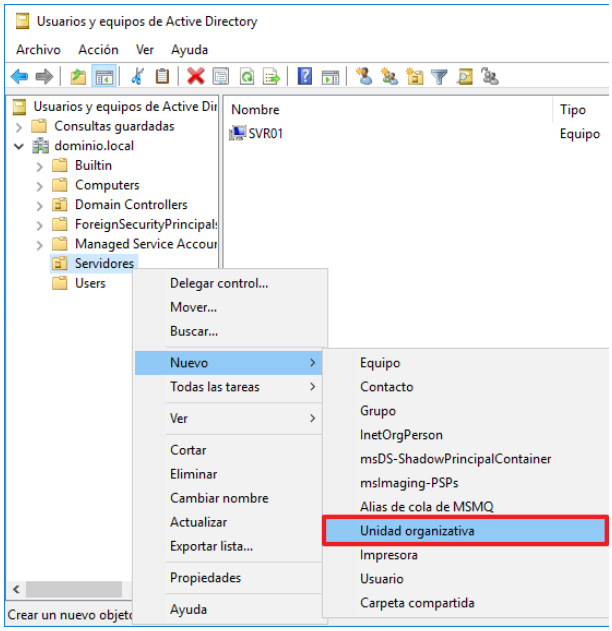
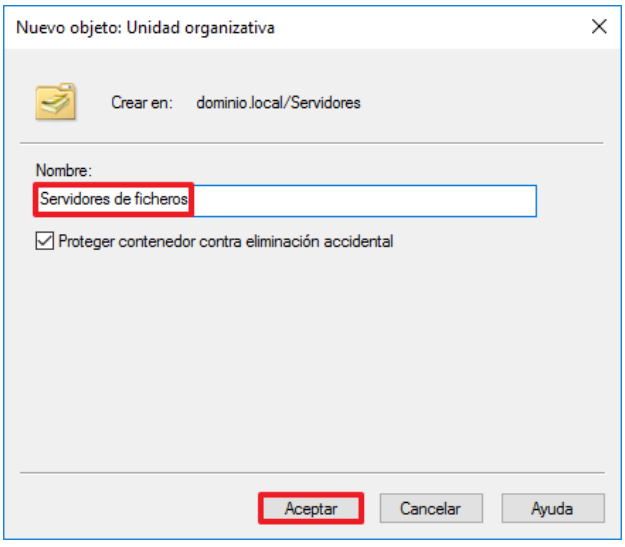
Los pasos que se describen a continuación se realizarán sobre un equipo Controlador de Dominio del dominio al que va a pertenecer el Servidor de ficheros que se está asegurando.

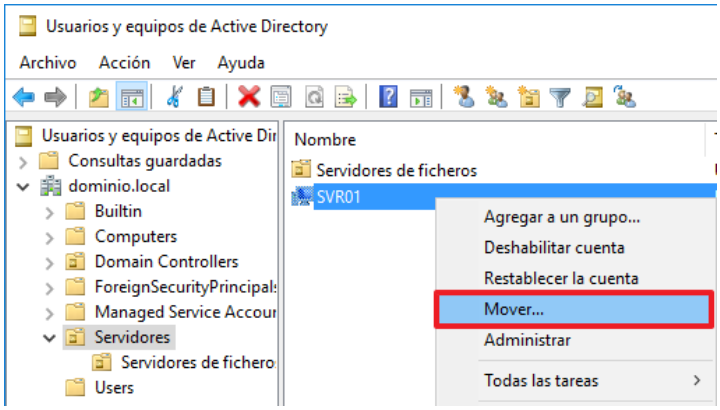
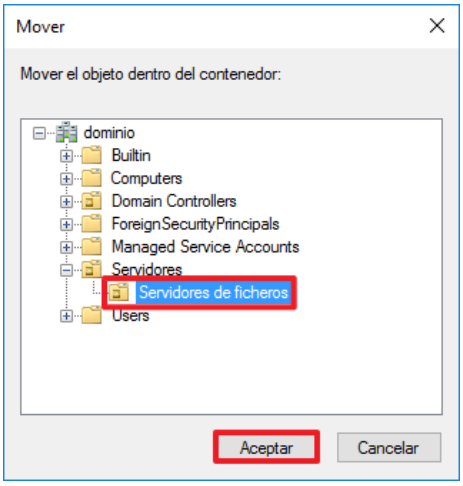
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	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”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

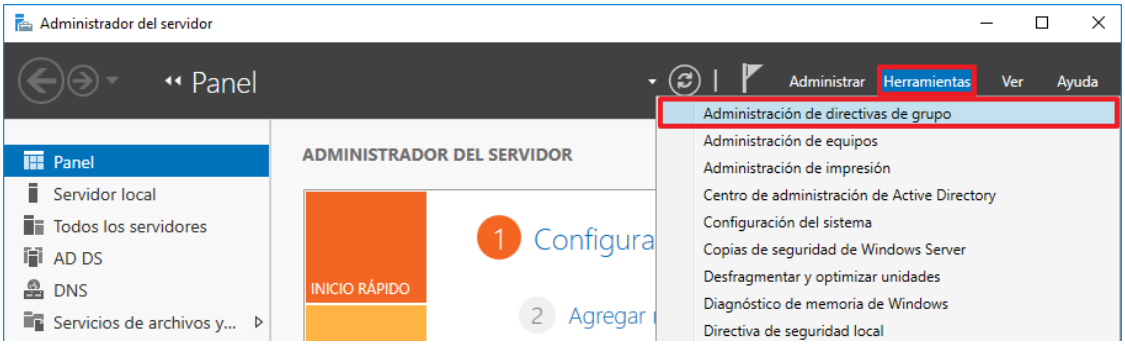
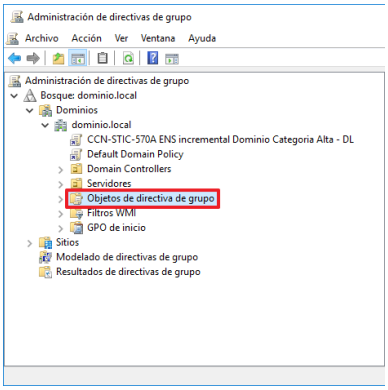
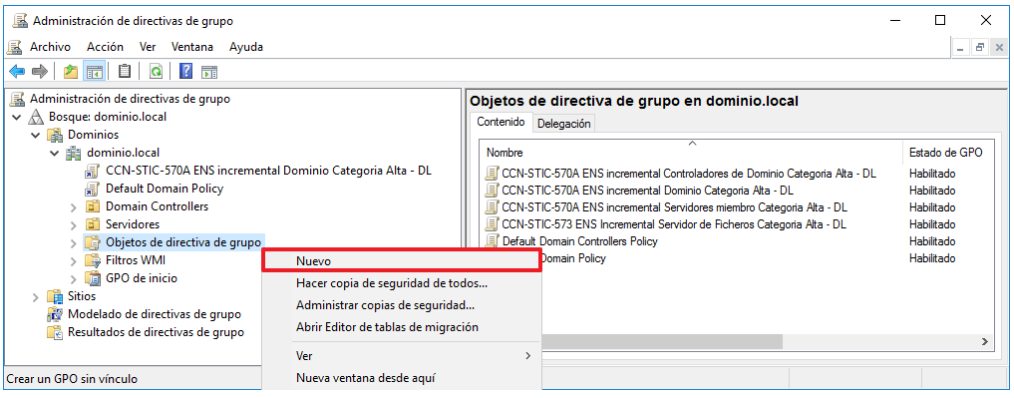
Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí”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

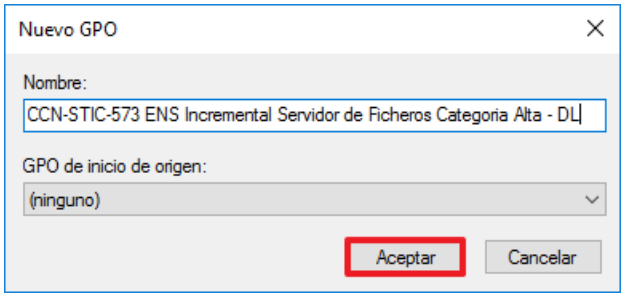
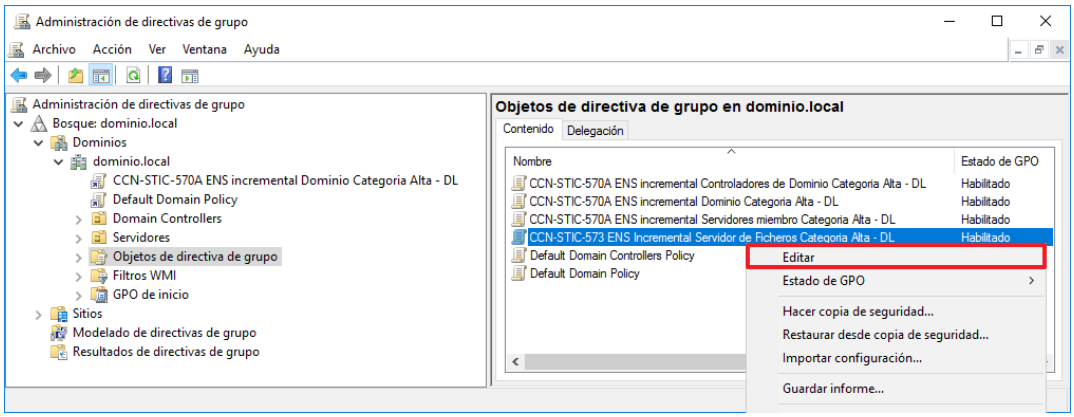
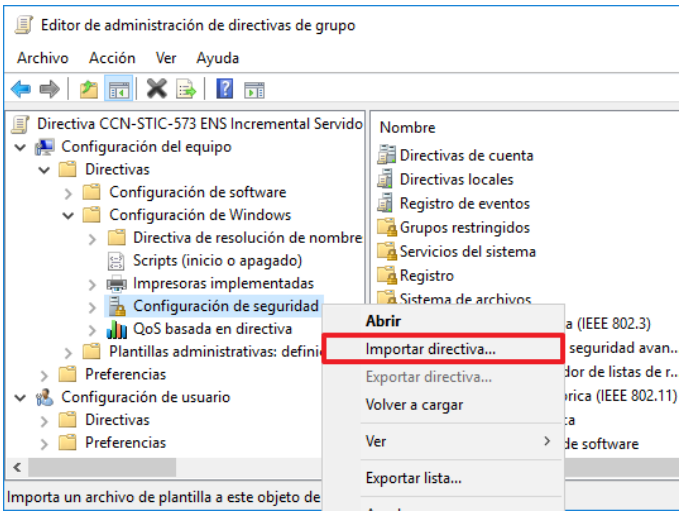
Paso	Descripción
8.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Introduzca las credenciales y pulse "Sí" para continuar. 
9.	Copie el fichero "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta - DL.inf" ubicado en "C:\Scripts" en el directorio "C:\Windows\Security\Templates". 
10.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 

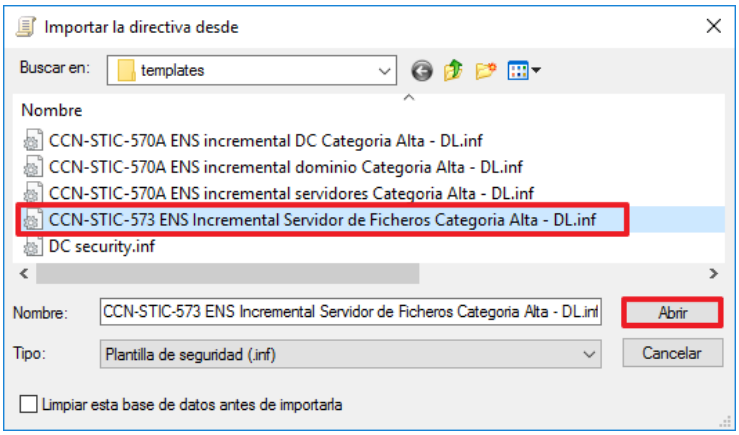
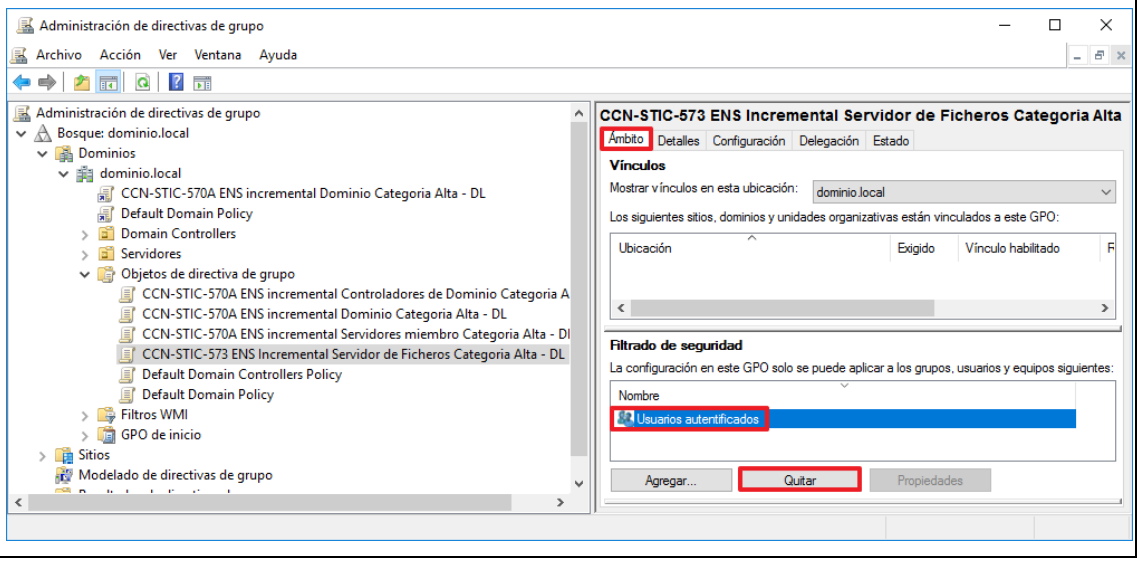
Paso	Descripción
11.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 
12.	A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”** 

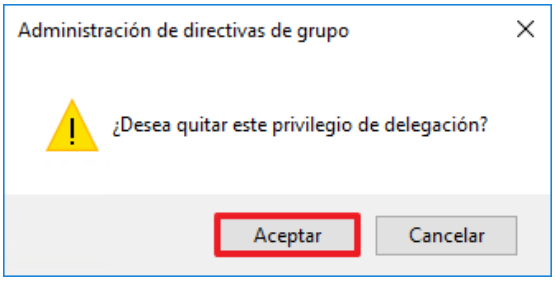
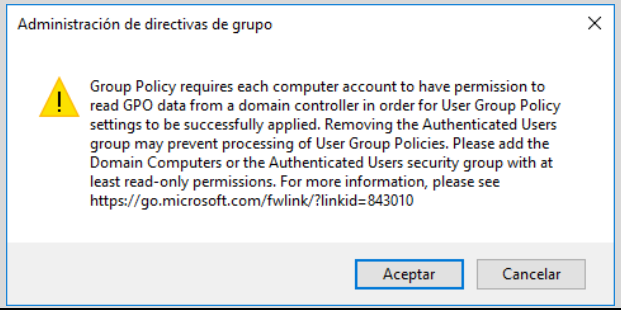
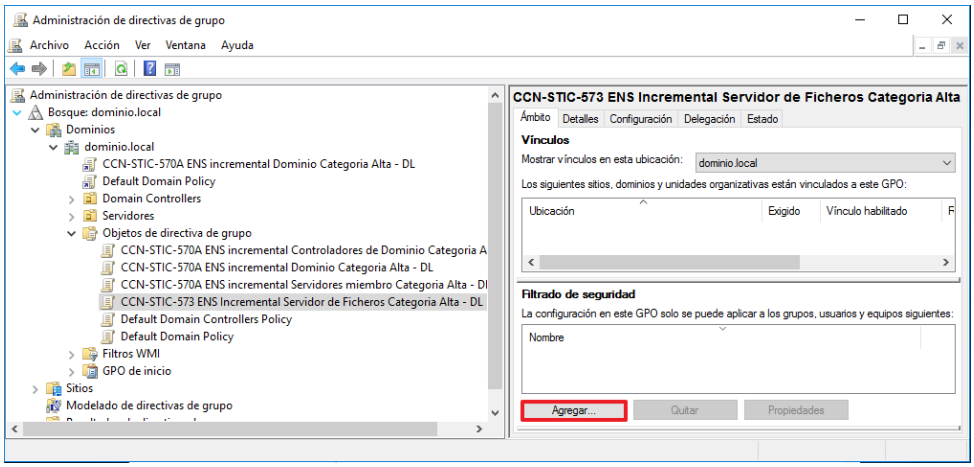
Paso	Descripción
13.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> →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

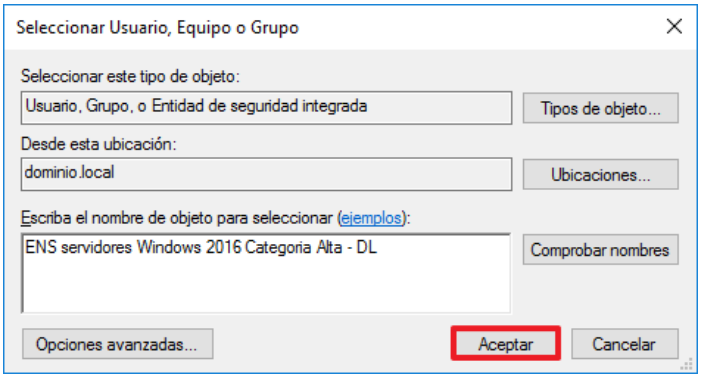
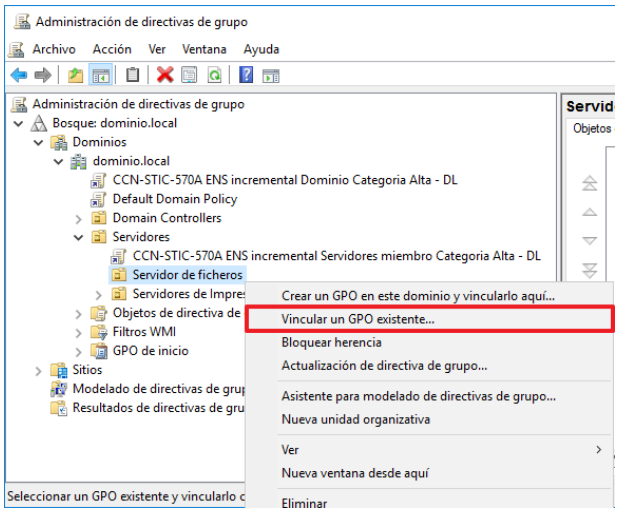
Paso	Descripción
15.	Una vez creada la nueva unidad organizativa, deberá mover los servidores de ficheros a la unidad organizativa “Servidores de ficheros”. Para ello, deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva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

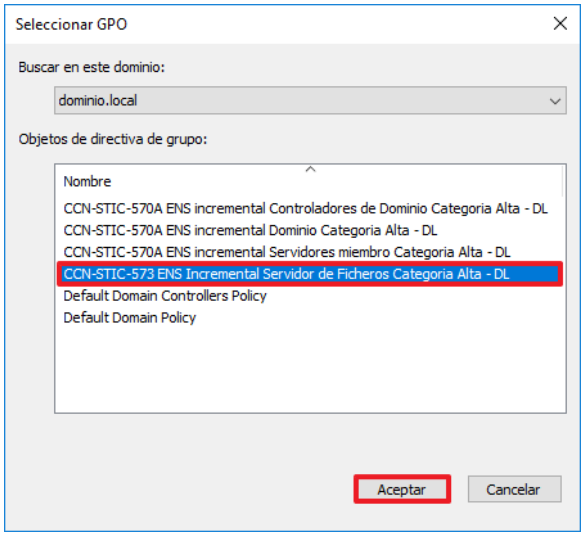
Paso	Descripción
19.	Inicie la consola “Administración de directivas de grupo”. Para ello pulse sobre el botón “**Herramientas → Administración de directivas de grupo**”. 
20.	Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en **“Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”**. 
21.	Pulse con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción del menú contextual “Nuevo”. 

Paso	Descripción
22.	Establezca para la nueva GPO el nombre “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria Alta - DL” y pulse “Aceptar”. 
23.	A continuación, pulse con el botón derecho sobre la GPO recién creada y seleccione la opción del menú contextual “Editar”. 
24.	Ubíquese sobre el nodo **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción del menú contextual “Importar directiva…”. 

Paso	Descripción
26.	Seleccione la plantilla de seguridad “CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria Alta - DL.inf” ubicada en “C:\Windows\Security\Templates”. Pulse sobre el botón “Abrir” para continuar. 
27.	Cierre el “Editor de administración de directivas de grupo”.
28.	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 autentificados”. Pulse sobre el botón “Quitar”. 

Paso	Descripción
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.  **Nota:** Si le aparece la siguiente advertencia ignórela y pulse “Aceptar”. 
30.	A continuación, pulse sobre el botón “Agregar…”. 

Paso	Descripción
31.	Agregue los grupos de usuarios que contengan los equipos con el rol “Servidor de ficheros” y pulse “Aceptar” para finalizar.  **Nota:** Para este ejemplo se utiliza el grupo “ENS servidores Windows 2016 categoria alta - DL” que contiene el servidor con el rol “Servidor de ficheros”.
32.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de ficheros”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de ficheros”.
33.	Seleccione con el botón derecho la unidad organizativa y pulse sobre la opción del menú contextual “Vincular GPO existente…”. 

Paso	Descripción
34.	A continuación, localice la GPO configurada anteriormente, "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria Alta - DL", y pulse "Aceptar". 
35.	Cierre la consola "Administración de directivas de grupo" y elimine la carpeta "C:\Scripts".

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 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.

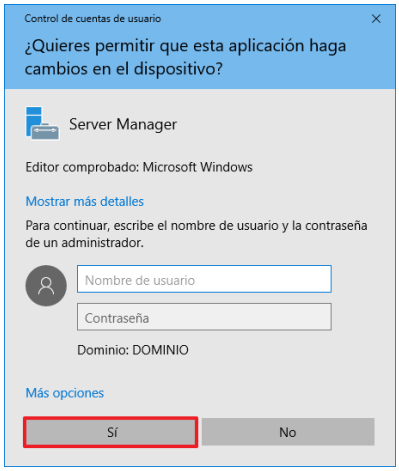
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

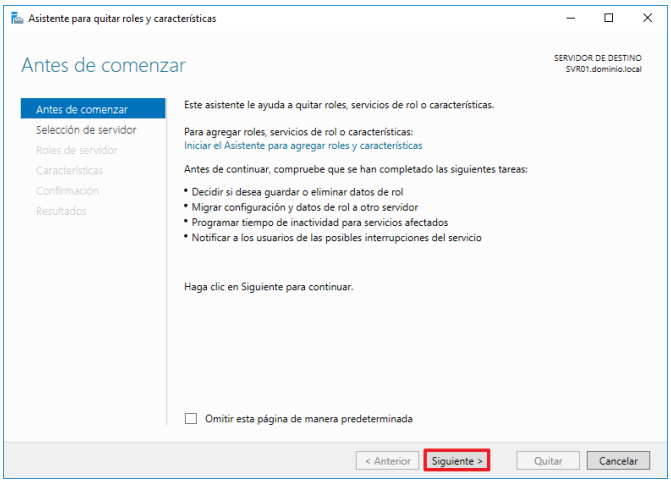
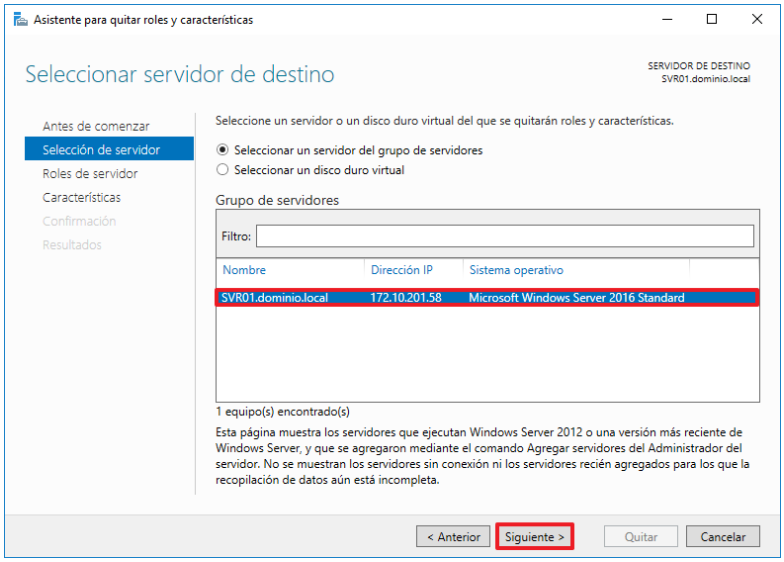
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

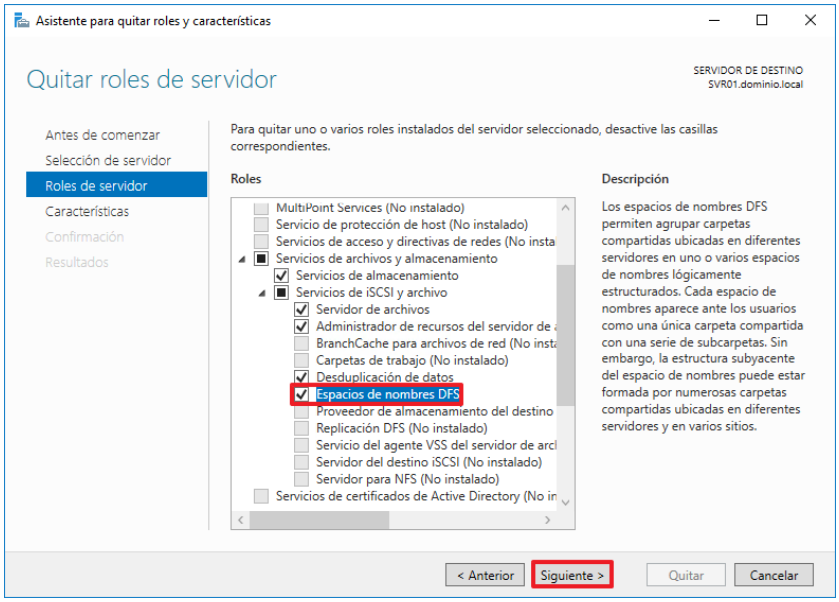
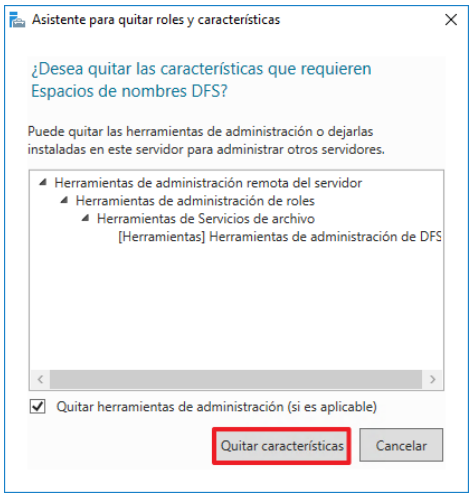
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

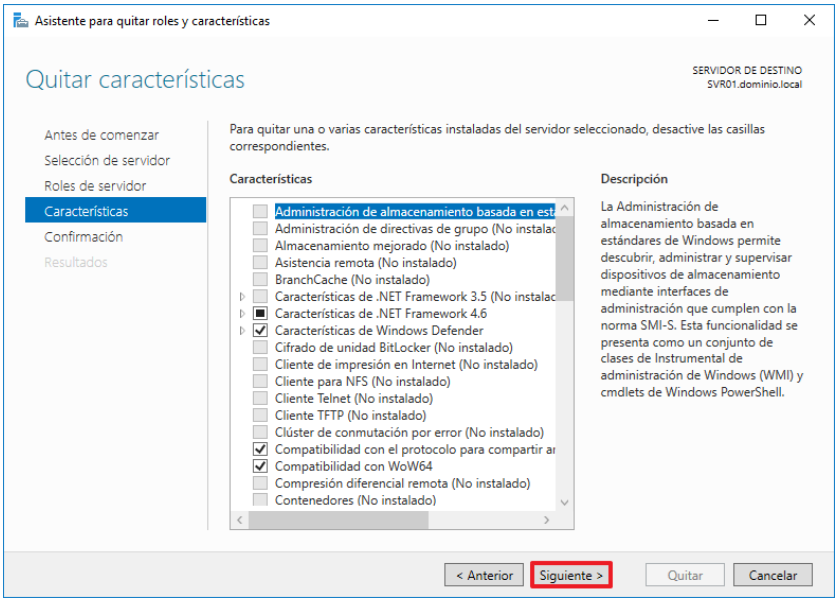
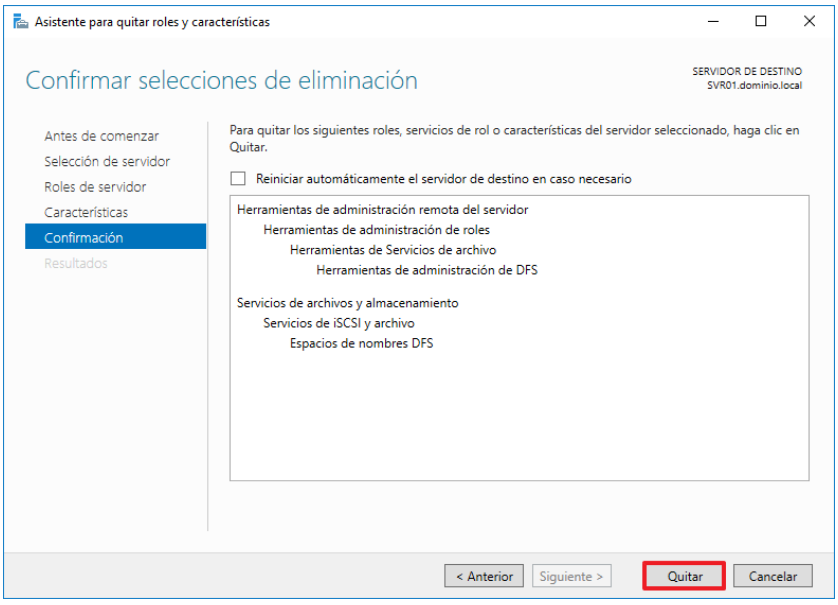
En el procedimiento que se describe a continuación, a modo de ejemplo, se desinstala un rol que actualmente no está siendo utilizado por el Servidor de ficheros.

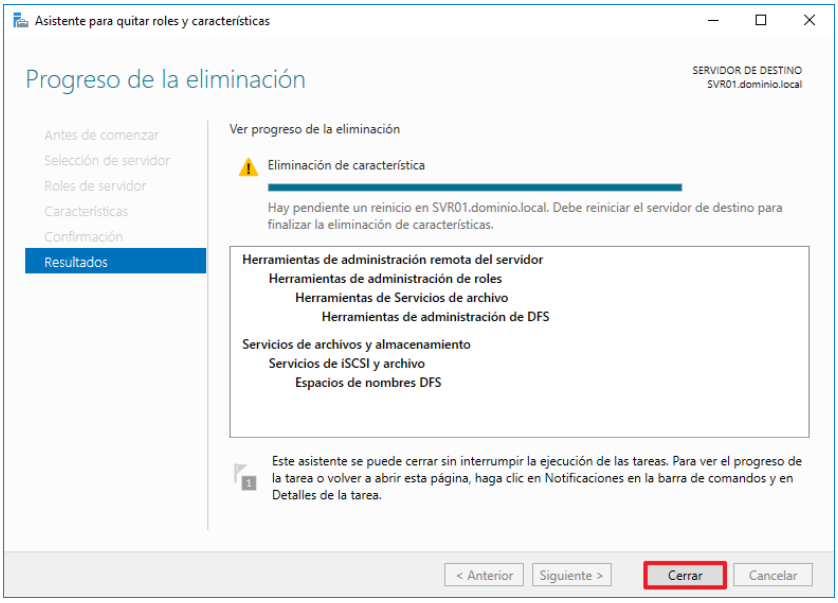
Nota: Para continuar con el siguiente paso a paso deberá realizar previamente el "ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR MIEMBRO O CONTROLADOR DE DOMINIO QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA O ALTA DEL ENS" de la guía "CCN-STIC-570A - Implementación del ENS en Microsoft Windows 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
36.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.
37.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
38.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Introduzca las credenciales y pulse "Sí" para continuar. 

Paso	Descripción
39.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 
40.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
41.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

Paso	Descripción
42.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Espacios de nombres DFS”.
43.	En el caso de que el rol posea características que dependen de él se lanzara una ventana para decidir si eliminar sus características asociadas.  **Nota:** En este ejemplo se eliminan las características que dependen del rol.

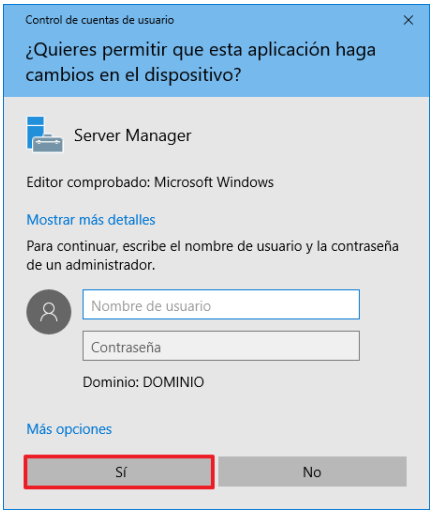
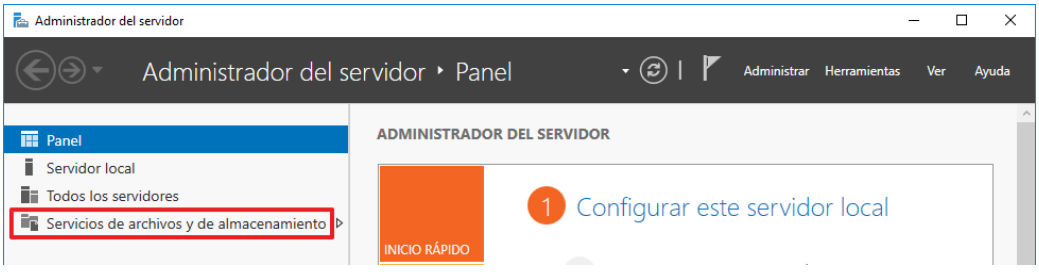
Paso	Descripción
44.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
45.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

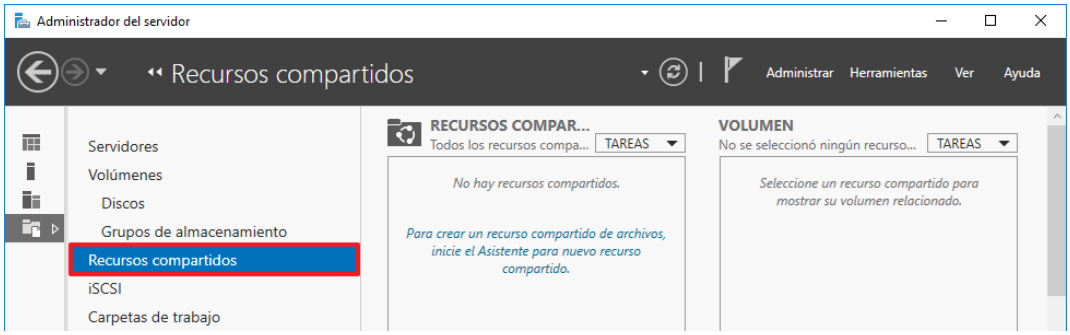
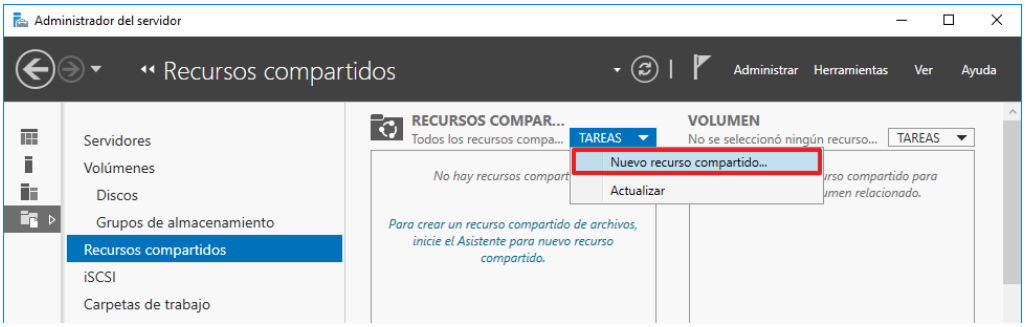
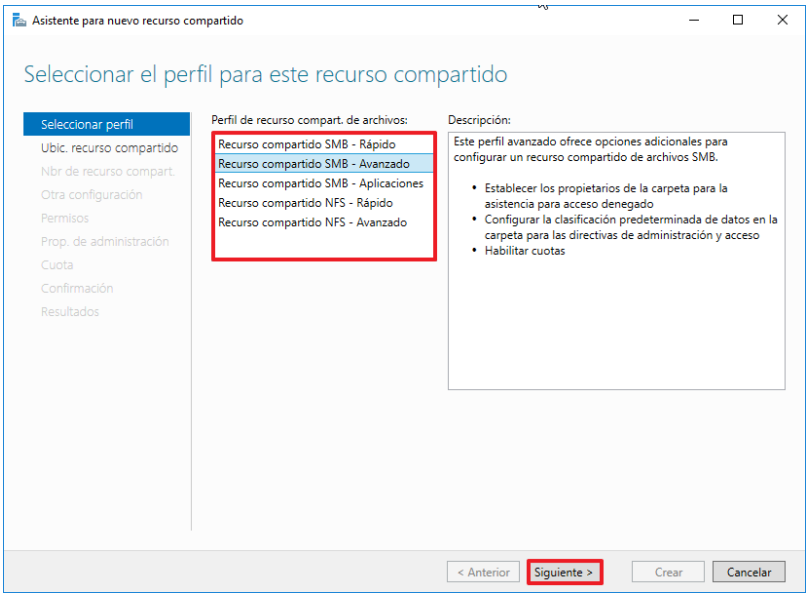
Paso	Descripción
46.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar. 
47.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
48.	A continuación, deberá desvincular la GPO creada anteriormente para eliminar un rol.

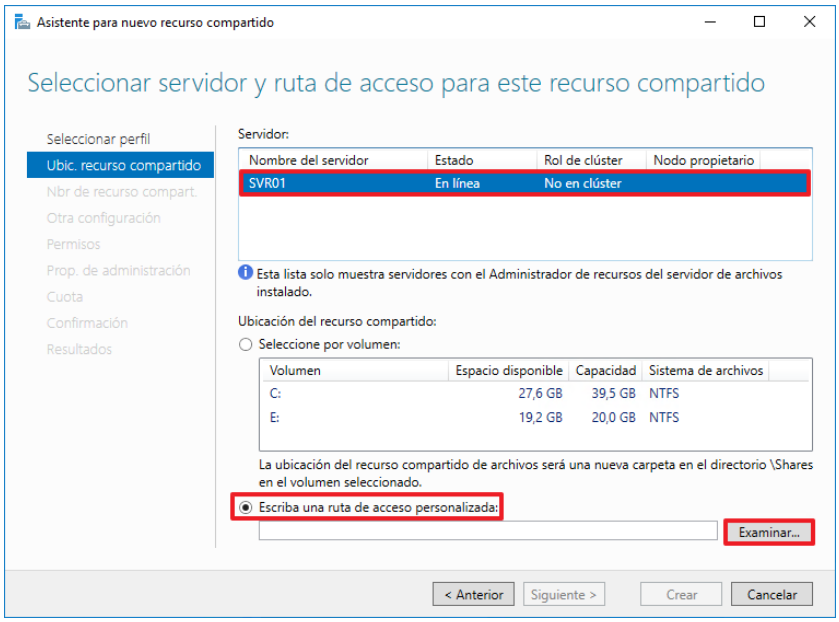
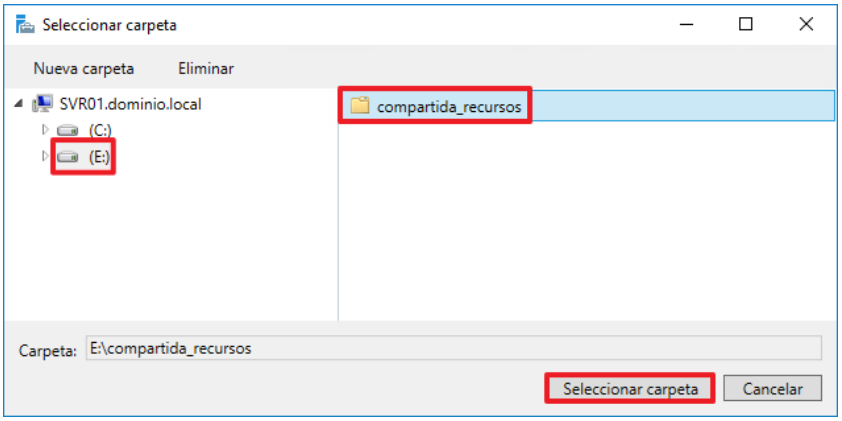
2.2. COMPARTICIÓN DE RECURSOS

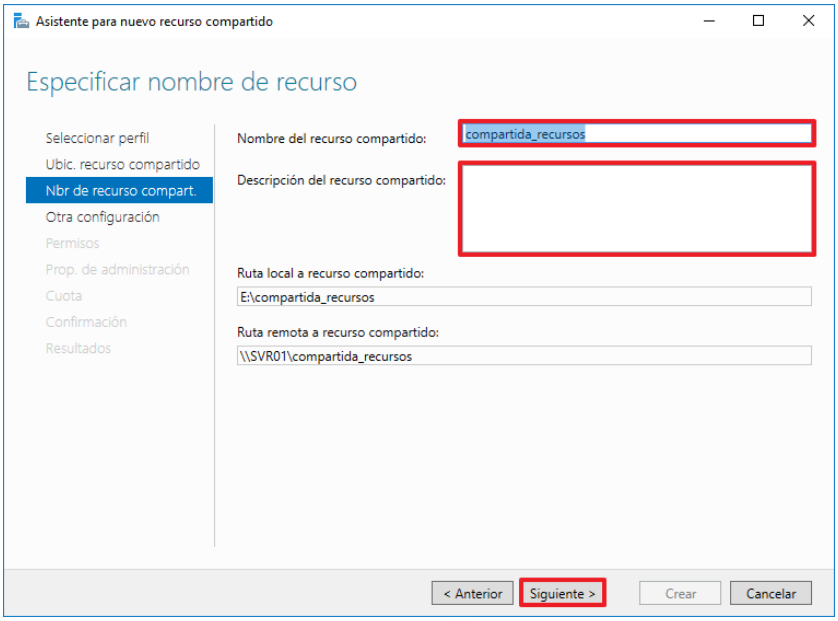
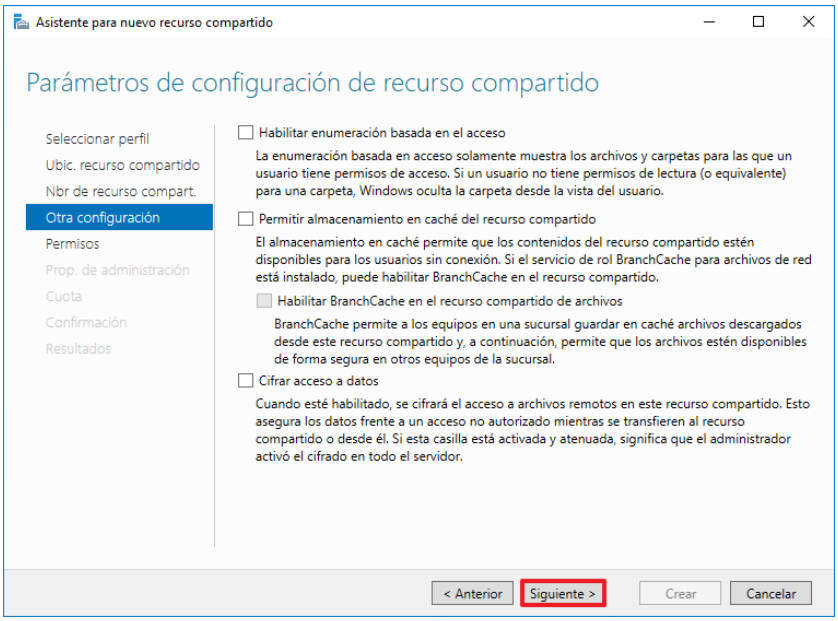
Es importante determinar que recursos se comparten en el Servidor de ficheros. Dependiendo de que recursos se compartan pueden generarse accesos indeseados, es por ello que tal y como indica el ENS es recomendable que los recursos que se comparten en el Servidor de ficheros estén alojados en otra ubicación de disco diferente a la del sistema operativo y que ésta solo se utilice para el alojamiento de recursos, evitando con ello exponer más información de la estrictamente necesaria.

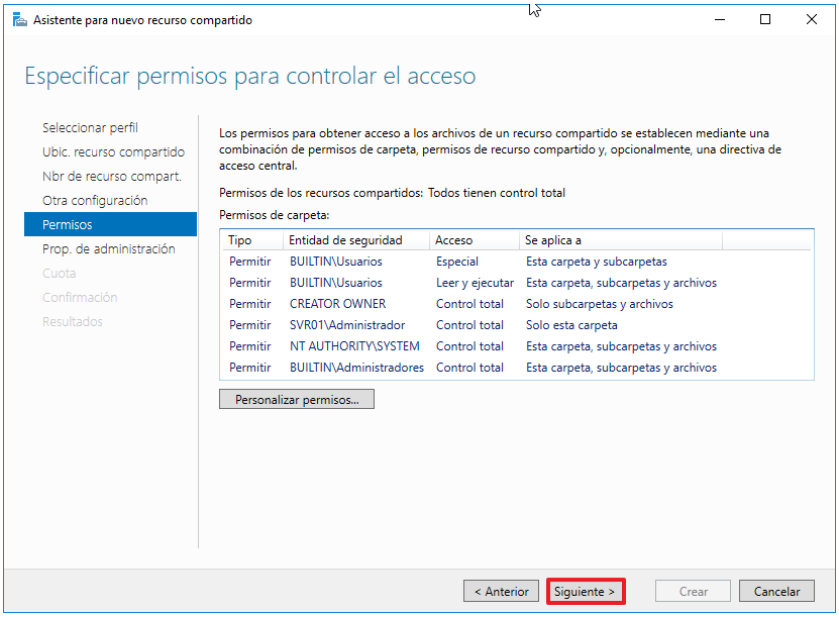
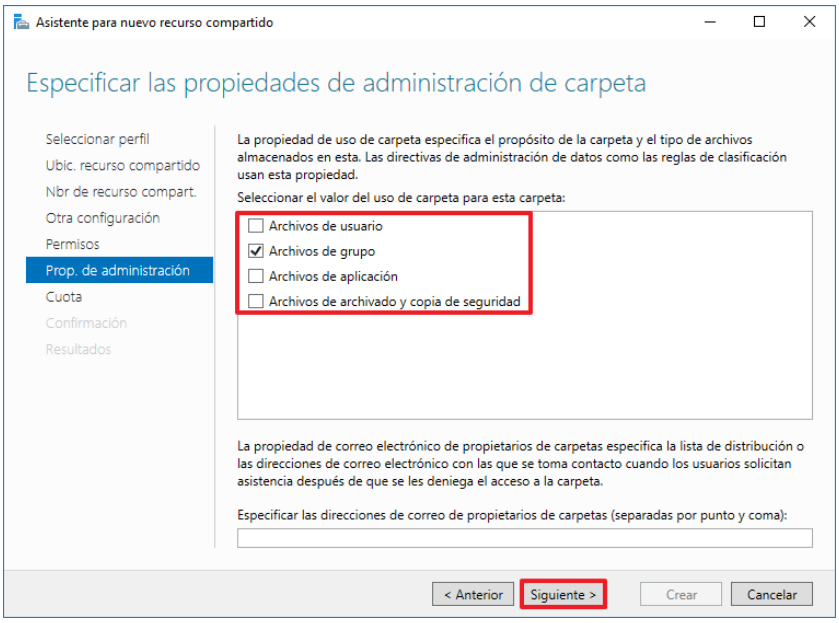
En este apartado se determinará la gestión de los recursos que son compartidos a través del Servidor de ficheros.

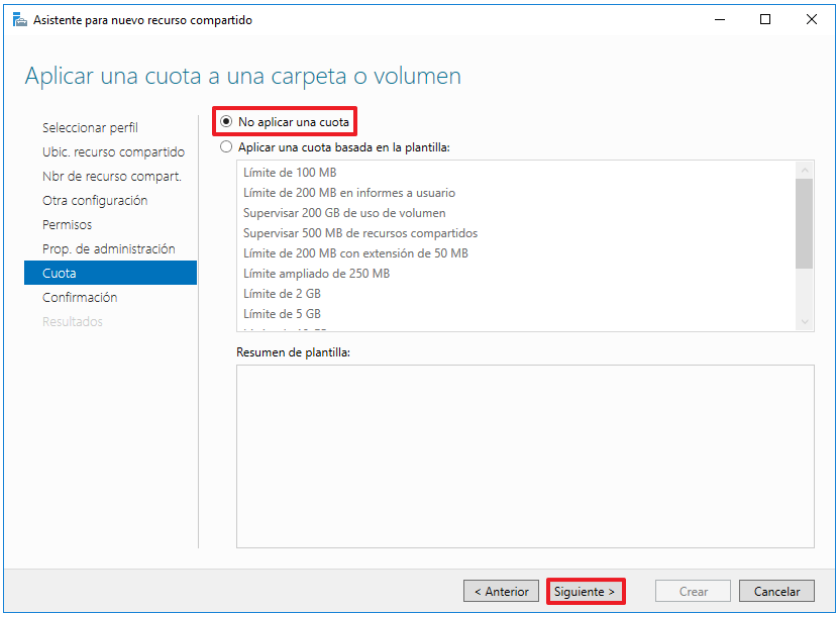
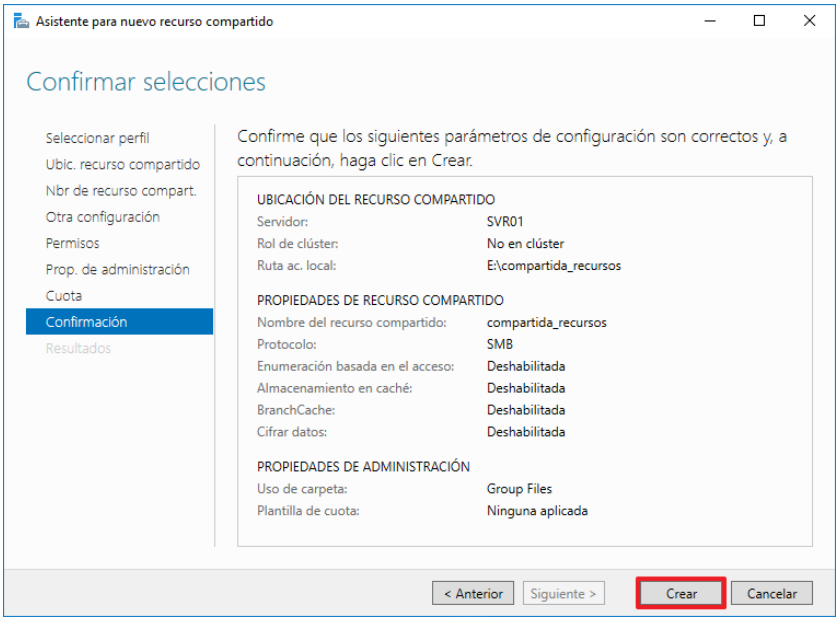
Paso	Descripción
49.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de ficheros.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
50.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
51.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Introduzca las credenciales y pulse "Sí" para continuar. 
52.	A continuación, pulse sobre "Servicios de archivos y de almacenamiento". 

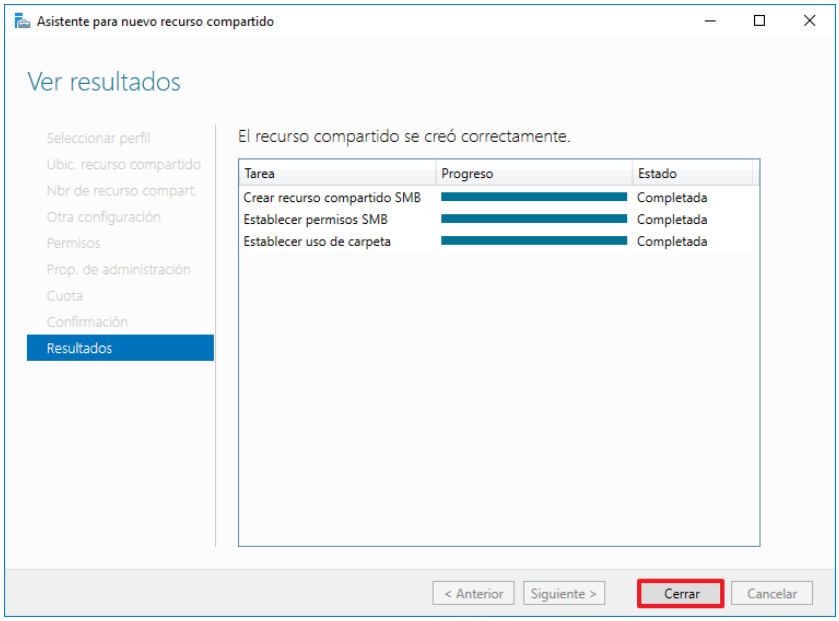
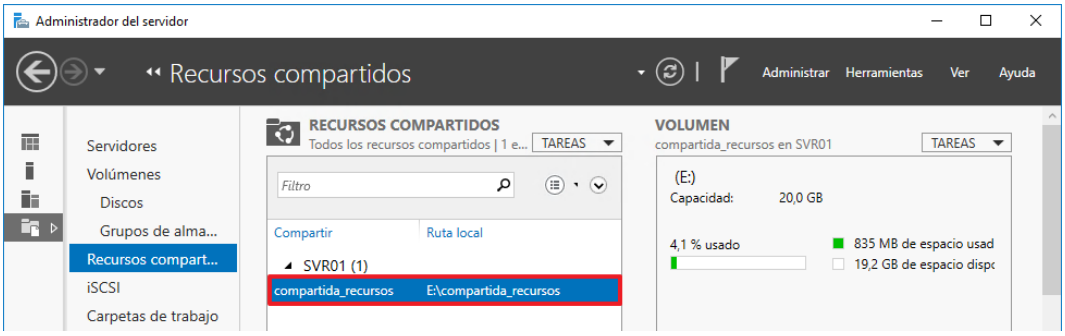
Paso	Descripción
53.	Seleccione la sección “Recursos compartidos”. 
54.	En el apartado “Recursos compartidos” pulse sobre el desplegable “TAREAS” y seleccione la opción “Nuevo recurso compartido…”. 
55.	Se iniciará el asistente para añadir un nuevo recurso compartido. En el apartado “Seleccionar perfil” seleccione un perfil de recurso compartido de archivos y pulse “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la opción “Recurso compartido SMB – Avanzado”.

Paso	Descripción
56.	Seleccione el servidor sobre el que desea crear el recurso compartido. A continuación seleccione la opción “Escriba una ruta de acceso personalizada:” y pulse sobre el botón “Examinar…”. 
57.	Ante la ventana emergente navegue y seleccione el recurso que desea compartir. Pulse sobre “Seleccionar carpeta” para continuar.  **Nota:** Para este ejemplo se comparte un directorio creado previamente denominado “compartida_recursos” en una ubicación dedicada a recursos compartidos denominada “Datos (E:)”. Ajuste esta configuración a las necesidades de su organización.
58.	A continuación, pulse sobre “Siguiente >” para continuar con el asistente.

Paso	Descripción
59.	En el apartado “Nbr. De recurso compart.” Establezca un nombre para el recurso y una descripción del mismo si lo desea. Pulse sobre “Siguiente >”.  **Nota:** En este ejemplo se mantiene el nombre del recurso seleccionado en el apartado anterior del asistente.
60.	En el apartado “Otra configuración” seleccione los parametros de configuración de recurso compartido que precise y pulse “Siguiente >”.  **Nota:** Para este ejemplo no se ha seleccionado ninguna configuración adicional.

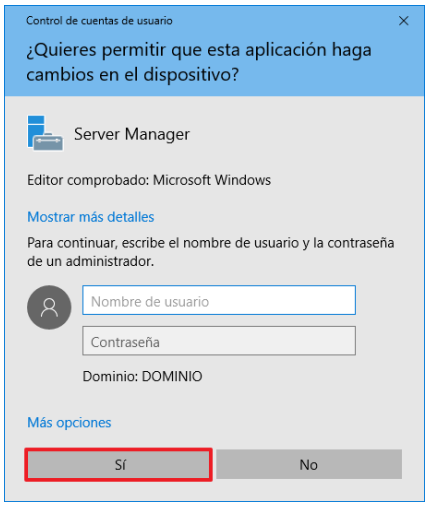
Paso	Descripción
61.	Pulse “Siguiente >” en el apartado “Permisos”.  **Nota:** Los permisos de acceso a los archivos del recurso compartido se configurarán posteriormente.
62.	Seleccione en el apartado “Prop. De administración” una categorización para el recurso compartido si lo desea y pulse el botón “Siguiente >”.  **Nota:** Para este ejemplo se utiliza la categorización “Archivos de grupo”. Adapte esta configuración a su entorno.

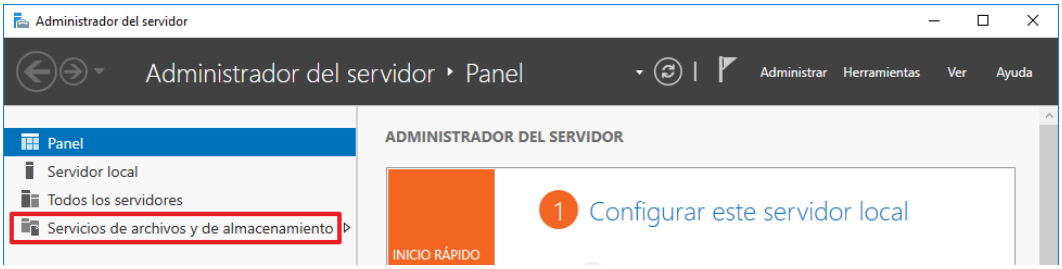
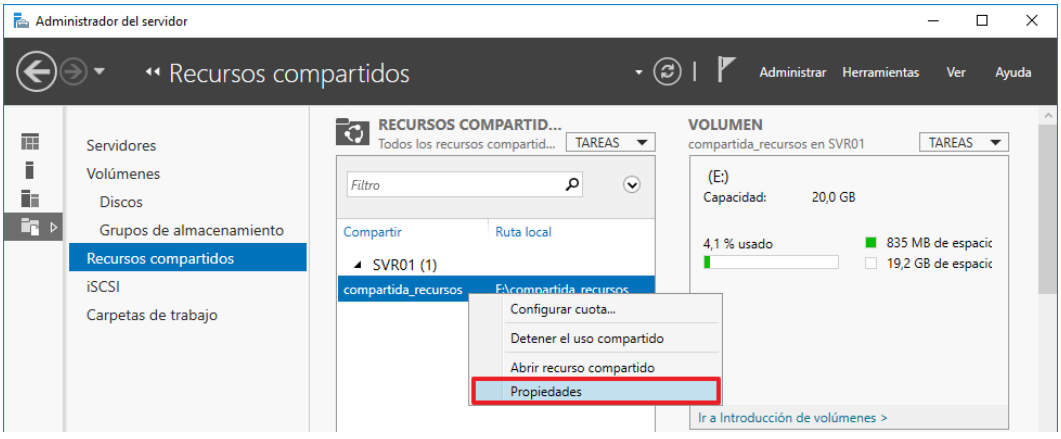
Paso	Descripción
63.	Pulse “Siguiente >” en el apartado “Cuota”.  **Nota:** En este ejemplo se deja marcado la opción por defecto “No aplicar una cuota”.
64.	En el apartado “Confirmación” pulse sobre el botón “Crear”. 

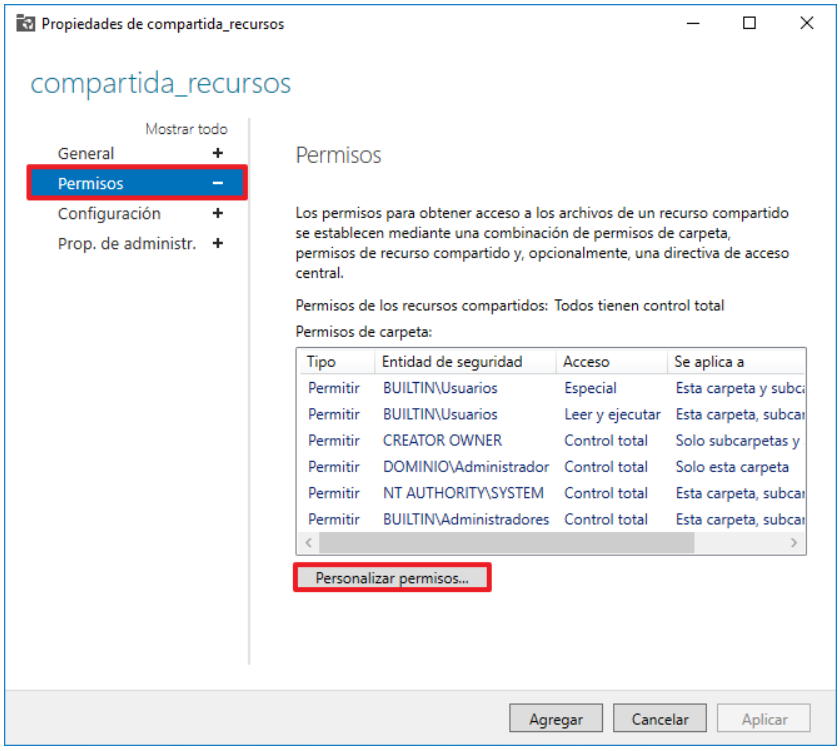
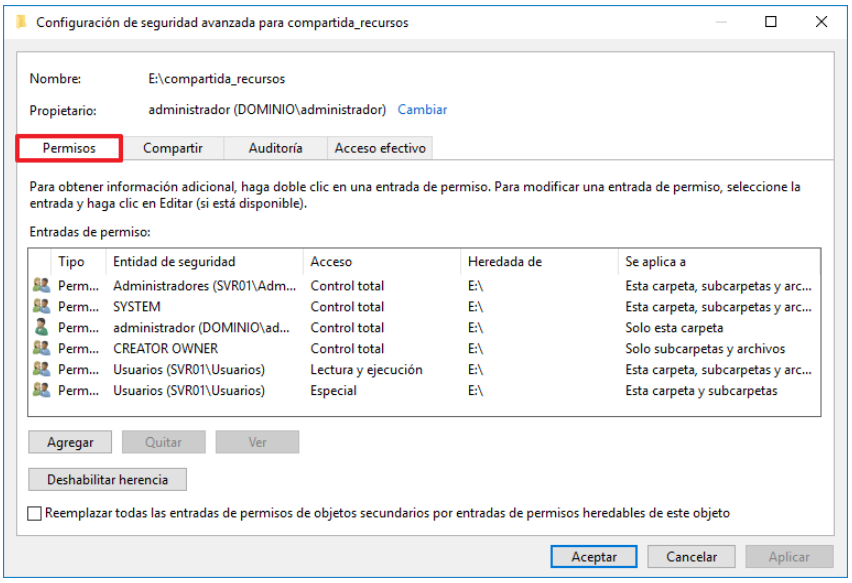
Paso	Descripción
65.	En el apartado “Resultados” se mostrará el proceso de creación del recurso. Cuando finalice pulse sobre “Cerrar”. 
66.	Podrá comprobar desde el “Administrador del servidor” el recurso que se acaba de compartir. 

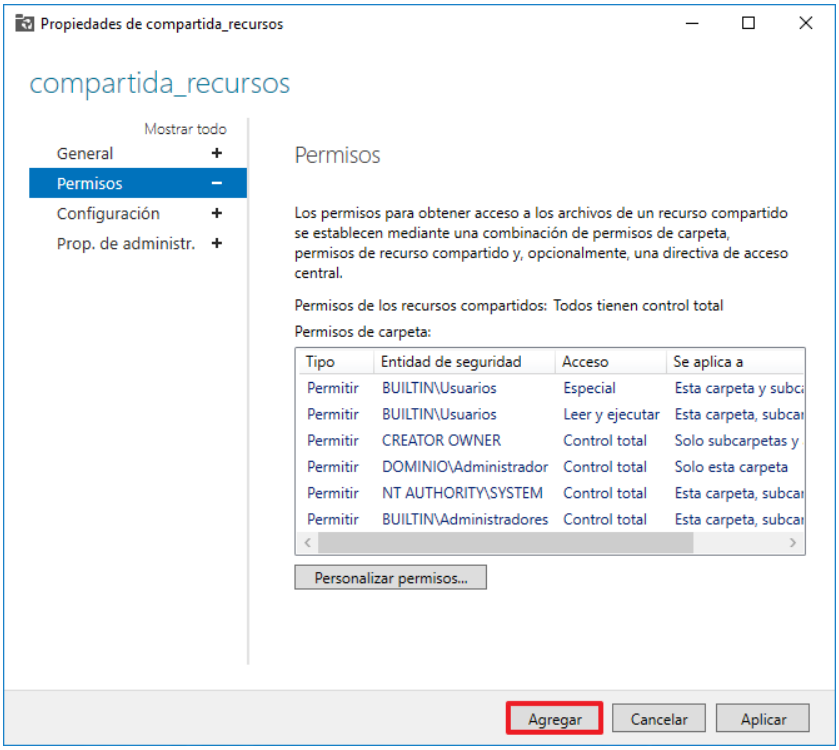
2.3. SEGURIDAD SOBRE LOS RECURSOS COMPARTIDOS

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos del Servidor de ficheros según el marco operacional de categoría alta establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

Paso	Descripción
67.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
68.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
69.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 

Paso	Descripción
70.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
71.	Seleccione la sección “Recursos compartidos”. 
72.	Seleccione con el botón derecho el recurso sobre el que desea modificar los permisos y pulse la opción “Propiedades”.  **Nota:** En este ejemplo se editan las propiedades del recurso denominado “compartida_recursos”.

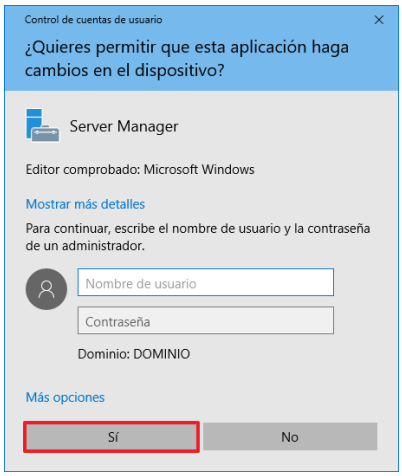
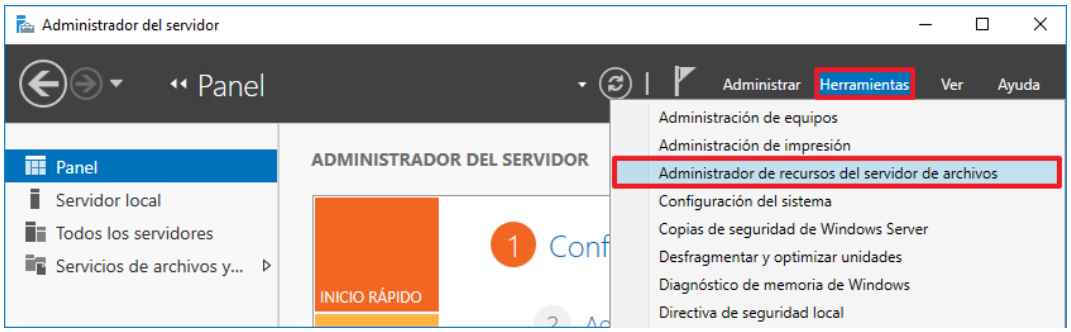
Paso	Descripción
73.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos…”. 
74.	A continuación, en la pestaña “Permisos” edite los permisos que desee para el recurso compartido.  **Nota:** Tenga en consideración que deberá eliminar por seguridad el grupo “Todos” de cualquier recurso que este compartido.

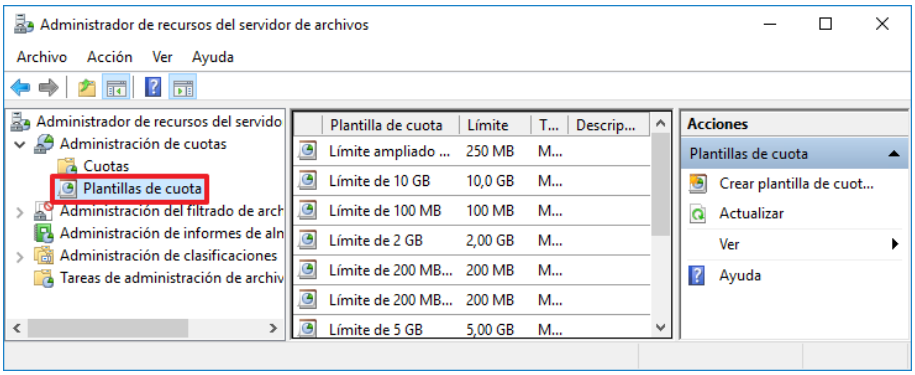
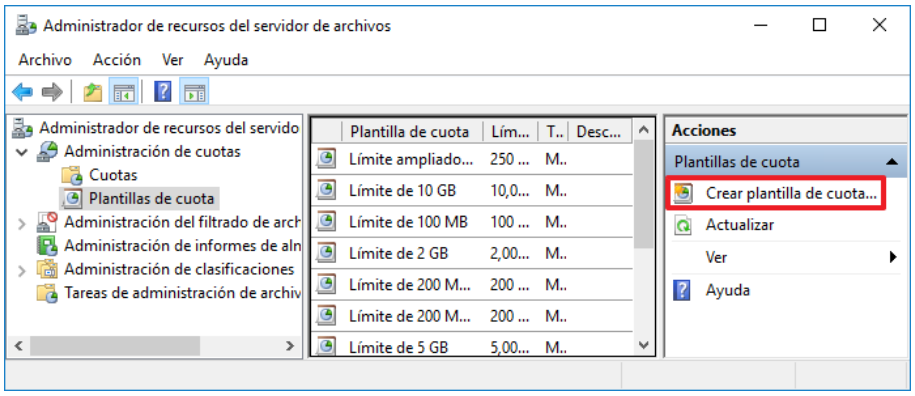
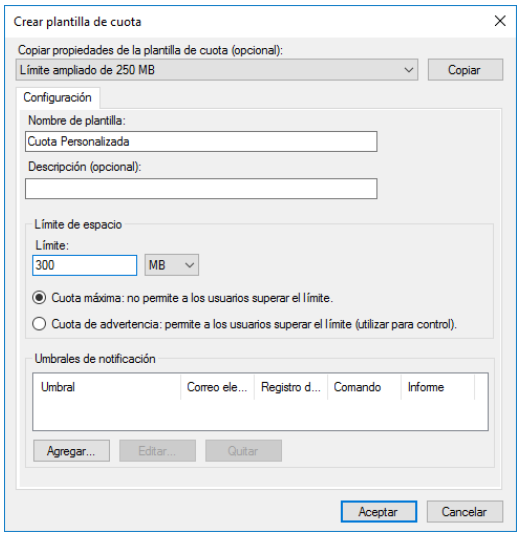
Paso	Descripción
75.	Para finalizar, pulse sobre “Aceptar” y después sobre el botón “Agregar” para hacer efectivos los cambios. 

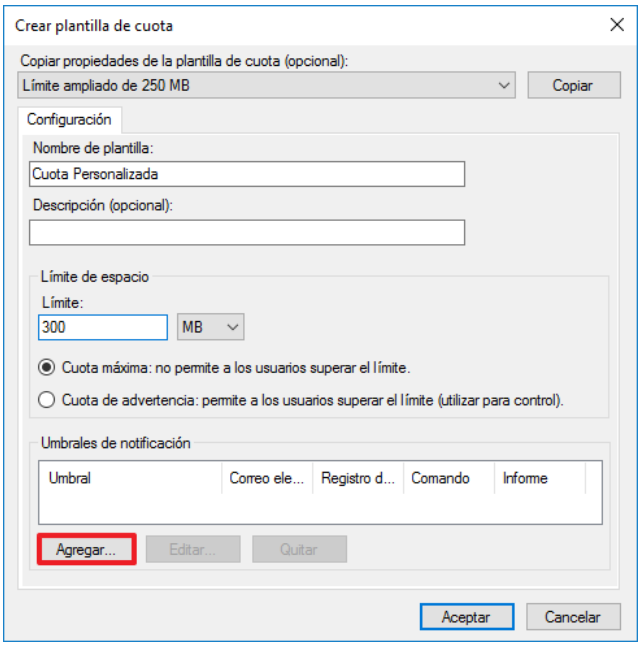
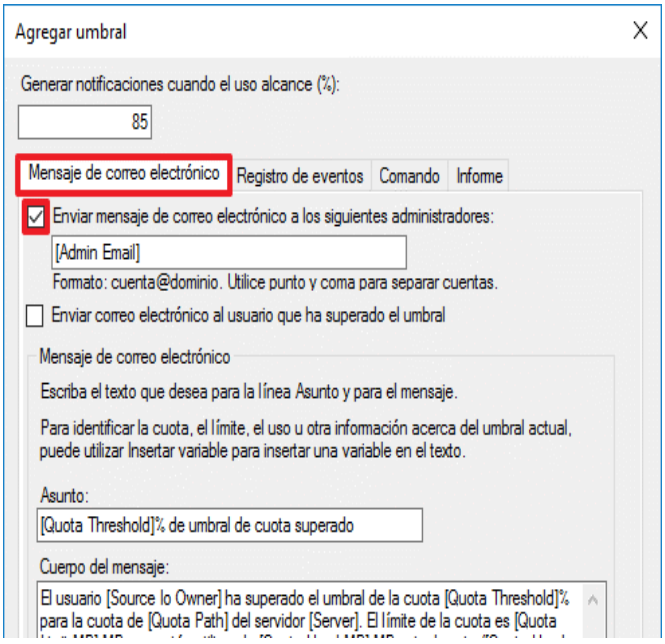
2.4. CUOTAS DE DISCO

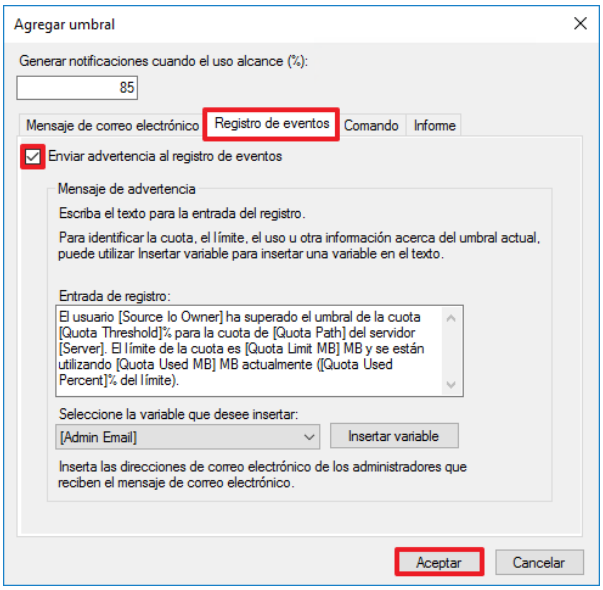
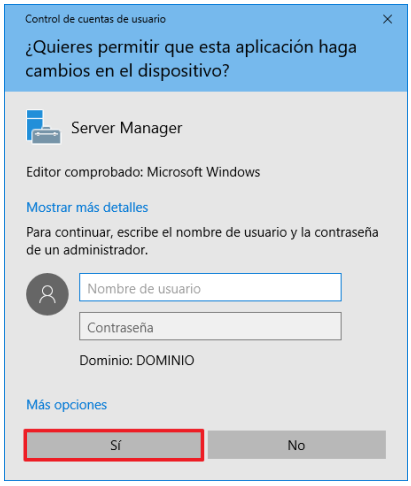
Con la aplicación del ENS para la categoría alta sobre el “Servidor de ficheros” será necesario configurar las cuotas de disco para prevenir un uso excesivo de los recursos y el sistema pueda reaccionar frente a los incidentes que se puedan provocar.

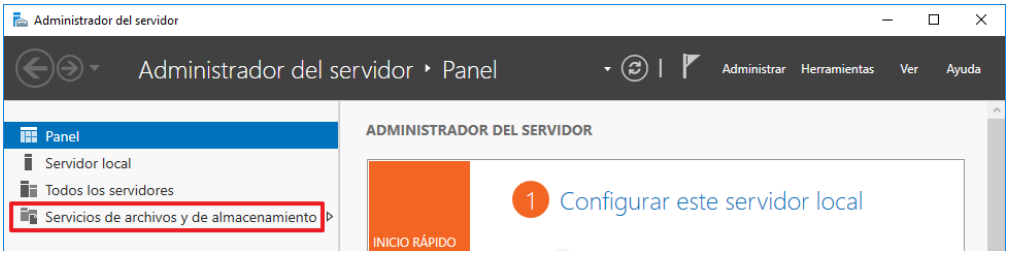
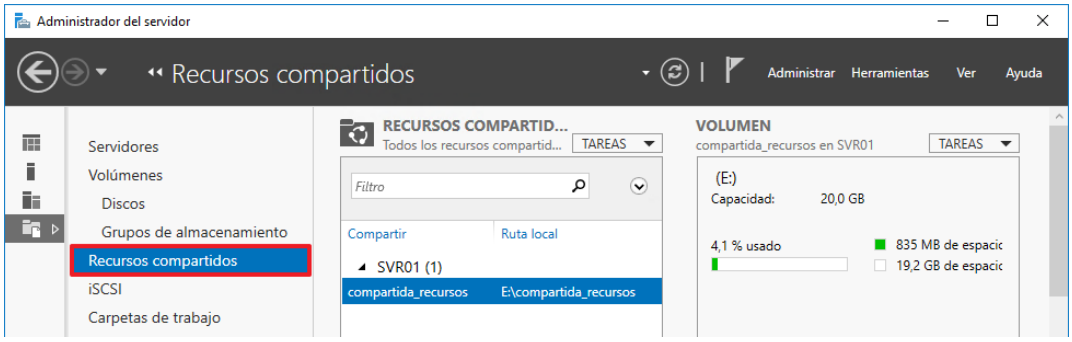
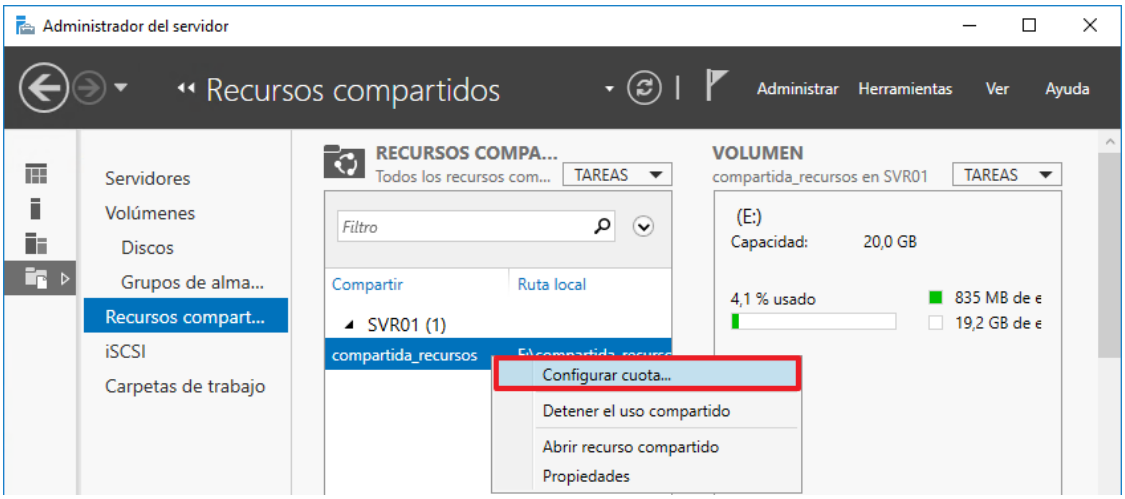
Paso	Descripción
76.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

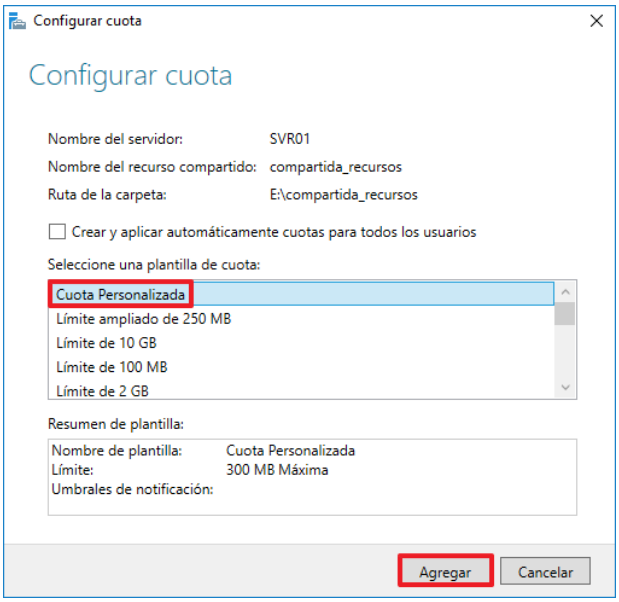
Paso	Descripción
77.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
78.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 
79.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 

Paso	Descripción
80.	Expanda el nodo **"Plantillas de cuota" desde la ruta "Administrador de recursos del servidor de archivos (local) → Administración de cuotas → Plantillas de cuota"** tal y como se muestra a continuación. 
81.	En el panel "Acciones" seleccione "Crear plantilla de cuota…". 
82.	En la nueva ventana emergente, establezca la configuración deseada para la cuota y pulse "Aceptar" para finalizar la creación de la cuota.  **Nota:** En este ejemplo se utiliza el nombre "Cuota Personalizada" y se da un valor límite de 300MB.

Paso	Descripción
83.	Debido a la aplicación de la categoría alta del ENS es aconsejable agregar un umbral de notificaciones para avisar del estado de uso de los recursos compartidos. Para ello pulse sobre el botón “Agregar…” en el apartado “Umbrales de notificación”. 
84.	Configure la pestaña de “Mensaje de correo electrónico adaptándolo a las necesidades de su organización. 

Paso	Descripción
85.	Pulse en la pestaña de “Registro de eventos” y configúrela adaptándola a las necesidades de su organización. Cuando finalice pulse “Aceptar” y pulse de nuevo sobre “Aceptar” para finalizar la configuración de la cuota.  **Nota:** En este ejemplo se ha configurado el umbral para que envíe un mensaje de correo electrónico y genere una advertencia en el registro de eventos cuando se supere el umbral establecido.
86.	A continuación, abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
87.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 

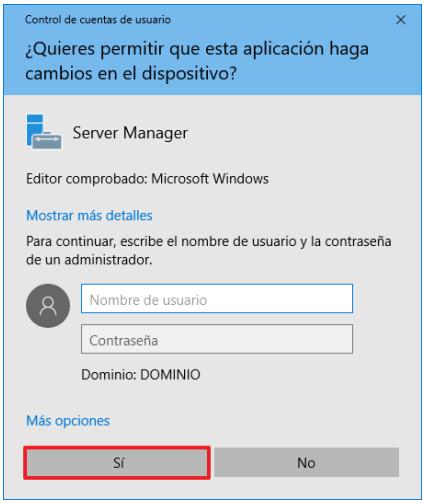
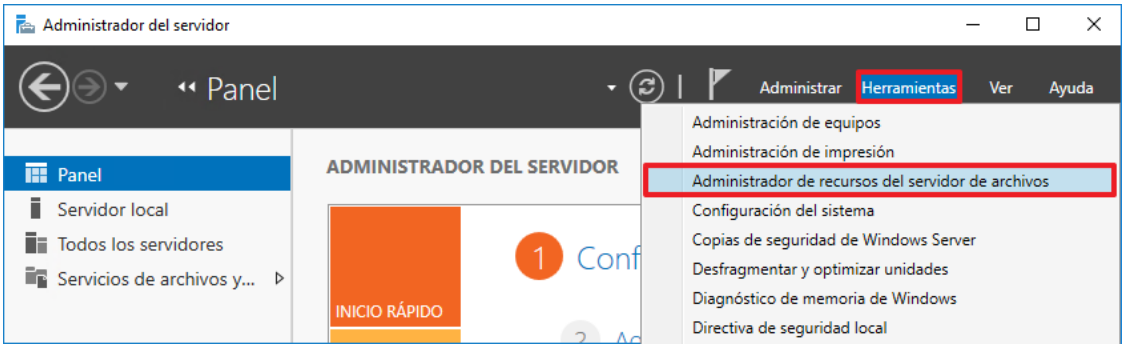
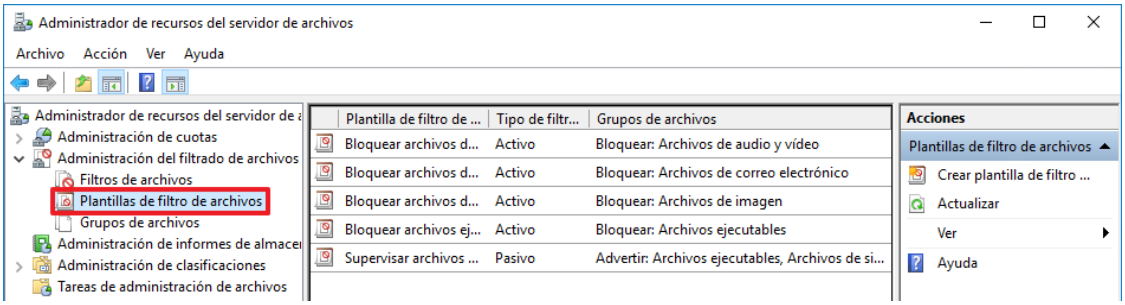
Paso	Descripción
88.	Pulse sobre “Servicios de archivos y de almacenamiento”. 
89.	Seleccione la sección “Recursos compartidos”. 
90.	Seleccione con el botón derecho el recurso sobre el que desea aplicar la cuota configurada anteriormente y pulse la opción “Configurar cuota…”. 

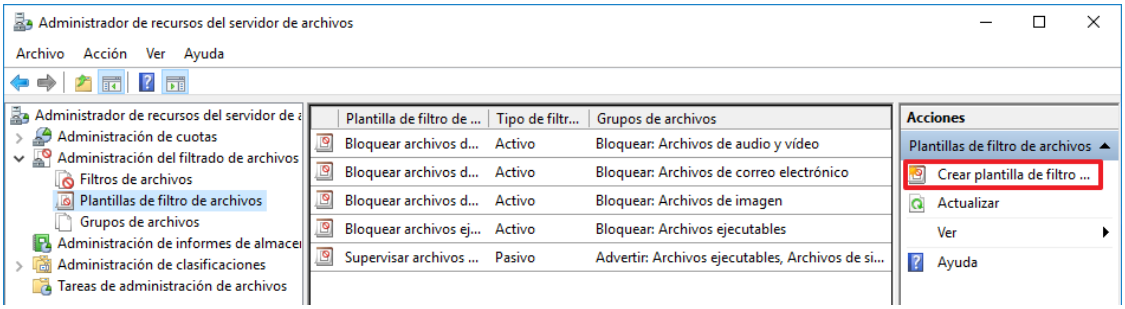
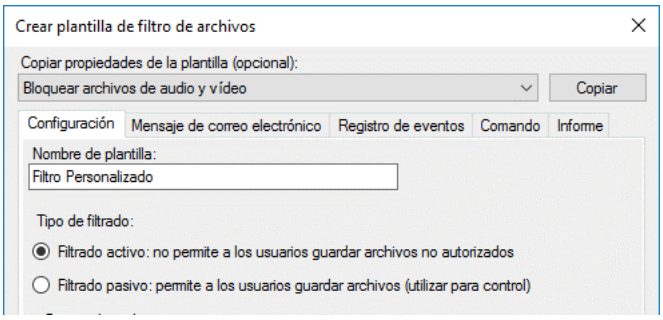
Paso	Descripción
91.	En la nueva ventana emergente seleccione una cuota creada por defecto por el sistema o una cuota creada específicamente para el recurso compartido. Pulse “Agregar” para finalizar.  **Nota:** En este ejemplo se aplica la cuota denominada “Cuota Personalizada”, creada anteriormente. Si no aparece la cuota creada anteriormente reinicie el “Administrador del servidor”.

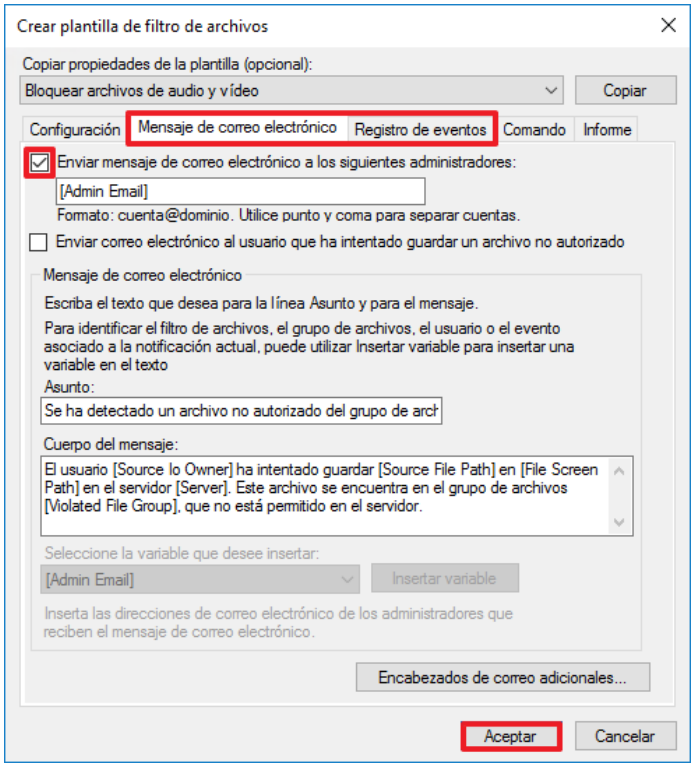
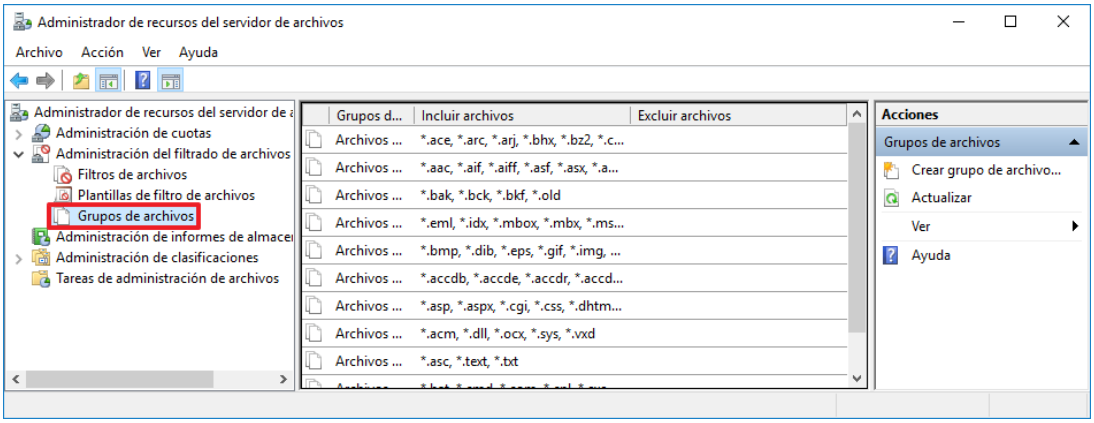
2.5. FILTRADO DE ARCHIVOS

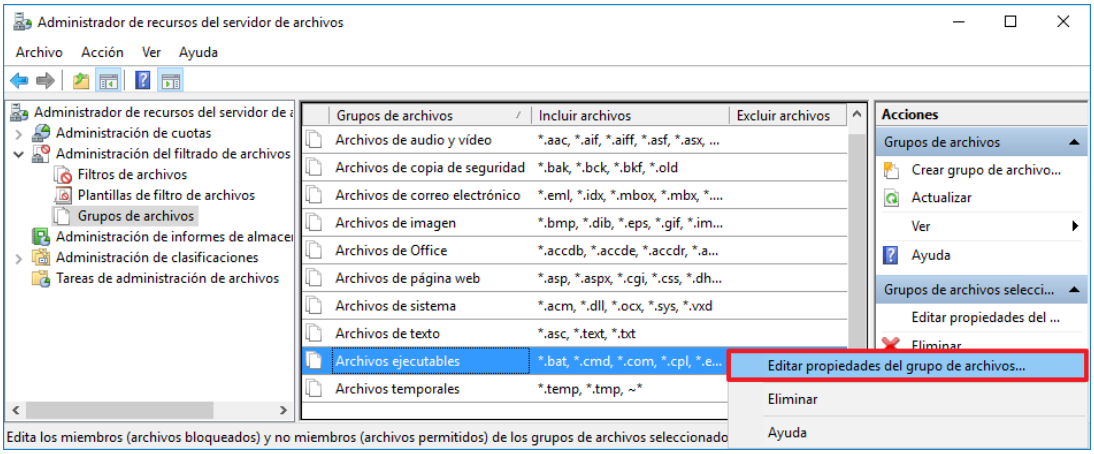
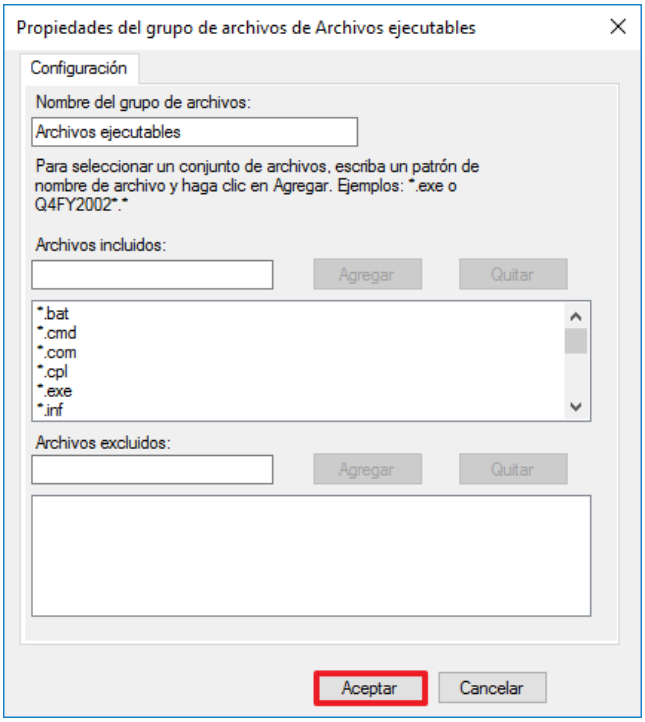
Según lo establecido en el marco operacional para equipos “Servidor de ficheros” que les sea de aplicación la categoría alta de ENS, será necesario configurar el filtrado de archivos para prevenir la introducción en éste de archivos indeseados o que puedan poner en riesgo la seguridad del sistema.

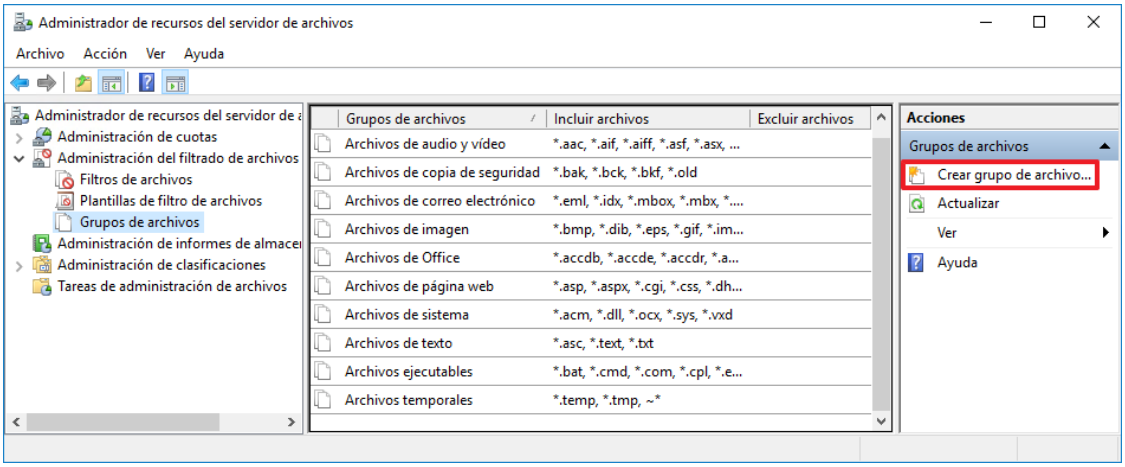
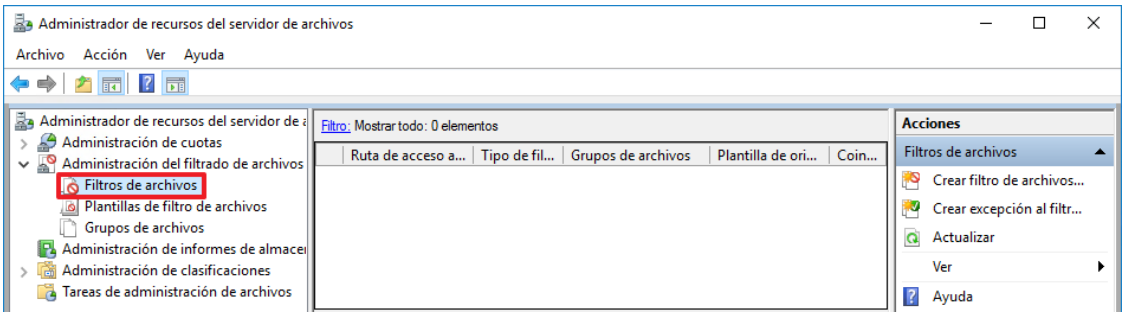
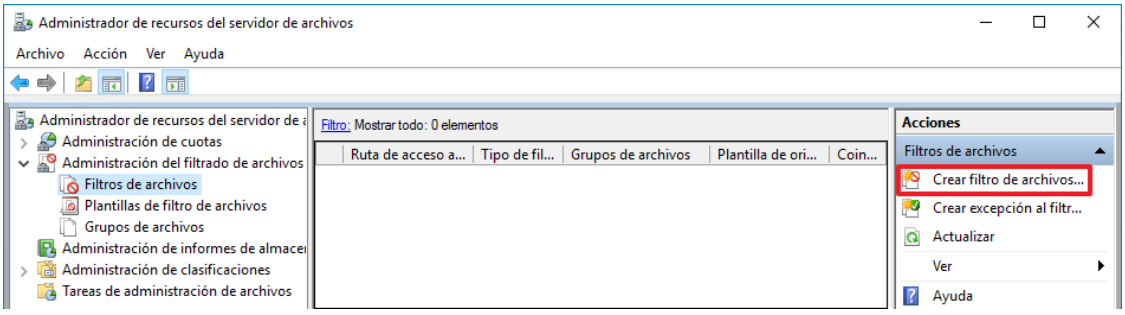
Paso	Descripción
92.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

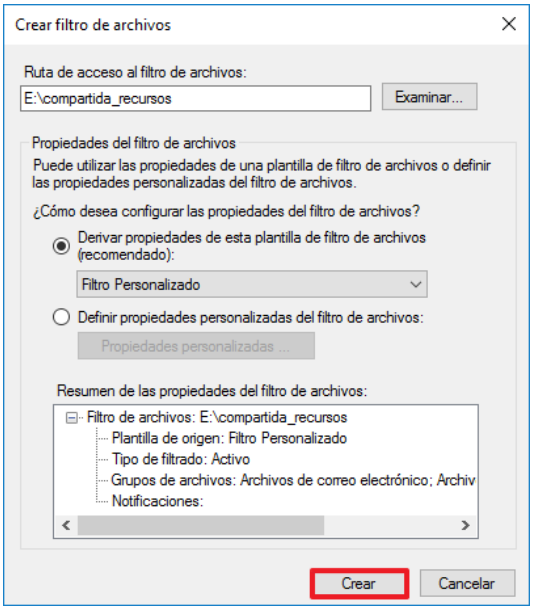
Paso	Descripción
93.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
94.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 
95.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
96.	Expanda el nodo “Plantillas de filtro de archivos” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Plantillas de filtro de archivos”** tal y como se muestra a continuación. 

Paso	Descripción
97.	En el panel “Acciones” seleccione “Crear plantilla de filtro”. 
98.	Ajuste y establezca la configuración para realizar un filtro adecuado que evite comprometer la seguridad del sistema.  **Nota:** En este ejemplo se crea un filtro denominado “Filtro Personalizado” que bloquea archivos de correo electrónico, archivos de imagen y archivos ejecutables.

Paso	Descripción
99.	Adicionalmente y tratándose de la categoría alta del ENS es aconsejable configurar un mensaje de correo y un registro en el visor de eventos para establecer un seguimiento de los archivos que se intentan almacenar en el Servidor de ficheros. Pulse “Aceptar” cuando haya finalizado la configuración.  **Nota:** En este ejemplo se configura un envío de correo electrónico y una entrada en el registro de eventos.
100.	Expanda el nodo “Grupos de archivos” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Grupos de archivos”** tal y como se muestra a continuación. 

Paso	Descripción
101.	Seleccione cualquier grupo de archivos con el botón derecho y pulse sobre la opción del menú contextual “Editar propiedades del grupo de archivos…”.  **Nota:** Para este ejemplo se edita el grupo de archivos “Archivos ejecutables”.
102.	En la ventana emergente configure los tipos de archivos que se bloquean y cuales están excluidos. Pulse “Aceptar” para finalizar. 

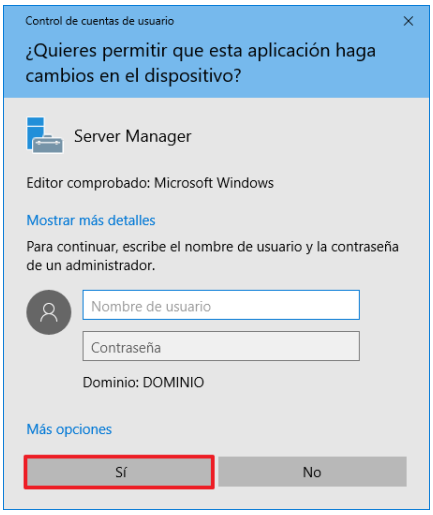
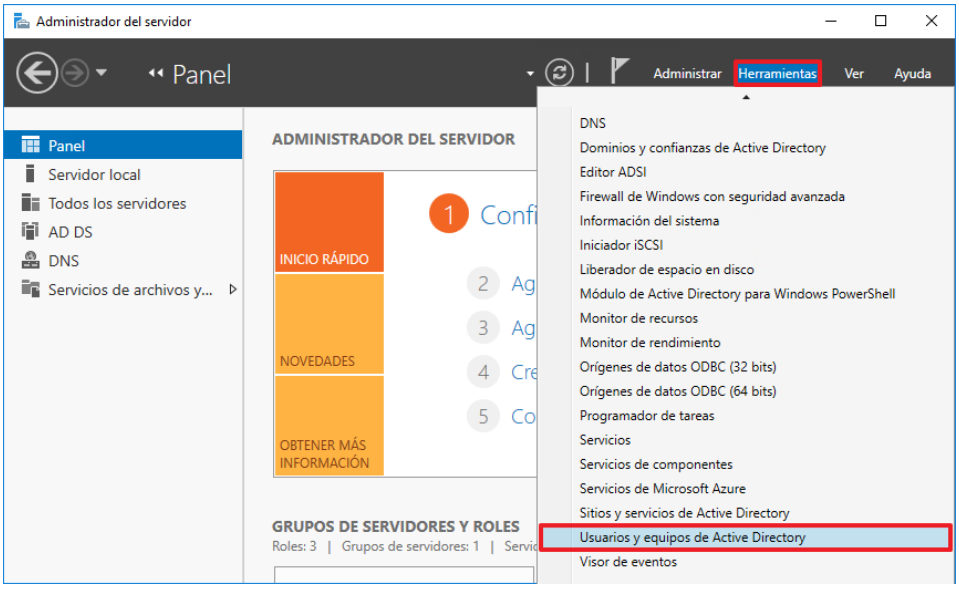
Paso	Descripción
103.	Además, es posible crear un grupo personalizado de archivos para bloquear o excluir seleccionando la opción “Crear grupo de archivos…” en el panel “Acciones”. 
104.	Expanda el nodo **“Filtros de archivos” desde la ruta “Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Filtros de archivos”** tal y como se muestra a continuación. 
105.	En el panel “Acciones” seleccione “Crear filtro de archivos…”. 

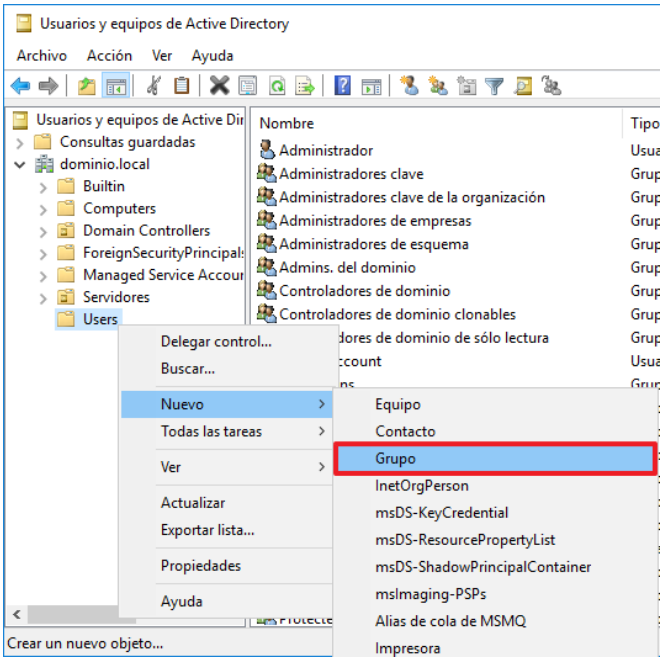
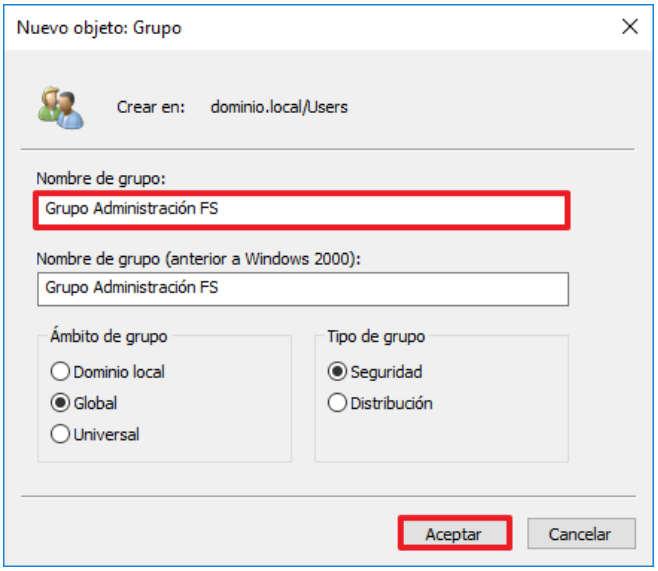
Paso	Descripción
106.	En la ventana emergente seleccione el recurso sobre el que desea aplicar un filtro de archivos y escoja el filtro a aplicar. Pulse “Crear” para finalizar.  **Nota:** Para este ejemplo se ha utilizado el recurso ubicado en “E:\Compartida_Recursos” y se le ha aplicado el filtro creado anteriormente denominado “Filtro Personalizado”.

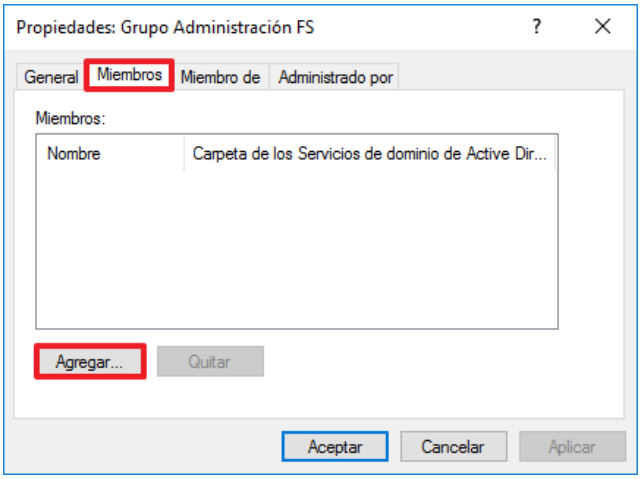
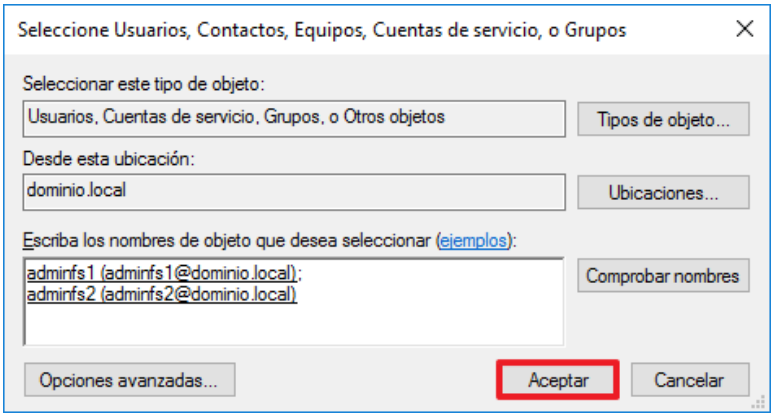
2.6. SEGREGACIÓN DE ROLES

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

Paso	Descripción
107.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
108.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
109.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 
110.	Acceda al apartado “Herramientas” y seleccione “Usuarios y Equipos de Active Directory”. 

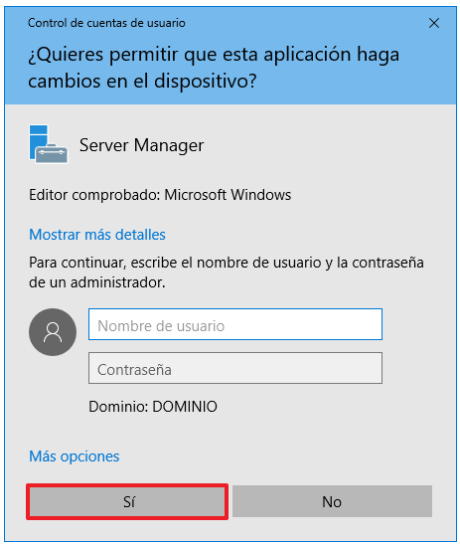
Paso	Descripción
111.	Despliegue el nodo **"<su dominio> → Users"**. Pulse con el botón derecho sobre "Users" y seleccione la opción del menú contextual **"Nuevo → Grupo"**. 
112.	Establezca el nombre de grupo deseado para su organización y pulse "Aceptar".  **Nota:** En este ejemplo se utiliza el nombre "Grupo Administración FS".

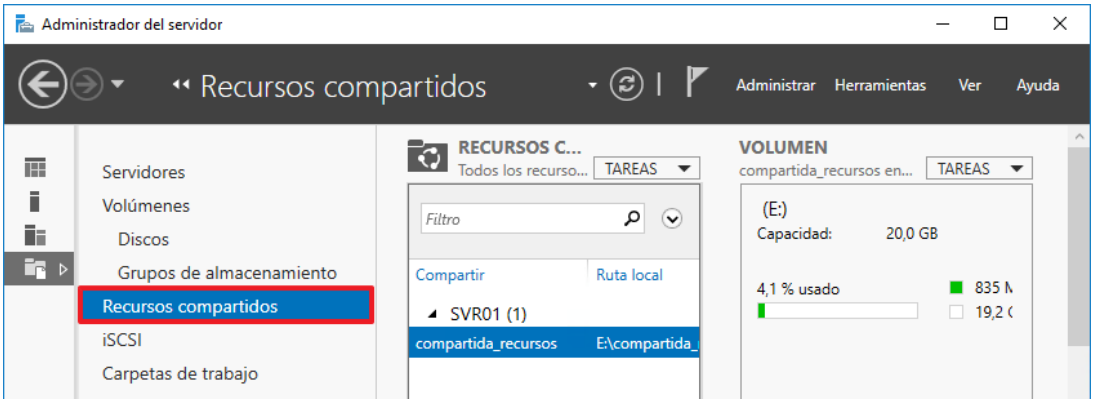
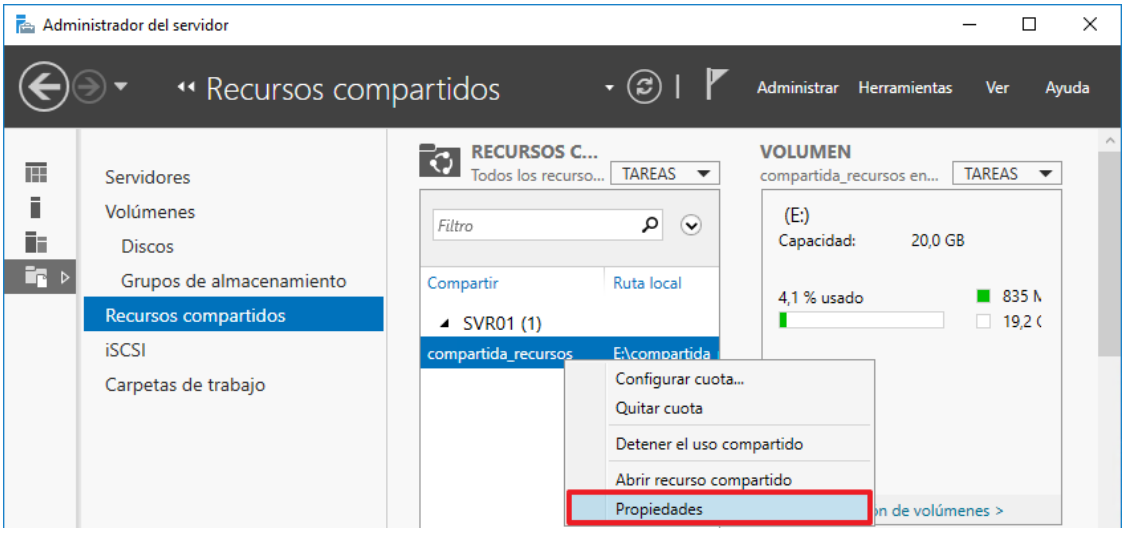
Paso	Descripción
113.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar…” para añadir usuarios al grupo. 
114.	Añada los usuarios que desee al grupo y pulse “Aceptar”.  **Nota:** En este ejemplo se añaden los usuarios “adminfs1” y “adminfs2” utilizados para la creación de esta guía.”

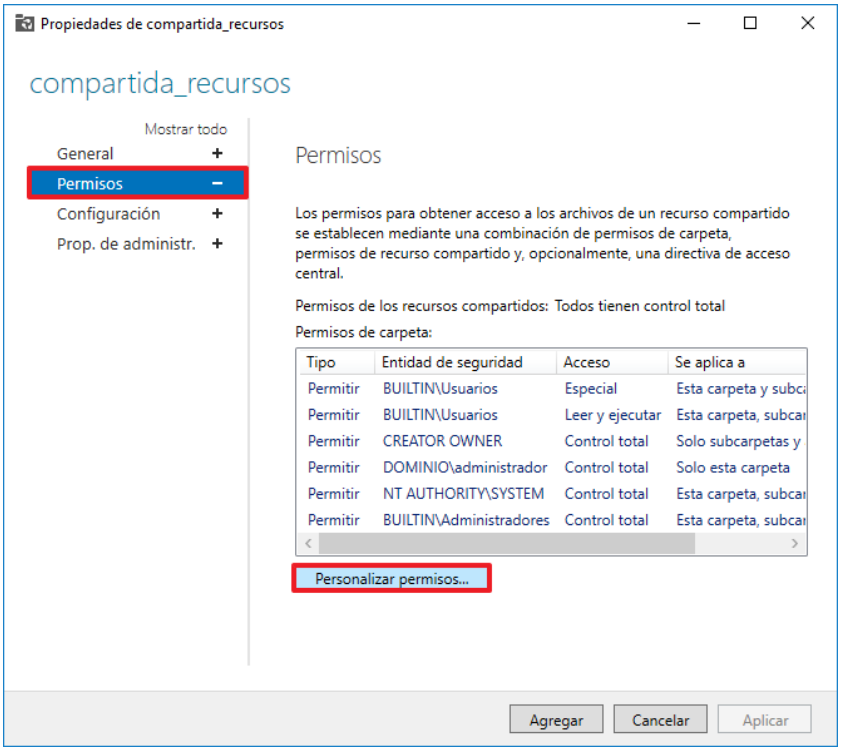
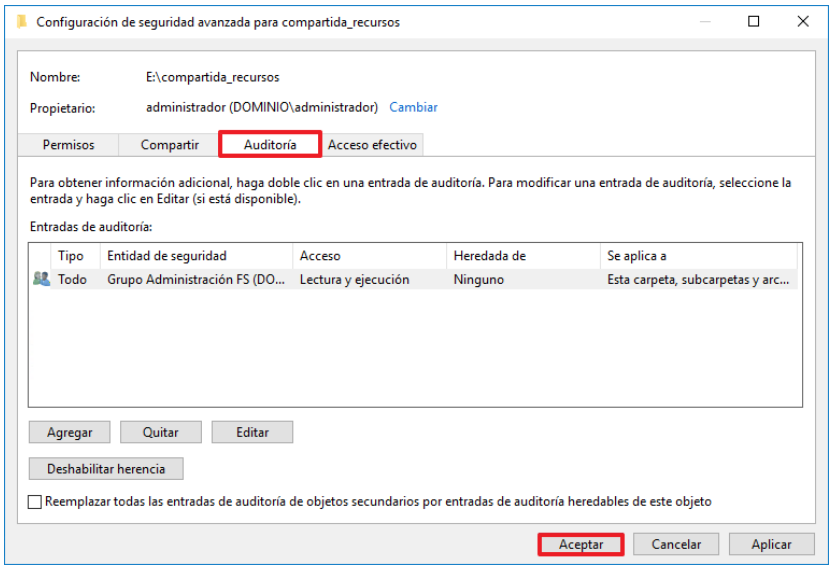
2.7. AUDITORIA DE ARCHIVOS

Con la aplicación del ENS para la categoría alta sobre el Servidor de ficheros quedará registrado el uso de los recursos compartidos del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información, con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

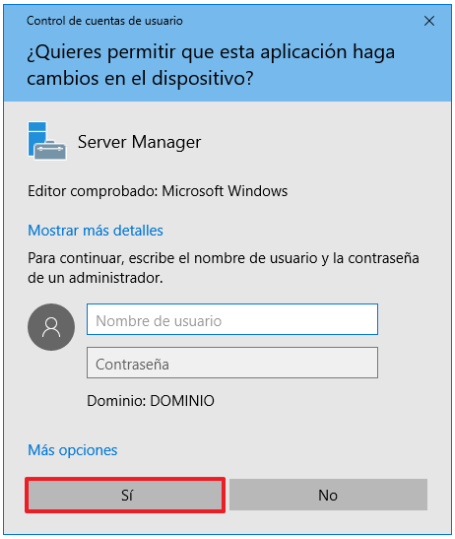
Paso	Descripción
115.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
116.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
117.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 

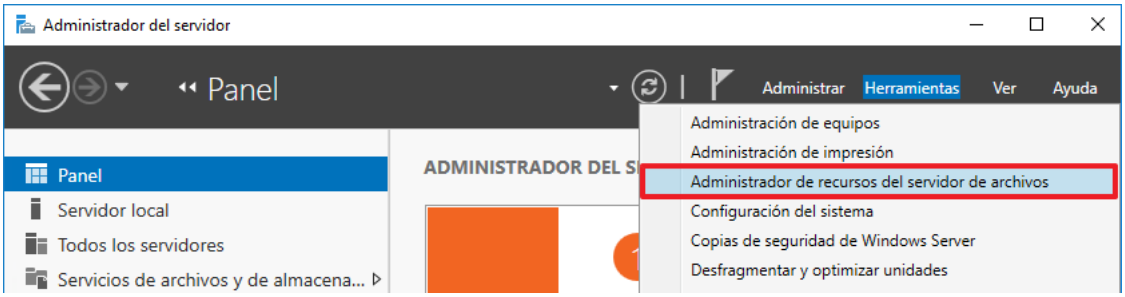
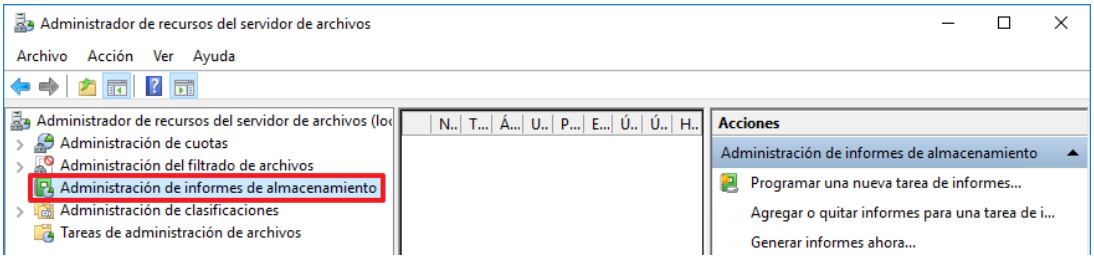
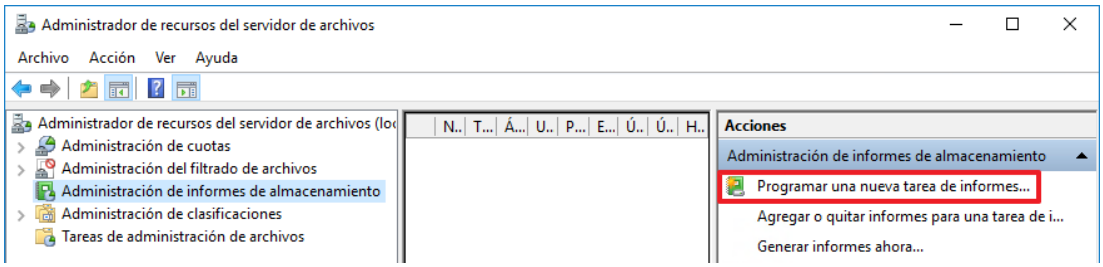
Paso	Descripción
118.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
119.	Seleccione la sección “Recursos compartidos”. 
120.	Seleccione con el botón derecho el recurso sobre el que desea gestionar la auditoría y pulse la opción “Propiedades”.  **Nota:** En este ejemplo se selecciona el recurso compartido creado anteriormente “compartida_recursos”.

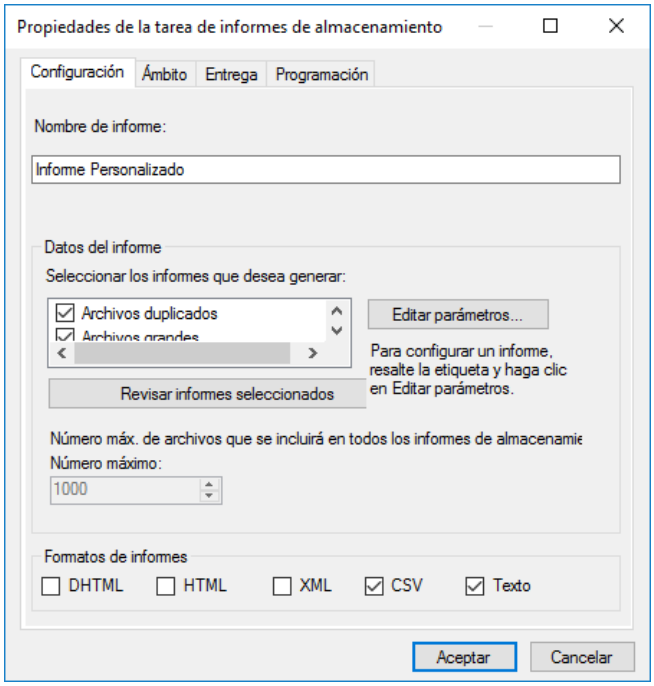
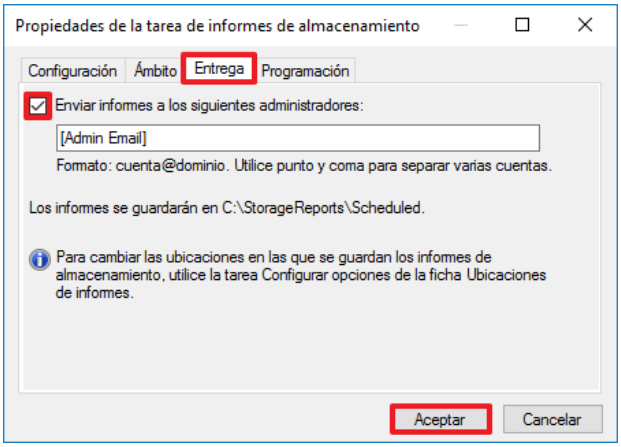
Paso	Descripción
121.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos…”. 
122.	Acceda a la pestaña “Auditoría” y configure ésta acorde a las necesidades de su organización. Pulse “Aceptar” y después en la ventana de propiedades del recurso compartido pulse “Agregar” para finalizar el proceso.  **Nota:** En este ejemplo se añade el grupo denominado “Grupo Administración FS”.

2.8. INFORMES DE ALMACENAMIENTO

Con la aplicación del ENS para la categoría alta sobre el Servidor de ficheros será necesario configurar los informes de almacenamiento con el objetivo de tener un control sobre los ficheros que están alojados en el sistema y así evitar poner en riesgo la seguridad de éste.

Paso	Descripción
123.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
124.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
125.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales y pulse “Sí” para continuar. 

Paso	Descripción
126.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
127.	Expanda el nodo “Administración de informes de almacenamiento” desde la ruta **“Administrador de recursos del servidor de archivos (local) → Administración de informes de almacenamiento”** tal y como se muestra a continuación. 
128.	En el panel “Acciones” seleccione “Programar una nueva tarea de informes…”. 

Paso	Descripción
129.	Determine en la ventana emergente la configuración deseada para los informes de almacenamiento sobre un recurso.  **Nota:** En este ejemplo se ha configurado un informe con el nombre “Informe Personalizado” para el recurso denominado “compartida_recursos”.
130.	Debido a la aplicación de la categoría alta del ENS es recomendable configurar la entrega de los informes a las cuentas de correo electrónico que deseen recibir los informes. Para ello vaya a la pestaña “Entrega” y configure el correo. Pulse “Aceptar” para finalizar la configuración de los informes. 

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA SERVIDORES DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

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 el punto de la guía "ANEXO A.4.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE FICHEROS MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores Windows 2016 con implementación de seguridad de categoría alta del ENS.

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

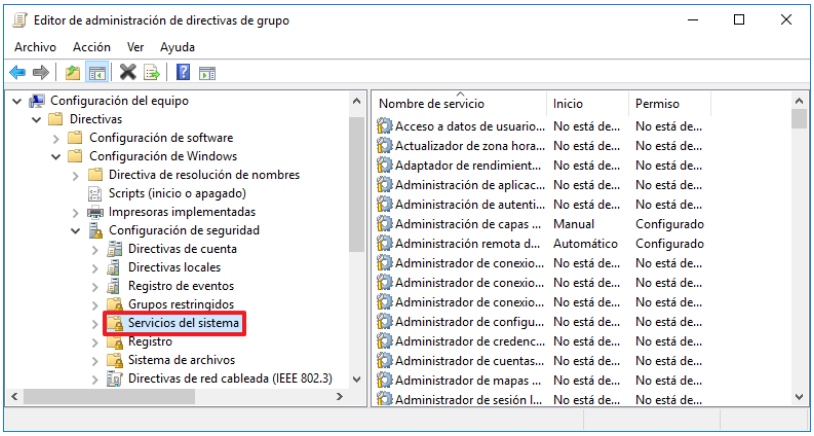
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de ficheros, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el controlador de dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

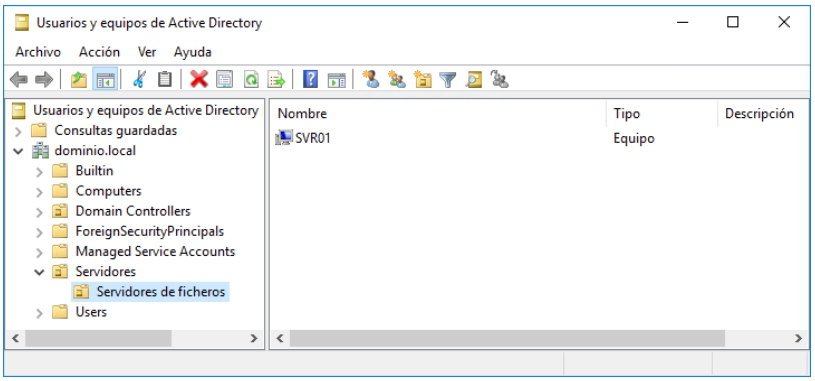
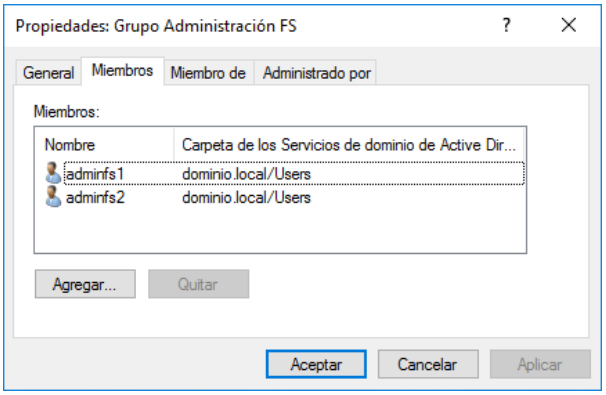
b) En el servidor de ficheros:
   i. Administrador de Windows (explorer.exe).
   ii. Servicios (services.msc).
   iii. Administrador de recursos del servidor de archivos (fsrm.msc).
   iv. Carpetas compartidas (fsmgmt.msc).

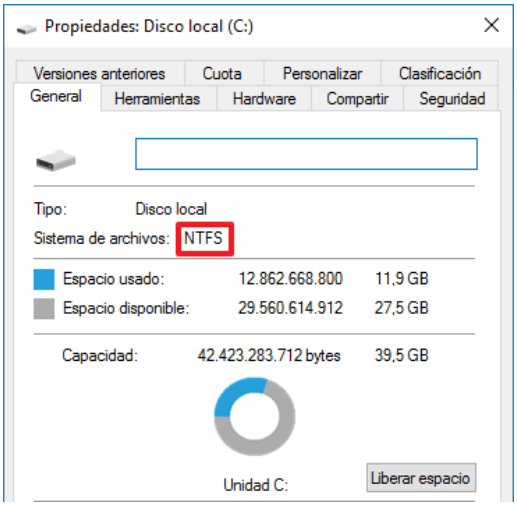
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado en este documento. Deberá adaptar los pasos según la configuración de su organización.

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.

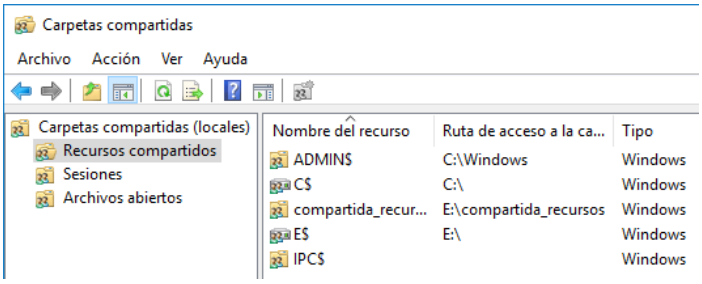
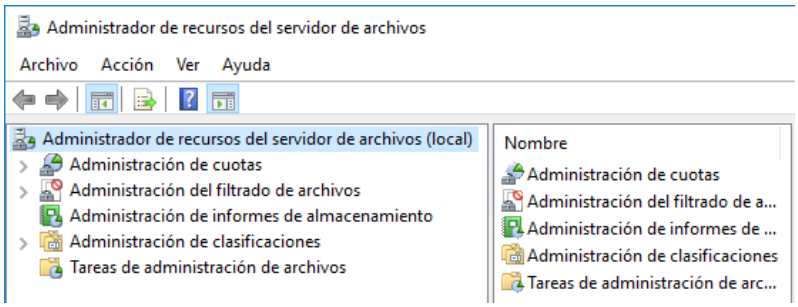
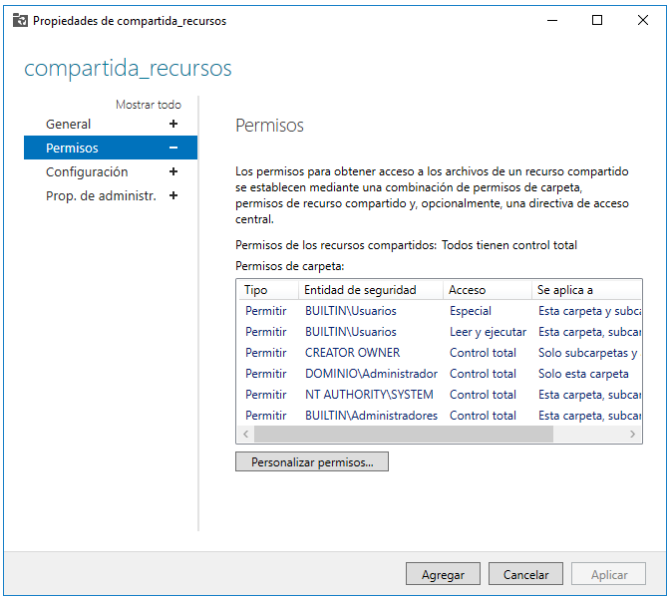
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta - DL		Utilice el Administrador de directivas de grupo (**Inicio → Herramientas administrativas → Administración de directivas de grupo**) y despliegue el menú hasta llegar a las unidades organizativas que contienen los Servidores de ficheros. Verifique que está creada la política "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta - DL". **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros".
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta - DL		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta - DL" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-573 ENS Incremental Servidor de Ficheros Categoria alta – DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema".** 

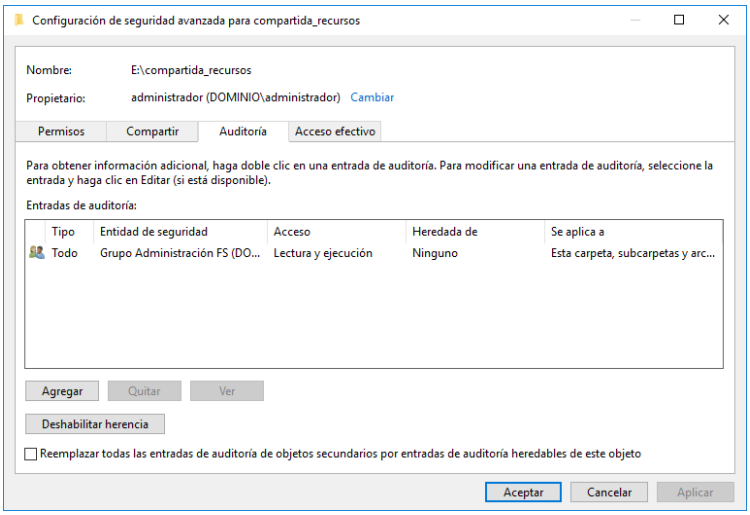
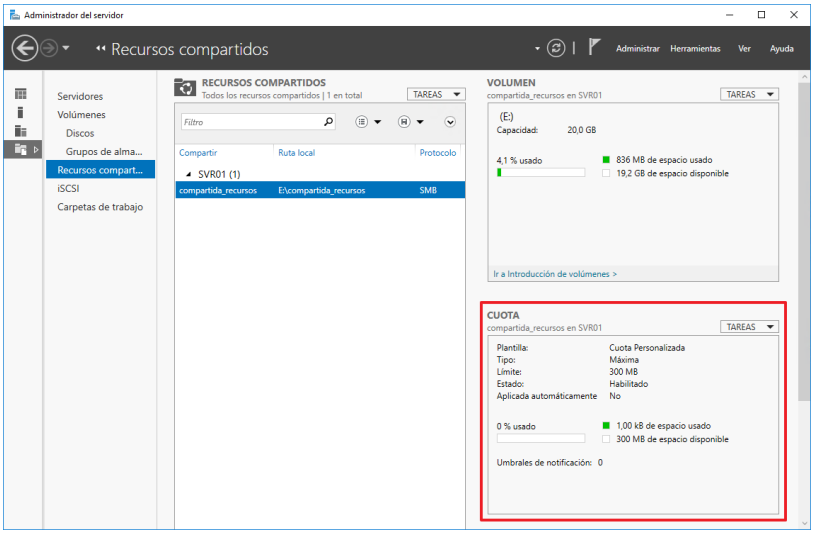
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permisos	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

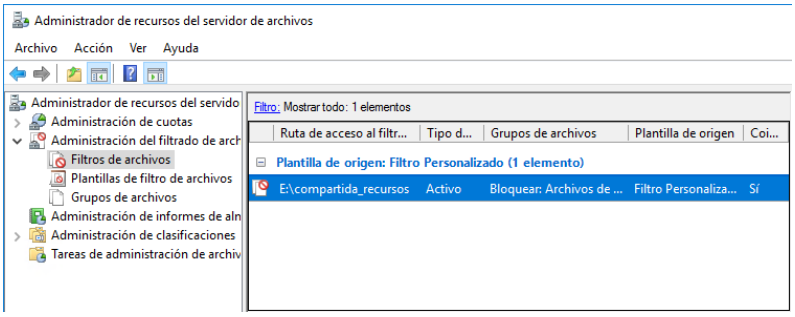
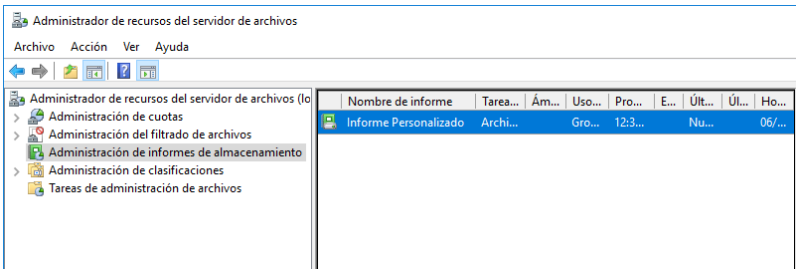
Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que los servidores de ficheros están dentro de las Unidades Organizativas correspondientes		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Ficheros. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de ficheros que se están asegurando. **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de ficheros". 
5. Verifique que existen grupos para administrar los recursos compartidos del Servidor de ficheros.		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y compruebe que existen grupos con usuarios para asignar posteriormente a los recursos compartidos con los permisos adecuados.  **Nota:** Para la creación de esta guía se utiliza el grupo "Grupo Administración FS" con los usuarios "adminsfs1" y "adminsfs2".
6. Inicie sesión en un Servidor de ficheros		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos**, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 
8. Verifique que los servicios del sistema relacionados con el servidor de ficheros están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permisos	OK/NOK
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administrador de informes de almacenamiento del servidor de archivos	SRMReports	Automático		
Administrador de recursos del servidor de archivos	SrmSvc	Automático		
Administración remota de Windows	WinRM	Automático		
SMP de espacios de almacenamiento de Microsoft	smphost	Manual		
Servicio de desduplicación de datos	ddpsvc	Manual		
Servidor	LanmanServer	Automático		

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique que la instalación del servidor de ficheros se ha realizado correctamente.		Utilizando la herramienta de administración de ficheros (ejecutando "fsmgmt.msc" desde, botón derecho sobre **Inicio → Ejecutar**…), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 
10. Verifique que la instalación del servidor de ficheros se ha realizado correctamente.		Utilizando la herramienta de administración de ficheros (ejecutando "fsrm.msc" desde, botón derecho sobre **Inicio → Ejecutar**…), verifique que la consola se inicia y presenta el servidor local como un servidor de ficheros. 
11. Verifique que los recursos compartidos poseen los permisos adecuados para los diferentes usuarios.		Desde el Administrador del servidor acceda al apartado **"Servicios de archivos y almacenamiento → Recursos compartidos"**. Haga clic derecho sobre uno de los recursos compartidos y seleccione "Propiedades". Acceda a la sección "Permisos" y verifique los permisos que posee el recurso. 

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que los recursos poseen una auditoría configurada.		En la sección "Permisos", pulse sobre "Personalizar permisos…". Acceda a la pestaña auditoría y verifique su configuración.  **Nota:** Para la realización de esta guía se activa la auditoría para el grupo denominado "Grupo Administración FS".
13. Verifique que los recursos compartidos poseen las cuotas de disco adecuadas.		Desde el Administrador del servidor acceda al apartado **"Servicios de archivos y almacenamiento → Recursos compartidos"**. Seleccione cualquier recurso y observe el aparatado "Cuota" para comprobar cuál de las disponibles tiene aplicada cada recurso.  **Nota:** Para la realización de esta guía se aplica la cuota denominada "Cuota Personalizada" sobre "E:\compartida_recursos".

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que los recursos compartidos poseen el filtrado de archivos adecuado.		Utilizando la herramienta de administración de ficheros (ejecutando "fsrm.msc" desde, botón derecho sobre **Inicio → Ejecutar**…) verifique en el nodo **"Administración del filtrado de archivos → Filtros de archivos"** que existen filtros aplicados a los recursos compartidos.  **Nota:** Para la realización de esta guía se aplica un filtro sobre el recurso denominado "compartida_recursos".
15. Verifique que se han configurado informes de almacenamiento para los recursos compartidos.		Utilizando la misma herramienta verifique en el nodo **"Administración de informes de almacenamiento"** que están configurados los informes para los distintos recursos.  **Nota:** Para la realización de esta guía se crea un informe para el recuso denominado "compartida_recursos".