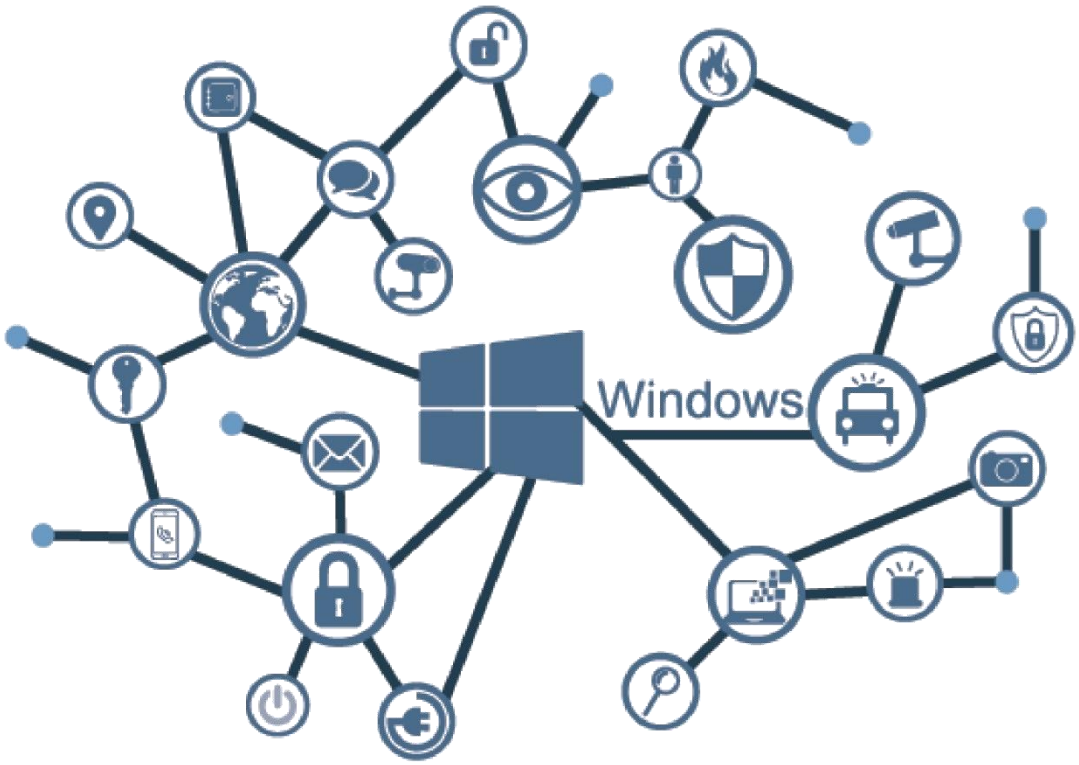
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 573-25

PERFILADO DE SEGURIDAD PARA SERVIDOR DE FICHEROS (SERVIDOR MIEMBRO DE UN DOMINIO)



MAYO 2025

MINISTERIO
DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO 083-25-134-1
Fecha de Edición: mayo de 2025

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2025.05.26 14:06:22 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

INDICE

1. INTRODUCCIÓN

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

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

Por ejemplo, en el caso de un entorno para un servidor miembro de un dominio con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2016, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-570A en el servidor miembro con Windows Server 2016.

b) Guía CCN-STIC-574 Internet Information Services (IIS) 10.

c) Guía CCN-STIC-576 Microsoft Exchange Server 2016 en Windows 2016.

Nota: En versiones anteriores del sistema operativo Microsoft Windows es posible que puedan encontrarse guías de seguridad y referencias bajo la numeración de guías de la serie 800. No obstante, la serie 500 corresponde a la tecnología Microsoft encontrándose en esta serie todos los documentos aplicables en sus productos más nuevos.

2. OBJETO

El propósito de este documento de seguridad (guía) es proporcionar los elementos y directrices para aplicar y garantizar la seguridad en equipos que implementen sistemas operativos Windows Server y que prestan el servicio de Servidor de Ficheros.

Para la definición de las medidas de seguridad asociadas a este documento, se ha tomado en consideración las necesidades técnicas aplicables descritas en el 'Anexo II' del ENS, así como lo definido en la guía CCN-STIC-301 y los posibles riesgos asociados al uso de un sistema operativo. Se trata de la aproximación del MARCO MODERNO DE SEGURIDAD que desde el Centro Criptológico Nacional se persigue para una adaptación adecuada al ecosistema en cuestión, el cual basa sus pilares fundamentales en los siguientes objetivos:

a) Las medidas a adoptar estarán condicionadas no solo por la normativa aplicable y el presente documento sino también por el análisis de riesgos preceptivo de cada escenario (sistema de información – CIS), la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.

b) Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca **utilizando la Declaración de Aplicabilidad Técnica o Perfil de Cumplimiento Técnico Específico (PCTE)** como elemento fundamental sobre el que vertebrar la seguridad. Se tomará de igual modo en cuenta el **Perfil de Cumplimiento Específico (PCE)** aplicable al conjunto del organismo y sus sistemas de información.

c) El Perfil de Cumplimiento Técnico Específico y las medidas establecidas por medio del **presente documento cumplen los requisitos técnicos para que los sistemas TIC se adapten a cualquier CALIFICACIÓN DE LA INFORMACIÓN** tomando en consideración la categorización de los sistemas definida en el ENS.

d) Las guías se revisarán y se actualizarán según las nuevas amenazas, avances tecnológicos y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.

La configuración planteada se ha diseñado para adaptarse a las características específicas de cada entorno, en función de las necesidades de este, pero cumpliendo los mínimos de seguridad definidos bajo el PCTE, los cuales, si no es posible aplicar deberán ser cubiertos por medio de medidas complementarias (vigilancia) y/o compensatorias.

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

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

3. ALCANCE

La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones según diferentes escenarios. En particular, se incluirá la configuración para asegurar **servidores basados en un sistema operativo "Microsoft Windows Server"**, instalados en español con la versión completa del producto (experiencia de escritorio), actuando con el **rol de Servidor de Ficheros**.

El documento no se centrará en una edición y versión concreta del producto o servicio, como pueda ser un Servidor de Ficheros en Windows Server 2016 o en Windows Server 2019, sino que será de utilidad para **cualquier edición y versión de Windows Server** (siendo recomendable su aplicación desde la edición Windows Server 2016 en adelante). Esto será posible siempre que estas configuraciones puedan ser de aplicación o bien cuando los aspectos técnicos del propio sistema operativo permitan la aplicación de las medidas definidas en el presente documento.

Nota: Para la elaboración del presente documento y la definición de medidas de seguridad se ha hecho uso del sistema operativo Windows Server 2022 Standard.

Las **medidas de seguridad** contempladas en este documento **se podrán aplicar a sistemas ya implementados o nuevos sistemas**, minimizando el impacto en entornos que se encuentren ya en producción.

Nota: Cuando un nuevo sistema operativo o producto no permita aplicar las medidas de seguridad asociadas a este documento se estudiará la necesidad de elaborar una nueva guía de seguridad o bien incluir apartados y descripciones adicionales para estas situaciones.

Por otro lado, las configuraciones a implementar y definidas en el presente documento, según se ha indicado con anterioridad, se basan en las necesidades para **cubrir los aspectos técnicos definidos en el ENS en función de la calificación de la información manejada por los sistemas**, pero tomando en consideración todas las categorías y dimensiones de seguridad requeridas según cada medida (Confidencialidad – C, Integridad – I, Trazabilidad – T, Autenticidad – A y Disponibilidad – D).

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad que **deberá ser adaptada a las necesidades propias de cada organización y sistema de información que así lo requiera**.

Este documento incluye:

a) Descripción de uso de esta guía. Explicación acerca de los elementos contenidos en este documentos y asociados al mismo, así como las consideraciones para identificar, seleccionar y aplicar las medidas de seguridad necesarias.

b) Perfil de cumplimiento técnico específico. Medidas aplicables del ENS y sus correspondientes refuerzos a nivel técnico sobre el producto del que versa esta guía de seguridad.

c) Medidas de seguridad de mejora. Basado en un PCTE adicional, este apartado recogerá una serie de medidas técnicas, las cuales se basan en las necesidades definidas por otras normativas oficiales aplicables, principalmente la guía de seguridad CCN-STIC-301.

   De igual modo, y sin que dependa de una normativa específica, se establecerán una serie de medidas de seguridad adicionales basadas en el estado tecnológico del producto afectado y reconocidas en el marco de referencia. También pueden considerarse otras propias resultantes de la experiencia de productos anteriores o simples mecanismos recomendados por el fabricante.

d) Nuevas medidas de seguridad. A medida que el sistema operativo Windows Server disponga de nuevas configuraciones de seguridad de interés que cubran las medidas aplicables, se incluirá en dicho punto la explicación sobre dichas parametrizaciones. Esto tiene por objetivo cumplir lo indicado en el apartado anterior sobre la actualización en el tiempo según las nuevas amenazas y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.

Nota: Este punto no se encontrará disponible en la primera versión de esta guía.

e) Guía paso a paso. Permitirá implantar y establecer las configuraciones de seguridad definidas y creadas para sistemas operativos Windows Server, cuando estos realicen las funciones de Controlador de Dominio o servidor miembro de un dominio.

Dentro del presente documento, no se contempla un entorno basado en un sistema operativo Windows Server no unido a un dominio (Independiente), no obstante, es posible extrapolar las configuraciones definidas para que sean de igual aplicación.

4. DESCRIPCIÓN DE USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de aplicación de seguridad que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Independiente de la aplicación de medidas asociadas a esta guía, debe cubrirse todo el espectro de necesidades recogidas bajo las indicaciones del ENS, así como el resto de normativa aplicable que pueda intervenir para la correcta adecuación de los sistemas de información TIC.

b) Dada la necesidad anterior, previo a la aplicación de medidas descritas en el presente documento, y según se especifica en el ENS, se tendrá en consideración que el análisis y la gestión de los riesgos es uno de los puntos esenciales del proceso de seguridad. En este sentido deberá prestarse especial atención a los riesgos asociados a un equipo que cumple con el rol de Servidor de Ficheros.

   i. Identificación de riesgos del producto o tecnología. Se recomienda realizar un inventario de riesgos que puedan existir por la propia naturaleza del producto o tecnología, como por la funcionalidad prevista por la organización.

ii. Cuantificación de probabilidad de cada riesgo. Se deberá cuantificar la probabilidad de ocurrencia de cada riesgo en función de las condiciones particulares que cada organización conoce de sus sistemas.

iii. Cuantificación de impacto de cada riesgo. Se deberá cuantificar el impacto en las operaciones y en el negocio, en función de las condiciones particulares que cada organización conoce de sus sistemas.

iv. Cuantificación de superficie de exposición del sistema o servicio. La organización deberá determinar el nivel de superficie de exposición que tendrá el activo (servicio que presta o información que maneja).

c) El mismo sistema de información deberá diseñarse, reestructurarse o adecuarse para otorgar los mínimos privilegios en su uso reduciendo también de este modo la superficie de exposición.

d) Para conocer, los requisitos mínimos indispensables para el sistema TIC y, por lo tanto, las medidas de seguridad a aplicar, cada organización u organismo deberá establecer una categoría para su sistema. Según se expone en el 'Artículo 40' del ENS y relacionado con la información anterior "La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad". De igual modo "La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad".

   Por todo lo anterior, dentro de un sistema, producto o servicio, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos. Por ende, la categorización del sistema será la correspondiente al mayor nivel de alguna de las dimensiones de seguridad.

Nota: Es posible obtener más información dentro del 'Anexo I' del ENS relativo a la categorización de un sistema de información.

- https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

e) Realizadas las acciones anteriores, debe tenerse en cuenta que, además de los requisitos a cumplir para la instalación del rol Servidor de Ficheros, puede ser necesario comprobar los requisitos de otros servicios y aplicaciones que vayan a ser implementadas posteriormente o que ya se encuentren instaladas, especialmente requisitos relacionados con el particionamiento de los discos. En la mayoría de los productos y/o servicios, como es el caso, se recomienda tener en **particiones distintas el sistema operativo y el resto de ficheros de la aplicación o aplicaciones**.

   La afirmación anterior se fundamenta en mejorar el rendimiento, así como para evitar ataques que consistan en ocupar la partición de sistema creando nuevos objetos en las bases de datos.

f) Además de la recomendación anterior, se exponen a continuación una serie de consideraciones de interés:

   i. Todos los discos y particiones deberán formatearse utilizando un sistema de archivos que permitan la aplicación de listas de control de acceso (en inglés ACL – Access Control List).

   ii. No instalar otros sistemas operativos en el equipo.

   iii. Asignar o modificar la contraseña para el usuario Administrador integrado para que esta sea compleja.

   iv. Establecer una nomenclatura de nombres (hostname) a los equipos y definir rangos de IP adecuados en función de sus necesidades, tratando de separar (segregar) siempre las redes de producción y de gestión.

   v. Instalar todas las actualizaciones de seguridad necesarias. Idealmente estas actualizaciones de seguridad se instalarán antes de conectar el equipo a la red o con el equipo conectado a una red segura.

g) Instalación del producto (en nuevas instalaciones). Una vez conocidos los riegos y las medidas de mitigación de éstos, se procederá con la instalación del producto o rol, en el caso de nuevas implementaciones. Si su producto o aplicación ya está instalado, es posible obviar este paso.

h) Aplicación de medidas de seguridad. Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación o perfiles, basándose en la calificación de la información manejada por los sistemas de información. Esto se ha realizado tomando en consideración lo indicado por la medida “MP.INFO.2 Calificación de la información”:

   - ESTÁNDAR.
   - USO OFICIAL.
   - MATERIAS CLASIFICADAS.

   Estos tres alcances englobarán configuraciones en función de la categoría de los sistemas de información que se definen bajo el Real Decreto del ENS, siendo estas las siguientes:

   - BÁSICA
   - MEDIA
   - ALTA
   - SISTEMAS CLASIFICADOS

Con el objetivo de facilitar la implantación de la configuración de seguridad definida bajo el presente documento es necesario explicar la agrupación de medidas aplicadas según la calificación de la información y la categoría del sistema de información. A continuación, se define una tabla que recopila dicha información.

		CALIFICACIÓN DE LA INFORMACIÓN/PERFIL		
		ESTÁNDAR	USO OFICIAL	MATERIAS CLASIFICADAS
CATEGORÍA DEL SISTEMA DE INFORMACIÓN	BÁSICA	✓	✗	✗
	MEDIA	✓	✓	✗
	ALTA DIFUSIÓN LIMITADA	✗	✓	✗
	CONFIDENCIAL RESERVADO	✗	✗	✓

Tabla 1. Selección de perfil de medidas de seguridad

Tomando en consideración la información de la tabla anterior es necesario aclarar los siguientes aspectos:

- En el caso de los sistemas de información de categoría media es posible establecer una configuración más o menos restrictiva en función de la calificación de la información que maneja. Esto se debe a que la información catalogada como USO OFICIAL puede ser atribuida solo en sistemas a partir de la categoría media.
- Para los sistemas de información enmarcados dentro de la categoría alta, se ha definido el perfil más restrictivo de modo que cumpla en todo momento con los refuerzos técnicos aplicables definidos bajo el marco del ENS.
- La selección del perfil a establecer se aplicará sobre el conjunto del sistema de información, no siendo posible la aplicación de diferentes perfiles en distintos equipos del sistema. Por ende, si por ejemplo una organización está enmarcada dentro de la categoría alta, en todos los equipos se deberán implementar las medidas establecidas para el perfilado USO OFICIAL, no pudiendo establecer configuraciones menos restrictivas en ningún otro equipo.

i) Definido el perfil a implementar, en este paso se aplicarán las medidas de seguridad necesarias, adicionales y recomendadas según el perfil de seguridad seleccionado y las posibles normativas adicionales aplicables (Ley de Secretos Oficiales, normativa CCN-STIC-301, entre otras).

j) Entorno de pruebas. Antes de aplicar esta guía en producción, deberá asegurarse de haberla probado en un entorno aislado y controlado, en el cual se habrán aplicado las configuraciones definidas en el presente documento, así como los cambios en la configuración que se ajusten a los criterios específicos de cada organización.

k) Pruebas de funcionalidad. Se recomienda diseñar y ejecutar un plan de pruebas de funcionalidad previo y posterior a la aplicación de medidas de seguridad en el entorno final, asegurando de este modo que las medidas aplicadas no han tenido un impacto en la funcionalidad de los servicios que este presta. Esto es debido a que alguna de las configuraciones puede haber deshabilitado o bloqueado funcionalidades que requiere la organización. En ese caso se podrán establecer directivas de excepción para revertir los cambios, asumiendo el riesgo que ello conlleva. De igual modo, estas excepciones, deberán quedar correspondientemente documentadas para conocer las desviaciones técnicas establecidas dentro de la documentación de seguridad del sistema de información.

5. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO ENS

El presente apartado recoge el conjunto de medidas de aplicación técnica que es posible aplicar según las necesidades descritas por el ENS al rol de Servidor de Ficheros, independientemente de la calificación de la información y/o la categoría asociada al sistema de información TIC.

Los elementos descritos a continuación es lo que se considera el Perfil de Cumplimiento Técnico Específico (PCTE), asociado al rol Servidor de Ficheros.

A continuación, se indica una tabla en la que se expone dicho perfil, a partir de que categoría se aplicaría cada medida de seguridad y si dispone de refuerzo o mejoras a medida que aumenta la categoría.

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2

Tabla 2. Perfil de cumplimiento específico para sistemas operativos Windows Server

En total, según se puede apreciar en la tabla, es posible la aplicación directa de once (11) medidas de seguridad de forma técnica al sistema operativo Windows Server cuando ejerce la función de Servidor de Ficheros. Estás serán identificadas en los apartados posteriores, así como definidas a nivel técnico.

Nota: Es posible obtener información sobre la información de la tabla anterior y su interpretación en el 'Anexo II' del ENS relativo a definición de medidas de seguridad.

- https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

En los apartados posteriores se definirán los controles aplicables para el sistema operativo Windows Server y su aplicación a nivel técnico.

6. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO CCN-STIC

El presente apartado recoge el conjunto de medidas de aplicación técnica que es posible aplicar según las necesidades descritas por la guía de seguridad CCN-STIC-301 al rol de Servidor de Ficheros, independientemente de la calificación de la información, la categoría asociada al sistema de información TIC y/o nivel de clasificación de la información manejado.

Los elementos descritos a continuación es lo que se considera el Perfil de Cumplimiento Técnico Específico (PCTE), asociado al rol Servidor de Ficheros, del mismo modo que se exponía en el apartado anterior. Respecto al punto anterior ha sido añadida la columna denominada "MC" (Materias Clasificadas) asociada al perfil del mismo nombre.

A continuación, se indica una tabla en la que se expone dicho perfil, a partir de que categoría se aplicaría cada medida de seguridad y si dispone de refuerzo o mejoras a medida que aumenta la categoría.

Nota: Cuando la columna se encuentre definida en color magenta, aunque los refuerzos y aplicación puedan coincidir con su columna inmediatamente anterior, indicará que existen controles adicionales definidos bajo la guía de seguridad CCN-STIC-301. Adicionalmente, cuando dichos controles coincidan y hayan sido ampliados y aplicados técnicamente dispondrán de una nota aclaratoria.

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.1	Identificación	T A	aplica	+ R1	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3	+ R1 + R2 + R3

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	+ R1 + R2 + R3 + R4 + R5
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2	+ R1 + R2

Tabla 3. Perfil de cumplimiento específico para sistemas operativos Windows Server en MC

En total, según se puede apreciar en la tabla, es posible la aplicación directa de once (11) medidas de seguridad de forma técnica al sistema operativo Windows Server cuando ejerce la función de Servidor de Ficheros. Estás serán identificadas en los apartados posteriores, así como definidas a nivel técnico.

Nota: Es posible obtener información sobre la información de la tabla anterior y su interpretación en la guía de seguridad CCN-STIC-301.

En los apartados posteriores se definirán los controles aplicables para el rol de Servidor de Ficheros y su aplicación a nivel técnico.

ANEXO A. PASO A PASO DE CONFIGURACIÓN BASE DE SEGURIDAD SOBRE SERVIDOR DE FICHEROS

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento del rol de Servidor de Ficheros en los sistemas Windows Server, según los aspectos definidos en cada uno de los puntos anteriores de este documento.

El **presente apartado y paso a paso de ejemplo** establece la **configuración de seguridad base** para cumplir con los requisitos técnicos aplicables establecidos según el **perfilado ESTÁNDAR**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (ESTÁNDAR, USO OFICIAL o MATERIAS CLASIFICADAS) cuando así se indique.

De igual modo deberá tomar en consideración la **ejecución de pasos adicionales** cuando su **perfil aplicado sea USO OFICIAL o MATERIAS CLASIFICADAS**. El propio **documento indicará esta necesidad**.

A partir de configuración expuesta será posible, en función del preceptivo análisis de riesgos, superficie de exposición y categorización de cada sistema, establecer posibles configuraciones adicionales o rebajar las medidas de seguridad definidas.

Nota: Cuando el sistema operativo a asegurar maneje información la cual se califique con otra etiqueta, deberá evaluarse el perfilado a aplicar según lo descrito en el punto "4 DESCRIPCIÓN DE USO DE ESTA GUÍA", concretamente según se indica en el apartado "h)".

Este anexo, contempla la aplicación de seguridad basado en un entorno de dominio, tomando en este sentido los siguientes elementos:

a) Servidores miembro del dominio: Aplicable a aquellos equipos que proporcionen el servicio para la compartición de archivos (Servidor de Ficheros) dentro del dominio, se definirán medidas de seguridad mediante objetos GPO y se ejecutarán acciones manuales y automatizadas para finalizar las labores de configuración segura.

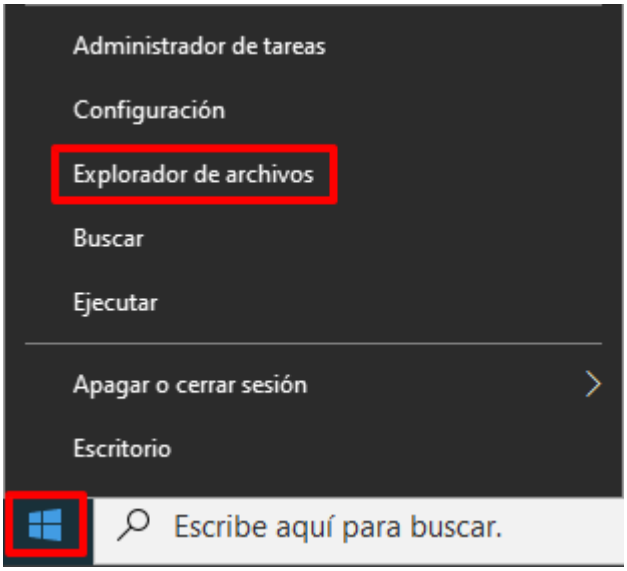
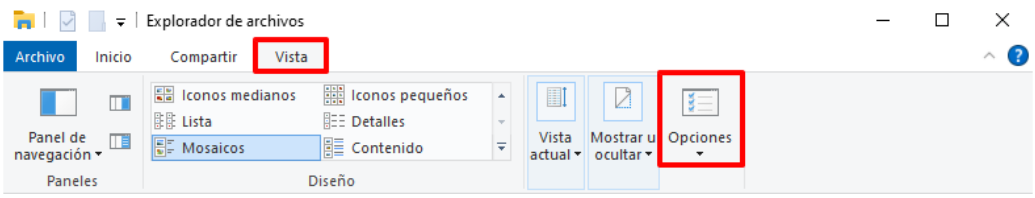
b) Configuraciones individuales: Es necesario indicar que ciertas medidas de seguridad no pueden ser aplicadas por medio de objetos GPO o configuraciones exactas a nivel de Windows. Esto es debido a que deben ser personalizadas por cada organización o adaptadas a esta. Por ello, se han dedicado apartados específicos que permitan establecer ejemplos de configuración sobre este tipo de medidas de seguridad.

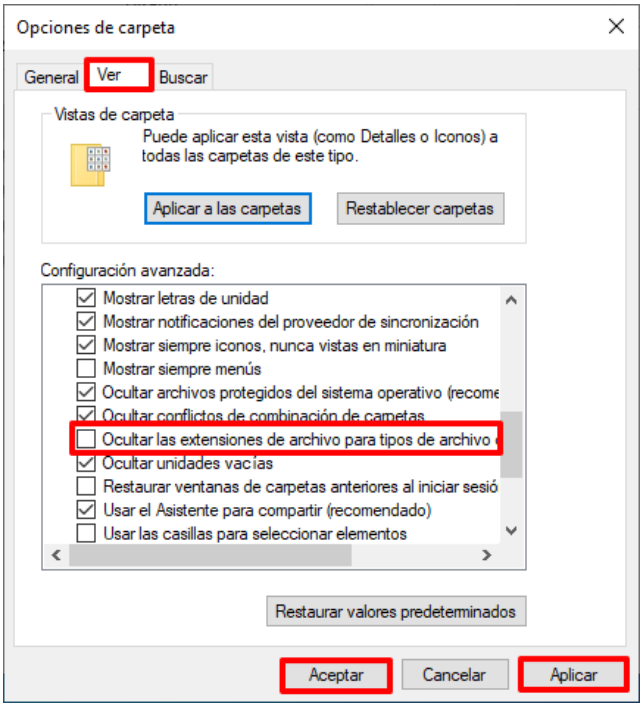
Se debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con el objeto de familiarizarse con el escenario y realizar las pruebas de funcionalidad oportunas.

Nota: Antes de comenzar con los siguientes apartados asegúrese de haber aplicado de manera adecuada la guía CCN-STIC-570A23 para equipos que son servidor miembro de un dominio.

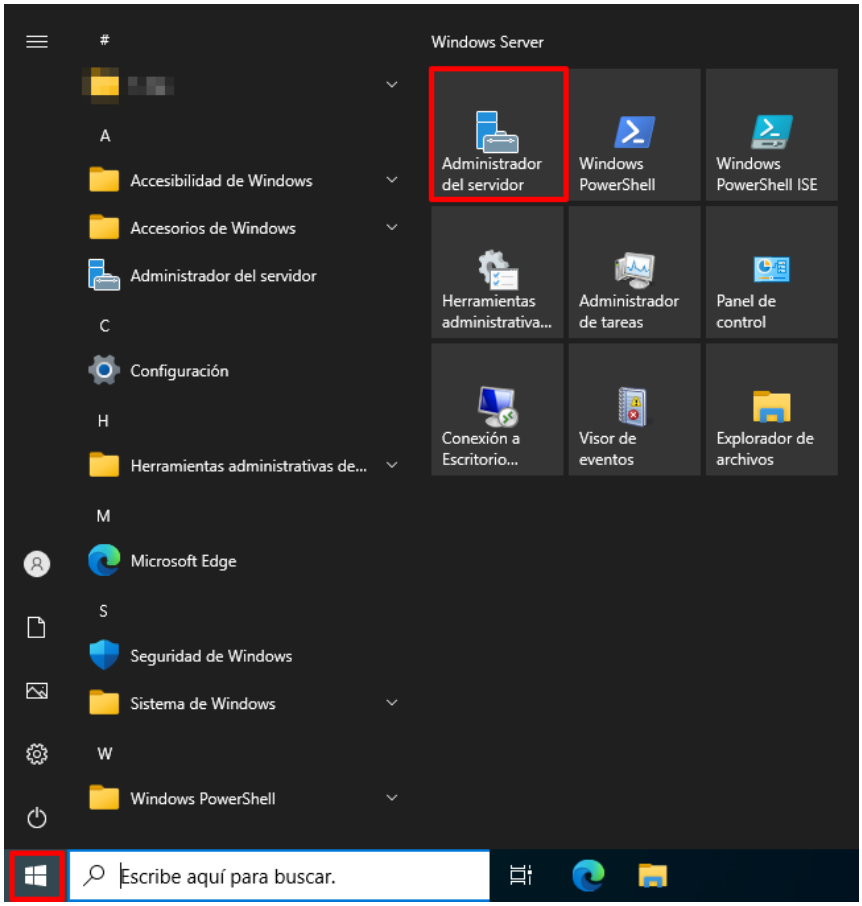
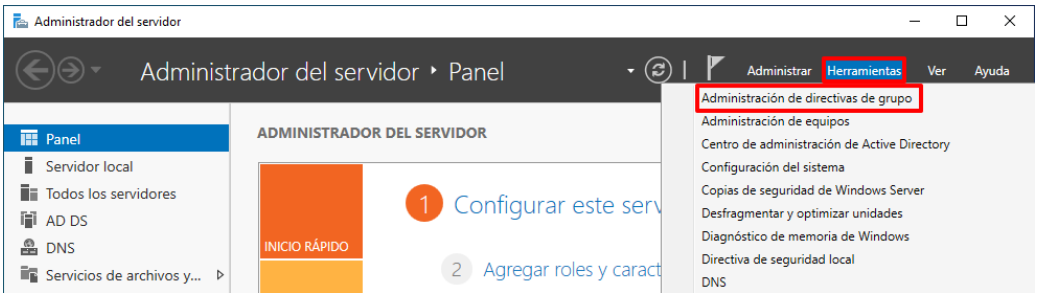
ANEXO A.1. PREPARACIÓN DEL DOMINIO

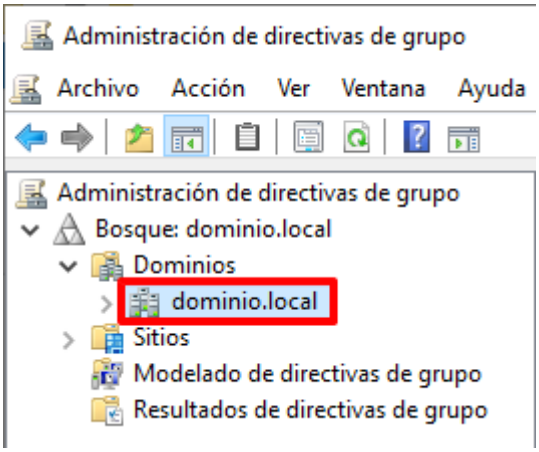
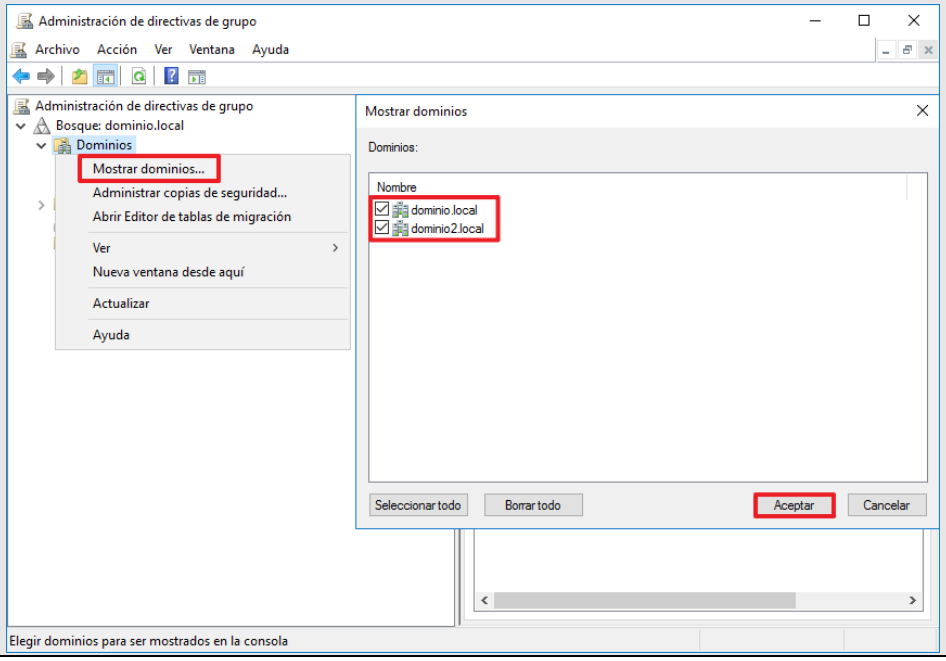
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las medidas de seguridad mediante objetos GPO. Solo es necesario realizar este procedimiento una (1) vez.

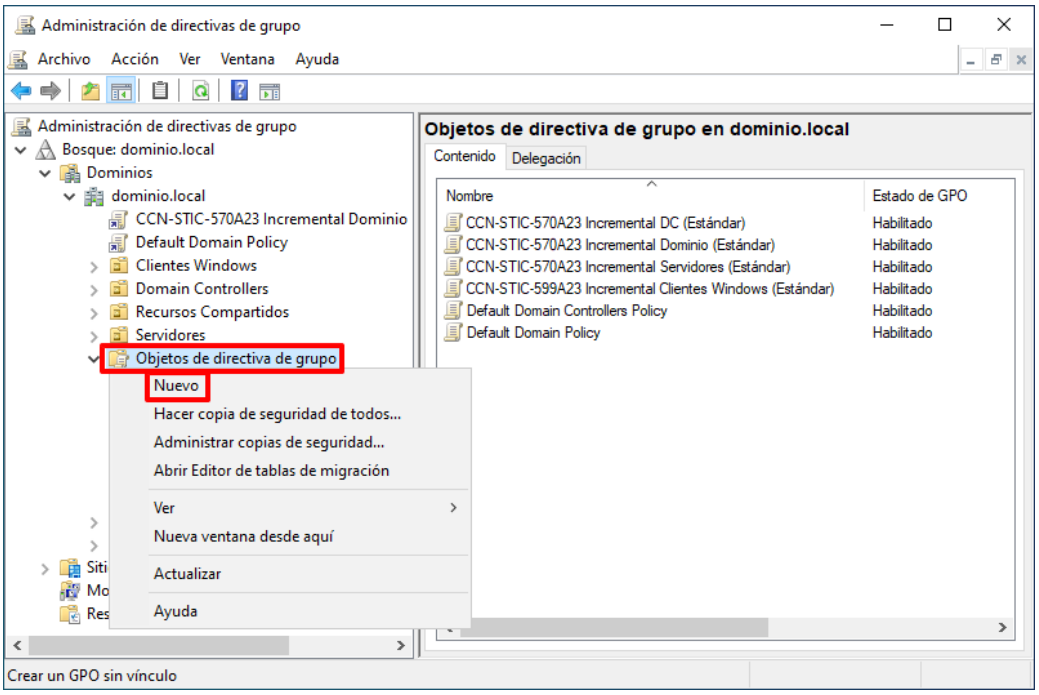
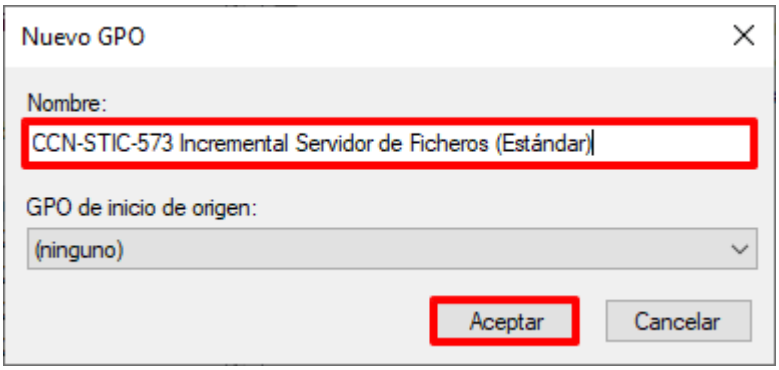
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad C:\.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-573”.
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”. 

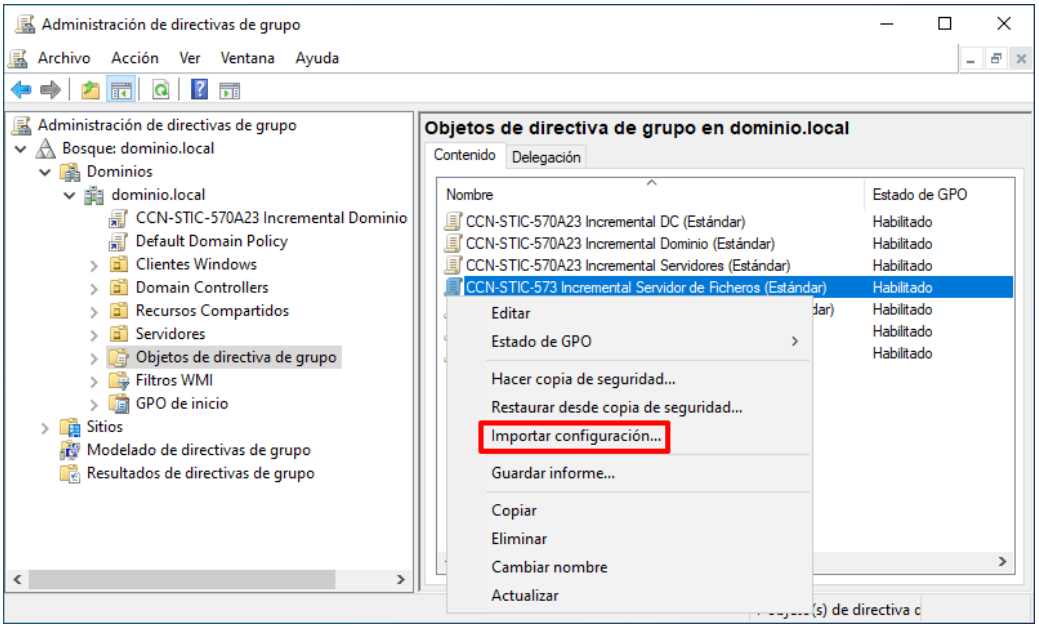
Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – ESTANDAR/USO OFICIAL/MATERIAS CLASIFICADAS • CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]).inf • CCN-STIC-573 Servidor de Ficheros - Configuracion completa FS ([TIPO DE PERFILADO]).bat – CCN-STIC-573 Servidor de Ficheros - Asistencia de acceso denegado.bat – CCN-STIC-573 Servidor de Ficheros - Auditoria de filtros.bat – CCN-STIC-573 Servidor de Ficheros - Auditoria DFS.bat – CCN-STIC-573 Servidor de Ficheros - Auditoria en Recursos Compartidos.bat – CCN-STIC-573 Servidor de Ficheros - Auditoria Servidor de Ficheros.bat – CCN-STIC-573 Servidor de Ficheros - Auditoria Servidor NFS.bat – CCN-STIC-573 Servidor de Ficheros - Autenticacion compartida.bat – CCN-STIC-573 Servidor de Ficheros - BranchCache para archivos de red.bat

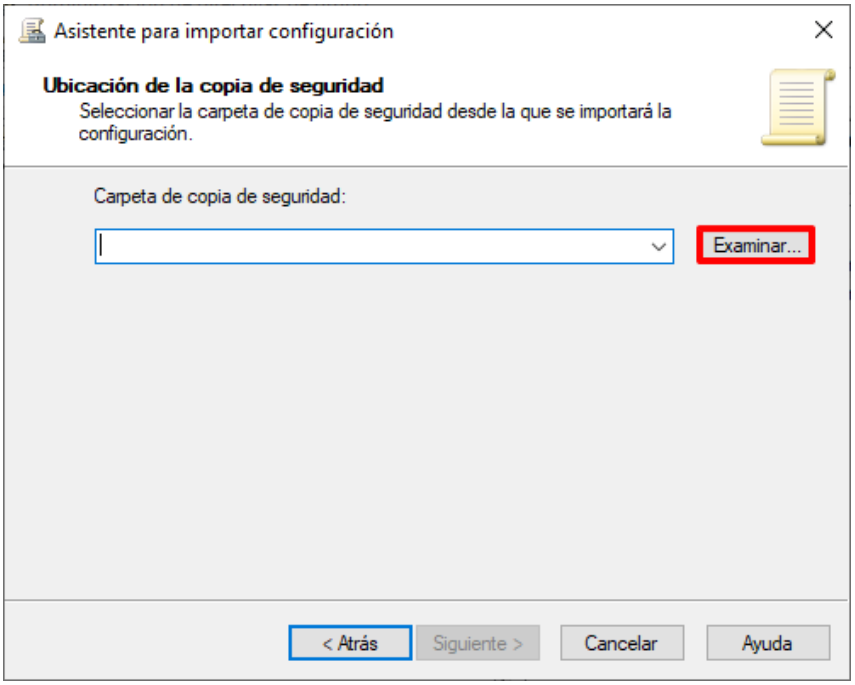
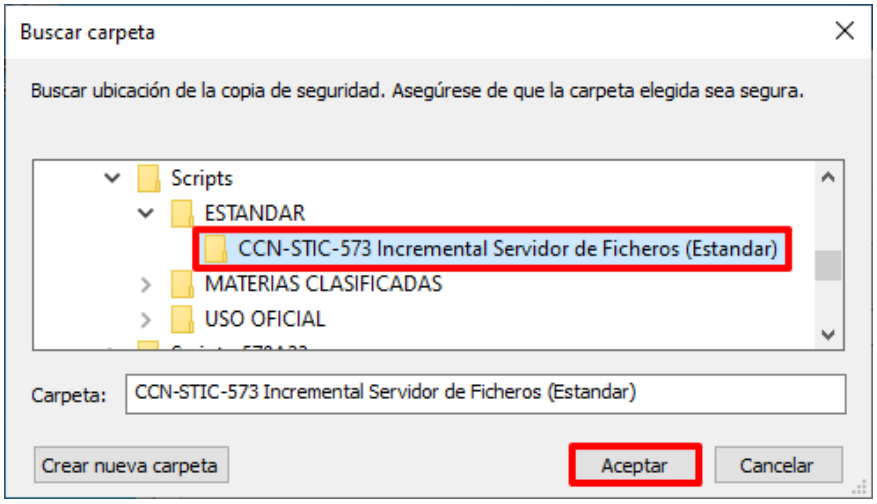
Paso	Descripción
	– CCN-STIC-573 Servidor de Ficheros - Cifrado de acceso a datos.bat – CCN-STIC-573 Servidor de Ficheros - Copia de seguridad configuracion FS.bat – CCN-STIC-573 Servidor de Ficheros - Copia de seguridad configuracion NFS.bat – CCN-STIC-573 Servidor de Ficheros - Desinstalar roles y caracteristicas.bat – CCN-STIC-573 Servidor de Ficheros - Habilitar ABE.bat – CCN-STIC-573 Servidor de Ficheros - Modo de arrendamiento.bat – CCN-STIC-573 Servidor de Ficheros - Protocolos NFS.bat – CCN-STIC-573 Servidor de Ficheros - Segregación de roles.bat – CCN-STIC-573 Servidor de Ficheros - Servidor NFS.bat – CCN-STIC-573_Comprobacion_instalacion_roles_DFS_NFS_BC_(ESTANDAR).ps1 – CCN-STIC-573_Comprobacion_instalacion_roles_DFS_NFS_BC_(UO-MC).ps1 – CCN-STIC-573_Configuracion_LeasingMode_y_NameHardeningLevel.ps1 – CCN-STIC-573_Configurar_BranchCache_para_archivos_de_red.ps1 – CCN-STIC-573_Configurar_Servidor_NFS.ps1 – CCN-STIC-573_Configurar_Servidor_NFS_protocolos.ps1 – CCN-STIC-573_Copia_seguridad_configuraciones_FS.ps1 – CCN-STIC-573_Copia_seguridad_configuraciones_NFS.ps1 – CCN-STIC-573_Definir_auditoria_en_recursos_compartidos.ps1 – CCN-STIC-573_Deshabilitar_Autenticacion_compartida.ps1 – CCN-STIC-573_Deshabilitar_Informacion_y_asistencia_acceso_denegado.ps1 – CCN-STIC-573_Desinstala_roles_y_caracteristicas_servidor_FS.ps1 – CCN-STIC-573_Habilitar_Auditoria_de_filtros.ps1 – CCN-STIC-573_Habilitar_Auditoria_DFS.ps1 – CCN-STIC-573_Habilitar_Auditoria_Servidor_NFS.ps1 – CCN-STIC-573_Habilitar_Cifrado_de_acceso_a_datos_y_cifrado_red.ps1 – CCN-STIC-573_Habilitar_Enumeracion_Basada_en_Acceso_ABE.ps1 – CCN-STIC-573_Habilitar_registro_acciones_File_Server.ps1

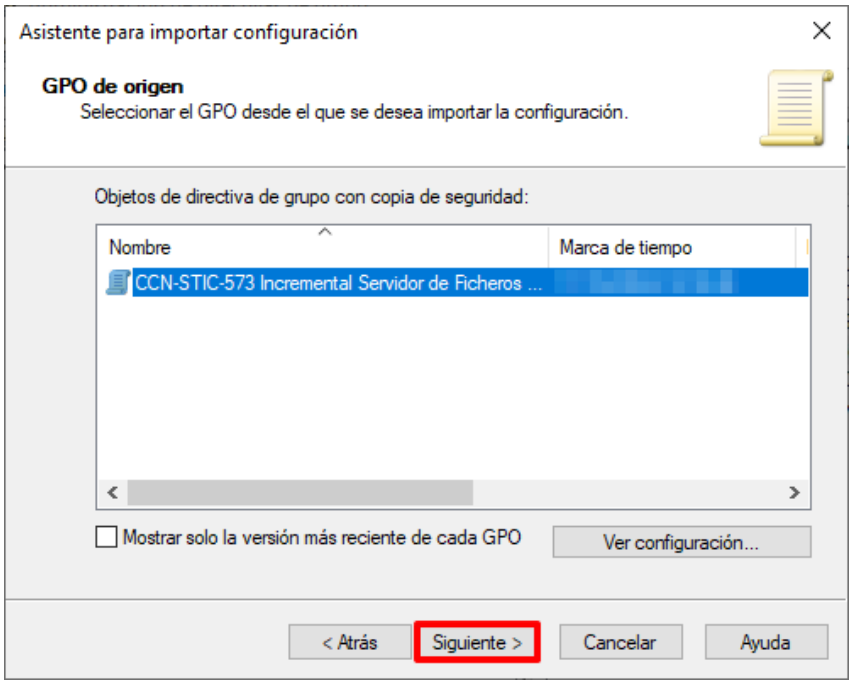
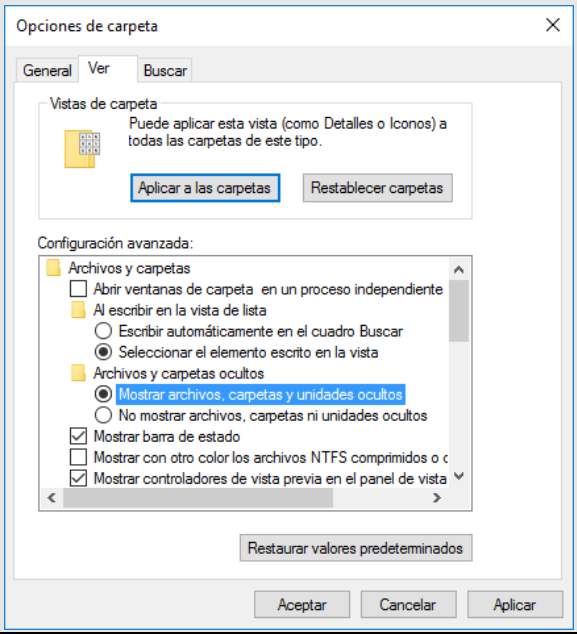
Paso	Descripción
8.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.
9.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 

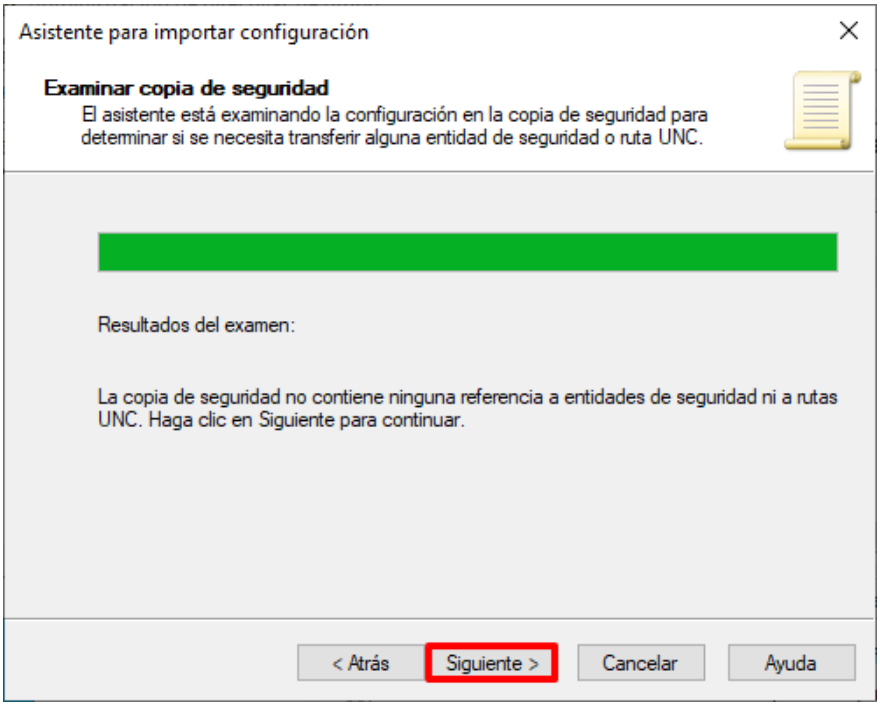
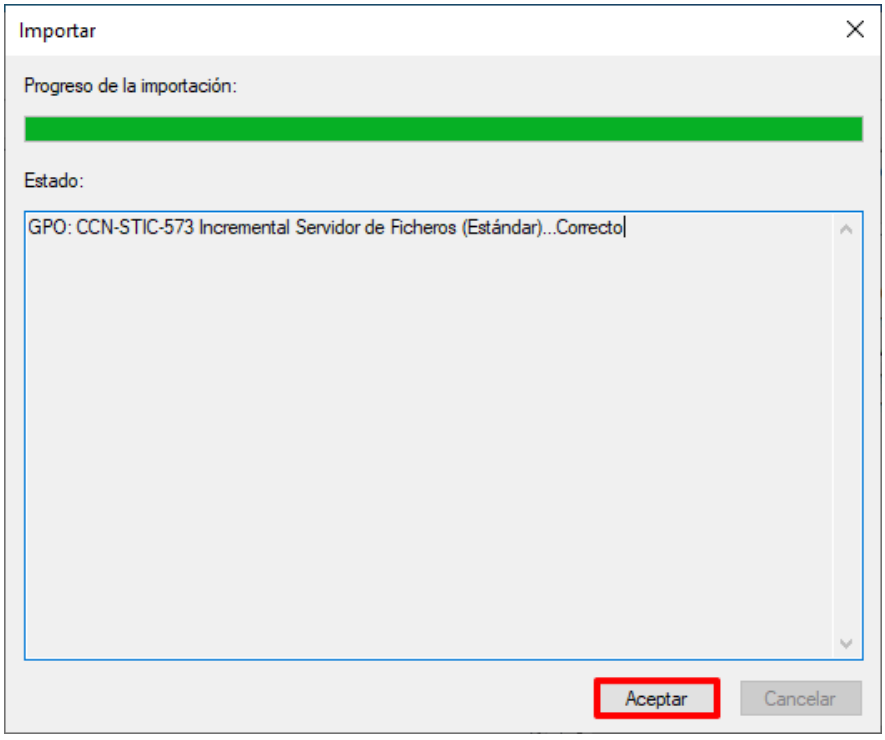
Paso	Descripción
10.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** Compruebe que realiza las tareas de administración sobre el dominio adecuado. Si no aparece su dominio en la ventana, utilice la opción "Mostrar dominios…" del menú contextual, marque los dominios que desea gestionar y pulse sobre "Aceptar" tal y como se indica a continuación. 

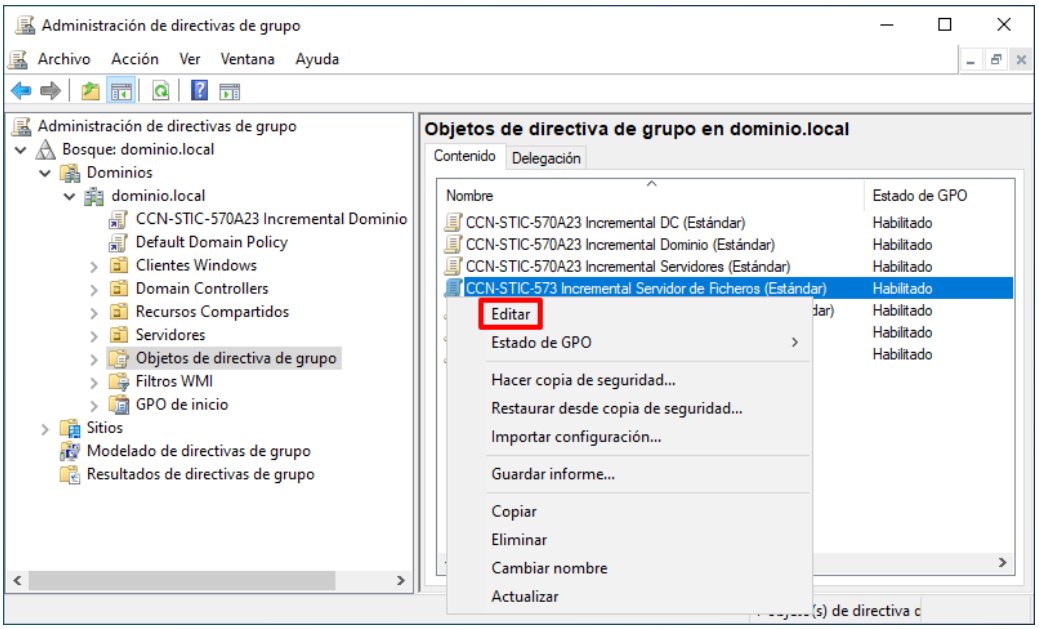
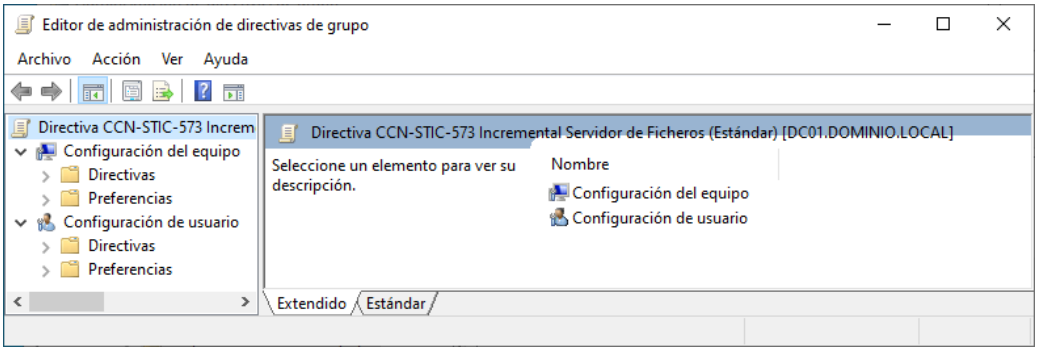
Paso	Descripción
11.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
12.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])**" y pulse el botón "Aceptar".  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

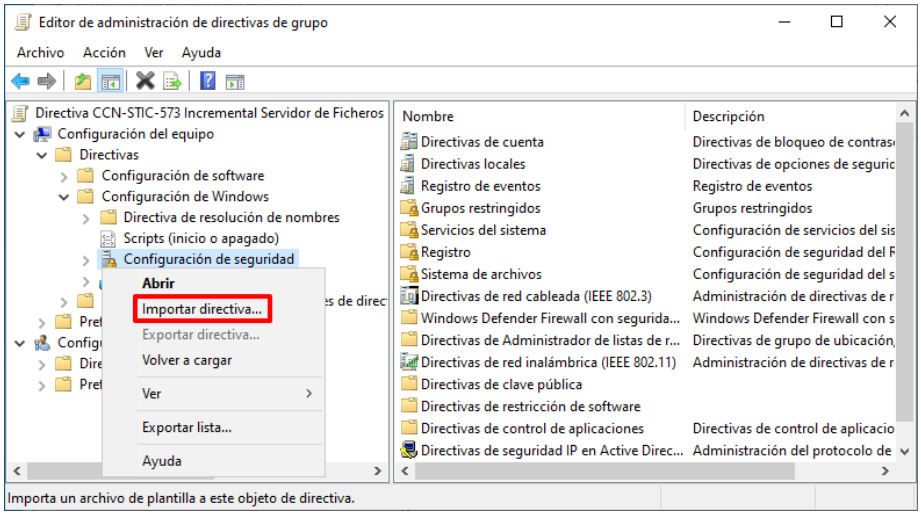
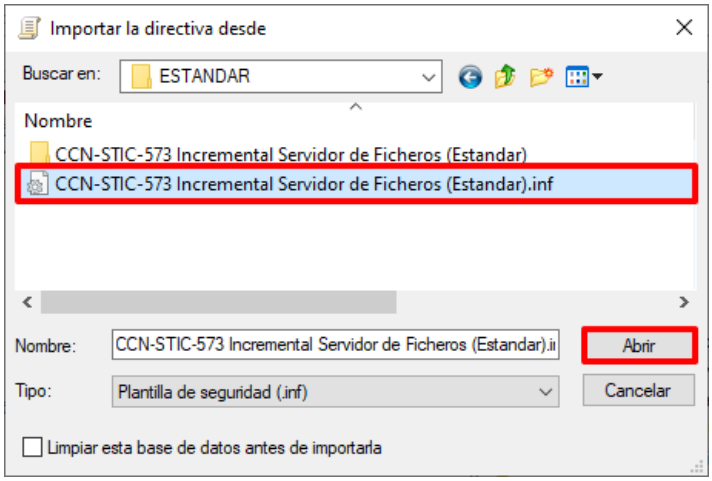
Paso	Descripción
13.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
14.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
15.	En la sección “Hacer copia de seguridad de GPO” pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad puesto que la política se encuentra vacía.

Paso	Descripción
16.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
17.	Seleccione la carpeta “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
18.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.

Paso	Descripción
19.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
20.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
21.	Para completar el asistente pulse sobre el botón “Finalizar”.
22.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse sobre “Aceptar”, no la tenga en consideración. 

Paso	Descripción
23.	Seleccione con el botón derecho el GPO recién creado, “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
24.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO. 

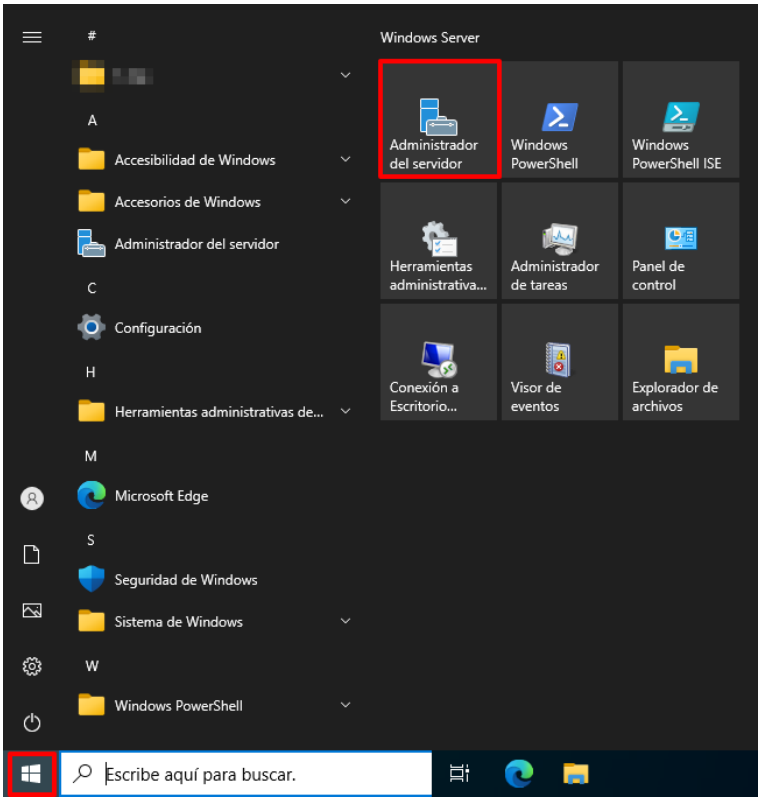
Paso	Descripción
25.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 
26.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
27.	Con eso habrá quedado importada la plantilla en el objeto GPO. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada sobre los objetos requeridos. Cierre la ventana "Editor de administración de directivas de grupo".

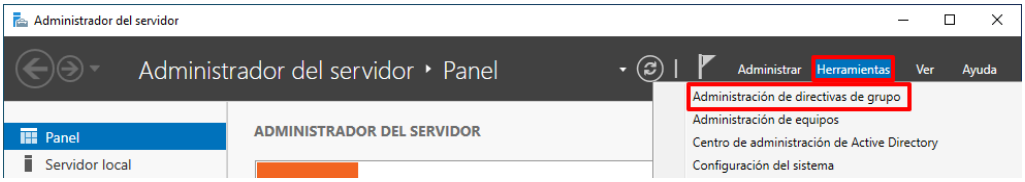
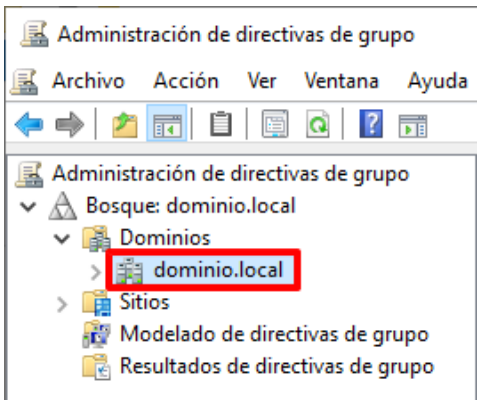
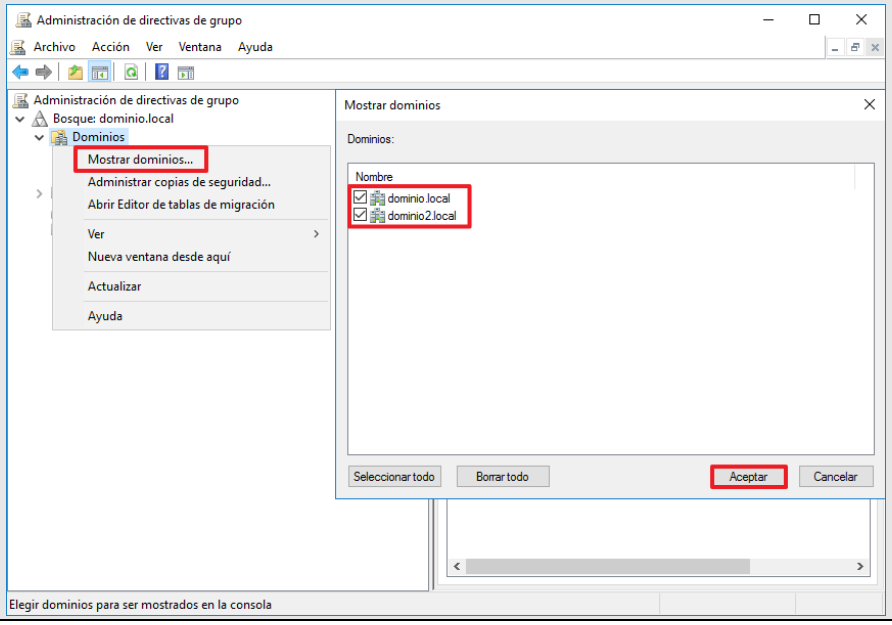
ANEXO A.2. CONFIGURACIÓN DE SEGURIDAD EN SERVIDOR DE FICHEROS

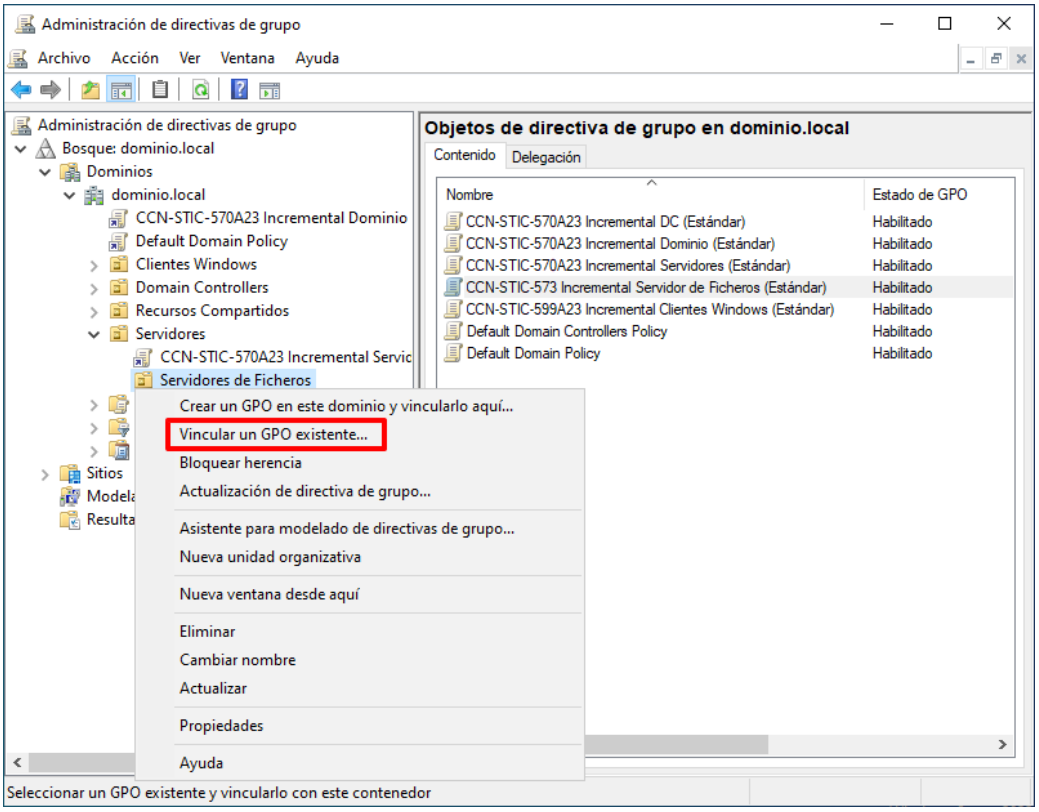
Una vez realizada la preparación de la configuración de seguridad necesaria a implementar, será necesario su aplicación sobre los objetos correspondientes, así como la ejecución de labores adicionales para cubrir todos los aspectos necesarios de seguridad.

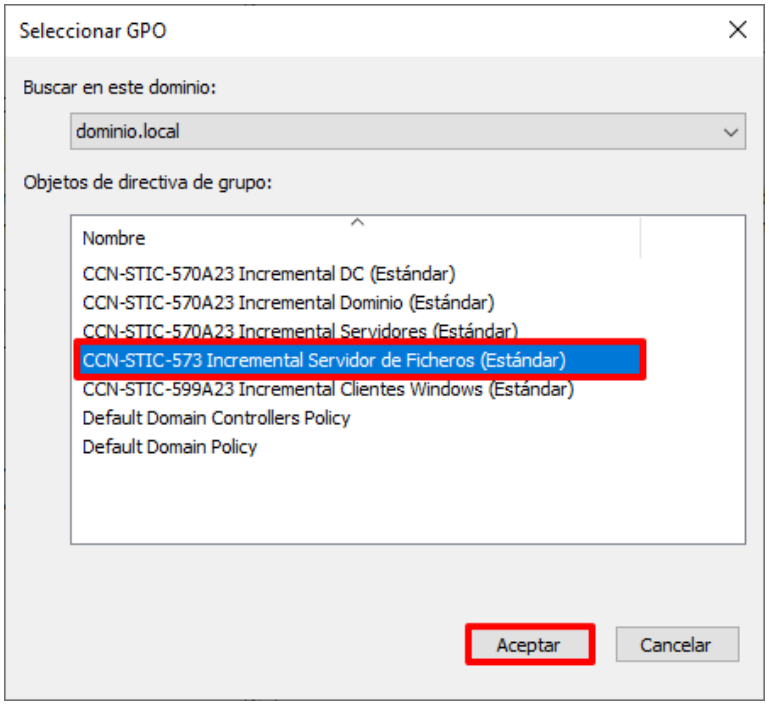
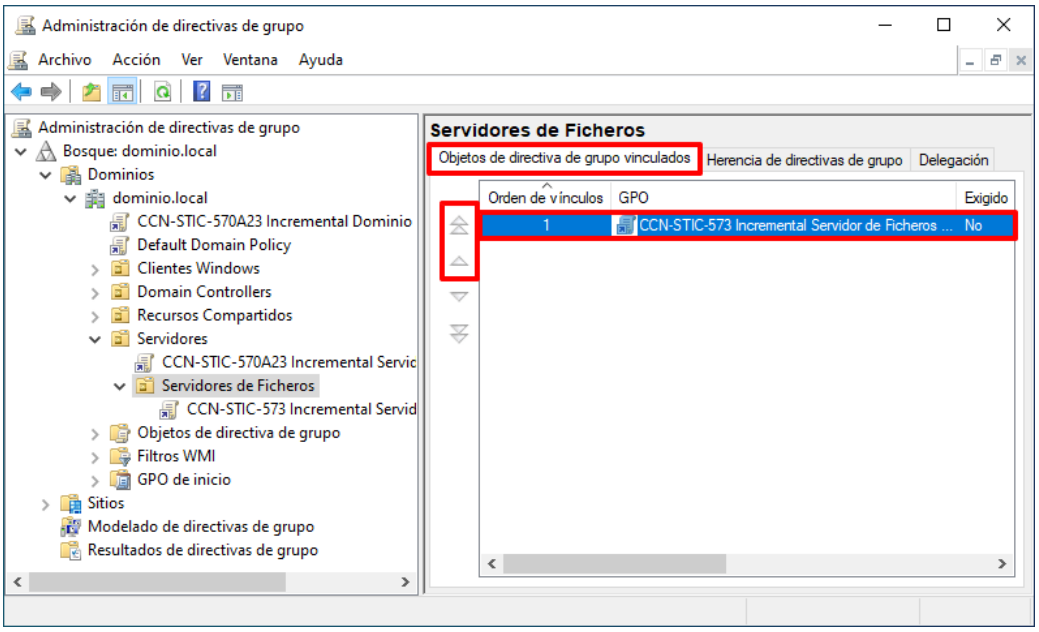
ANEXO A.2.1. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

A continuación, se definen los pasos a seguir para la adecuada aplicación de las políticas generadas en el punto anterior para aplicar la configuración de seguridad sobre el dominio y sobre los objetos de tipo Servidor de Ficheros. Solo es necesario realizar este procedimiento una (1) vez.

Paso	Descripción
28.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
29.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".

Paso	Descripción
30.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
31.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** Compruebe que realiza las tareas de administración sobre el dominio adecuado. Si no aparece su dominio en la ventana, utilice la opción “Mostrar dominios…” del menú contextual, marque los dominios que desea gestionar y pulse sobre “Aceptar” tal y como se indica a continuación. 

Paso	Descripción
32.	Identifique aquellas unidades organizativas donde se alojen aquellos objetos de tipo Servidor de Ficheros que se pretenden asegurar, y haciendo clic derecho sobre el contenedor seleccione la opción del menú contextual “Vincular un GPO existente…”.  **Nota:** En este ejemplo se hace uso de la unidad organizativa “Servidores → Servidores de Ficheros” creada para alojar los objetos de tipo servidor, con el rol de Servidor de Ficheros. Deberá adaptar este paso a las necesidades de su organización.

Paso	Descripción
33.	A continuación, seleccione el objeto GPO “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
34.	Seleccione el contenedor sobre el que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña “Objetos de directiva de grupo vinculados”, seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

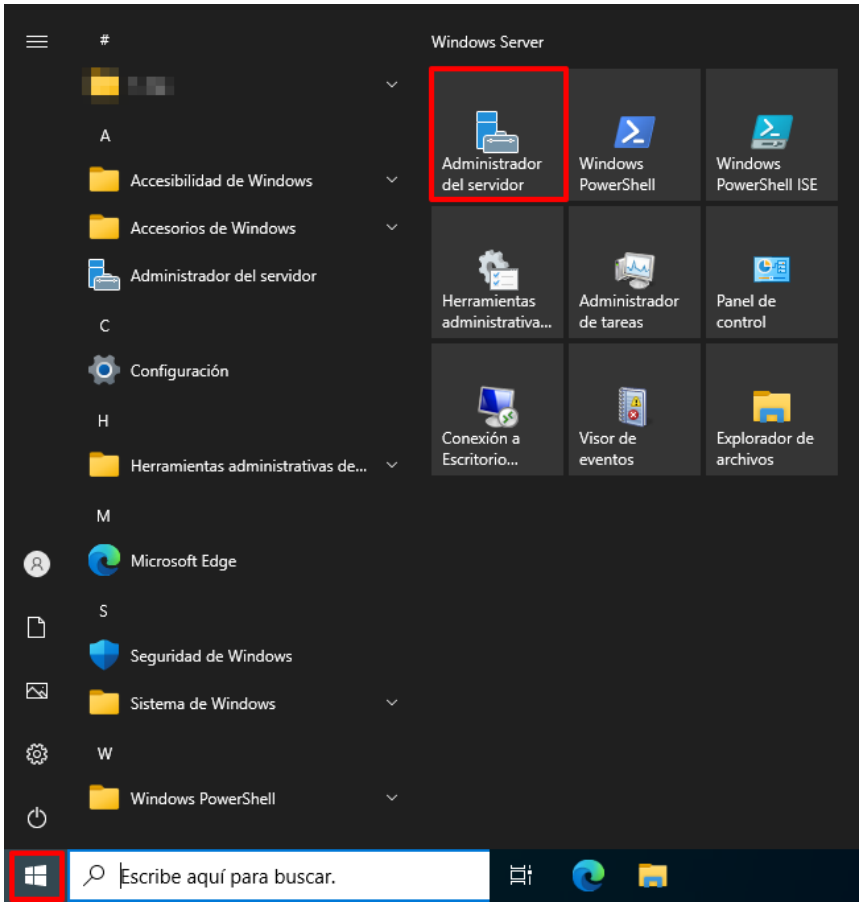
Paso	Descripción
35.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. Si desea realizar este filtrado siga los pasos indicados a continuación. En caso contrario, obvie el siguiente apartado y continue en el punto posterior. **Nota:** En el siguiente apartado se definirán los pasos para realizar una segregación por medio del uso de un grupo de seguridad.

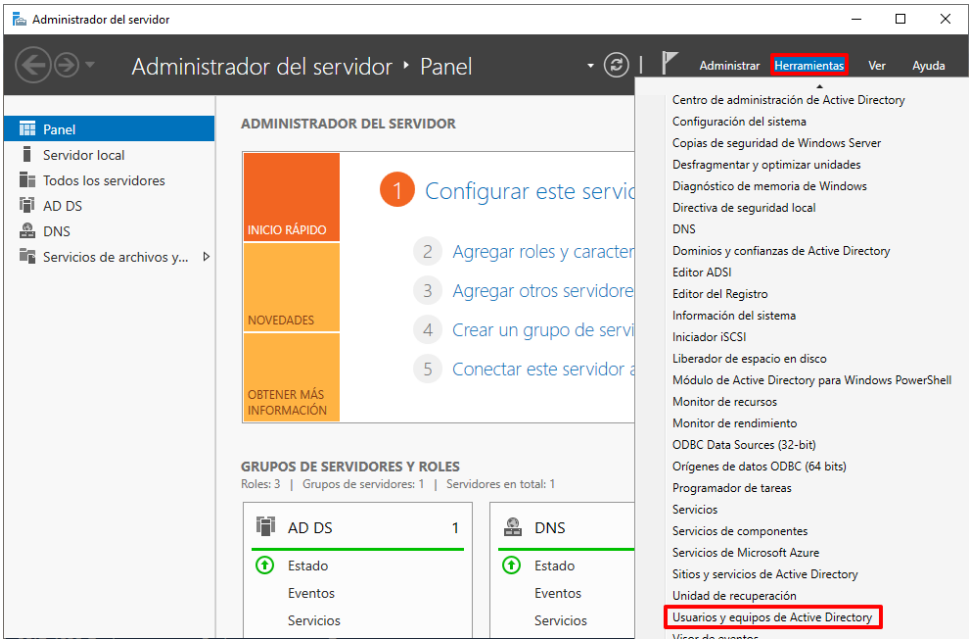
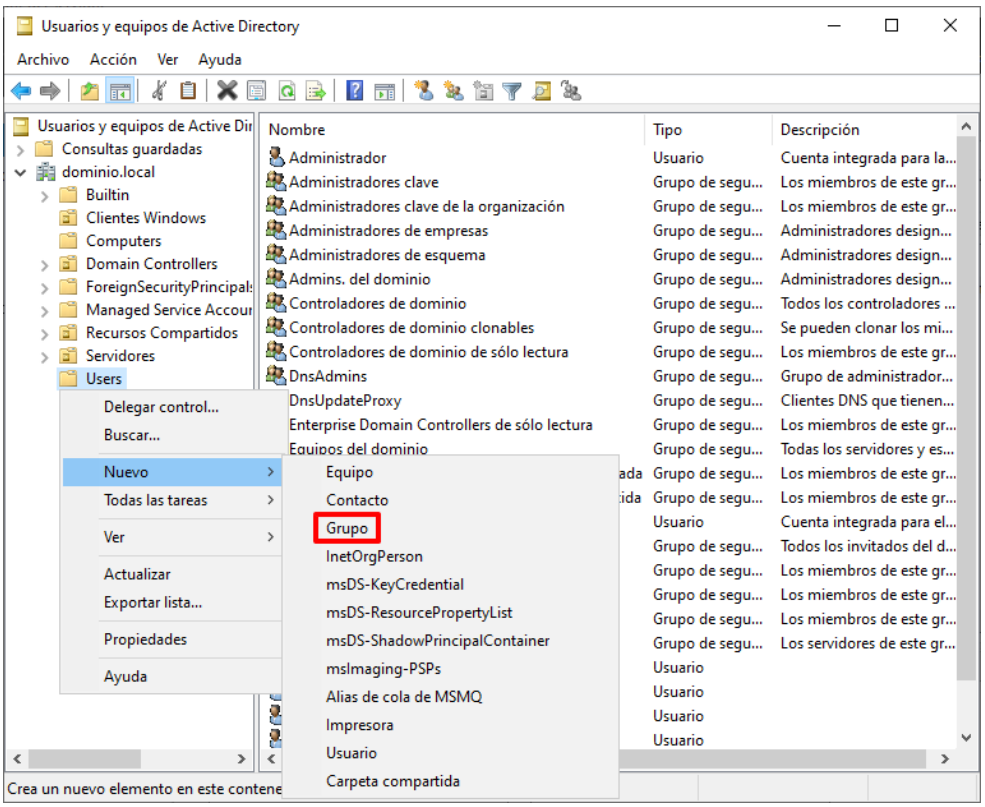
ANEXO A.2.2. FILTRADO DE SEGURIDAD DE OBJETOS GPO

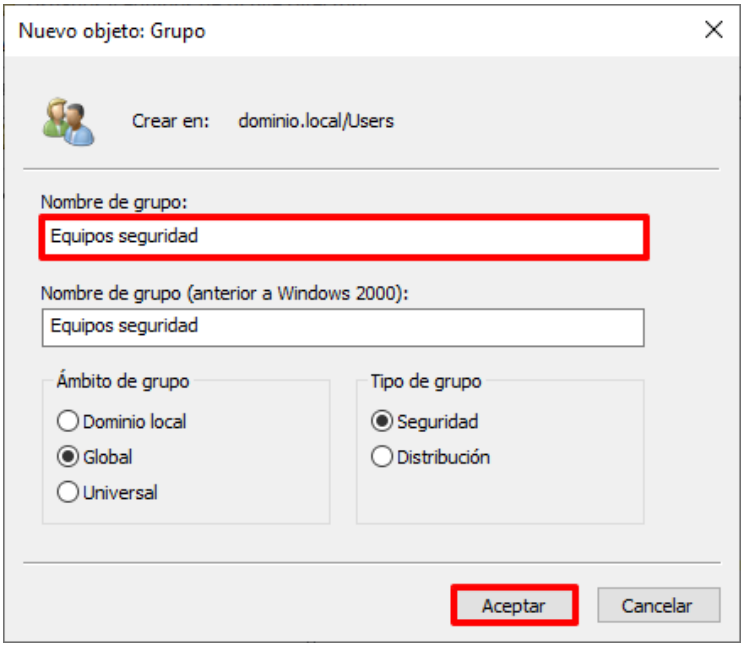
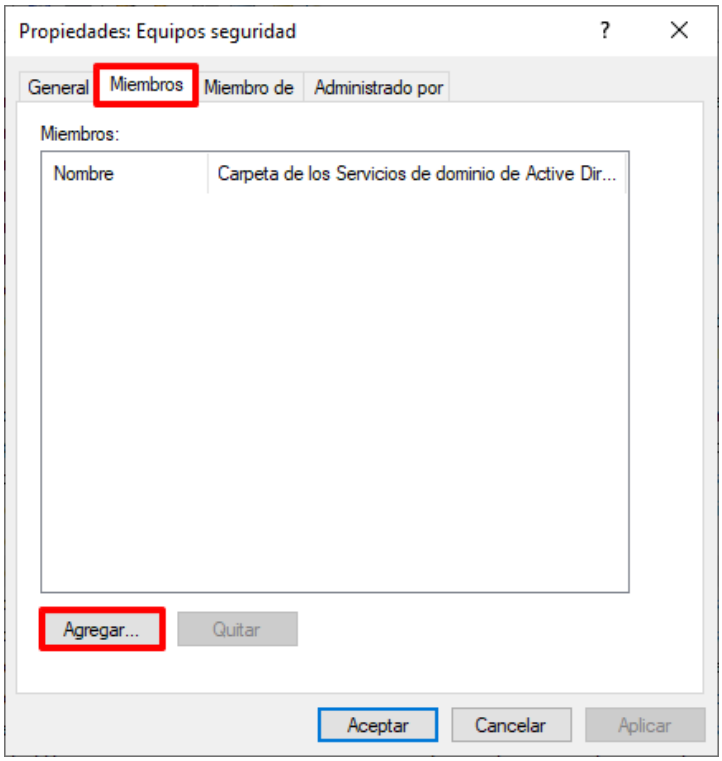
El presente apartado tiene como objetivo realizar una creación de un grupo de seguridad sobre el que aplicar el objeto GPO. Esto permitirá que solo se aplique el objeto GPO a los objetos incluidos dentro de dicho grupo, aunque en la unidad organizativa que se aplica el objeto GPO existan más objetos.

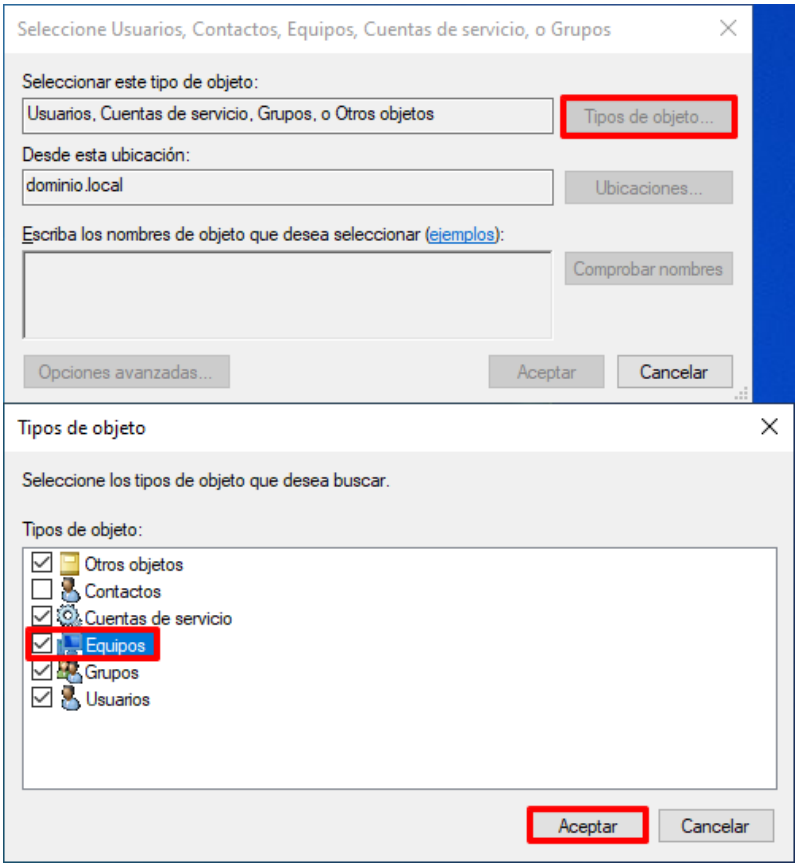
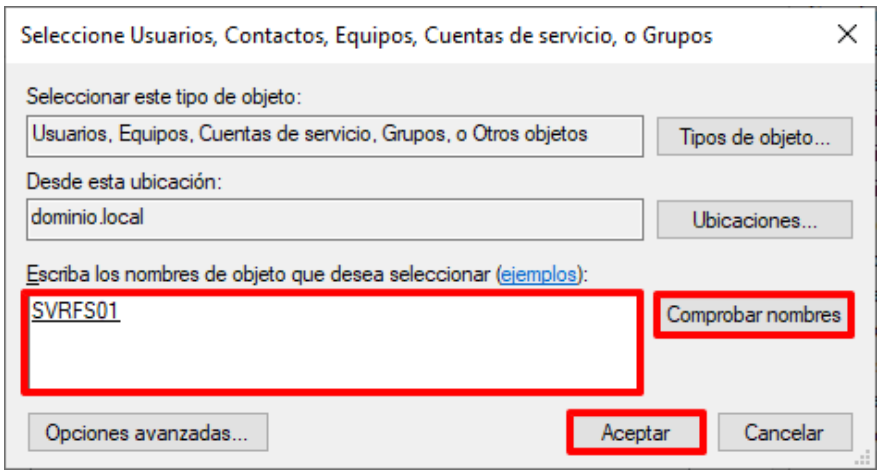
Nota: Estos pasos son opcionales y solo en caso de hacer uso de este tipo de filtrado para la aplicación de objetos GPO.

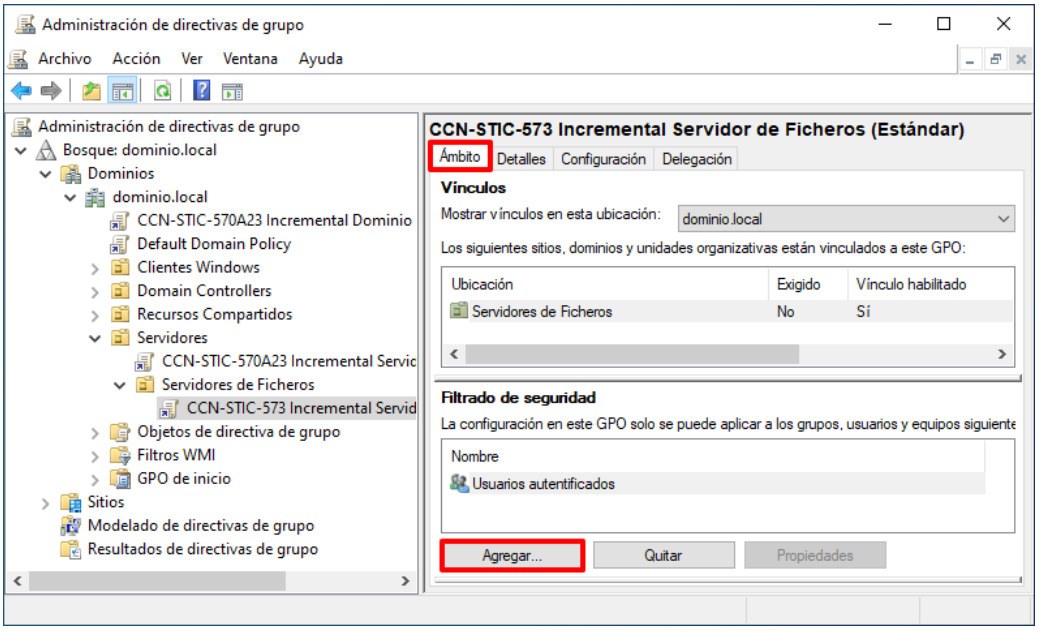
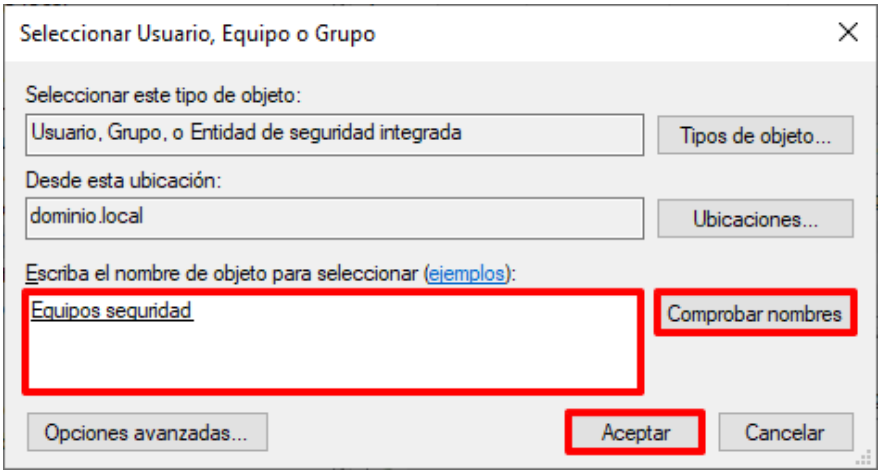
Paso	Descripción
36.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

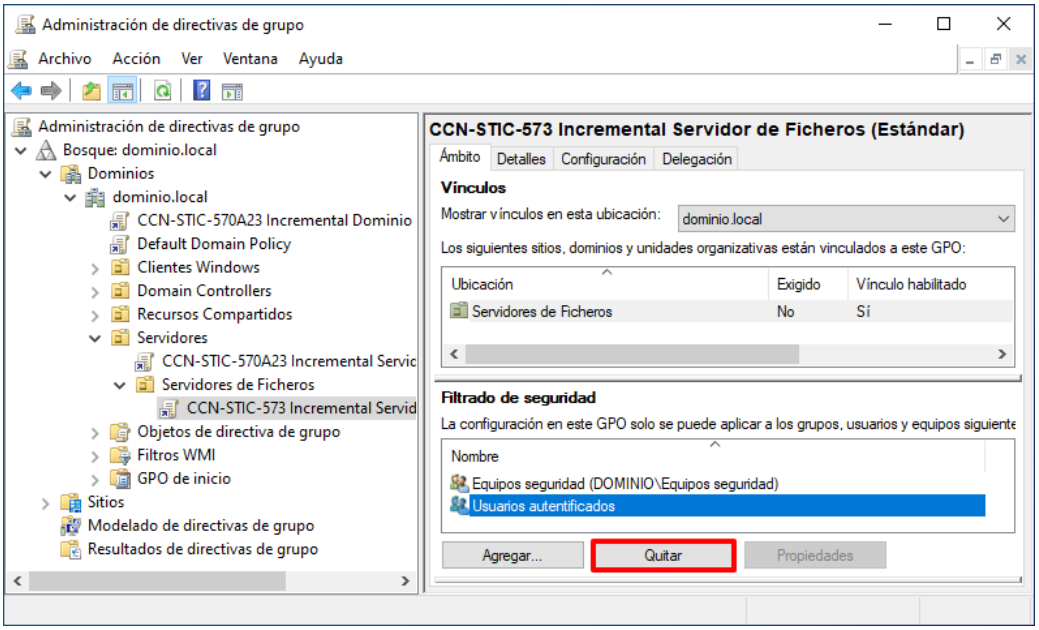
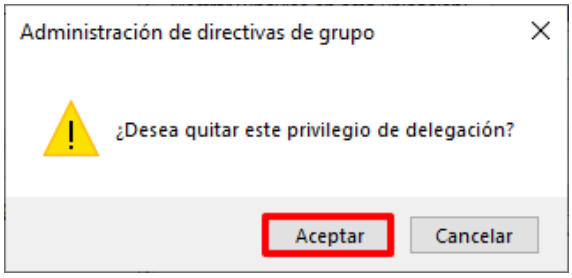
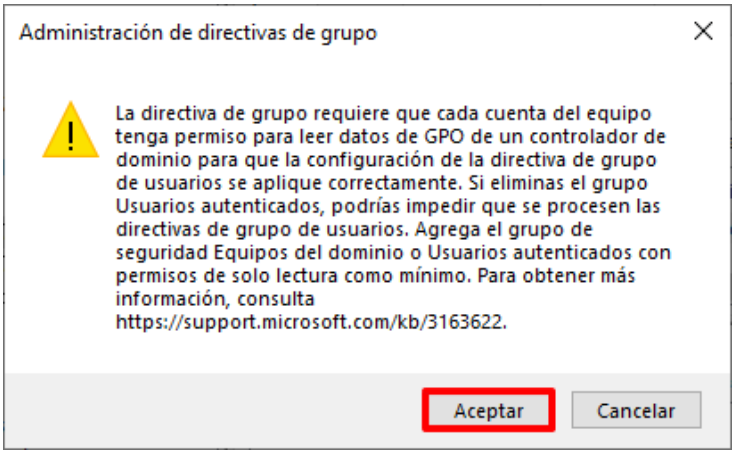
Paso	Descripción
37.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

Paso	Descripción
38.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
39.	En la consola “Usuarios y equipos de Active Directory”, despliegue y seleccione el nodo “<nombre de su dominio> → Users” y haciendo clic derecho sobre el nodo seleccione “Nuevo → Grupo”. 

Paso	Descripción
40.	En la ventana “Nuevo objeto: Grupo”, indique el nombre del grupo y pulse “Aceptar”  **Nota:** En este ejemplo se ha hecho uso del nombre “Equipos seguridad”.
41.	Haga doble clic sobre el grupo recién creado y sobre la ventana “Propiedades: [GRUPO CREADO]” acceda a la pestaña “Miembros”. A continuación, pulse sobre “Agregar…”. 

Paso	Descripción
42.	Pulse en la nueva ventana emergente sobre “Tipos de objeto…” y marque la opción “Equipos”. Pulse “Aceptar” para continuar. 
43.	Incluya los equipos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón “Comprobar nombres” para completar la información del equipo y pulse “Aceptar”.  **Nota:** Para este ejemplo se ha hecho uso del objeto de tipo equipo “SVRFS01”. Deberá reiniciar los equipos incluidos en el grupo para que estos adquieran la membresía de grupo necesaria.

Paso	Descripción
44.	A continuación, sobre la consola "Administración de directivas de grupo", diríjase a la unidad organizativa donde se encuentra vinculado el objeto GPO el cual se desea filtrar y selecciónelo. **Nota:** Para este ejemplo se hace uso del objeto GPO "CCN-STIC-573 Incremental Servidor de Ficheros (Estándar)".
45.	En el panel derecho, seleccione la pestaña ámbito y en el apartado "Filtrado de seguridad" pulse sobre "Agregar…". 
46.	En la ventana que se abrirá, incluya el grupo creado con anterioridad. Haga uso del botón "Comprobar nombres" para completar la información del grupo y pulse "Aceptar".  **Nota:** En este ejemplo se hace uso del grupo "Equipos seguridad" destinado a esta labor. Deberá adaptar esta configuración a las necesidades de su organización.

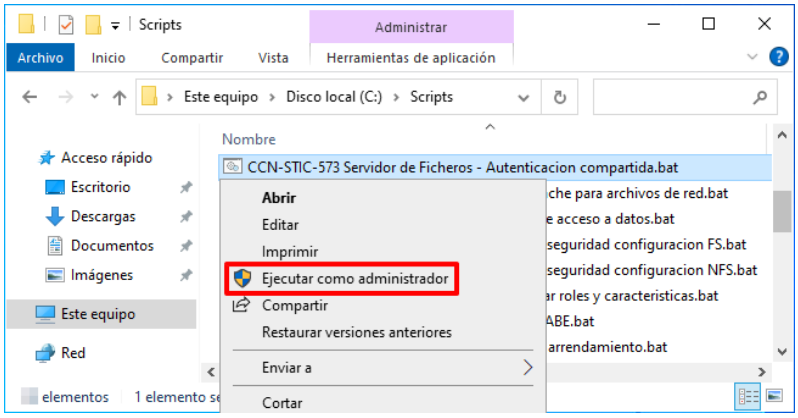
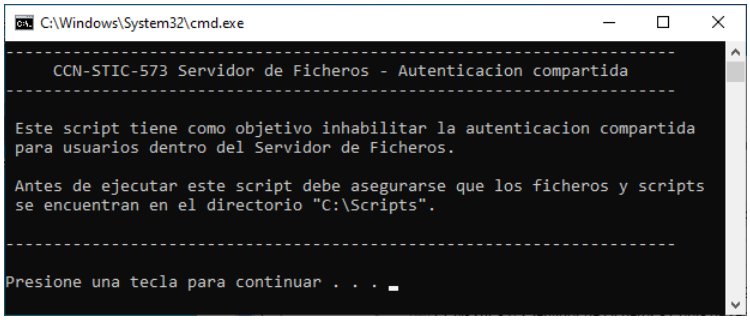
Paso	Descripción
47.	Posteriormente sobre el mismo apartado seleccione “Usuarios autentificados” y pulse sobre el botón “Quitar”. 
48.	Pulse sobre el botón “Aceptar” en el mensaje de advertencia. 
49.	Pulse de nuevo sobre el botón “Aceptar” ante el siguiente mensaje de advertencia. 

ANEXO A.2.3. IDENTIFICACIÓN

A continuación, se establecen las configuraciones necesarias para cumplir con la necesidad de disponer de un identificador único durante la autenticación dentro de los sistemas operativos Windows Server y aplicable sobre los equipos de tipo Servidor de Ficheros.

Nota: Puede simplificar las acciones de ejecución de scripts asociados a esta guía siguiendo las acciones definidas en el "ANEXO C.3 APLICACIÓN DE CONFIGURACIONES COMPLETAS". Este apartado indica los pasos para ejecutar todos los scripts asociados a la guía en una sola ejecución según el perfil seleccionado.

Una vez ejecutados los pasos del citado anexo regrese a este apartado para continuar de manera exclusiva con las acciones manuales e ignorando la ejecución de scripts. Deberá continuar con las acciones manuales del "ANEXO A.2.4 REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO".

Paso	Descripción
50.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
51.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Autenticacion compartida.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 
52.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

ANEXO A.2.4. REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

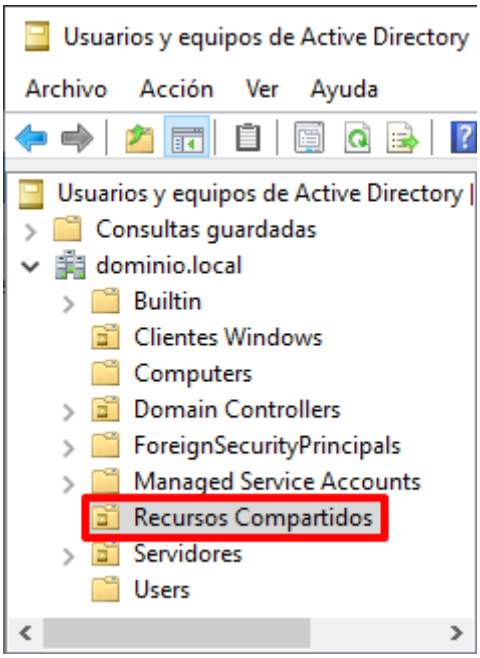
A continuación, se definirán las acciones para disponer de un adecuado control de acceso sobre los diferentes recursos compartidos que se encuentren alojados en un equipo bajo el rol Servidor de Ficheros.

Nota: Los pasos descritos a continuación son un ejemplo de cómo asignar accesos a usuarios, sin rechazar o validar la gestión por medio de consolas o herramientas adicionales que una organización pudiera disponer. Cada organización deberá adaptar los pasos descritos en el presente apartado en función de las necesidades de la misma.

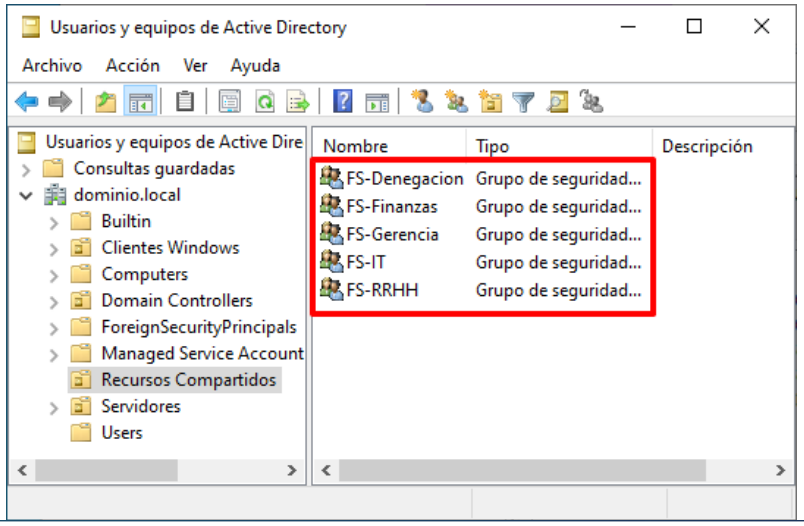
Para la elaboración de este paso a paso, se ha definido **un escenario a modo de ejemplo** que pretenda reflejar las acciones que deben llevarse a cabo. Para ello se define la siguiente información:

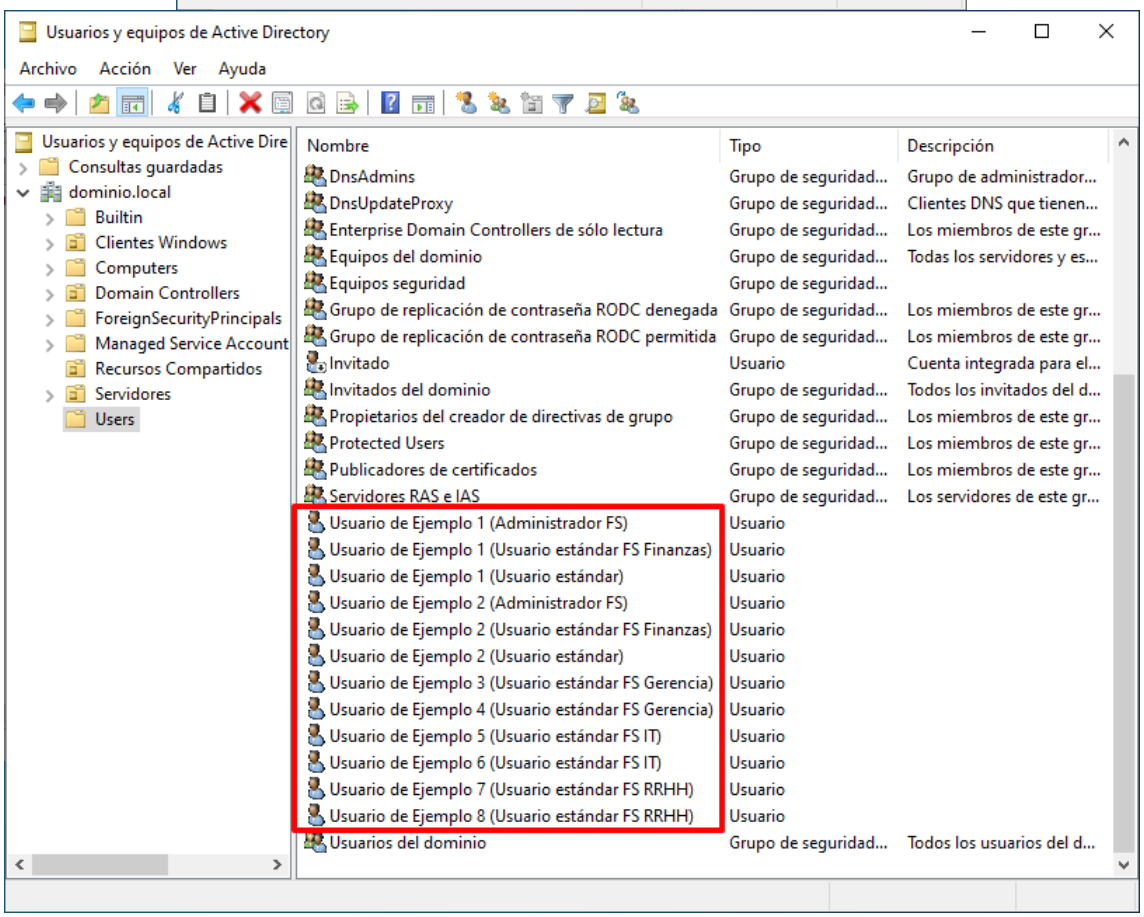
Nota: No es objeto de esta guía de seguridad definir o mostrar cómo se realizan las acciones de creación de recursos compartidos, usuarios y/o grupos de seguridad debido a que estas se conciben como labores de administración.

a) Unidades Organizativas (OU): Se ha generado una OU con el objetivo de alojar aquellos objetos de tipo "grupo" que permitan la asignación de permisos sobre directorios compartidos. Dicha OU se encuentra definida en el entorno de dominio como "Recursos Compartidos".

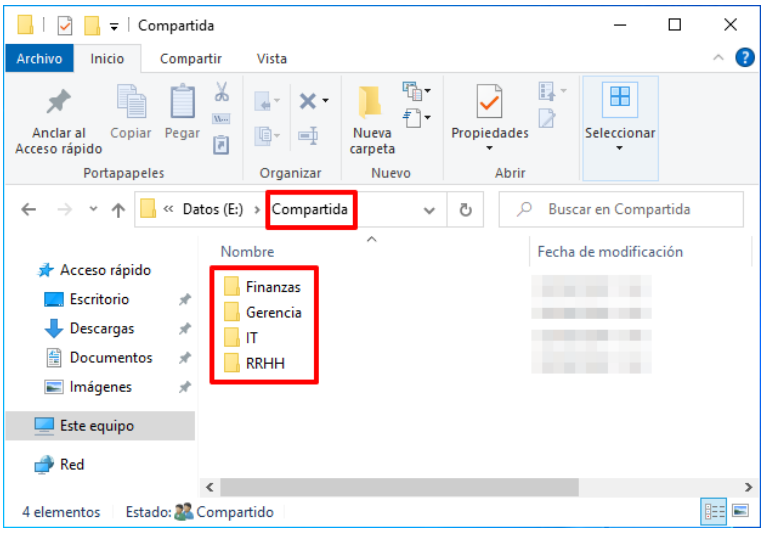


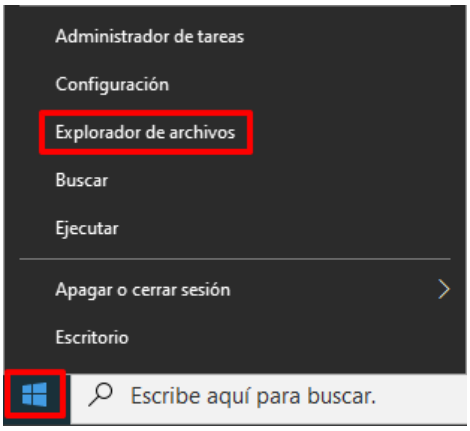
b) Grupos de seguridad y usuarios: Se han creado diversos grupos a modo de ejemplo con la intención de simular un entorno con directorios compartidos asociados a cada grupo. De igual modo se han creado usuarios de ejemplo que pueden ser asociados a dichos grupos.

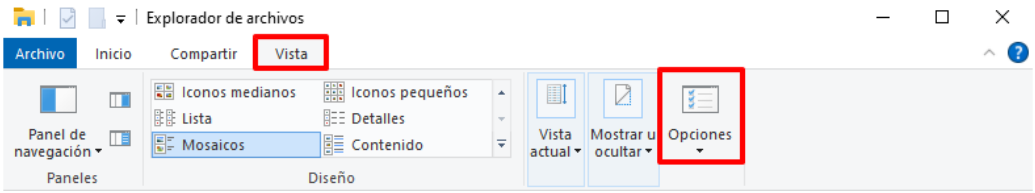
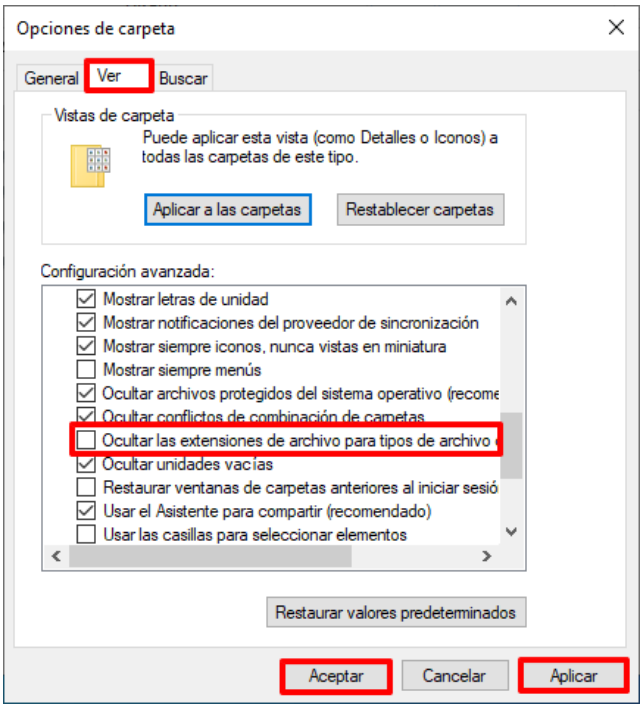


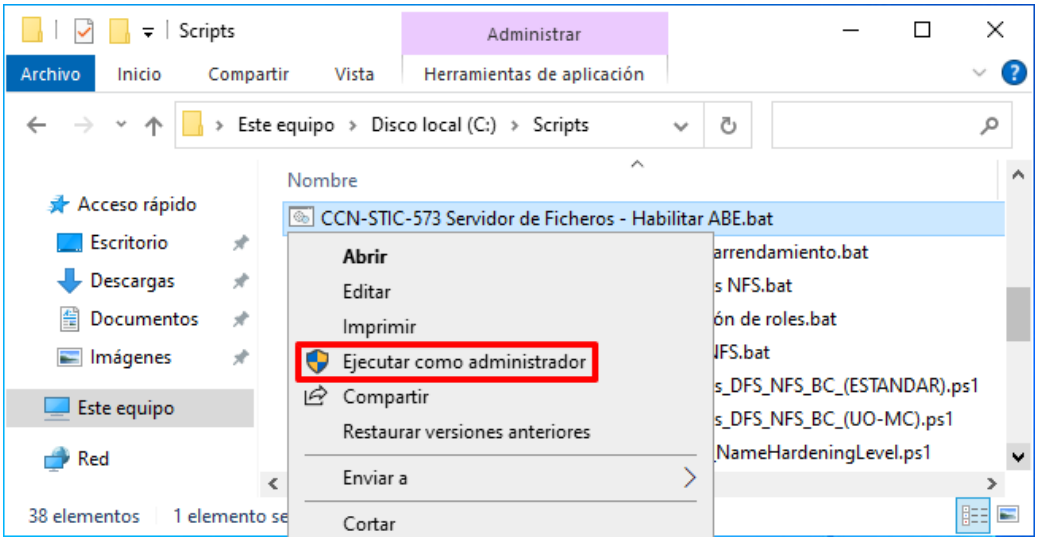
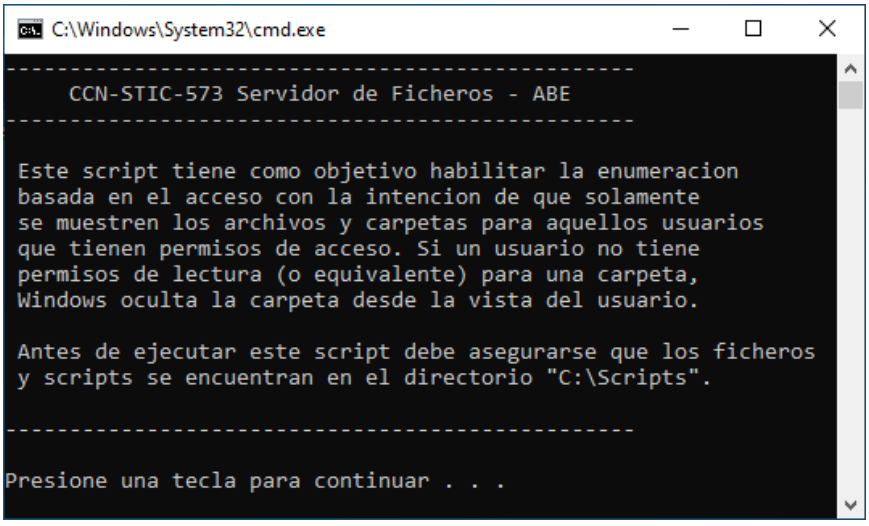


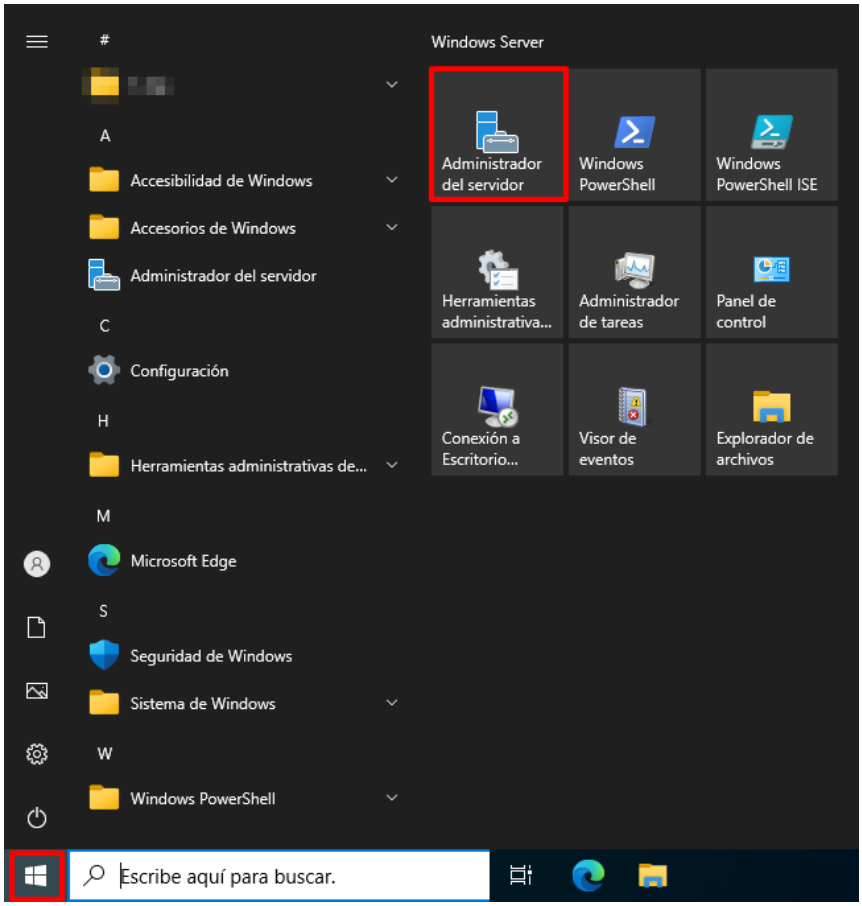
c) Recursos compartidos: En línea con la información anterior se ha generado un recurso compartido con diferentes directorios y ficheros de ejemplo en un almacenamiento dedicado para el servicio el cual permitan ejemplificar las acciones asociadas a este apartado, y que permita cumplir con los requisitos de acceso.

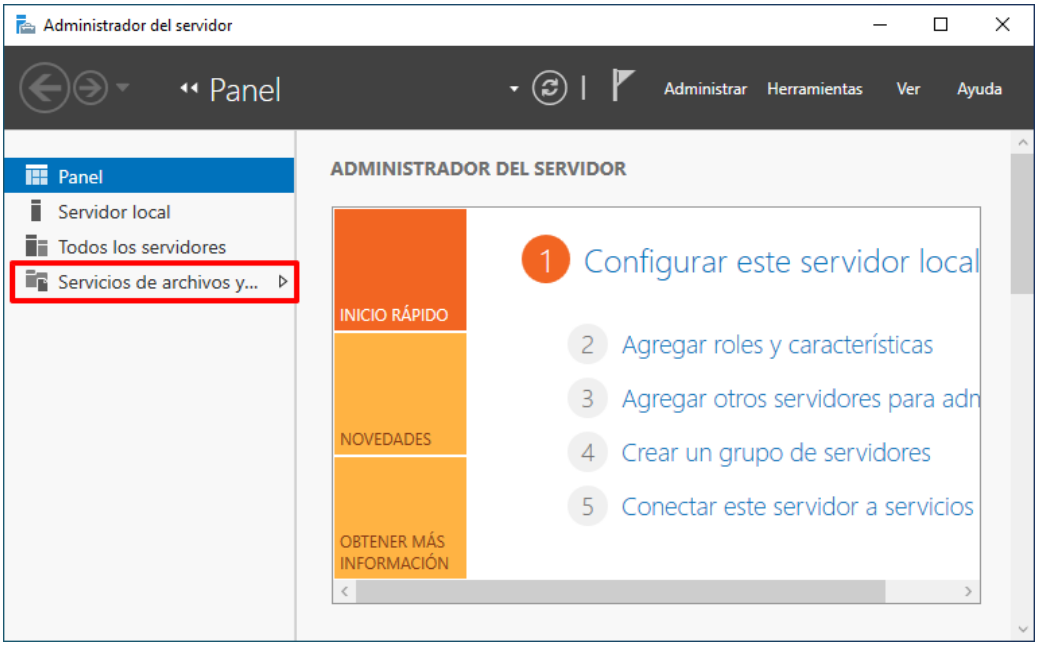
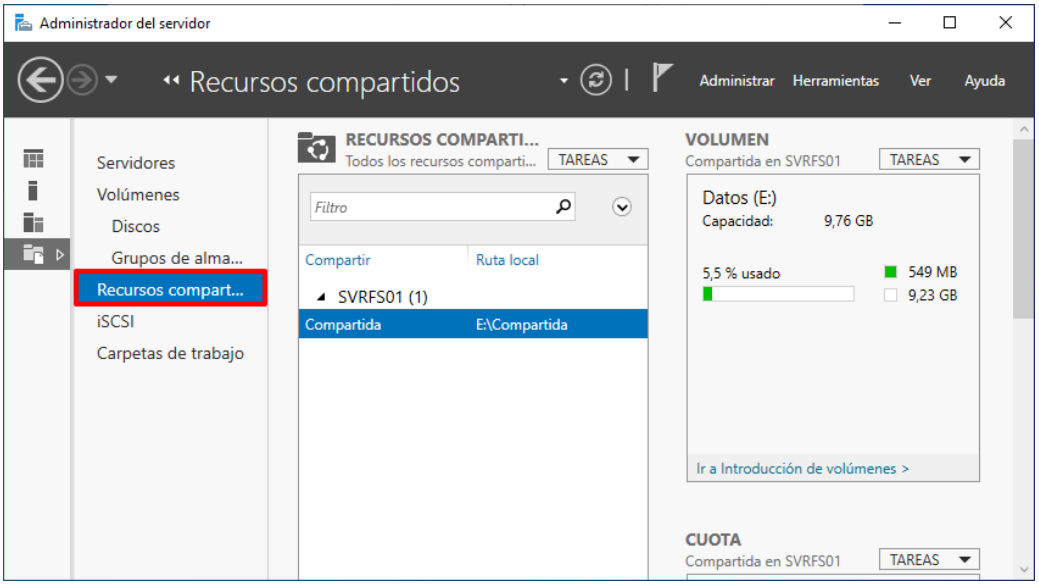


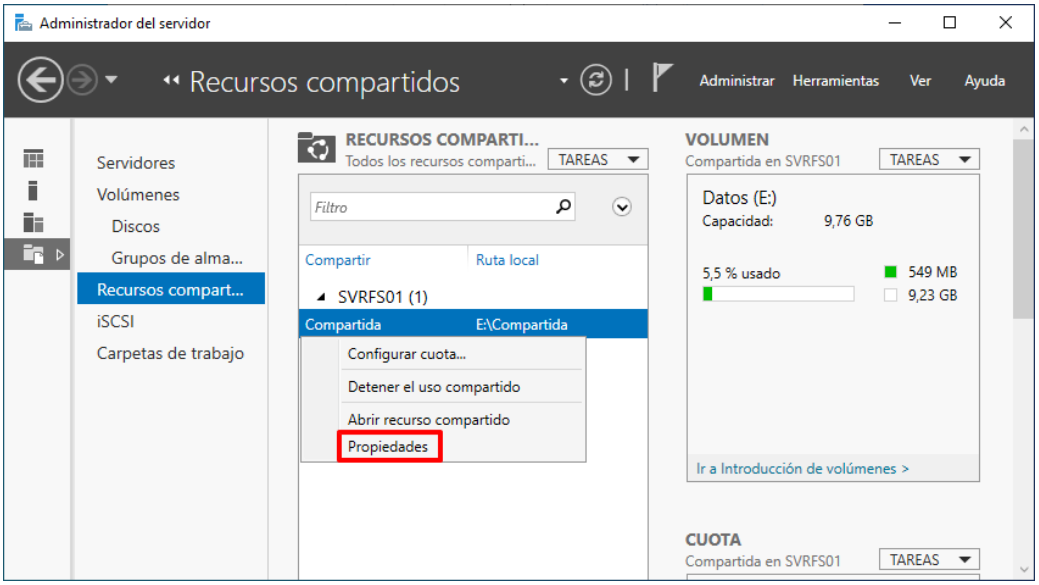
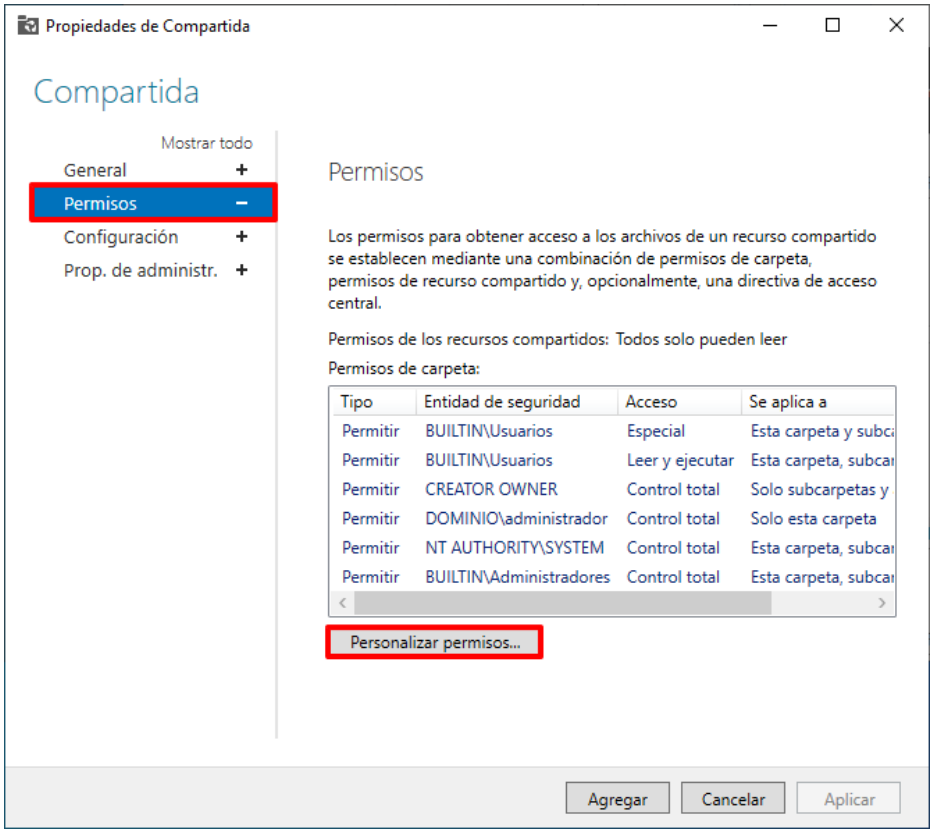
Paso	Descripción
53.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
54.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-573”.
55.	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”. 

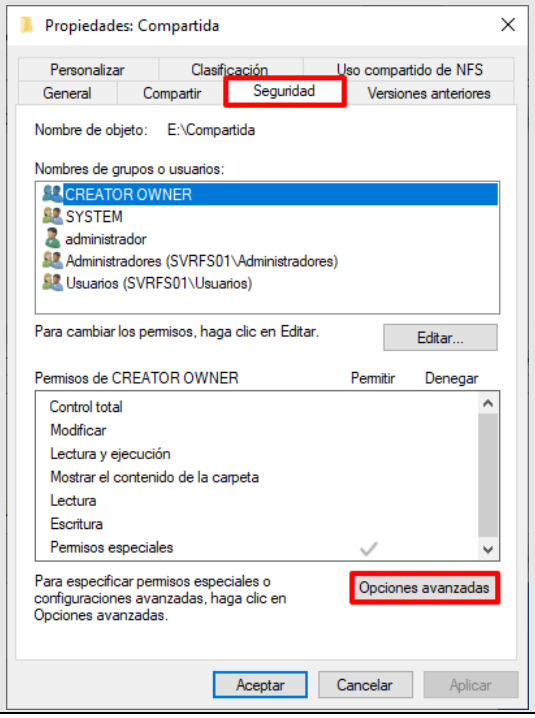
Paso	Descripción
56.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
57.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo 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”. 

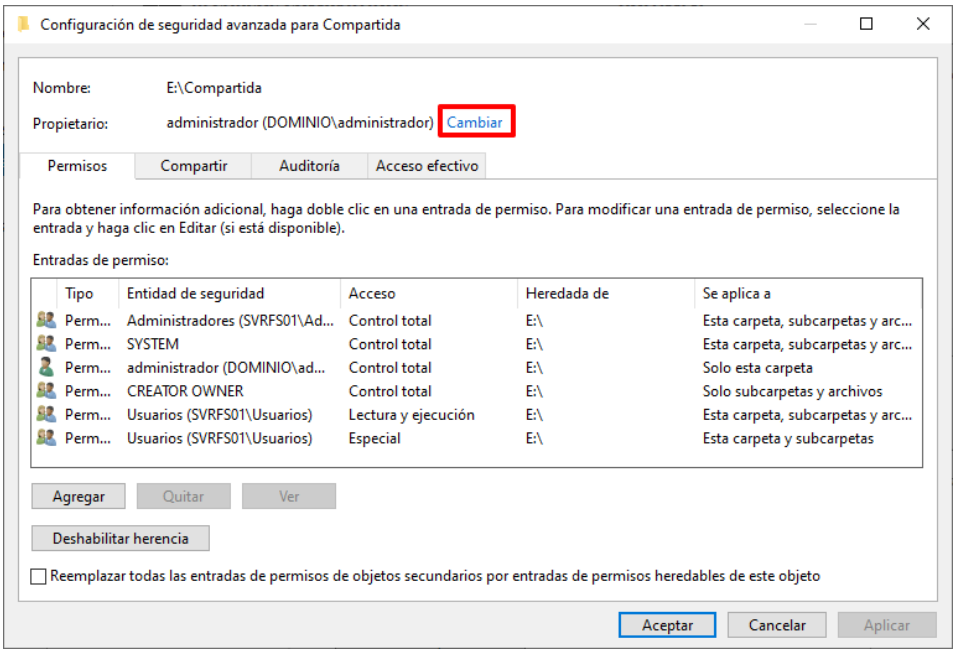
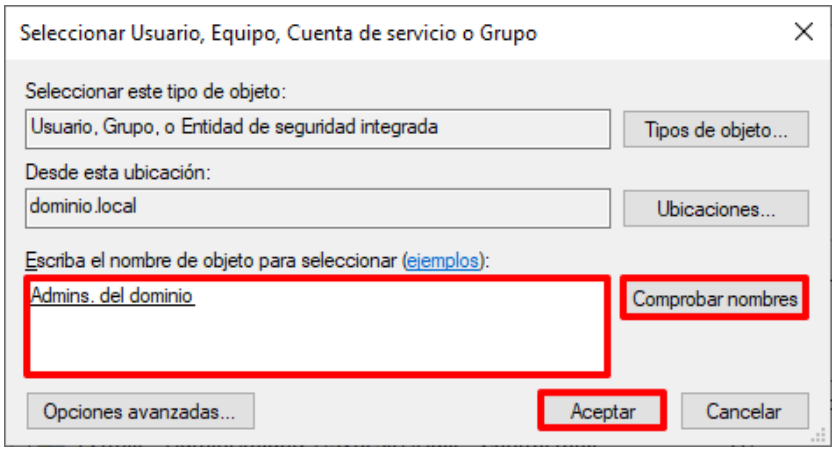
Paso	Descripción
58.	Diríjase al directorio “C:\Scripts” y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Habilitar ABE.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
59.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script.  **Nota:** Tenga en cuenta que deberá reiniciar el “Administrador del servidor” para ver este cambio de configuración reflejado en los diferentes recursos compartidos.

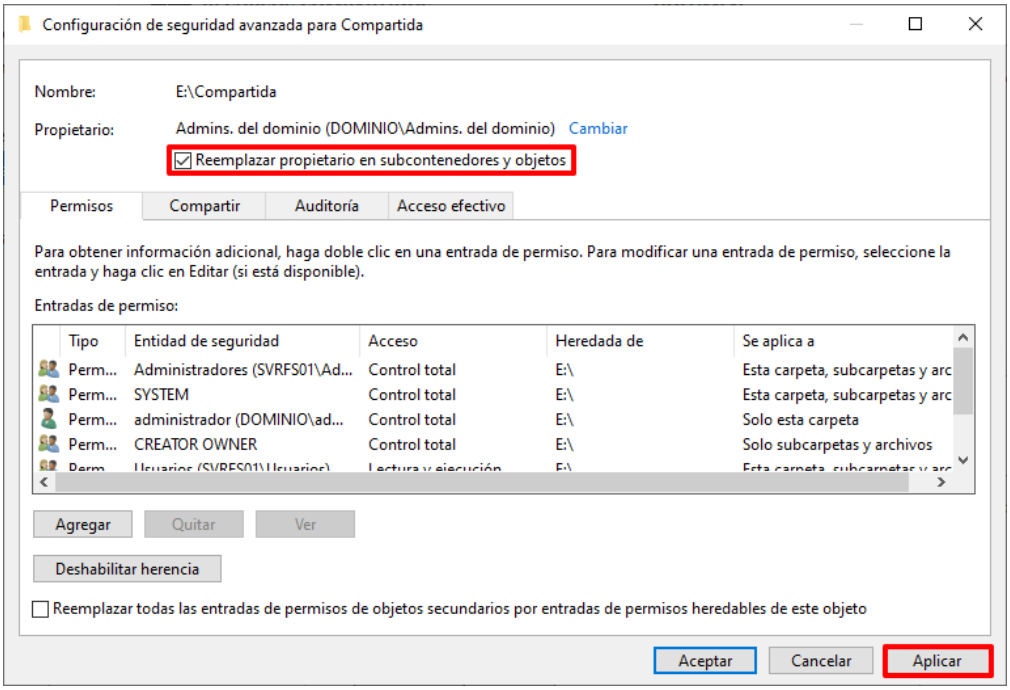
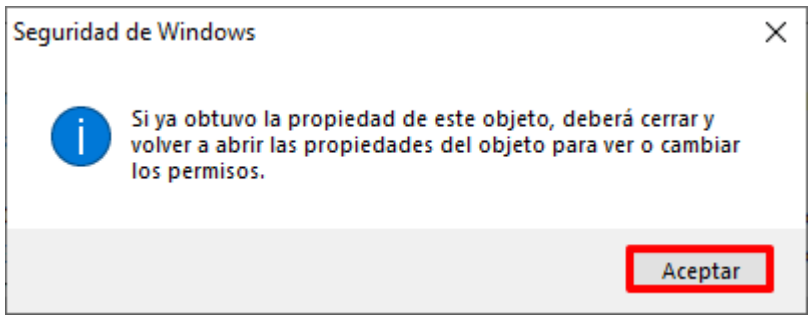
Paso	Descripción
60.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

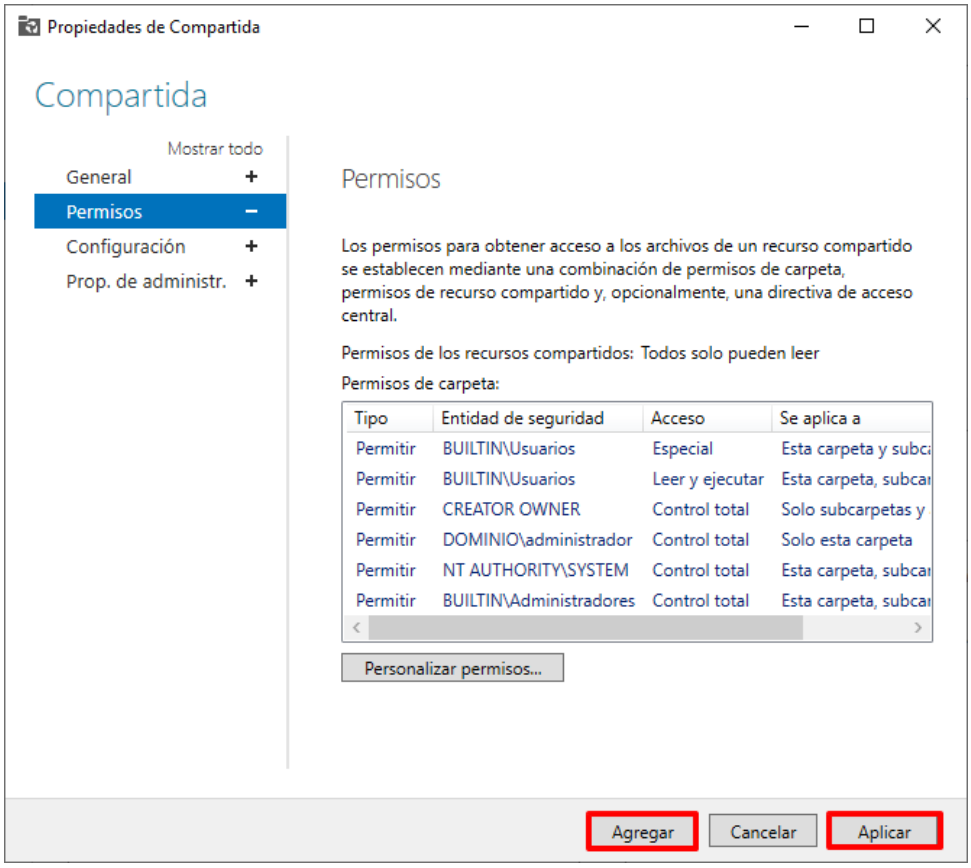
Paso	Descripción
61.	En la columna izquierda del “Administrador del servidor” seleccione “Servicio de archivos y de almacenamiento”. 
62.	A continuación, acceda al apartado “Recursos compartidos”. 

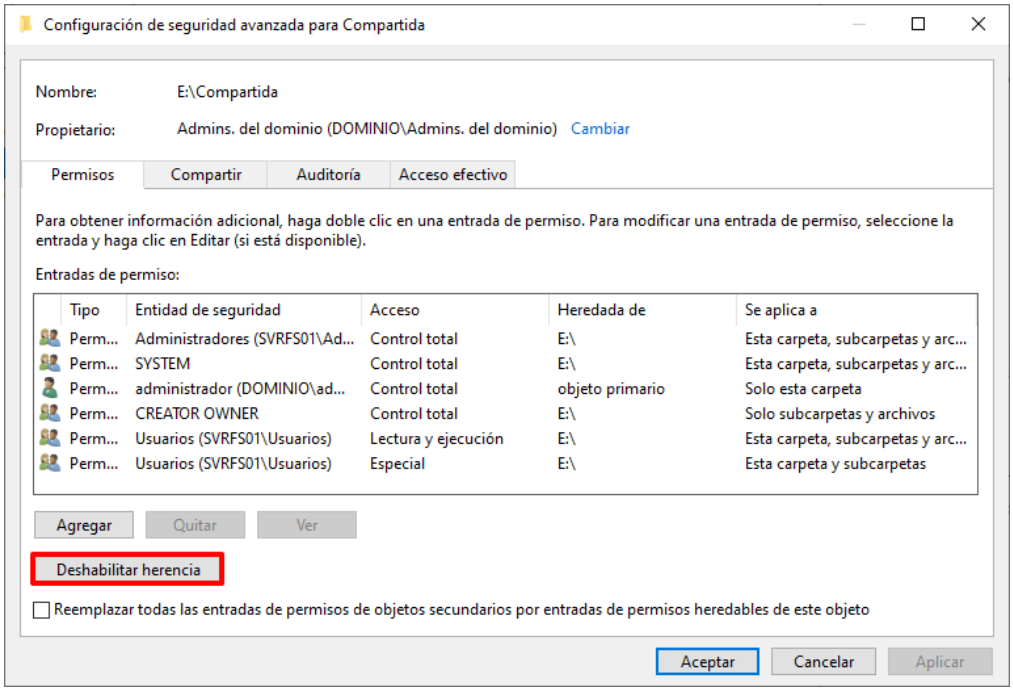
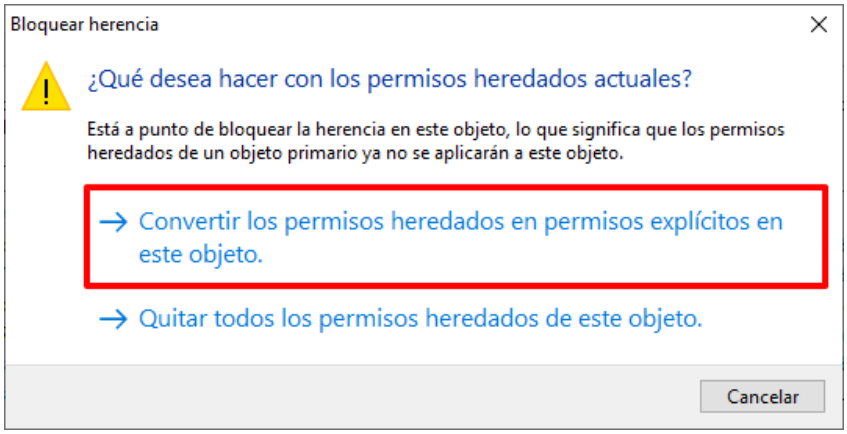
Paso	Descripción
63.	En el apartado central, sobre el recurso compartido bajo el que desee trabajar haga clic derecho y seleccione la opción del menú contextual “Propiedades”.  **Nota:** En este ejemplo se hace uso del recurso compartido definido como “Compartida”. Adapte estos pasos a las necesidades de su organización.
64.	En la nueva ventana emergente, diríjase al apartado “Permisos” y seleccione la opción “Personalizar permisos…”. 

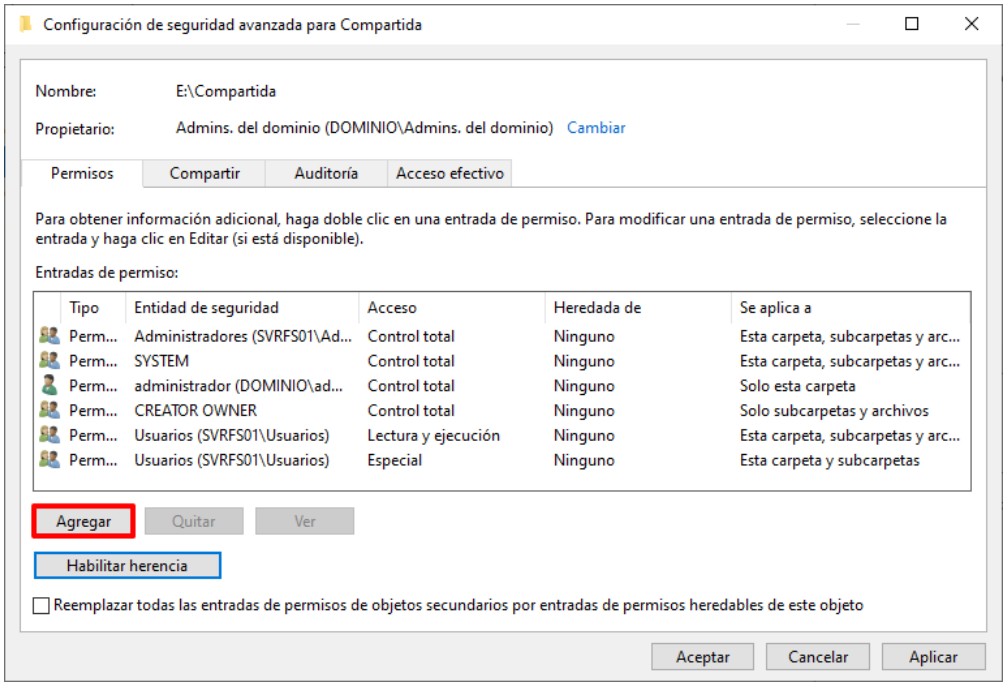
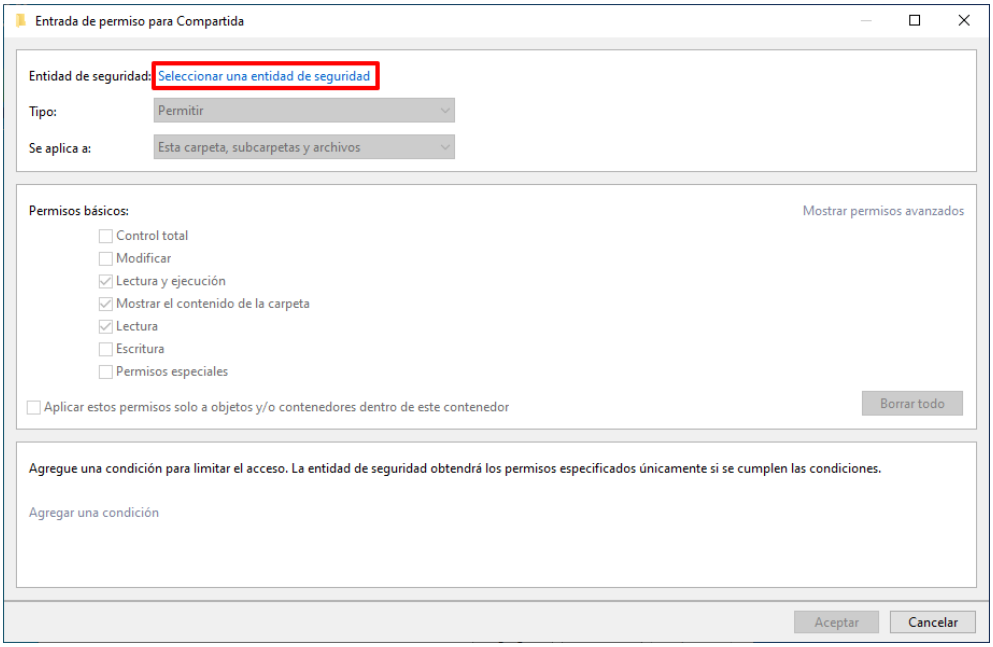
Paso	Descripción
65.	En la nueva ventana emergente deberá **evaluar y modificar ciertos valores según los requisitos necesarios** de su organización. En este sentido durante el ejemplo se van a definir y asignar los permisos de manera dedicada y única, entre otras opciones, con el objetivo de disponer de un buen control del acceso a los recursos compartidos. **Nota:** Puede obtener acceso a la misma ventana haciendo clic derecho sobre el directorio de Windows que se está compartiendo y seleccionando "Propiedades" del menú emergente. A continuación, diríjase a la pestaña "Seguridad" y pulse sobre "Opciones avanzadas". 

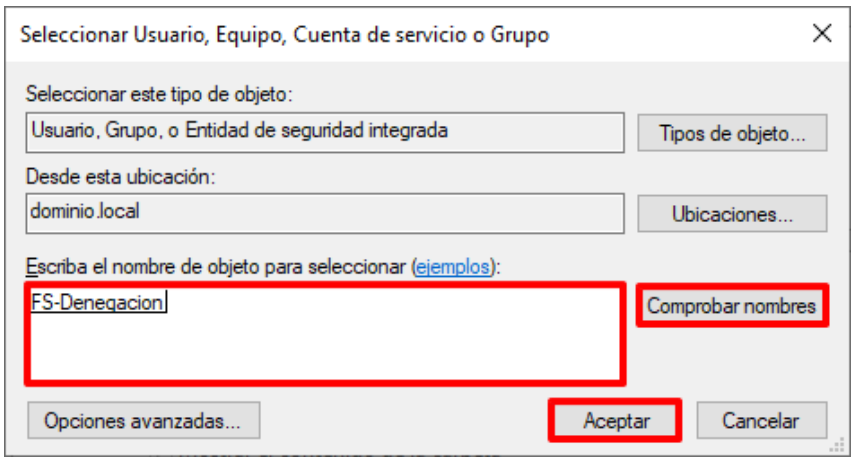
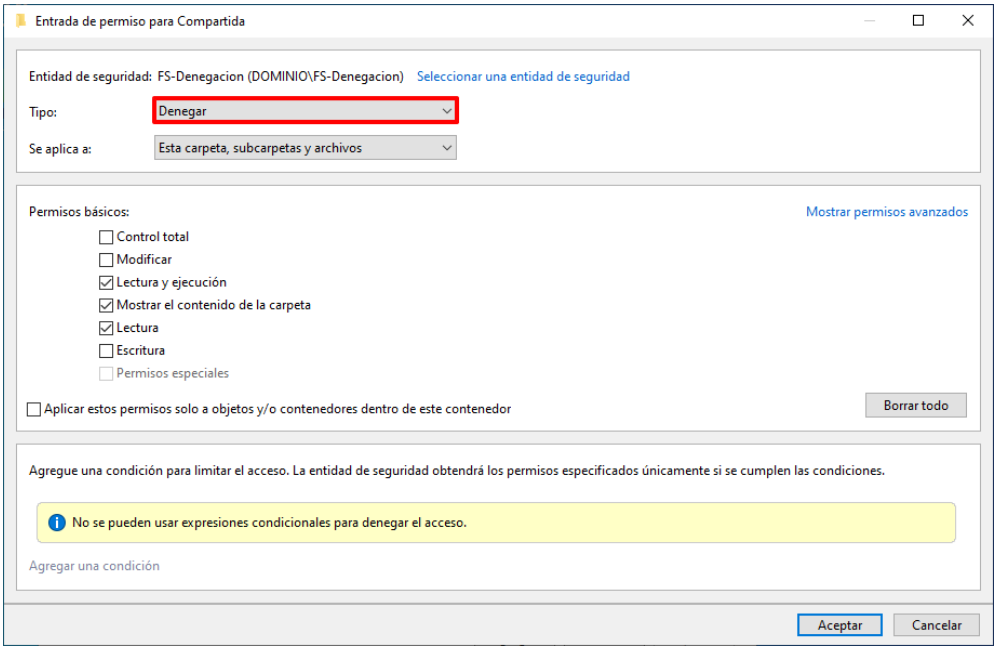
Paso	Descripción
66.	En primer lugar, se va a modificar la propiedad del recurso compartido. Esto se va a realizar debido a que cuando se crea un recurso de manera tradicional (crear un directorio de Windows que se comparte), por defecto se asigna la propiedad al usuario que lo crea. Esto puede provocar que se impidan realizar ciertas acciones si no se dispone de dicha propiedad. Para ello, pulse sobre el botón "Cambiar". 
67.	En la ventana emergente defina el grupo de usuarios propietario de dicho recurso, pulse sobre "Comprobar nombres" y por último sobre "Aceptar".  **Nota:** En este ejemplo se hace uso del grupo ya existente y por defecto "Admins. del dominio". Deberá adaptar esta configuración a las necesidades de su organización. Tenga en consideración que en el punto "ANEXO A.2.5 SEGREGACIÓN DE FUNCIONES Y TAREAS" se establecen las configuraciones para que un grupo de usuarios concreto sea el encargado de la gestión de los recursos compartidos. Asígnelo en este punto si no desea realizar un cambio posterior que requiera modificaciones adicionales.

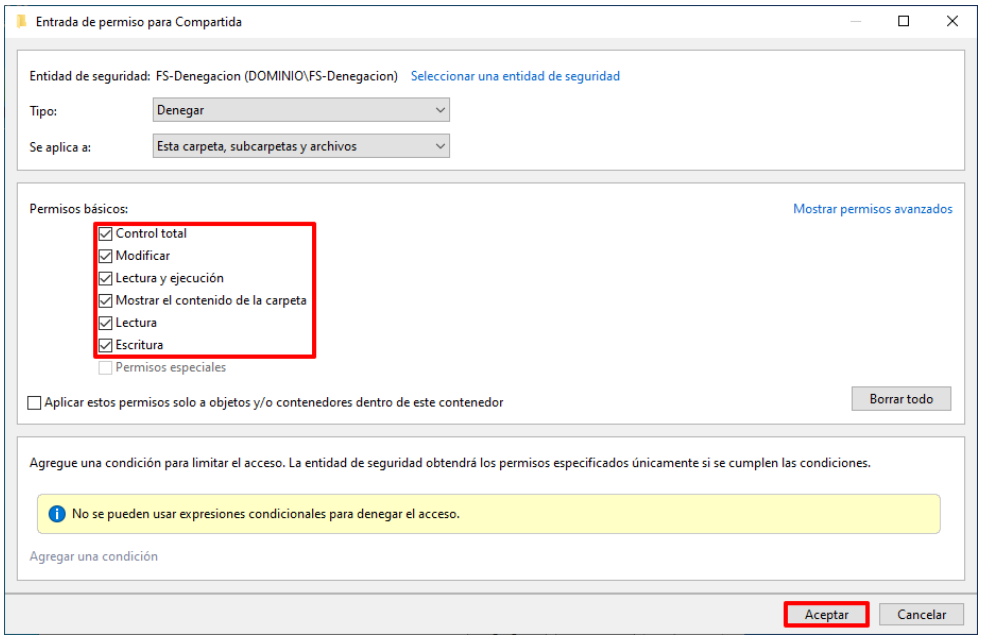
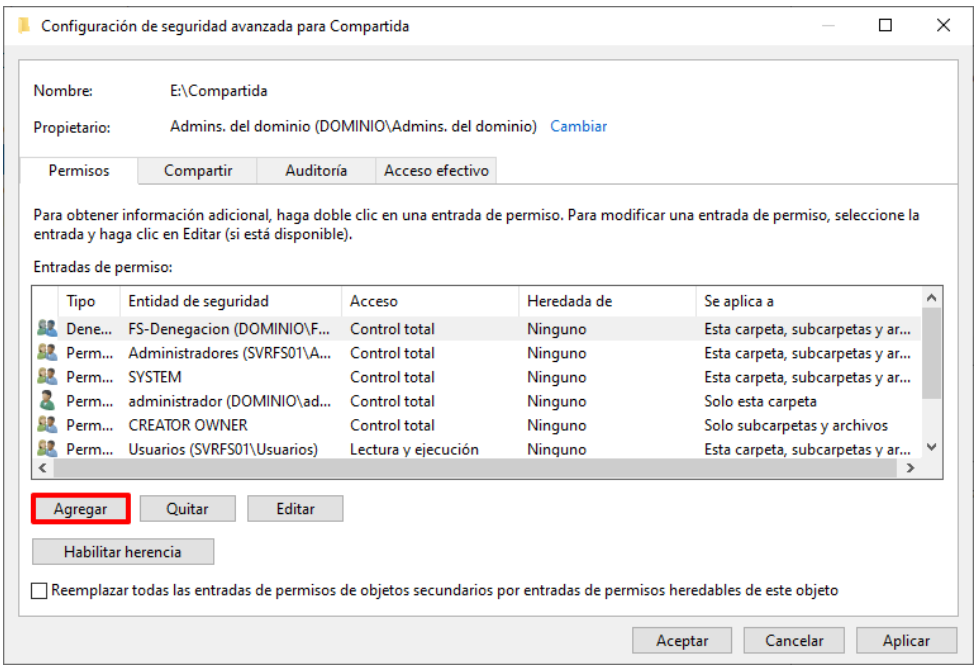
Paso	Descripción
68.	Marque ahora sobre la nueva opción que aparecerá “Reemplazar propietario en subcontenedores y objetos”. Pulse de igual modo sobre el botón “Aplicar”. Esto permitirá que todos los objetos dependientes de este cambien de igual modo su propiedad. 
69.	Pulse “Aceptar” sobre el mensaje emergente y de nuevo “Aceptar” sobre la ventana de permisos. 

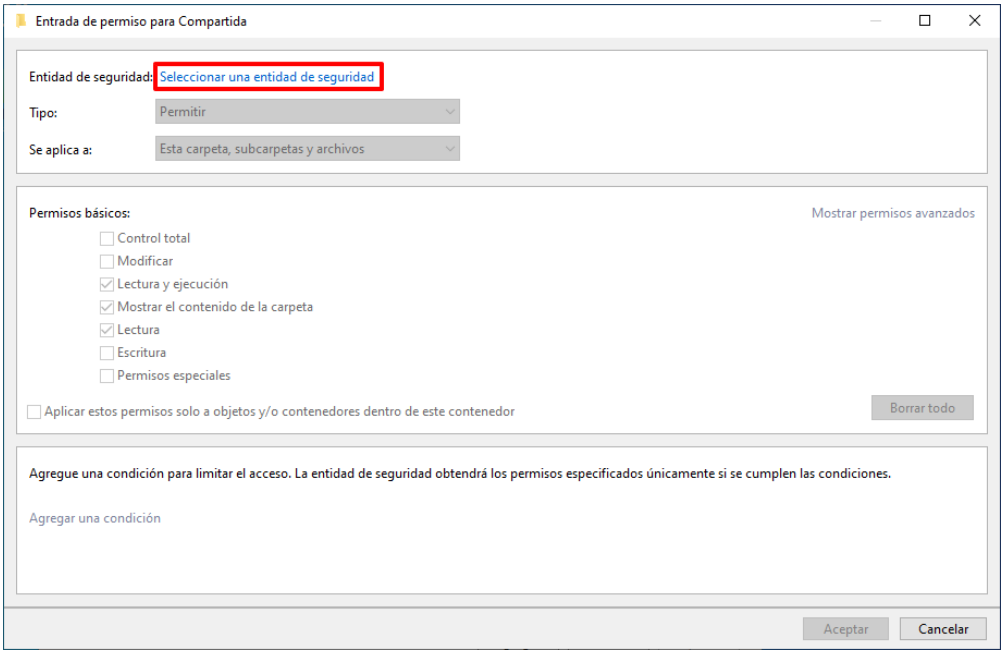
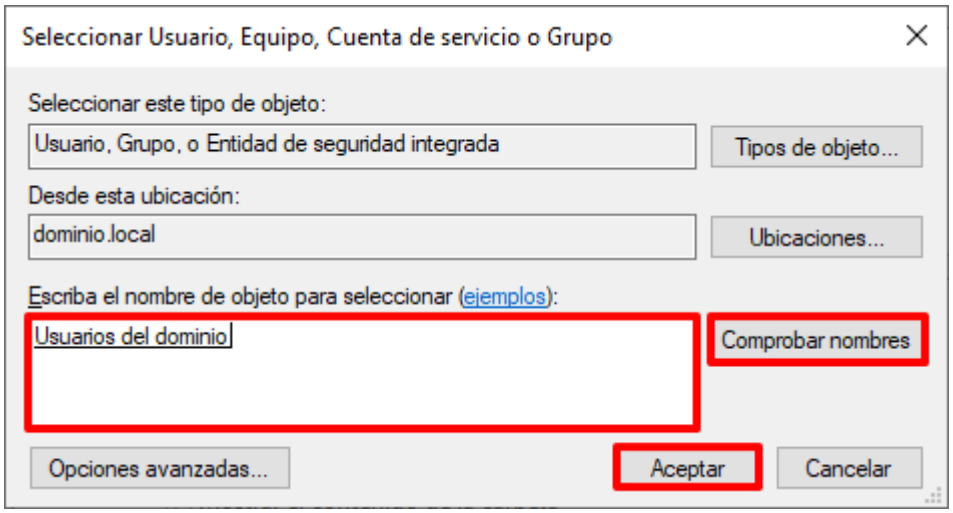
Paso	Descripción
70.	En la ventana “Compartida” pulse “Aplicar” y “Agregar”. 
71.	Vuelva a abrir la consola de permisos según se ha definido en los pasos “63” y “64”.

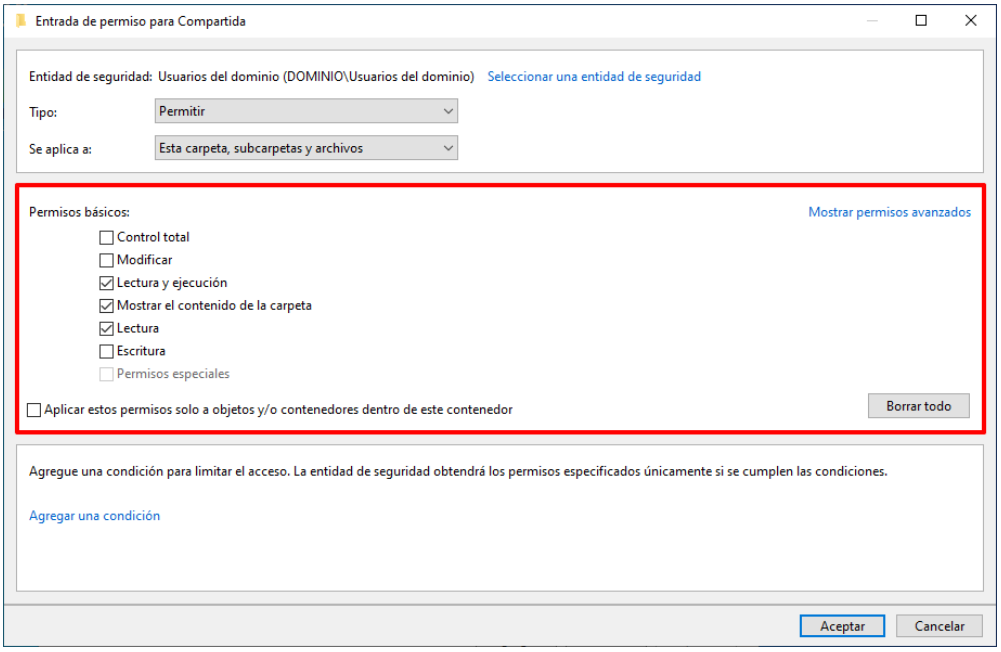
Paso	Descripción
72.	A continuación, se va a eliminar la herencia de permisos. Esto permitirá definir de manera personalizada los permisos para el recurso compartido, ya que por defecto todos los directorios y/o ficheros de manera predeterminada van a disponer de los permisos de su directorio "padre" (inmediatamente anterior). Para ello, haga clic sobre el botón "Deshabilitar herencia".  **Nota:** En este ejemplo el recurso compartido hereda los permisos del disco "E:\", donde se aloja.
73.	En la ventana emergente seleccione la opción "Convertir los permisos heredados en permisos explícitos en este objeto".  **Nota:** Si lo desea puede hacer uso de la opción "Quitar todos los permisos heredados de este objeto" para incluir a posteriori todos los permisos de manera manual.

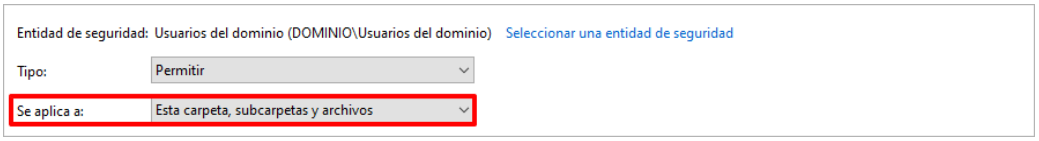
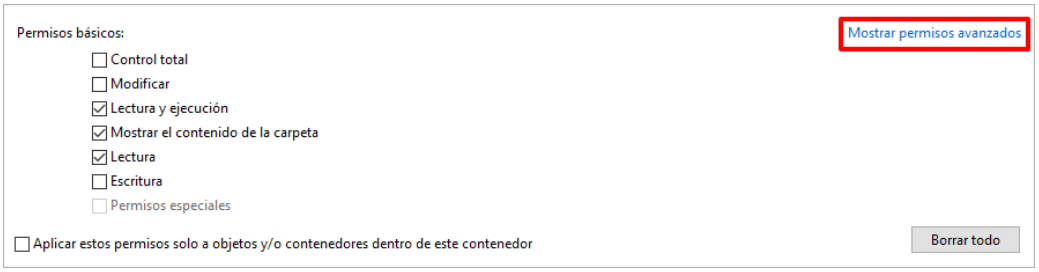
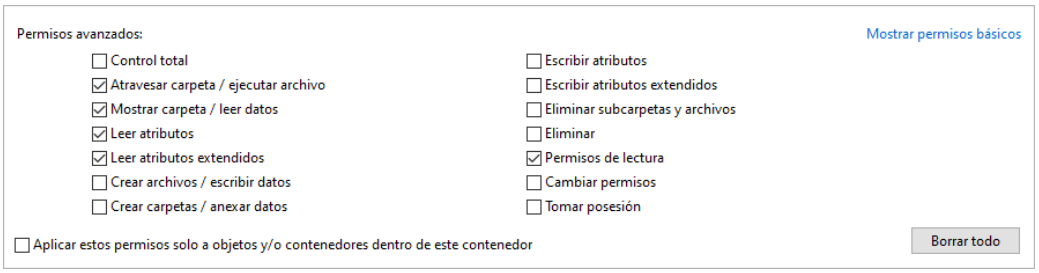
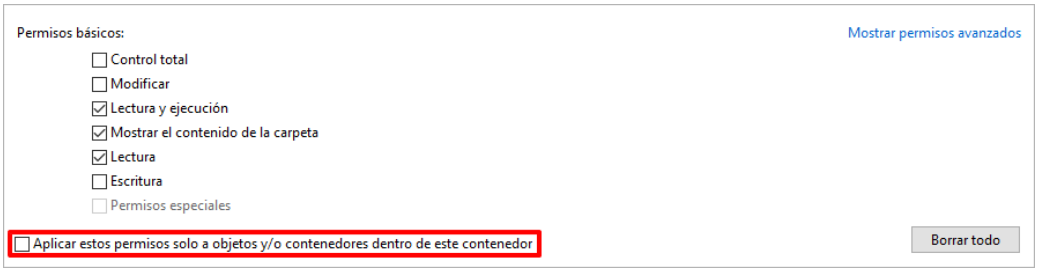
Paso	Descripción
74.	A continuación, pulse sobre la opción “Agregar”. 
75.	En la nueva ventana emergente, pulse sobre “Seleccionar una entidad de seguridad”. 

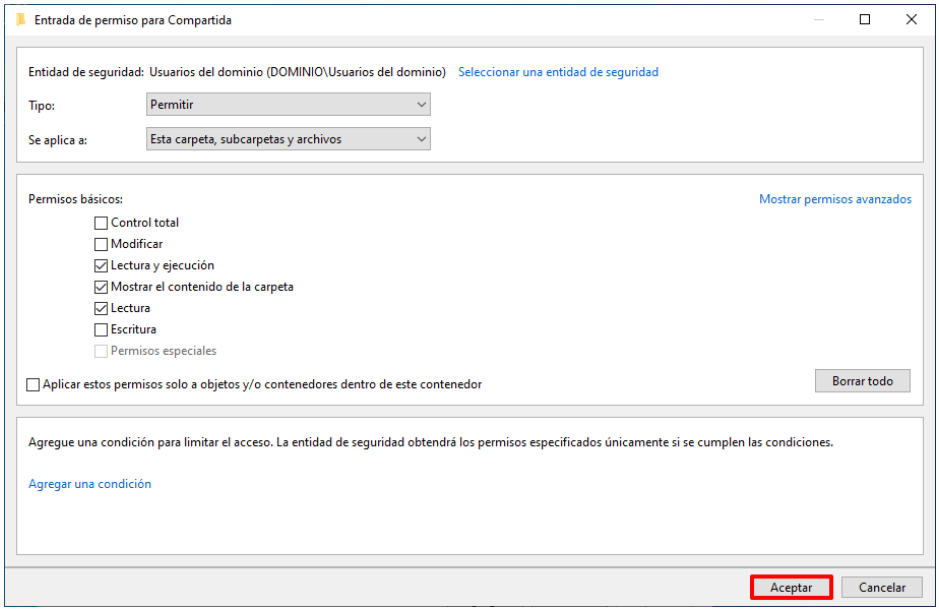
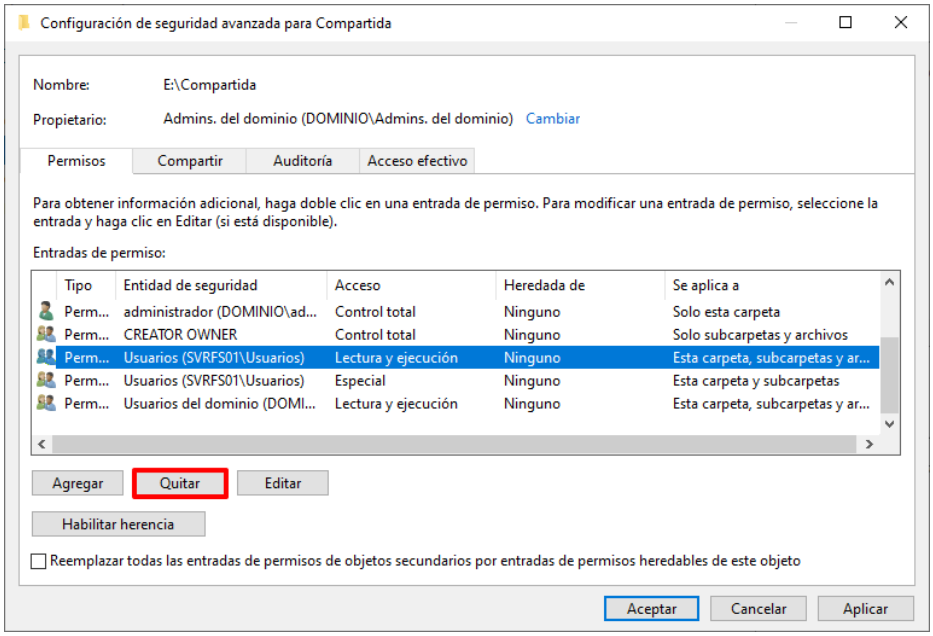
Paso	Descripción
76.	A continuación, **se va a definir un grupo que la pertenencia al mismo provoque limitar el acceso de manera rápida a los recursos compartidos** independientemente de la pertenencia a otros grupos. Defina el usuarios o grupo que desea incluir en el listado de permisos, pulse sobre el botón “Comprobar nombres” y pulse “Aceptar”.  **Nota:** En este ejemplo se hace uso del grupo de Active Directory “FS-Denegacion” creado para tal propósito. Deberá adaptar esta configuración a las necesidades de su organización. Tenga en consideración que esto **no impedirá el acceso a elementos internos del recurso compartido** bajo los cuales haya permisos explícitos para un usuario o grupo, por lo que deberá eliminar al usuario de la pertenencia a otros grupos o establecer permisos de denegación bajo ese recurso compartido del mismo modo que se ha realizado en este paso a paso, es decir, a los subrecursos.
77.	Posteriormente, en el apartado “Tipo:” defina “Denegar”. 

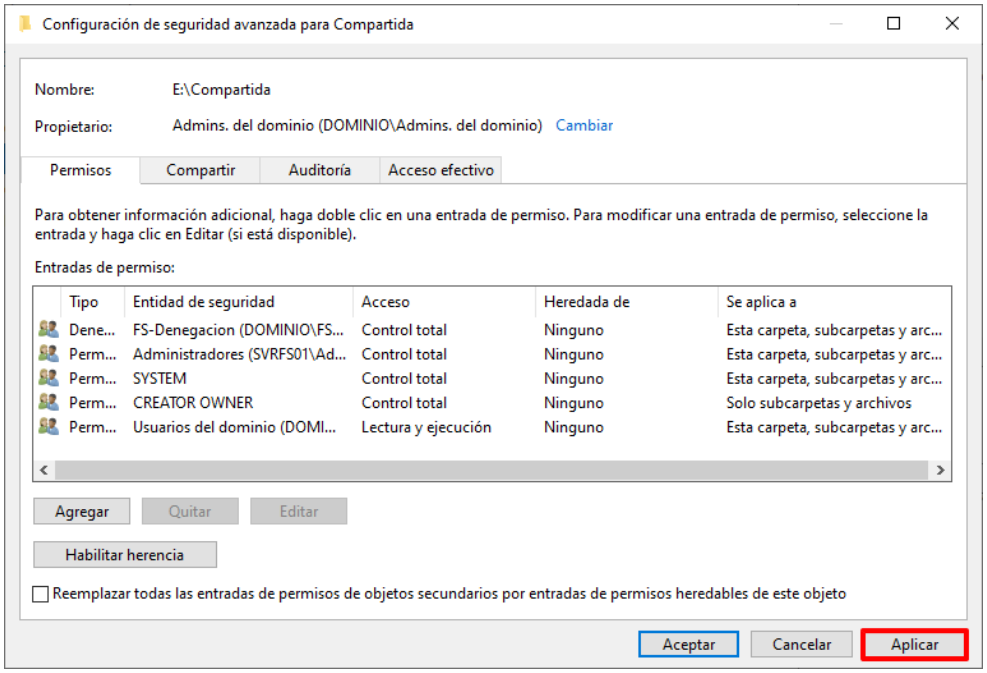
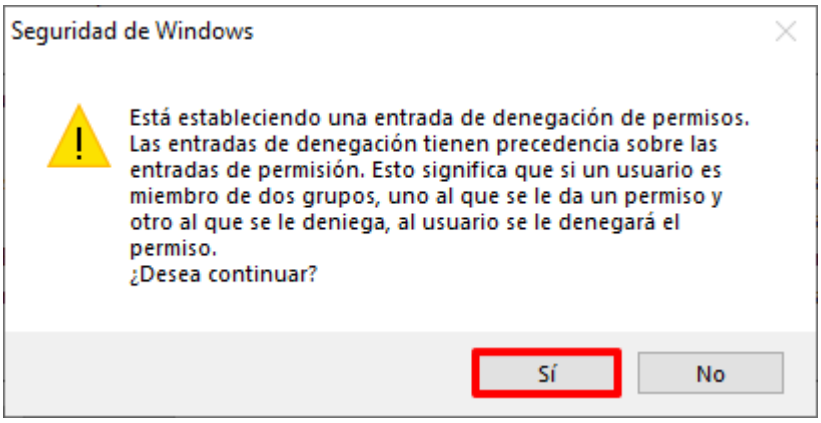
Paso	Descripción
78.	Por otro lado, en el apartado dedicado a permisos marque la opción “Control total” y asegúrese que el resto de opciones también se encuentran marcadas. Pulse “Aceptar” para finalizar.  **Nota:** No es necesario hacer uso de la opción “Mostrar permisos avanzados” dado que lo que se pretende es simplificar y limitar el acceso a todo aquel que sea requerido denegar los permisos de acceso por el motivo que sea.
79.	Posteriormente se deberá otorgar permiso a aquellas entidades que requieran del correspondiente requisito de acceso. Para ello, al igual que se realizó en pasos anteriores haga clic de nuevo sobre el botón “Agregar”. 

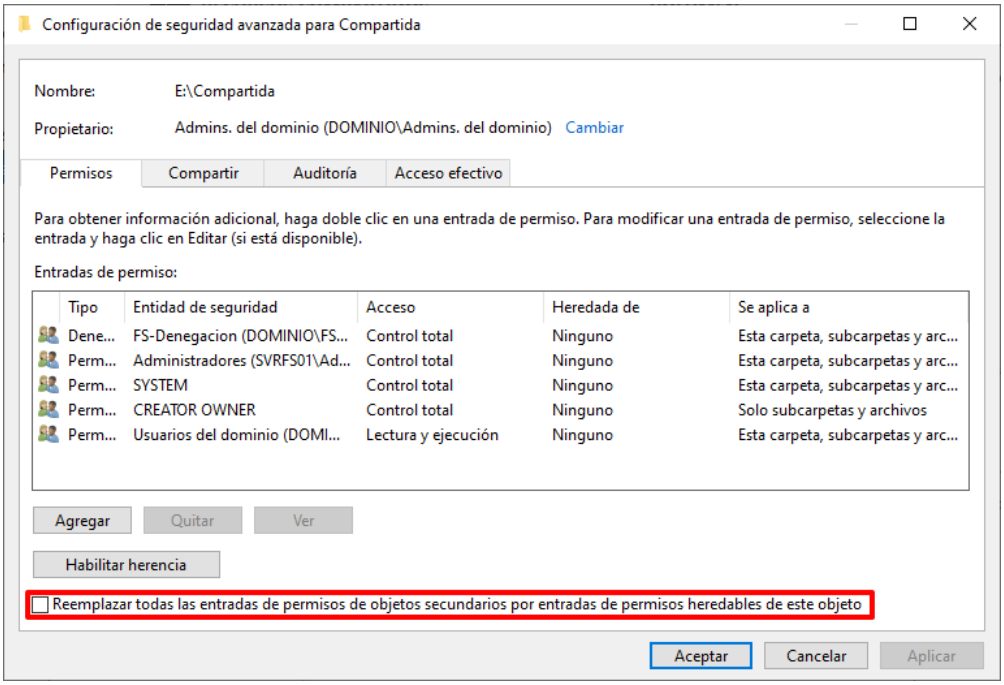
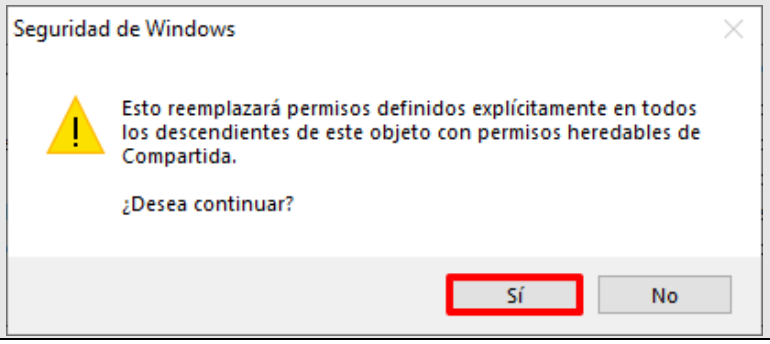
Paso	Descripción
80.	En la nueva ventana emergente, pulse sobre “Seleccionar una entidad de seguridad”. 
81.	Defina el usuarios o grupo que desea incluir en el listado de permisos, pulse sobre el botón “Comprobar nombres” y pulse “Aceptar”.  **Nota:** En este ejemplo se hace uso del grupo por defecto de Active Directory “Usuarios del dominio”. Esto se debe a que se entiende que se trata de un repositorio compartido con acceso para todos los usuarios pertenecientes a dicho dominio. Deberá adaptar esta configuración a las necesidades de su organización.

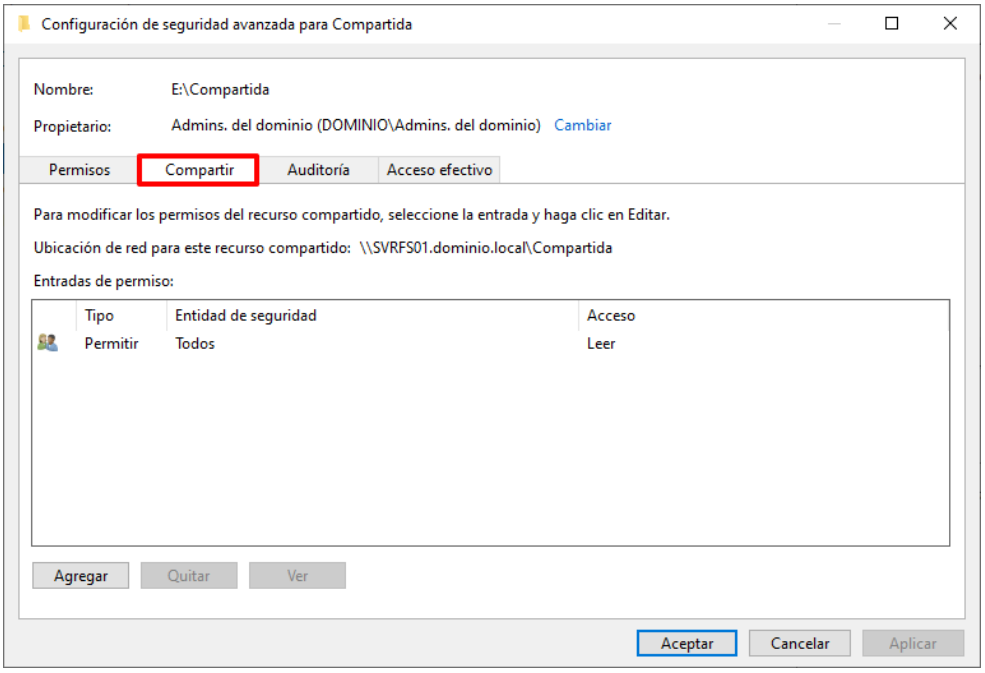
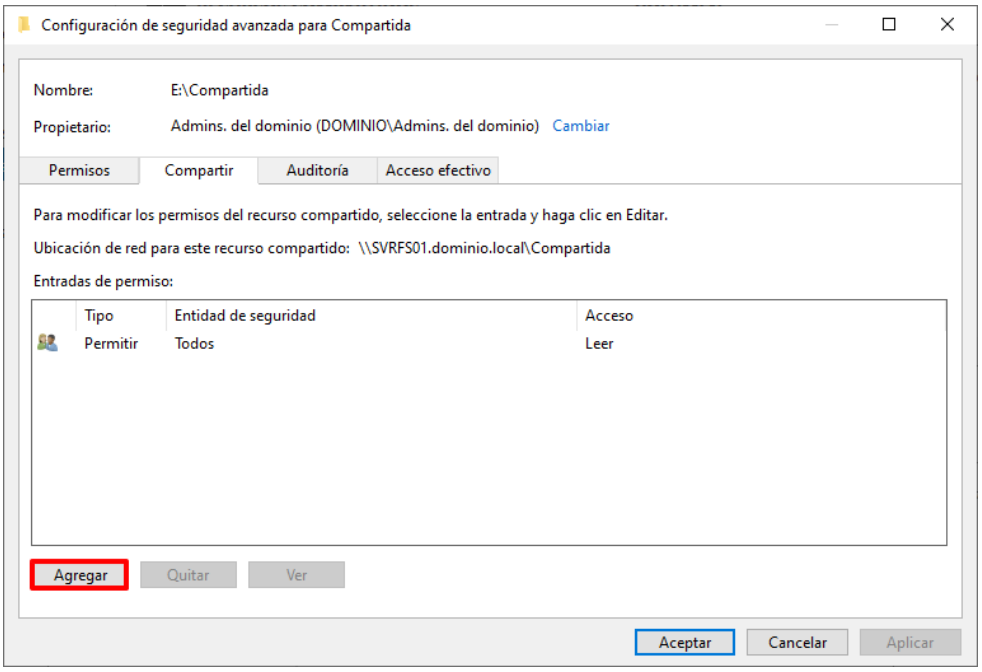
Paso	Descripción
82.	Agregada la entidad deseada, defina los permisos de los que dispondrá sobre el recurso compartido en el apartado definido a tal efecto.  **Nota:** En este ejemplo se permite a los usuarios la lectura y acceso al recurso compartido sin la capacidad de establecer ningún tipo de cambio y/o modificación.

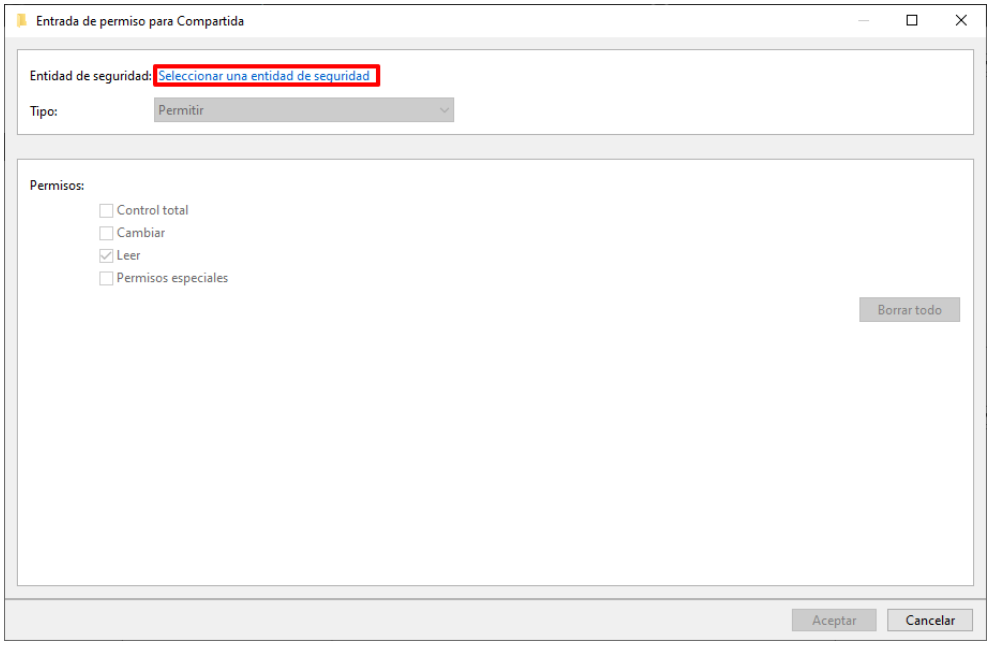
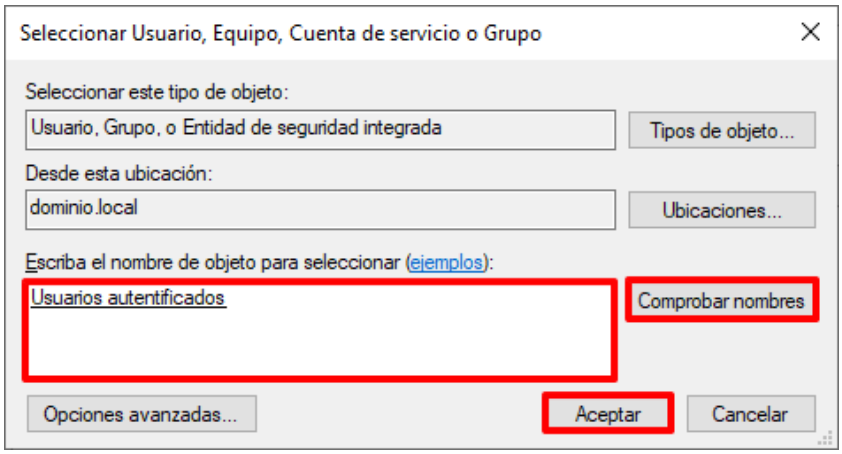
Paso	Descripción
83.	Si lo desea puede hacer uso de las siguientes opciones: – Se aplica a: Permite definir sobre qué elementos se aplicará la entidad de seguridad definida.  – Mostrar permisos avanzados: Permite establecer de una manera más rigurosa y granular las acciones que una entidad (usuario o grupo) puede realizar sobre el recurso. Por ejemplo, puede limitar el acceso a la lectura de los elementos que contiene el recurso compartido si un usuario o grupo no dispone de permisos específicos para ello, solo viendo aquello a lo que disponen de acceso.   – Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor: Esta opción permitirá que los permisos definidos para una entidad solo se apliquen sobre los recursos que este contiene en un nivel.  **Nota:** Puede obtener información adicional sobre esta opción a través del siguiente enlace: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776140(v=ws.10)?redirectedfrom=MSDN

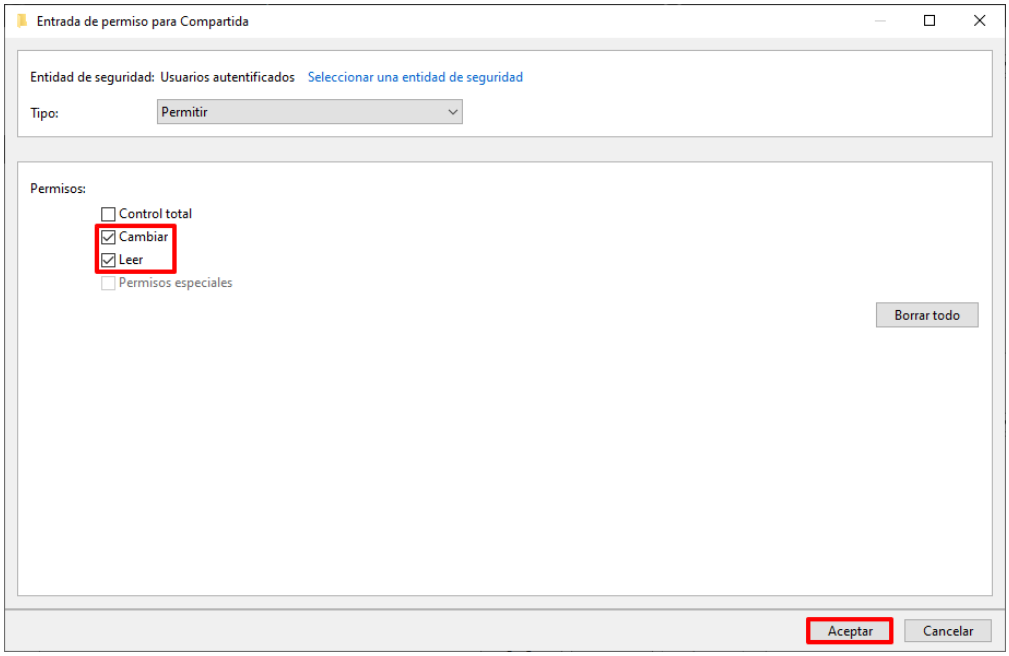
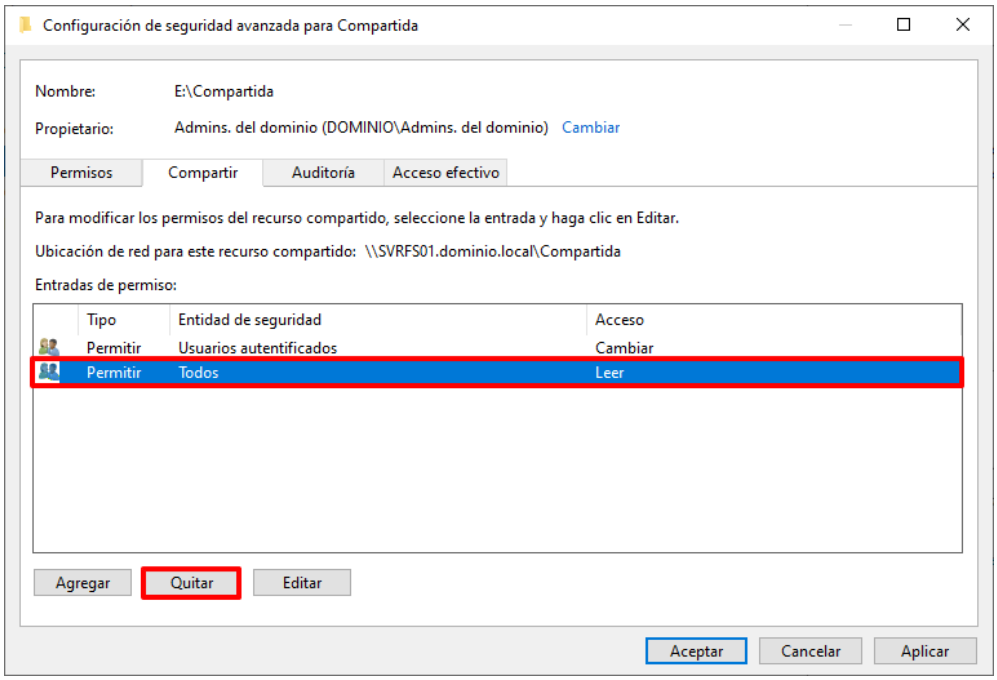
Paso	Descripción
84.	Pulse “Aceptar” para finalizar. 
85.	Repita los pasos “79” a “84” para todas las entidades de seguridad necesarias, adecuando los permisos según la necesidad.
86.	A continuación, deberá evaluar y retirar los permisos a aquellas entidades que no requieran de acceso a los recursos compartidos del servidor. Para ello, seleccione aquellas entidades que no requieran de dicho acceso y pulse sobre el botón “Quitar”.  **Nota:** En este ejemplo se hace uso de las entradas del grupo “Usuarios”, asignado de manera por defecto y del usuario “administrador”, el cual fue el usuario que creo el espacio compartido.

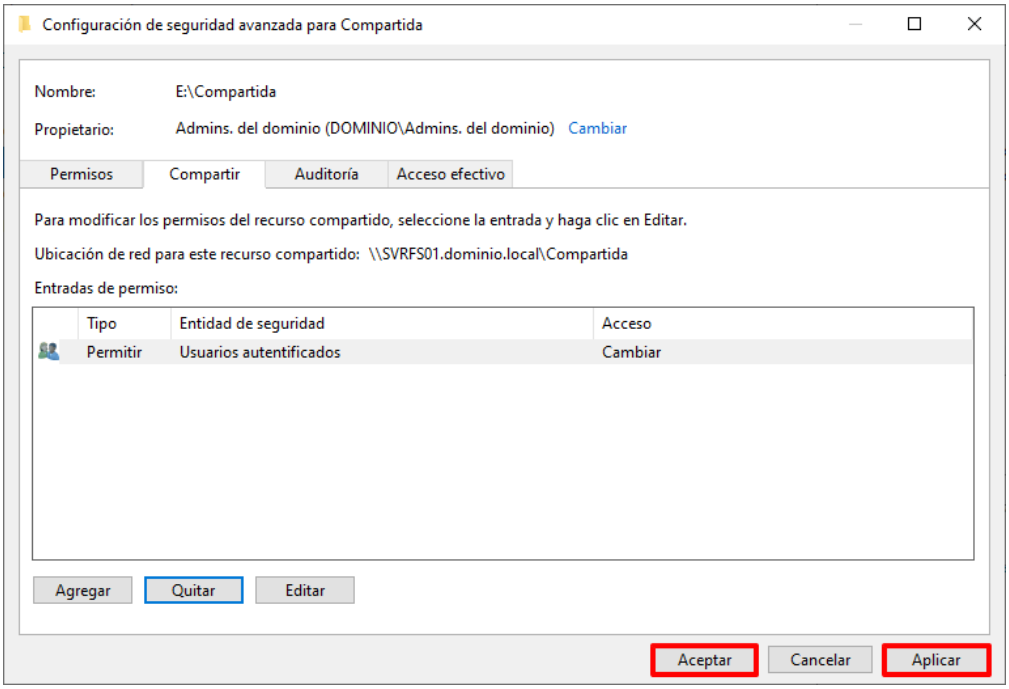
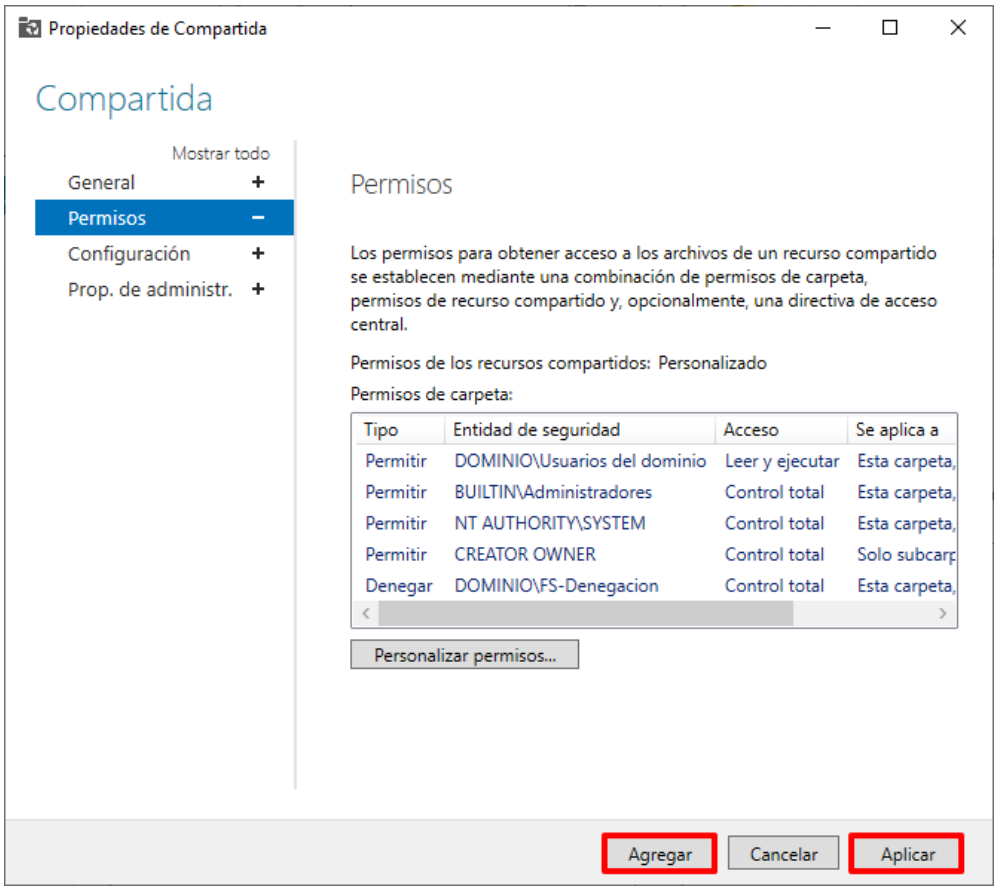
Paso	Descripción
87.	Una vez finalizado pulse “Aplicar”. 
88.	Pulse “Si” sobre el mensaje de advertencia.  **Nota:** Esta advertencia solo aparecerá en caso de que se establezcan permisos de denegación.

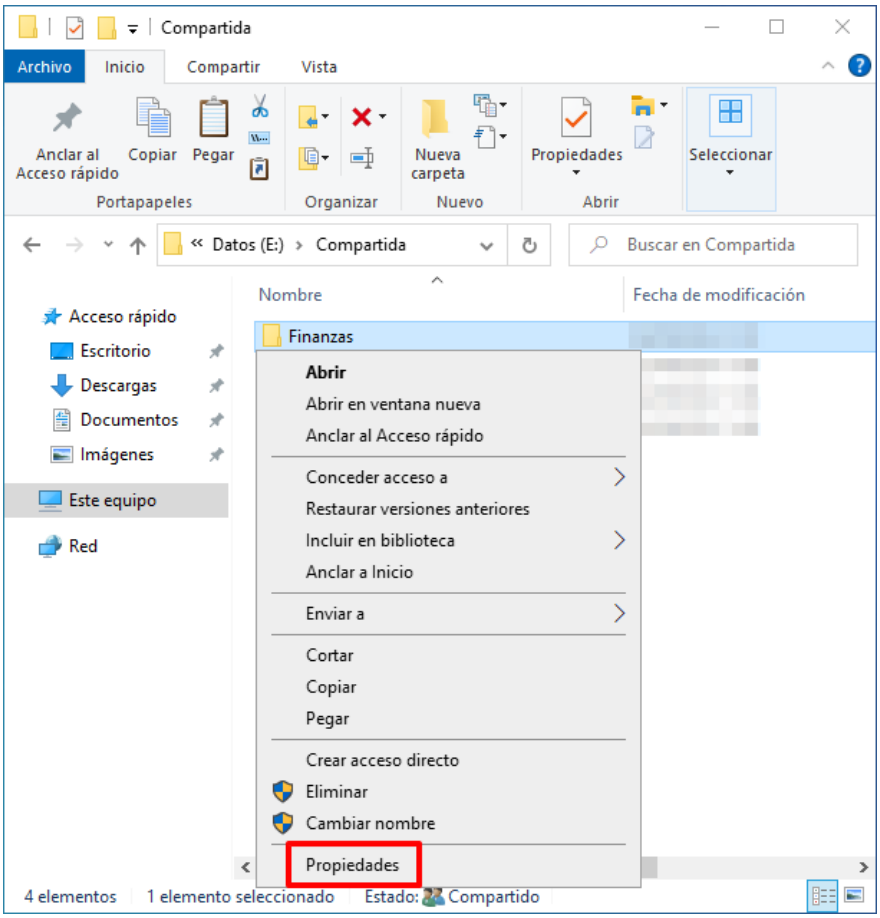
Paso	Descripción
89.	En caso de que requiera asegurar que los permisos definidos en el objeto principal sean otorgados al resto de directorios y archivos que este contiene por si la herencia no se encontrase habilitada, podrá hacer uso de la opción "Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto".  **Nota:** Tenga en consideración que esta acción sustituirá todos los permisos de los objetos secundarios aun cuando estos se hubieran definido sin herencia del objeto principal. Si utiliza la opción aparecerá una advertencia en la que deberá responder "Si" para aplicar los cambios. 

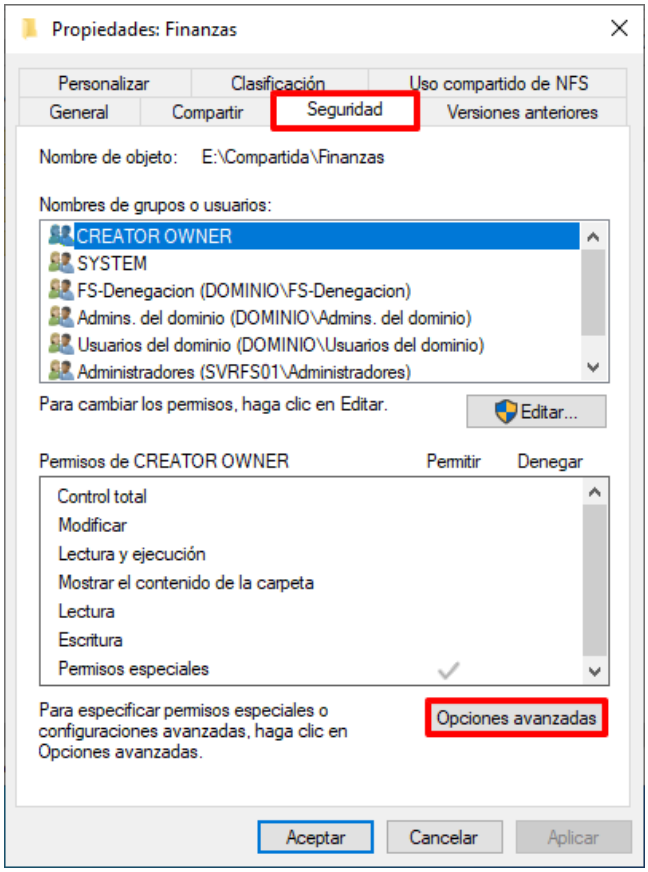
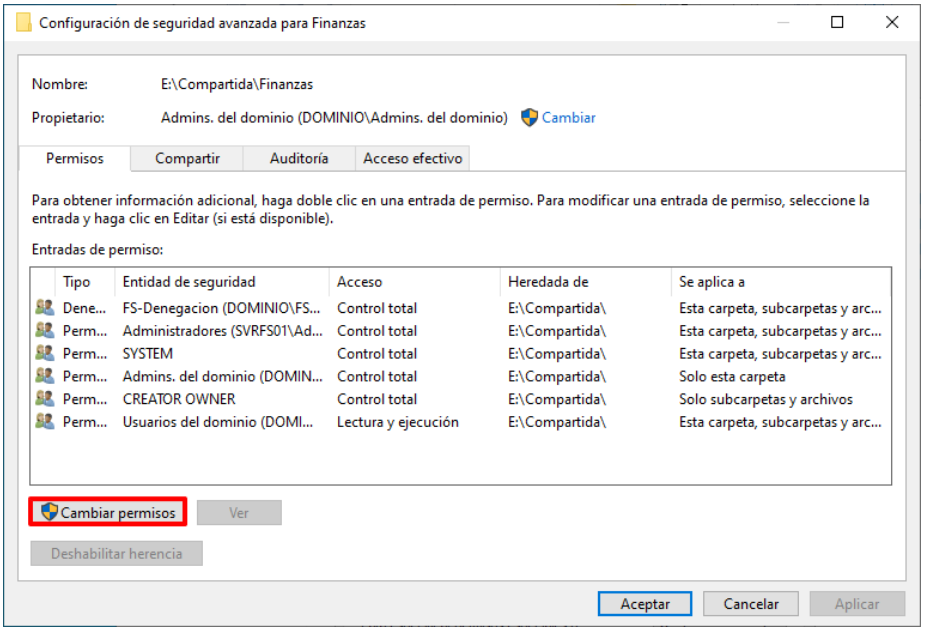
Paso	Descripción
90.	Diríjase ahora la pestaña “Compartir”. 
91.	Pulse sobre el botón “Agregar”. 

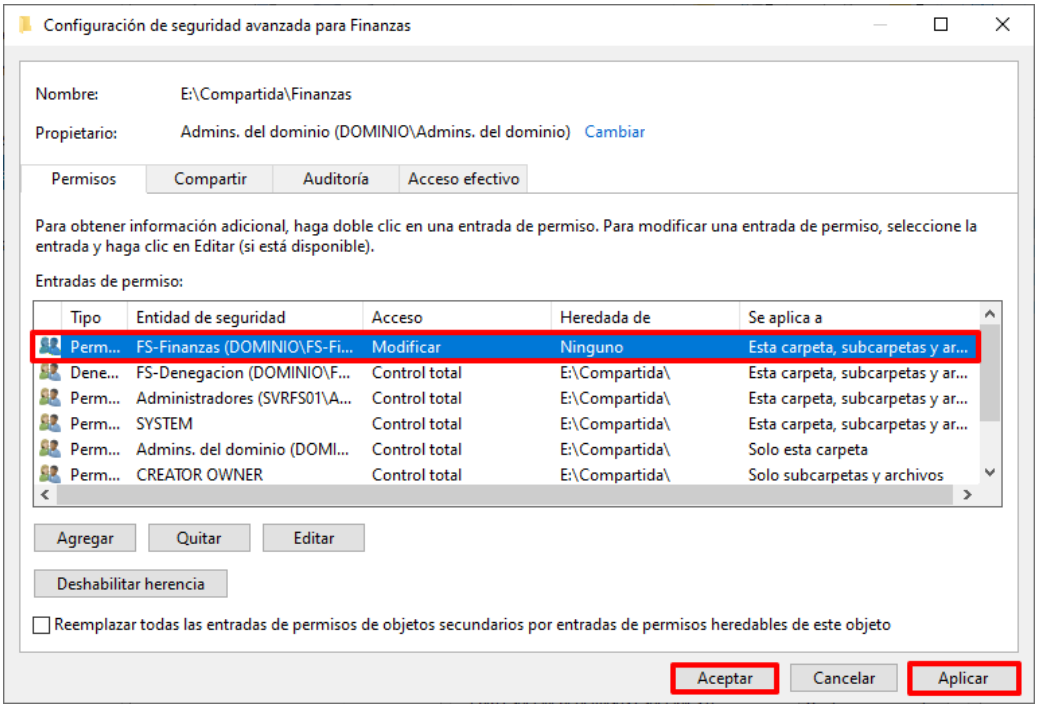
Paso	Descripción
92.	Pulse sobre “Seleccionar una entidad de seguridad”. 
93.	Incluya al grupo “Usuarios autentificados”, pulse sobre “Comprobar nombres” y a continuación pulse “Aceptar”. 

Paso	Descripción
94.	Mantenga exclusivamente los permisos “Leer” y “Cambiar”. Pulse “Aceptar” para continuar. 
95.	A continuación, seleccione el grupo “Todos” y pulse sobre “Quitar”.  **Nota:** Como norma general y por motivos de seguridad el grupo de usuarios “Todos” deberá ser retirado dado que por defecto incluye a todos los usuarios salvo a “ANONYMOUS LOGON”. Este último usuario, si estuviera asignado también debe ser retirado.

Paso	Descripción
96.	Pulse “Aplicar” y después “Aceptar” para finalizar. 
97.	Pulse “Aplicar” y “Agregar” para finalizar. 

Paso	Descripción
98.	Repita estas acciones (pasos “63” a “97”) sobre cada uno de los recursos compartidos de los que disponga su infraestructura. Recuerde que **los usuarios y/o grupos solo deben disponer de acceso y capacidad sobre aquellos directorios o recursos que así se determine**, no disponiendo de accesos adicionales. De igual modo se deberá **limitar los permisos de los usuarios y/o grupos a los estrictamente necesarios, no otorgando permisos adicionales** a la entidad seleccionada.
99.	Posteriormente sobre cada uno de los directorios que dispone el recurso compartido deberá establecer los permisos adecuados en función de la necesidad de acceso, si fuera requerido. **Nota:** Si este no fuera su escenario diríjase al “ANEXO A.2.5 SEGREGACIÓN DE FUNCIONES Y TAREAS”.
100.	Al no tratarse de recursos propiamente compartidos, deberá acceder a las opciones de permisos haciendo clic derecho sobre el directorio de Windows y seleccionando “Propiedades” del menú contextual.  **Nota:** Para este ejemplo se hace uso del directorio “Finanzas” creado para representar las configuraciones de este paso a paso.

Paso	Descripción
101.	A continuación, diríjase a la pestaña “Seguridad” y pulse sobre “Opciones avanzadas”. 
102.	Ahora dispondrá del acceso al mismo elemento de configuración que en pasos anteriores. Pulse sobre la opción “Cambiar permisos”. 

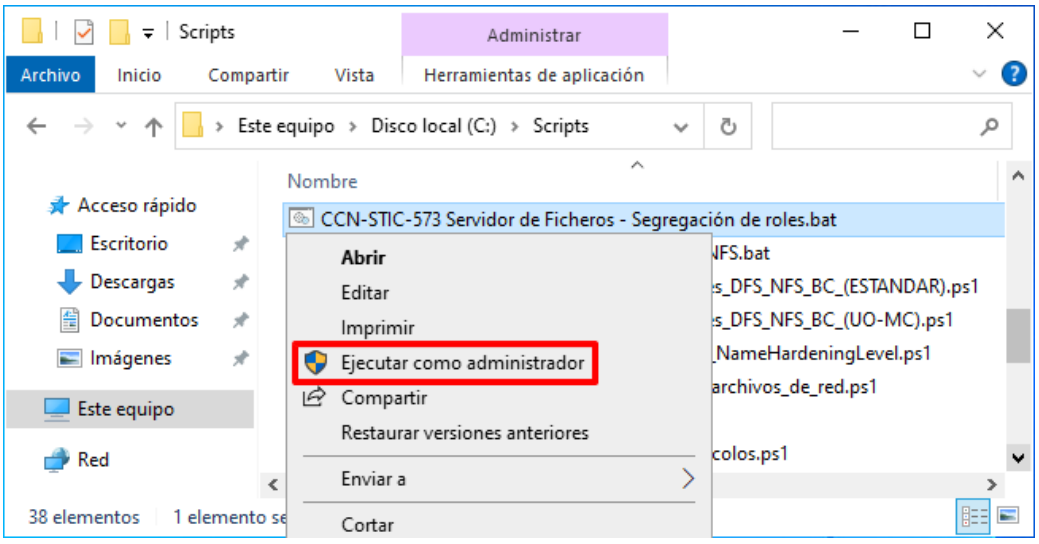
Paso	Descripción
103.	Dependiendo de la configuración que desee establecer podrá realizar parte o la totalidad de las acciones ejecutadas durante el presente apartado. El objetivo debe ser la asignación de permisos adecuados sobre los recursos que se están compartiendo solo para aquellos usuarios que así lo requieran. Dada la configuración anterior todos los usuarios con acceso al recurso compartido (usuarios del dominio) solo disponen de la capacidad de lectura, pero sin la posibilidad de crear o modificar objetos (ficheros, directorios, etc.).
104.	Realice las mismas acciones que en los pasos “79” a “84” para dar de alta una nueva entrada de permisos sobre el directorio con permisos de escritura (Modificar). Pulse “Aplicar” y “Aceptar” cuando haya finalizado de definir los permisos.  **Nota:** En este ejemplo se asocia al directorio el grupo “FS-Finanzas” creado para este paso a paso, con privilegios de escritura, de modo que los usuarios pertenecientes a dicho grupo podrán crear y modificar objetos dentro de este directorio, pero no sobre el resto, ni el principal compartido, aunque sí podrán verlos.
105.	Una vez realizada la asignación de permisos basado en grupos de seguridad sobre los diferentes recursos compartidos podrá facilitar o denegar el acceso a usuarios de manera ágil. Esto se realizará asignando estos a los grupos correspondientes.

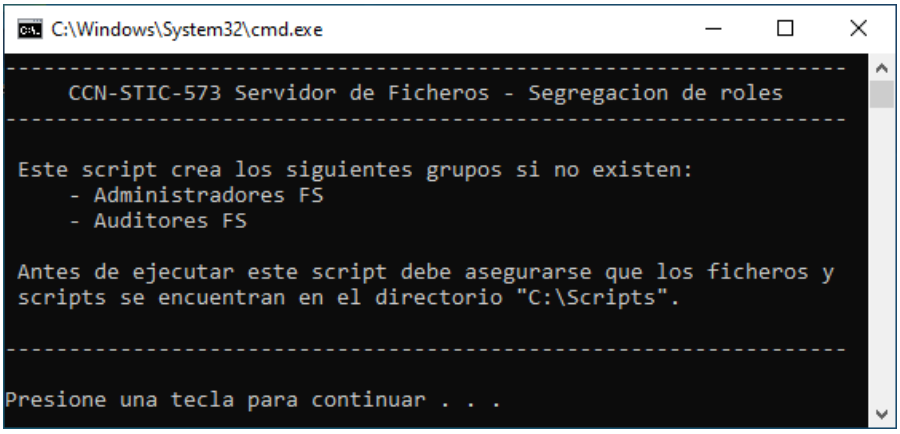
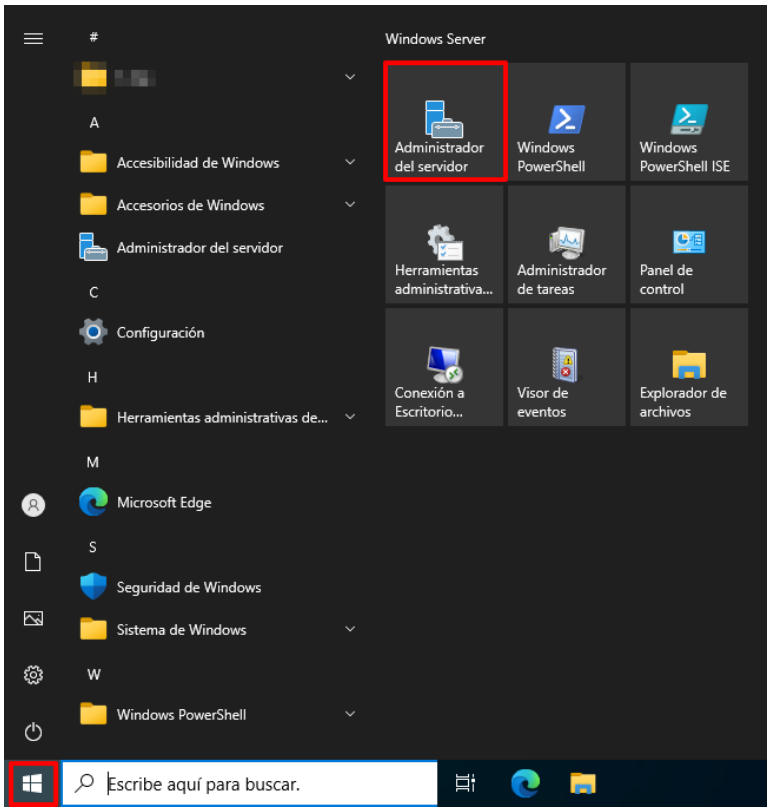
ANEXO A.2.5. SEGREGACIÓN DE FUNCIONES Y TAREAS

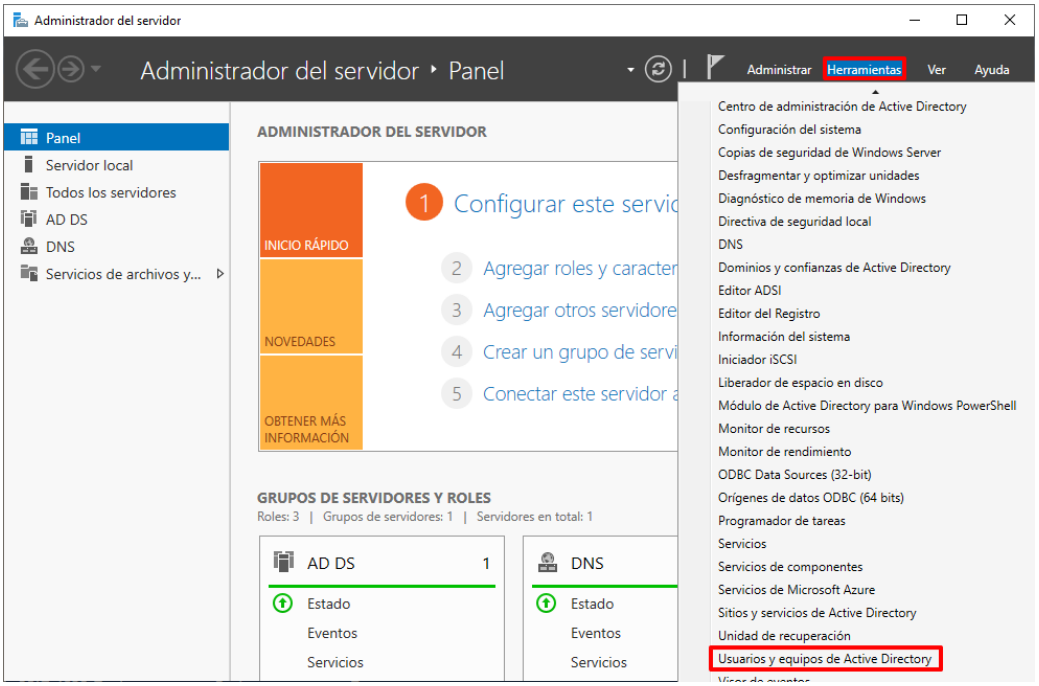
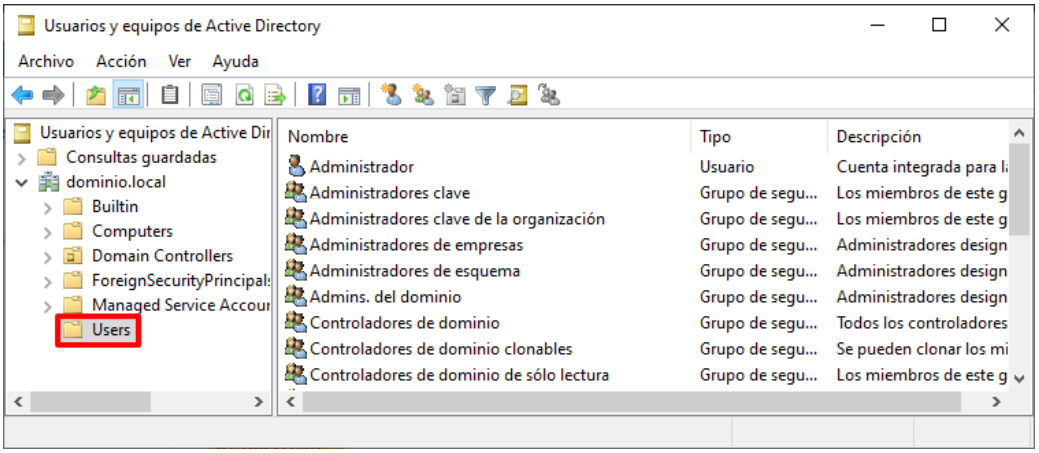
A continuación, se definirán las acciones para disponer de una adecuada segregación de funciones dentro de los sistemas operativos Windows Server y aplicable sobre los equipos de tipo Servidor de Ficheros.

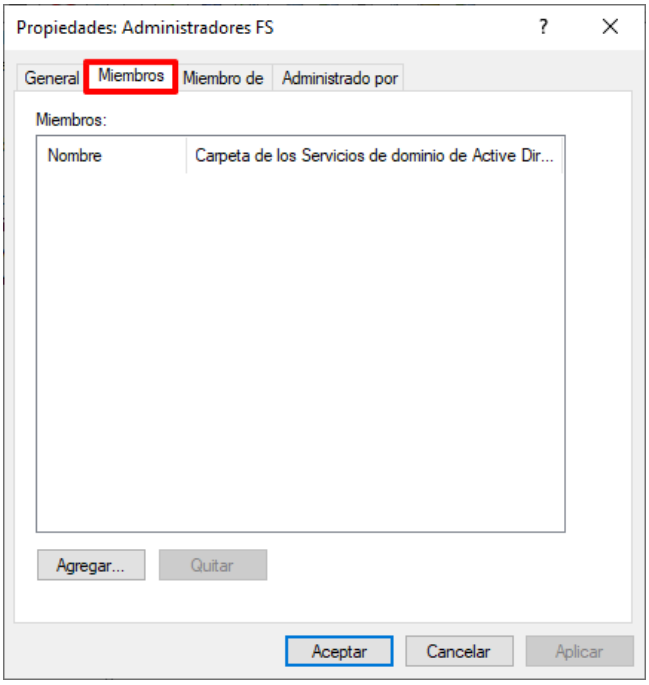
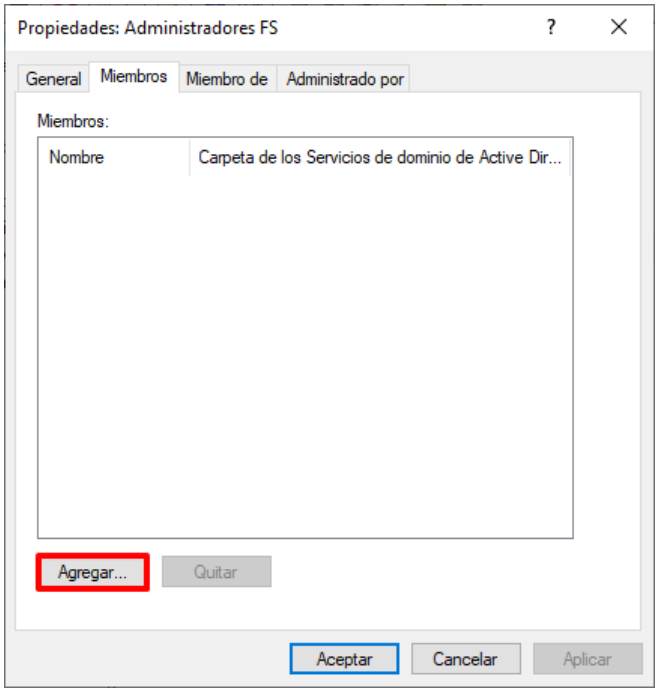
Nota: Los pasos descritos a continuación son un ejemplo de cómo segregar ciertas tareas, sin rechazar o validar la gestión por medio de consolas o herramientas adicionales que una organización pudiera disponer. Cada organización deberá adaptar los pasos descritos en el presente apartado en función de las necesidades de la misma.

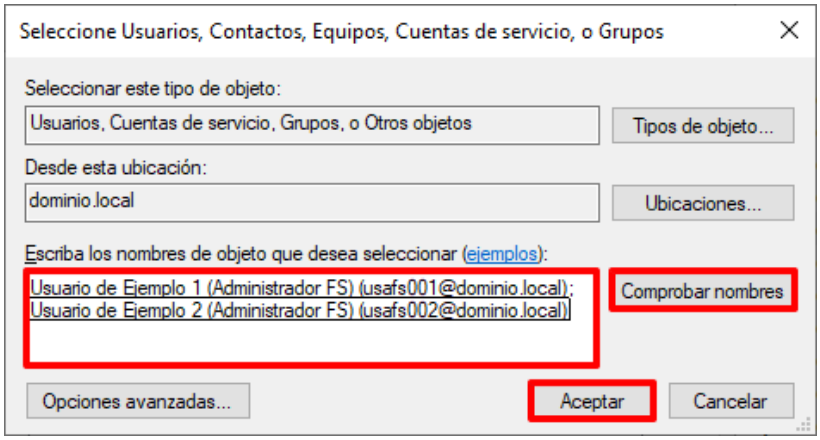
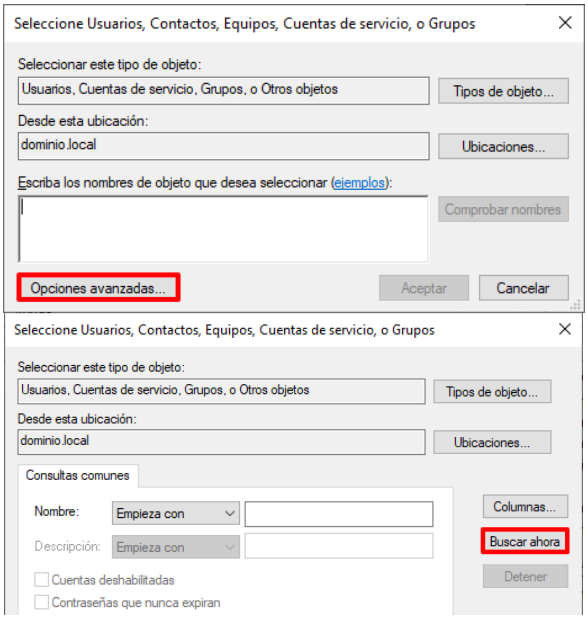
Para esta labor se van a generar diversos grupos que aúnen las funciones de administración y de operación/uso del servicio de compartición de ficheros.

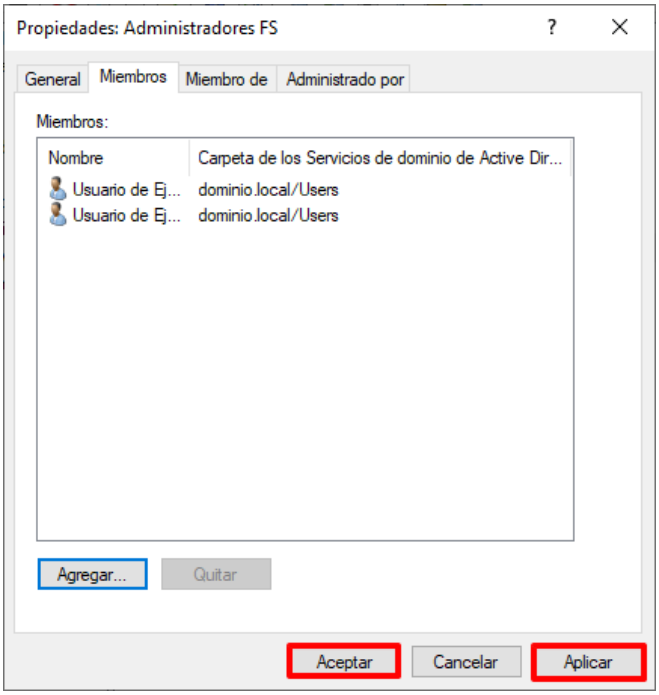
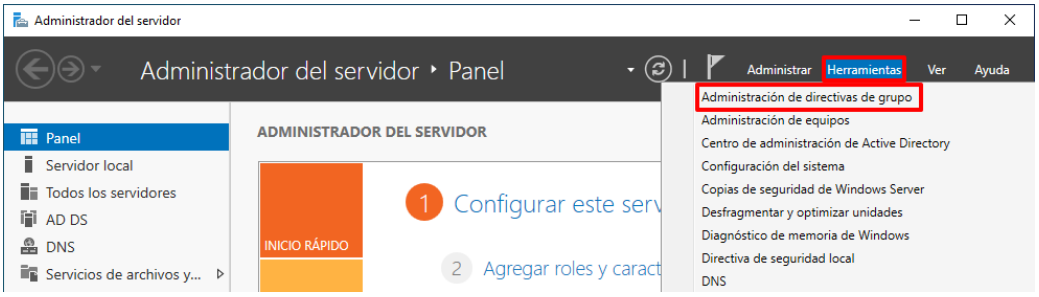
Paso	Descripción
106.	Inicie sesión en un servidor Controlador de Dominio del dominio. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
107.	Será necesario la creación de grupos dedicados de modo que la gestión de Servidores de Ficheros quede simplificada en la pertenencia a grupos.
108.	Si no desea realizar una creación de grupos personalizada o no dispone de estos grupos, diríjase al directorio "C:\Scripts" y ejecute el script "CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 

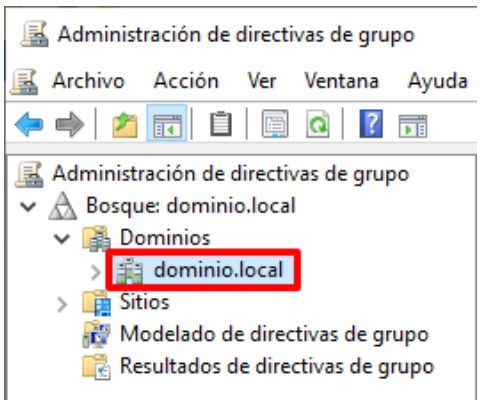
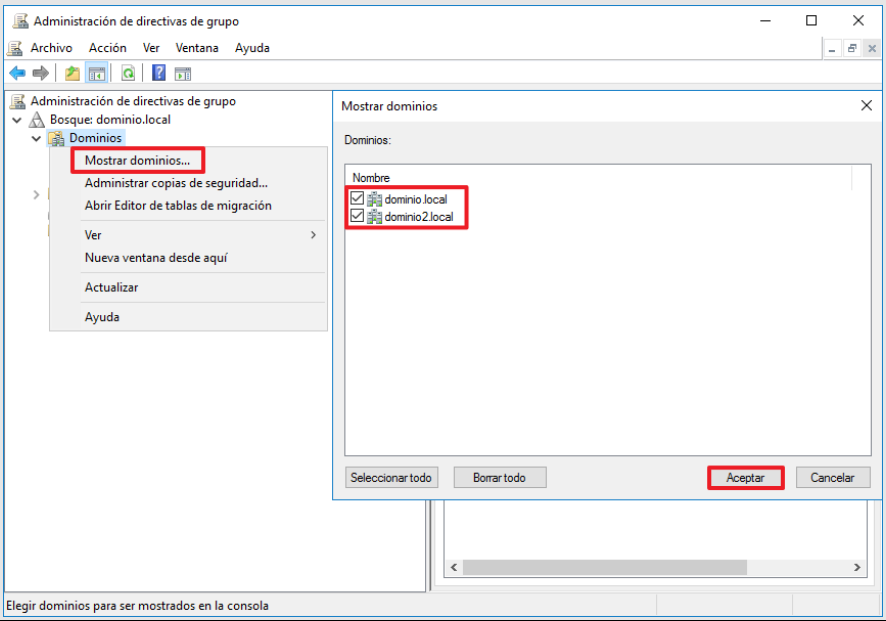
Paso	Descripción
109.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
110.	Tras la ejecución del script, entre los grupos generados se puede encontrar el siguiente grupo: – Administradores FS.
111.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

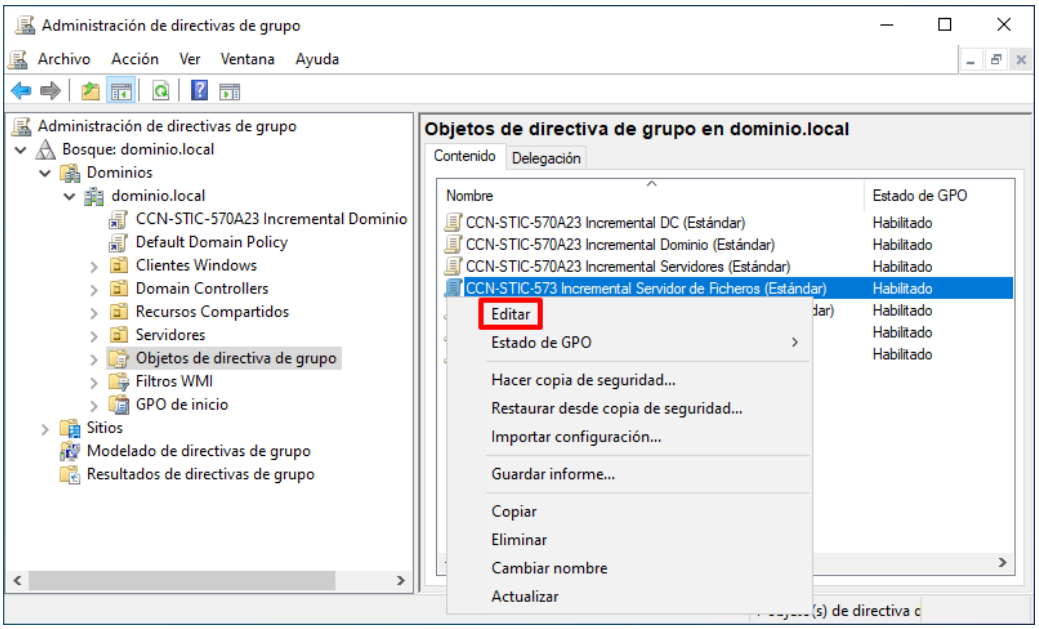
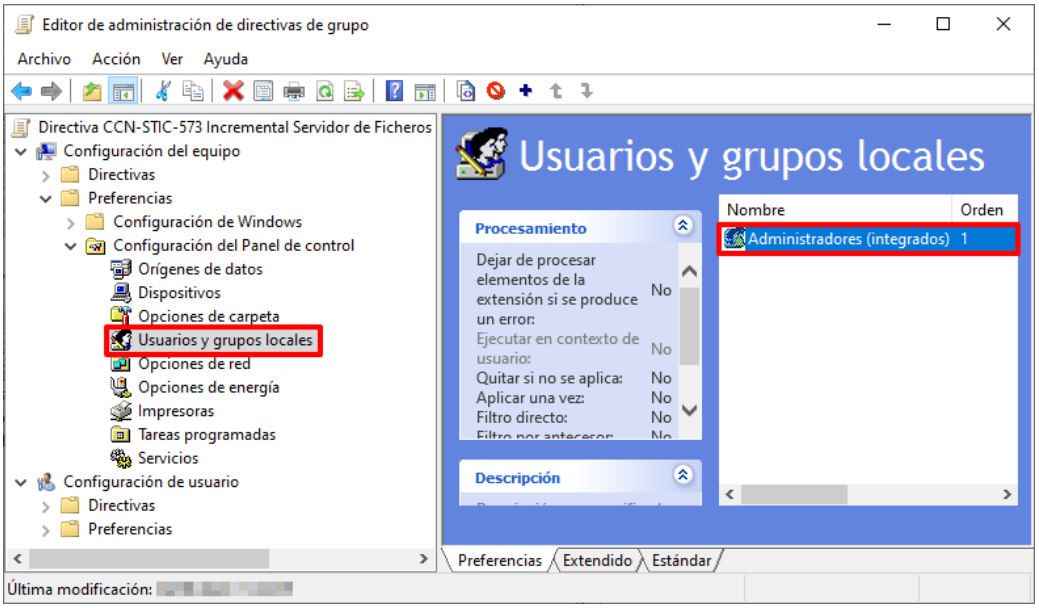
Paso	Descripción
112.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
113.	Sobre la consola “Usuarios y equipos de Active Directory”, seleccione y despliegue el nodo “<nombre de su dominio> → Users”. 

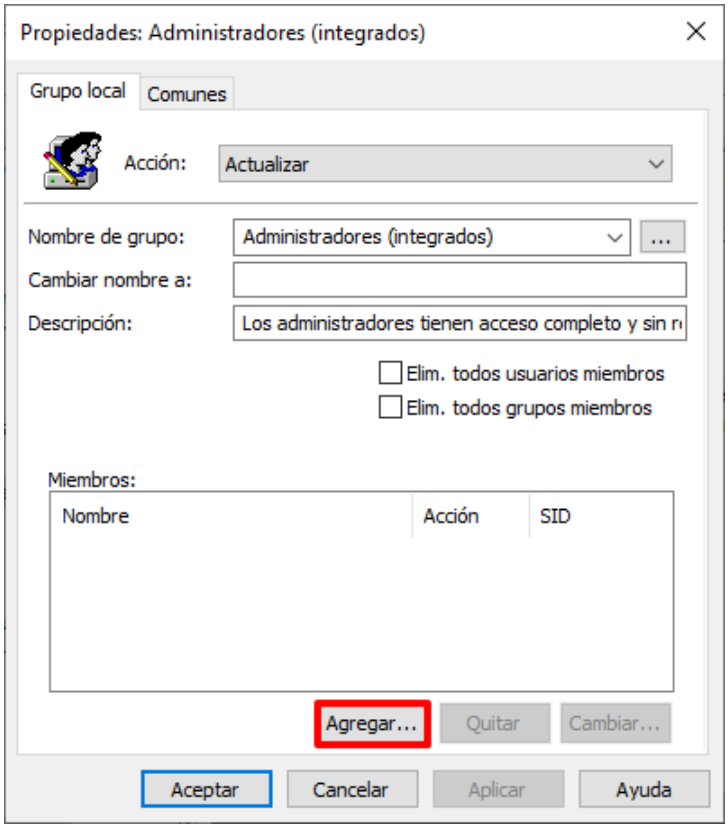
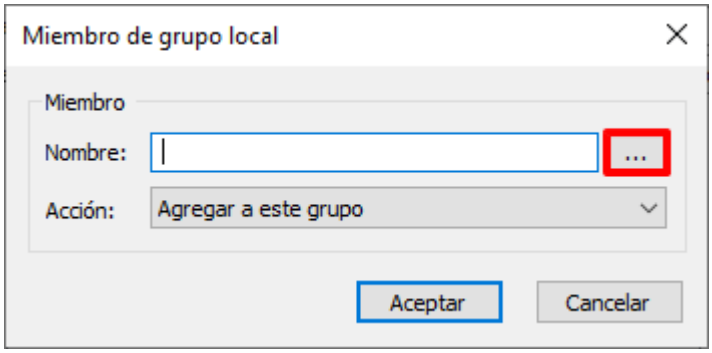
Paso	Descripción
114.	Haga doble clic sobre el grupo “Administradores FS” creado anteriormente y sitúese a continuación sobre la pestaña “Miembros”.  **Nota:** En este ejemplo se hace uso del grupo creado en pasos anteriores. Deberá adaptar los pasos descritos en caso de hacer uso de otro grupo de usuarios.
115.	En este ejemplo se va a añadir un par de usuarios para que dispongan de la capacidad de administración para Servidores de Ficheros. Para ello, pulse sobre el botón “Agregar…”. 

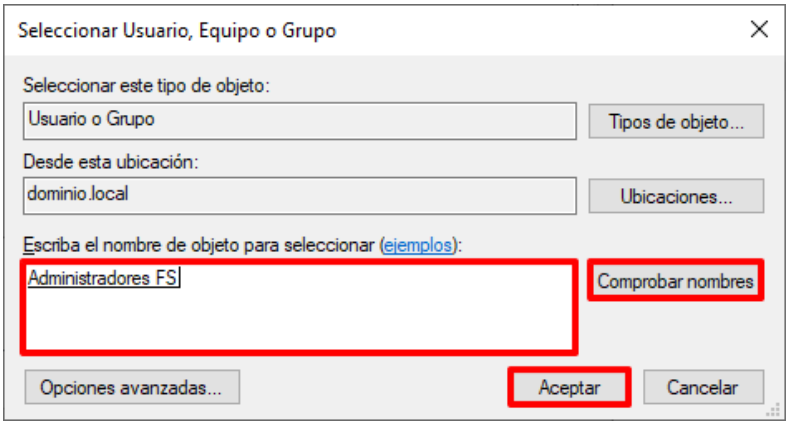
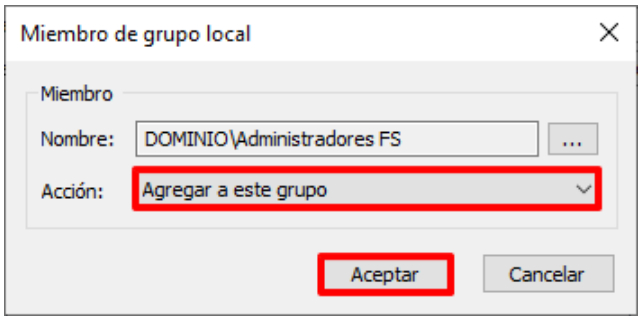
Paso	Descripción
116.	En la nueva ventana emergente introduzca el nombre de aquellas cuentas de usuario que desee que posean privilegios de administración sobre los equipos de tipo Servidor de Ficheros. Puede hacer uso del botón "Comprobar nombres" para identificar la cuenta de forma exacta y puede incluir varias cuentas separada por punto y coma (;). Pulse "Aceptar" cuando haya incluido a todos los usuarios o grupos necesarios.  **Nota:** En este ejemplo se hace uso de los usuarios: **usafs001** y **usafs002**. Deberá evaluar que usuarios de su organización deben pertenecer a este grupo y adaptar esta configuración a las necesidades de su organización. De igual modo garantice que al menos dos usuarios disponen de capacidad de administración.
117.	Si desconoce las cuentas de usuario puede hacer uso del botón "Opciones avanzadas…" y en la nueva ventana "Buscar ahora" para listar todos los usuarios. Pulse "Aceptar" cuando haya finalizado de incluir a los usuarios. 

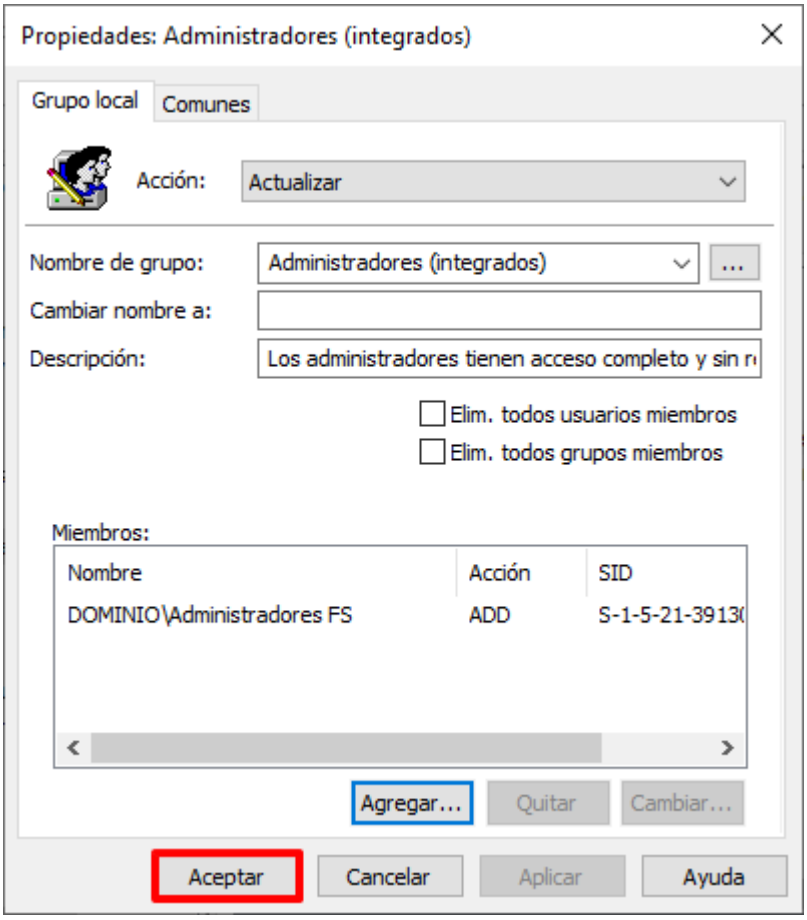
Paso	Descripción
118.	Pulse “Aplicar” y a continuación “Aceptar” para finalizar en la ventana “Propiedades: Administradores FS”. 
119.	A continuación, en el “Administrador del servidor”, en la parte superior derecha pulse sobre el botón “Herramientas” y seleccione “Administración de directivas de grupo”. 

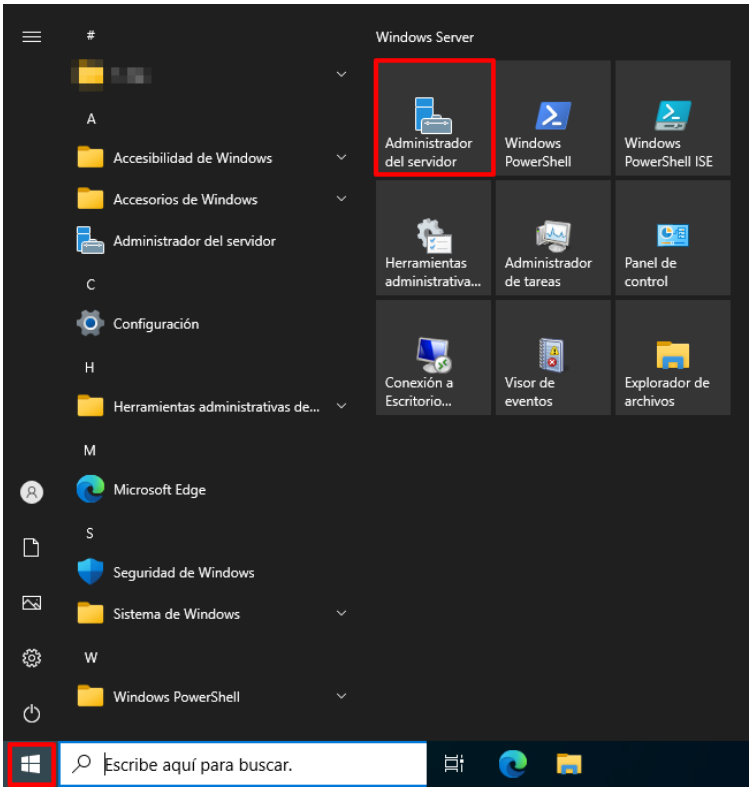
Paso	Descripción
120.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** Compruebe que realiza las tareas de administración sobre el dominio adecuado. Si no aparece su dominio en la ventana, utilice la opción "Mostrar dominios…" del menú contextual, marque los dominios que desea gestionar y pulse sobre "Aceptar" tal y como se indica a continuación. 

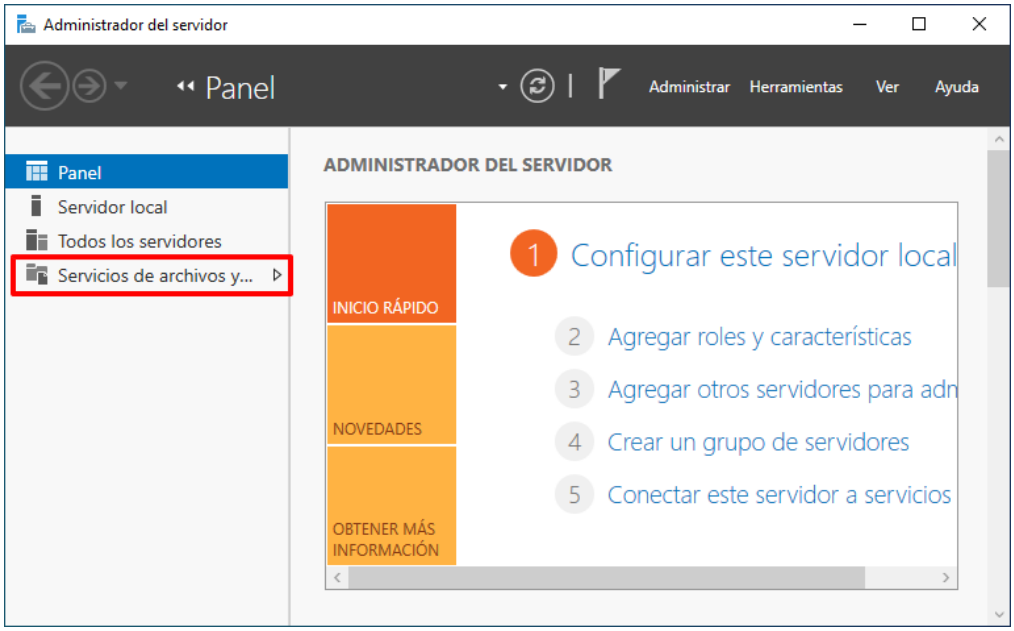
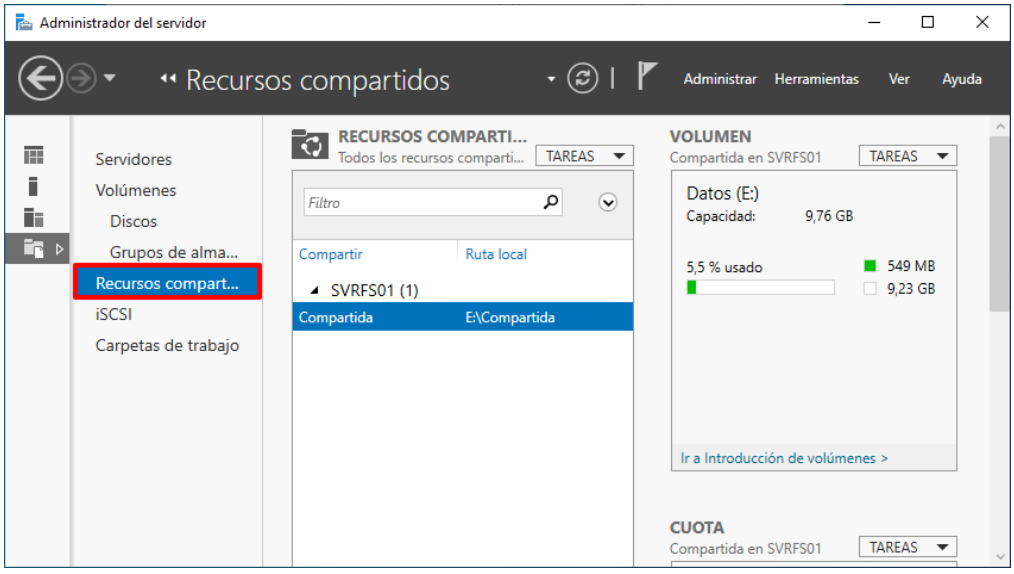
Paso	Descripción
121.	Seleccione con el botón derecho el objeto GPO “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
122.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) → Configuración del equipo → Preferencias → Configuración del Panel de control → Usuarios y grupos locales”**. En el panel derecho identifique el grupo “Administradores (integrados)” y haga doble clic sobre el mismo. 

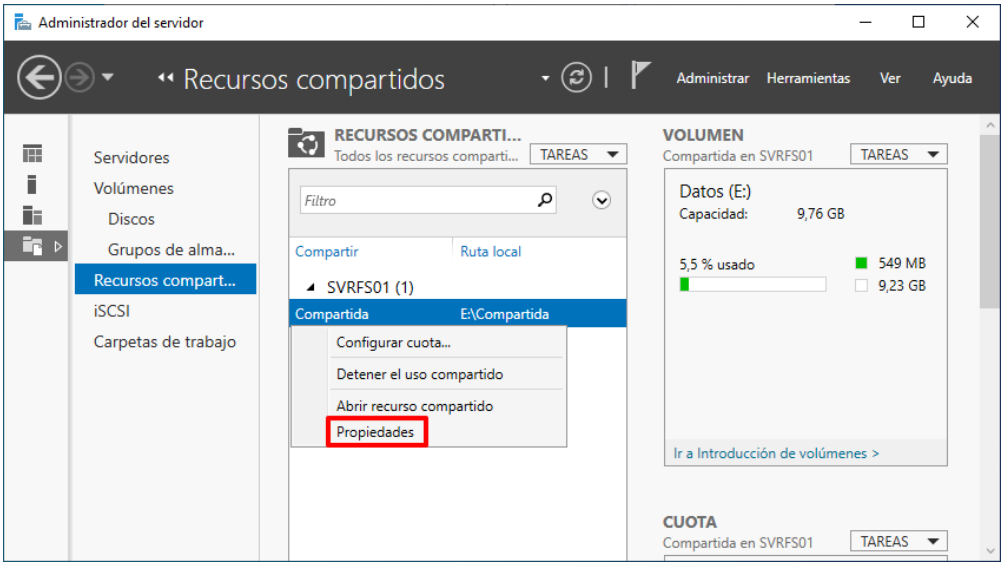
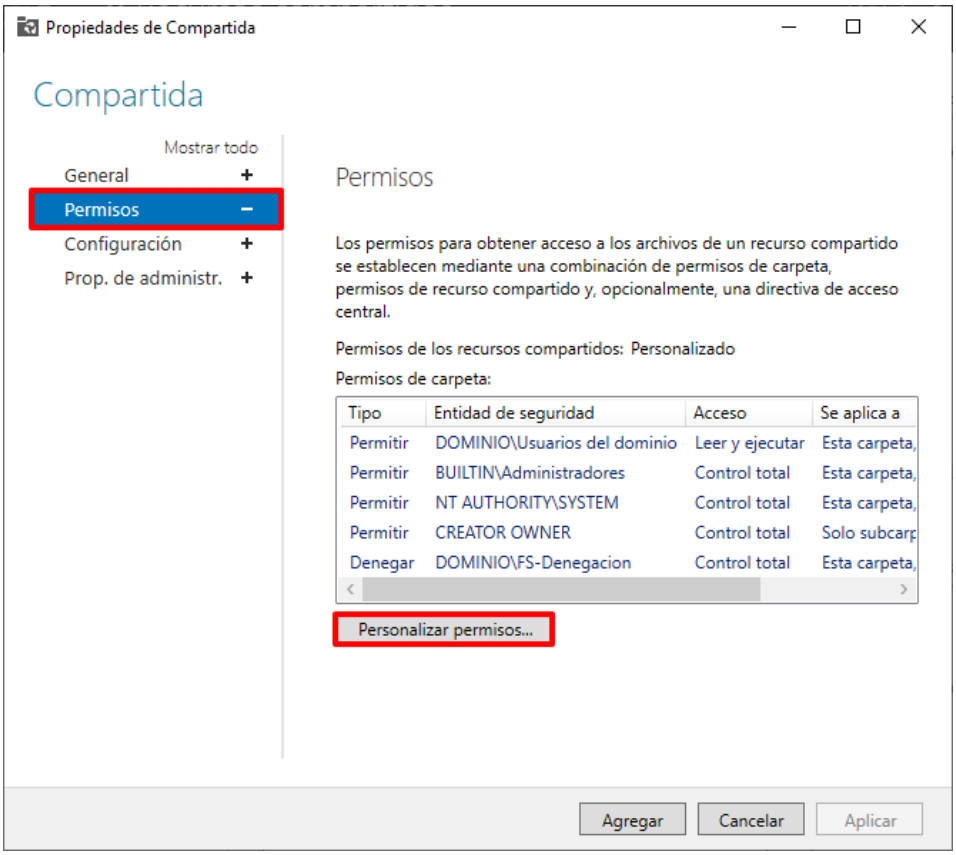
Paso	Descripción
123.	Pulse sobre el botón “Agregar…” para continuar. 
124.	En la nueva ventana emergente pulse sobre el botón “…”. 

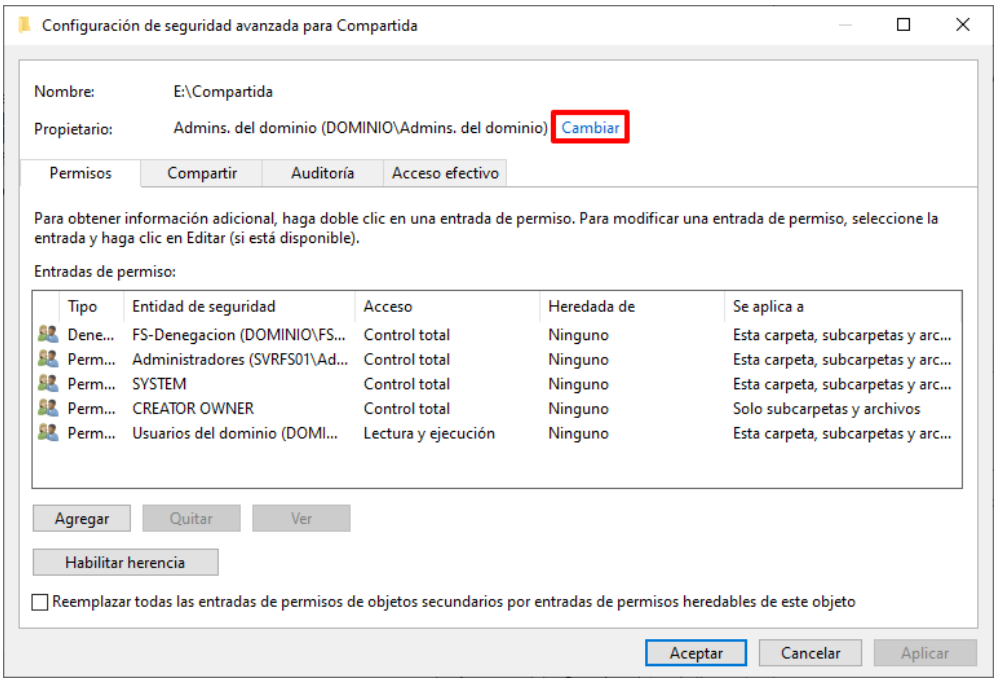
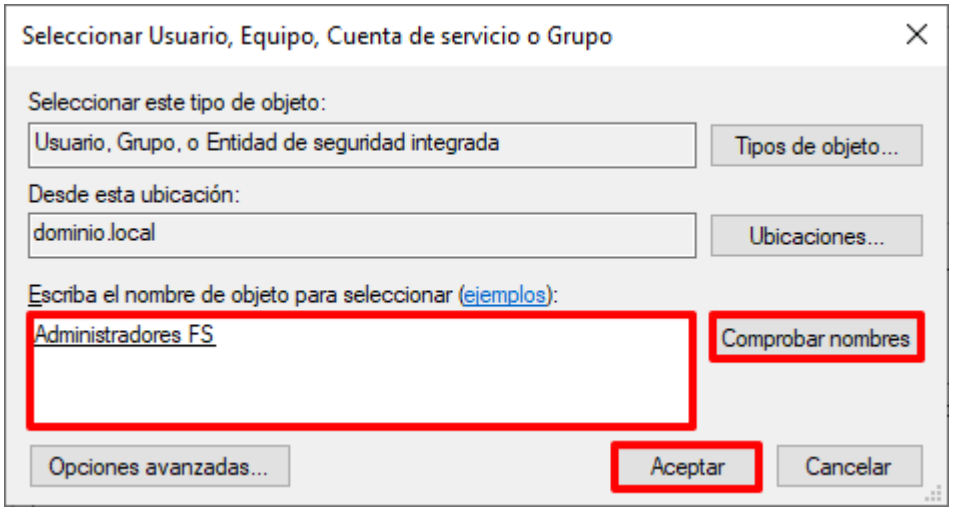
Paso	Descripción
125.	Escriba el nombre del grupo que desea incluir en el grupo integrado "Administradores". En este ejemplo, será el generado a través del script ejecutado en pasos anteriores ("Administradores FS"). Pulse sobre "Comprobar nombres" para completar el nombre y pulse "Aceptar".  **Nota:** El grupo "Administradores FS" habrá sido generado de forma automatizada si ha ejecutado previamente el script "CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat". En caso contrario puede ejecutar este script o bien crear el grupo de forma manual. Deberá adaptar esta configuración a las necesidades de su organización.
126.	En la anterior ventana emergente asegúrese de que la acción a realizar es "Agregar a este grupo" y pulse el botón "Aceptar". 

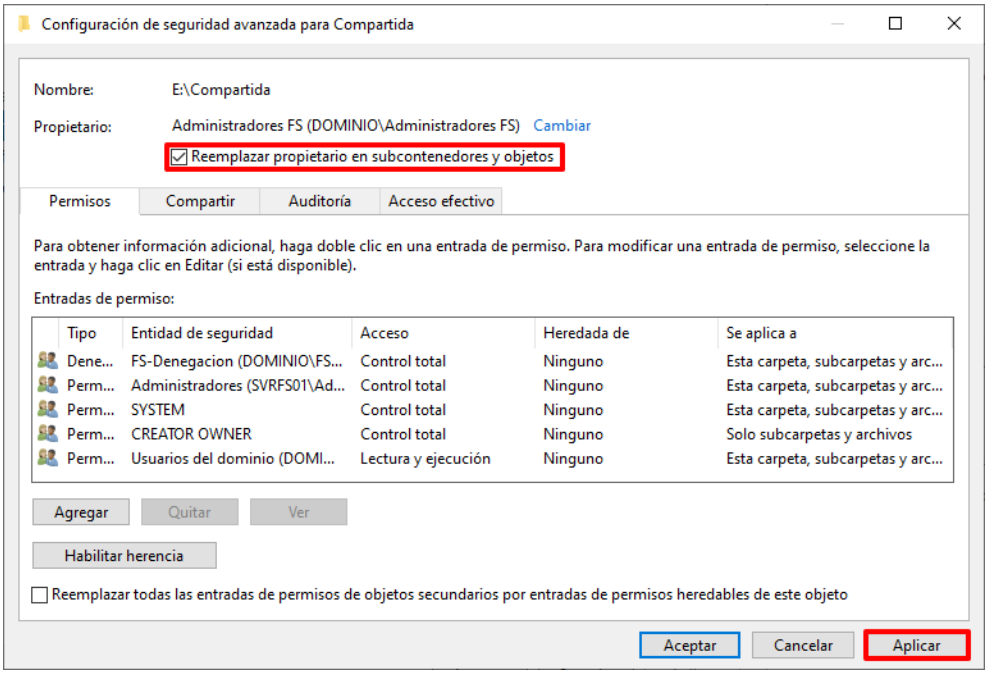
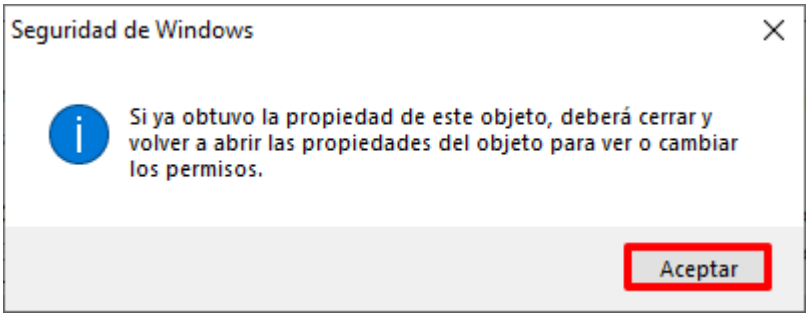
Paso	Descripción
127.	Para finalizar, pulse de nuevo sobre el botón “Aceptar”. 
128.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo el acceso los equipos de tipo Servidor de Ficheros para su gestión con privilegios administrativos elevados. Esto supone que a efectos prácticos disponen de capacidad de administración sobre el equipo y los elementos que contiene. Deberá limitar el acceso a aplicaciones y herramientas que no sean requeridas para evitar que estos usuarios puedan realizar tareas sobre estas. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.
129.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.

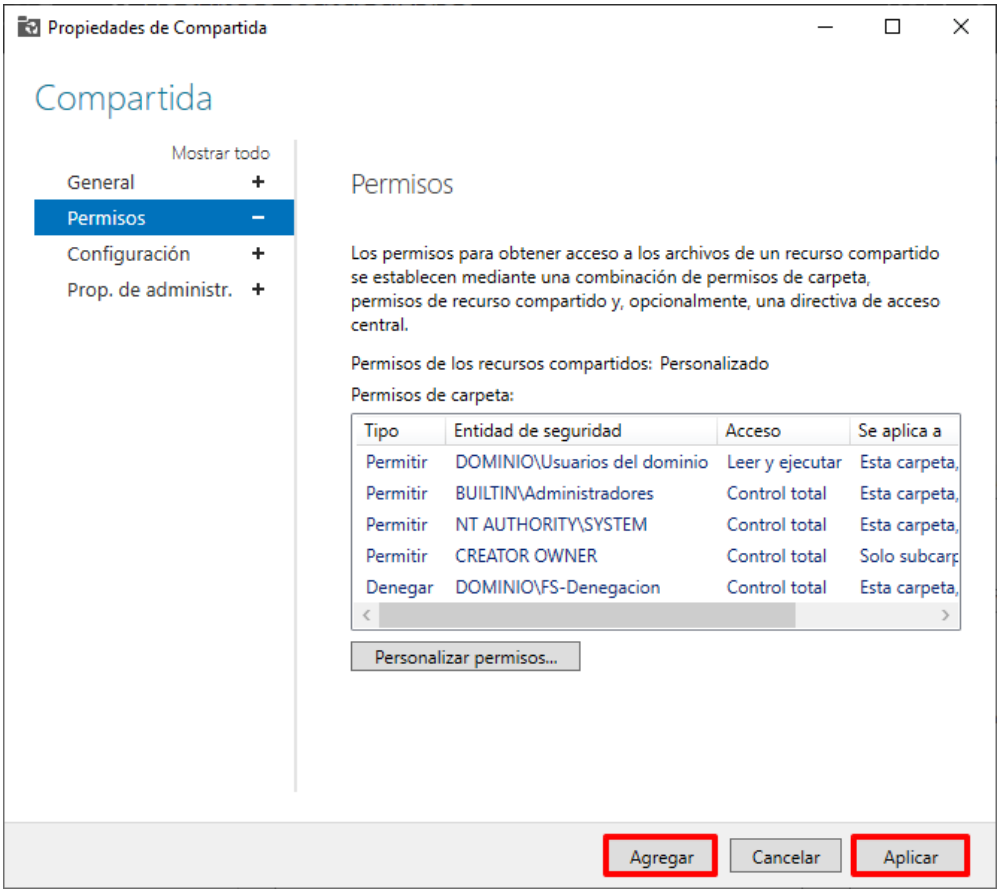
Paso	Descripción
130.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

Paso	Descripción
131.	En la columna izquierda del “Administrador del servidor” seleccione “Servicio de archivos y de almacenamiento”. 
132.	A continuación, acceda al apartado “Recursos compartidos”. 

Paso	Descripción
133.	En el apartado central, sobre el recurso compartido bajo el que desee trabajar haga clic derecho y seleccione la opción del menú contextual “Propiedades”.  **Nota:** En este ejemplo se hace uso del recurso compartido definido como “Compartida”.
134.	En la nueva ventana emergente, diríjase al apartado “Permisos” y seleccione la opción “Personalizar permisos…”. 

Paso	Descripción
135.	Se va a modificar la propiedad del recurso compartido con la intención de que sean los administradores del equipo con el rol de Servidor de Ficheros quienes gestionen los recursos. Para ello, pulse sobre el botón “Cambiar”. 
136.	En la ventana emergente defina el grupo de usuarios “Administradores FS”, pulse sobre “Comprobar nombres” y por último sobre “Aceptar”.  **Nota:** El grupo “Administradores FS” habrá sido generado de forma automatizada si ha ejecutado previamente el script “CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual. Deberá adaptar esta configuración a las necesidades de su organización.

Paso	Descripción
137.	Marque ahora sobre la nueva opción que aparecerá “Reemplazar propietario en subcontenedores y objetos”. Pulse de igual modo sobre el botón “Aplicar”. Esto permitirá que todos los objetos dependientes de este cambien de igual modo su propiedad.  **Nota:** Tenga en consideración que esta acción sustituirá los permisos de los subelementos del recurso compartido que haya configurado según lo indicado en el punto “ANEXO A.2.4 REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO”. En caso de ejecutar esta acción deberá de nuevo revisar los permisos asociados al resto de directorio y ficheros.
138.	Pulse “Aceptar” sobre el mensaje emergente, de nuevo “Aceptar” sobre la ventana de permisos. 

Paso	Descripción
139.	En la ventana “Compartida” pulse “Aplicar” y “Agregar”. 
140.	Repita los pasos “133” a “139” para todos los recursos compartidos de modo que la administración quede delegada en la entidad de seguridad definida a tal efecto.

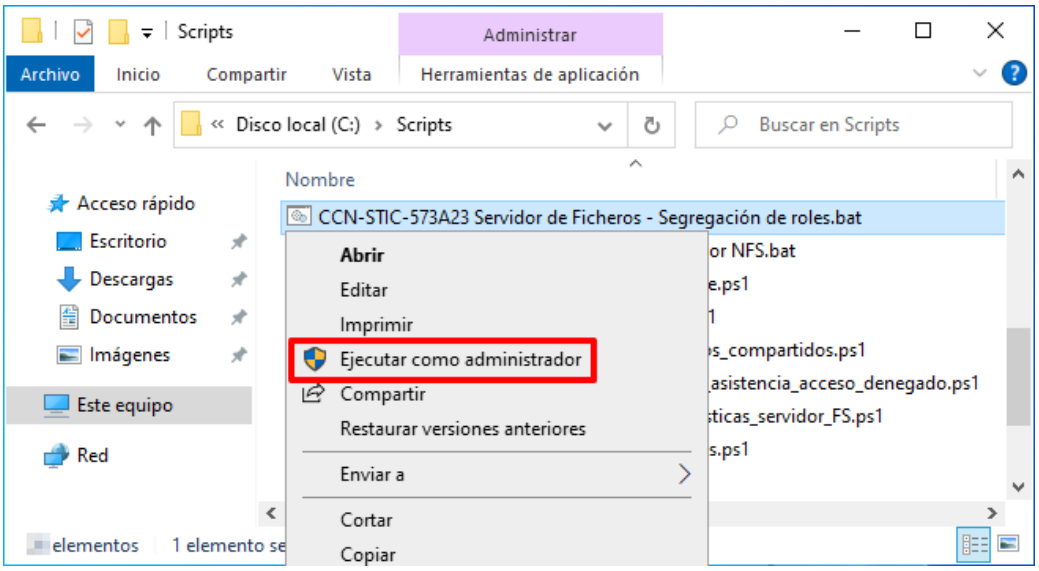
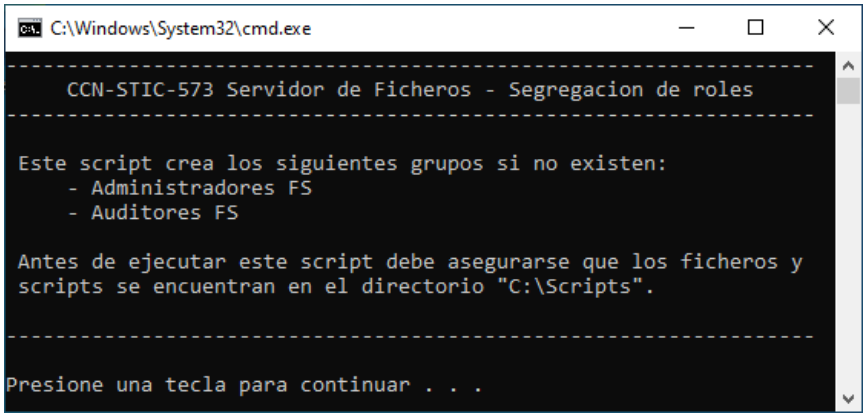
ANEXO A.2.5.1. SEGREGACIÓN DE FUNCIONES Y TAREAS (USO OFICIAL – MATERIAS CLASIFICADAS)

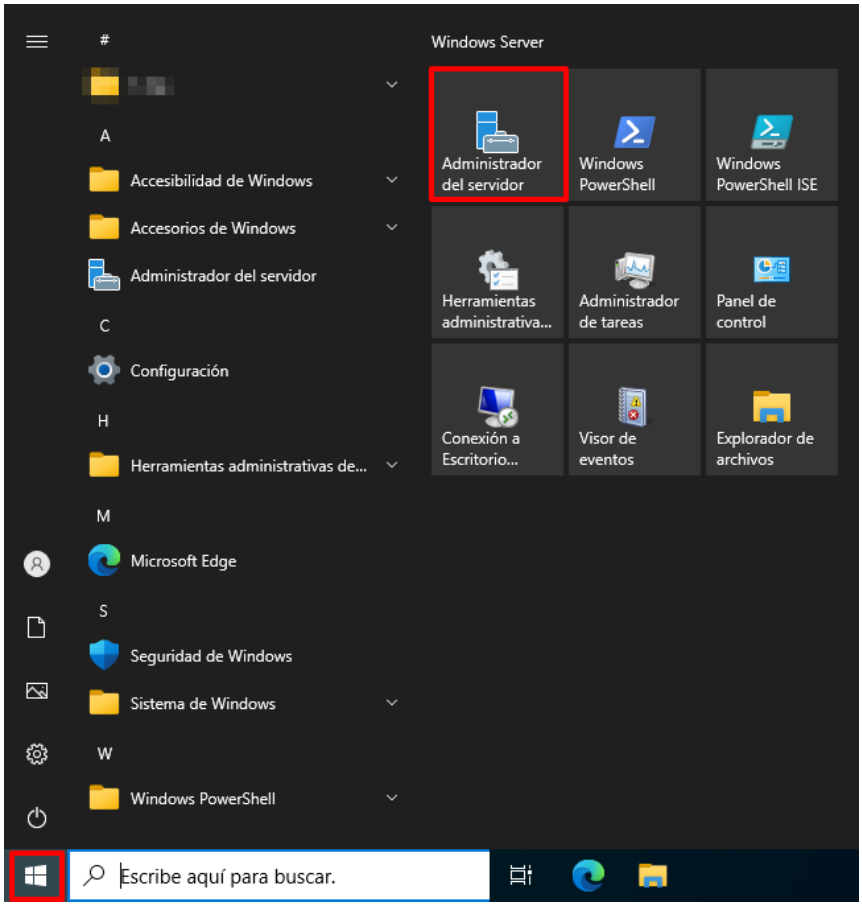
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

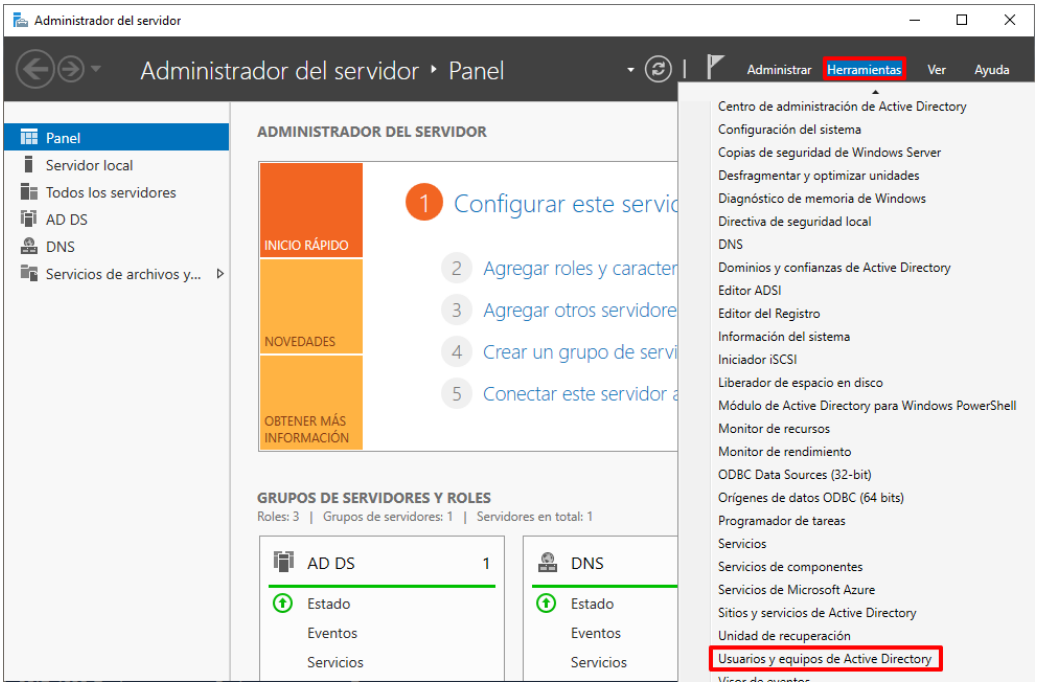
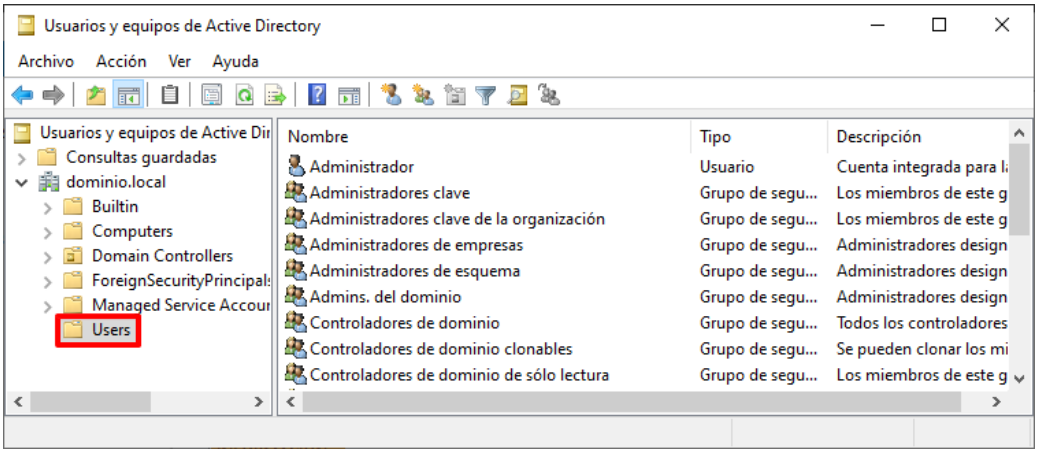
Ejecutadas las acciones anteriores, a continuación, se disponen los pasos que permitan realizar la siguiente segregación de funciones:

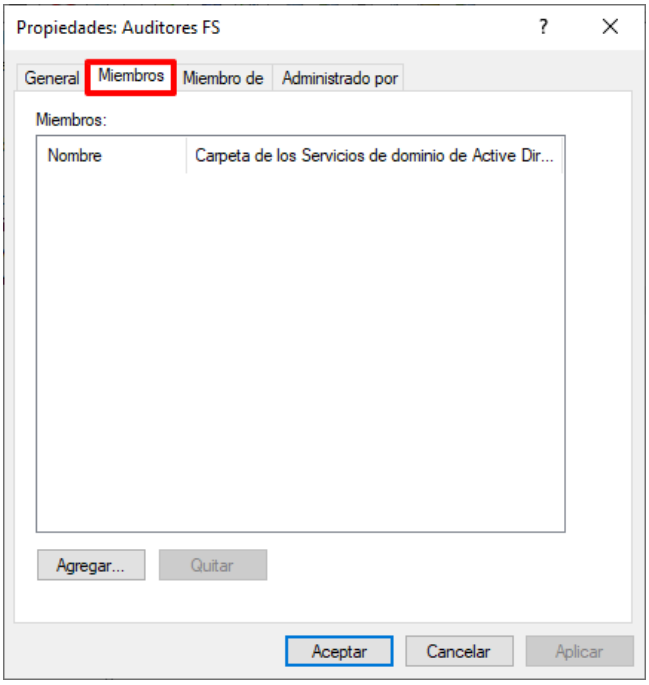
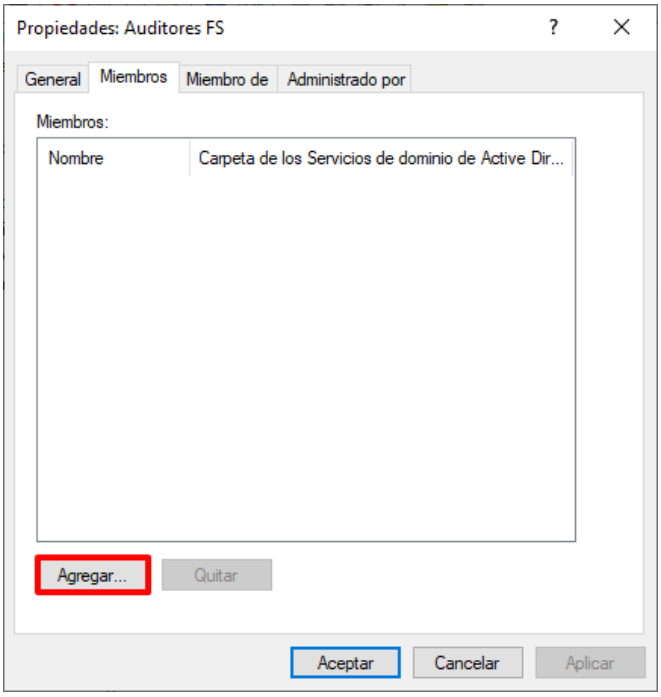
a) Auditoría de recursos compartidos.

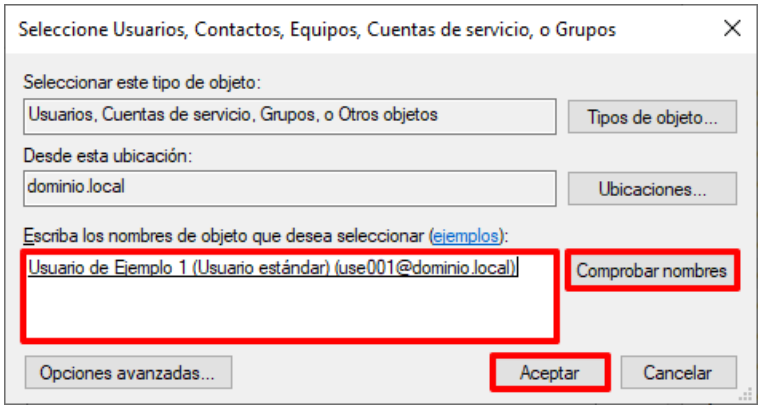
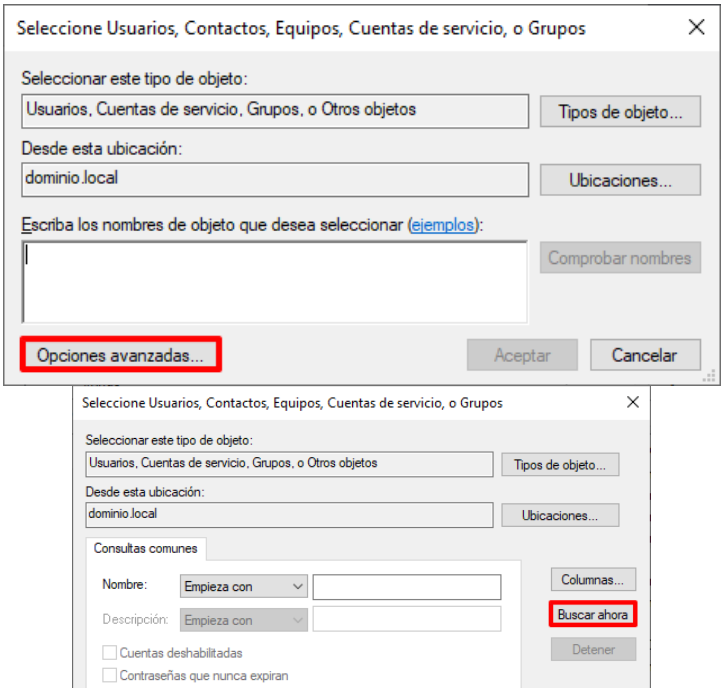
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

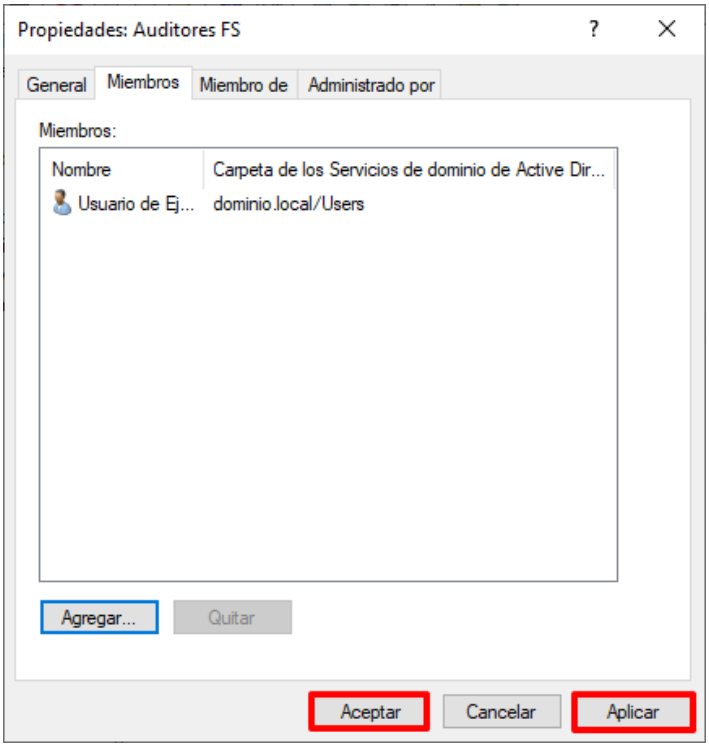
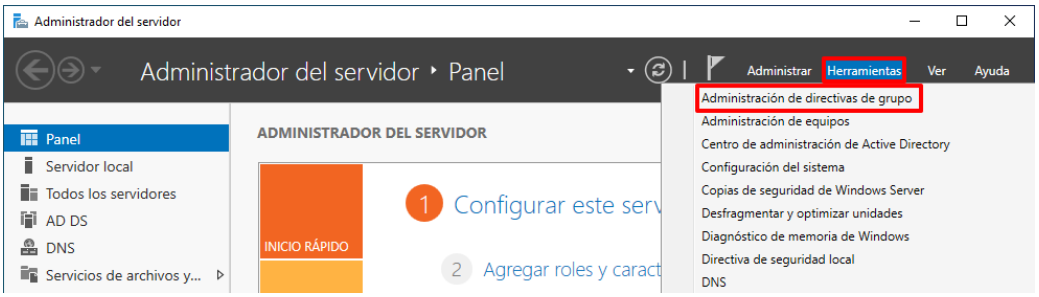
Paso	Descripción
141.	Inicie sesión en un servidor Controlador de Dominio del dominio. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
142.	Para la siguiente labor, será necesario la creación de grupos dedicados de modo que la capacidad de auditoría quede simplificada en la pertenencia a grupos. **Nota:** Si ya ejecutó anteriormente el Script "CCN-STIC-573 Servidor de Ficheros – Segregación de roles" en el "Paso 108" del presente apartado, continue en el "Paso 146". En caso contrario continúe en el siguiente punto.
143.	Si no desea realizar una creación de grupos personalizada o no dispone de estos grupos, diríjase al directorio "C:\Scripts" y ejecute el script "CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 
144.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

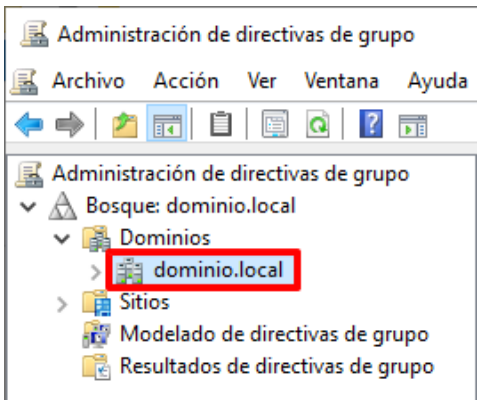
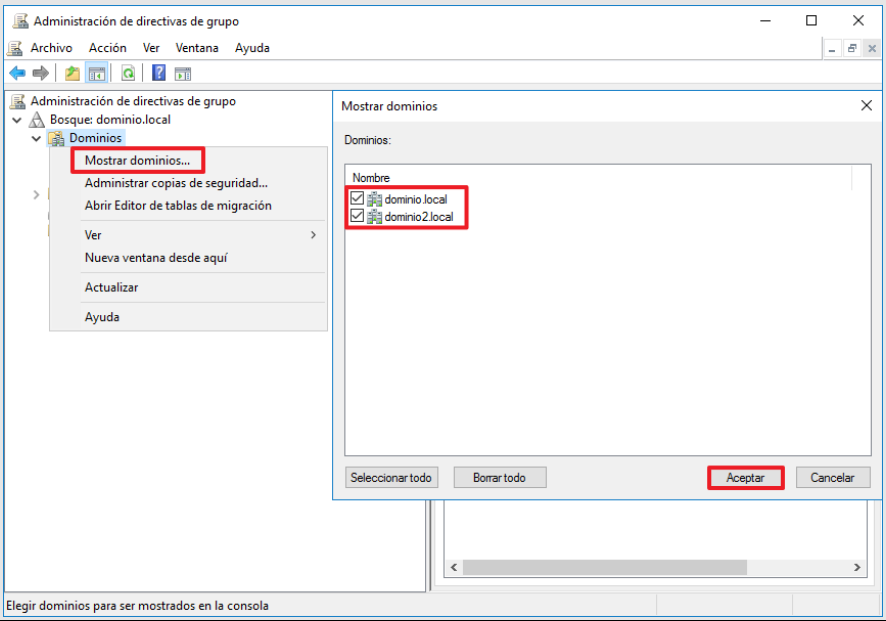
Paso	Descripción
145.	Tras la ejecución del script, entre los grupos generados se puede encontrar el siguiente grupo: – Auditores FS.
146.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

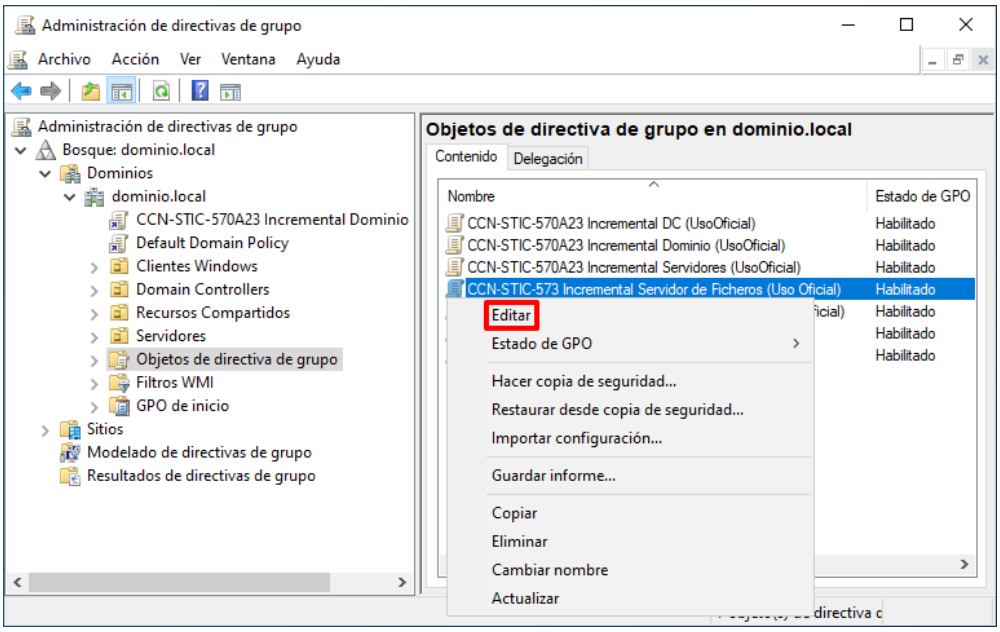
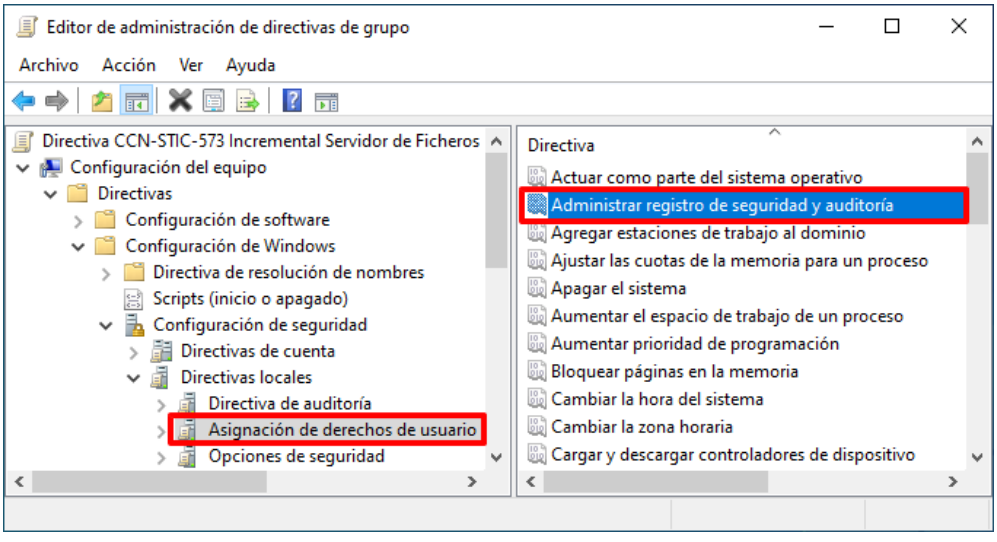
Paso	Descripción
147.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
148.	Sobre la consola “Usuarios y equipos de Active Directory”, seleccione y despliegue el nodo “<nombre de su dominio> → Users”. 

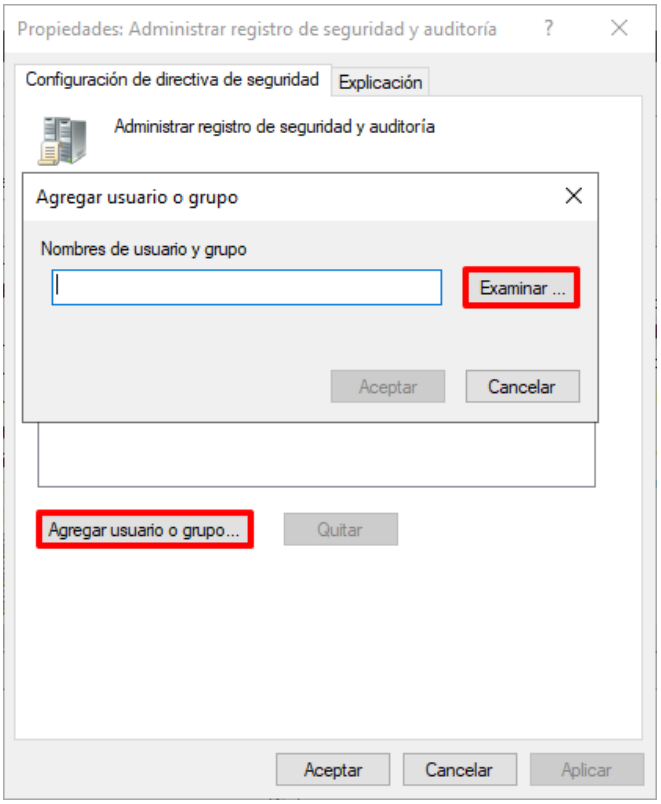
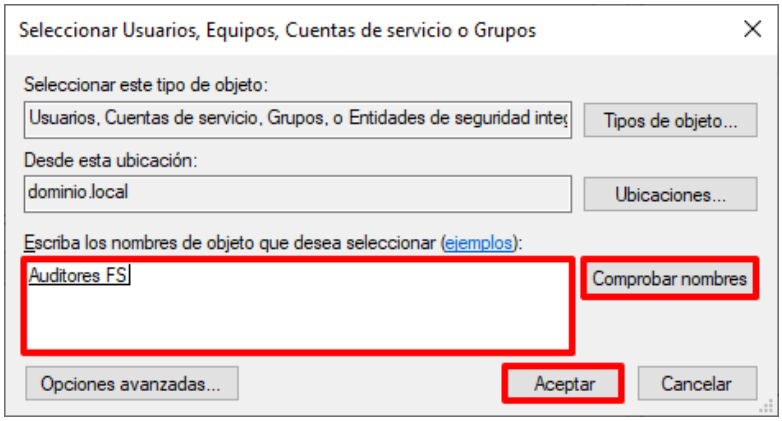
Paso	Descripción
149.	Haga doble clic sobre el grupo “Auditores FS” creado anteriormente y sitúese a continuación sobre la pestaña “Miembros”.  **Nota:** En este ejemplo se hace uso del grupo creado en pasos anteriores. Deberá adaptar los pasos descritos en caso de hacer uso de otro grupo de usuarios.
150.	En este ejemplo se va a añadir un par de usuarios para que dispongan de la capacidad de gestionar la auditoría para Servidores de Ficheros. Para ello, pulse sobre el botón “Agregar…”. 

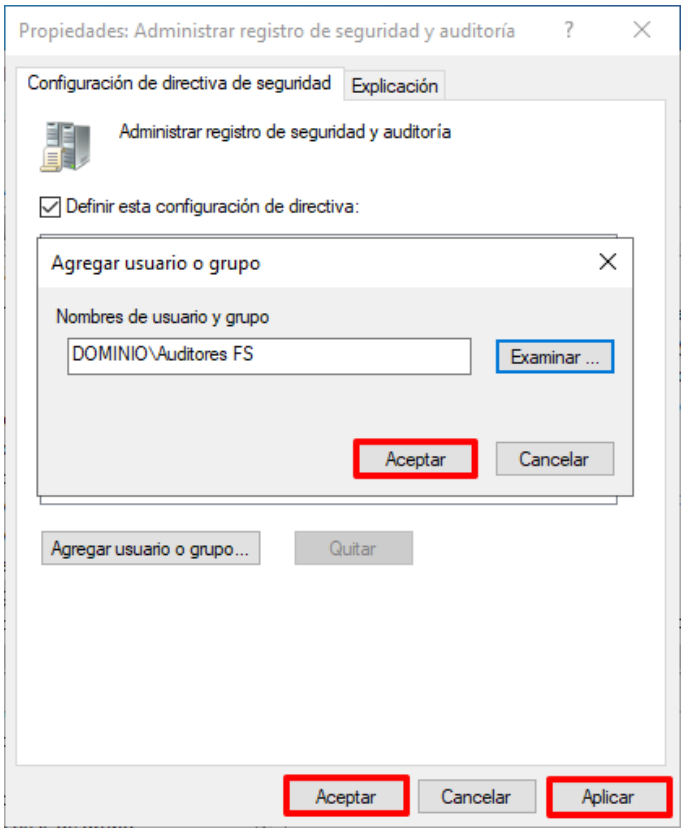
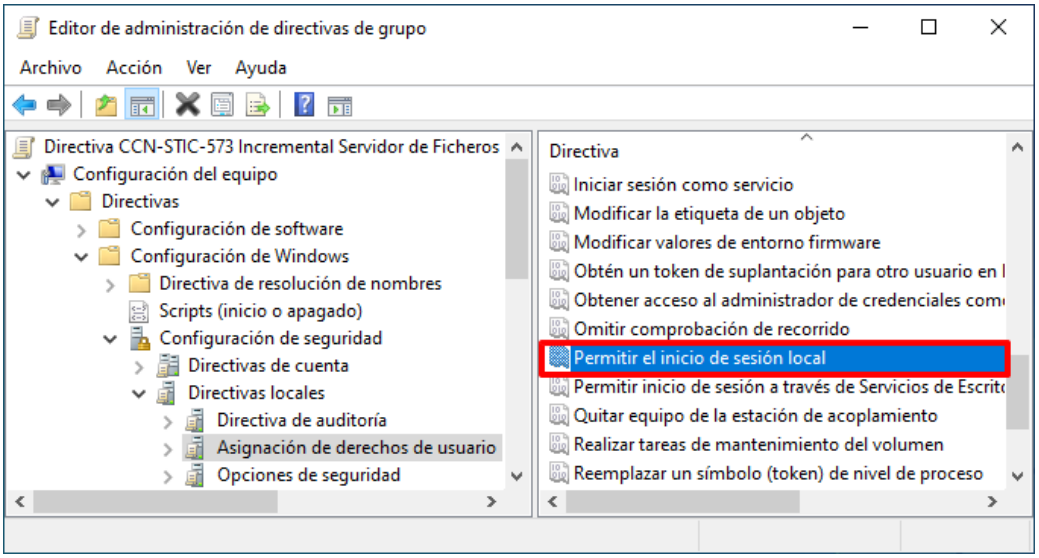
Paso	Descripción
151.	En la nueva ventana emergente introduzca el nombre de aquellas cuentas de usuario que desee que posean privilegios de auditoría sobre los equipos de tipo Servidor de Ficheros. Puede hacer uso del botón “Comprobar nombres” para identificar la cuenta de forma exacta y puede incluir varias cuentas separada por punto y coma (;). Pulse “Aceptar” cuando haya incluido a todos los usuarios o grupos necesarios.  **Nota:** En este ejemplo se hace uso del usuario: **use001**. Deberá evaluar que usuarios de su organización deben pertenecer a este grupo y adaptar esta configuración a las necesidades de su organización.
152.	Si desconoce las cuentas de usuario puede hacer uso del botón “Opciones avanzadas…” y en la nueva ventana “Buscar ahora” para listar todos los usuarios. Pulse “Aceptar” cuando haya finalizado de incluir a los usuarios. 

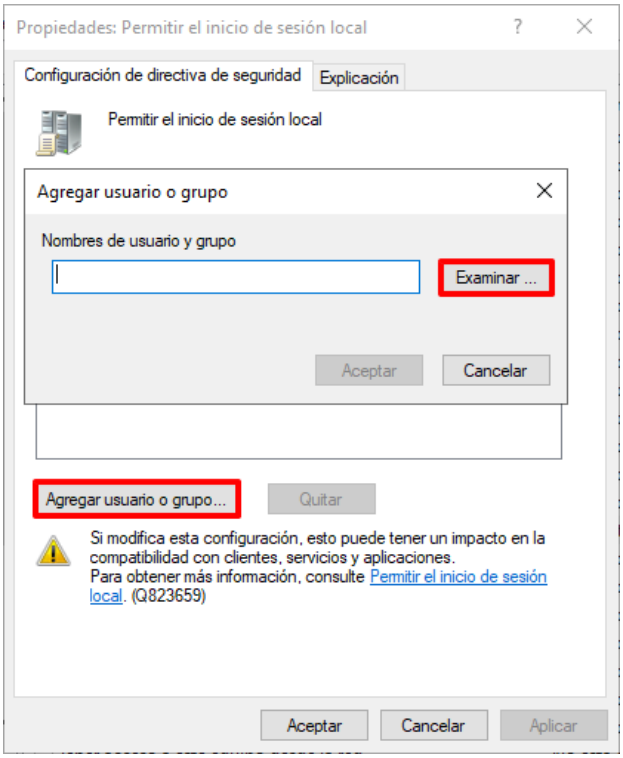
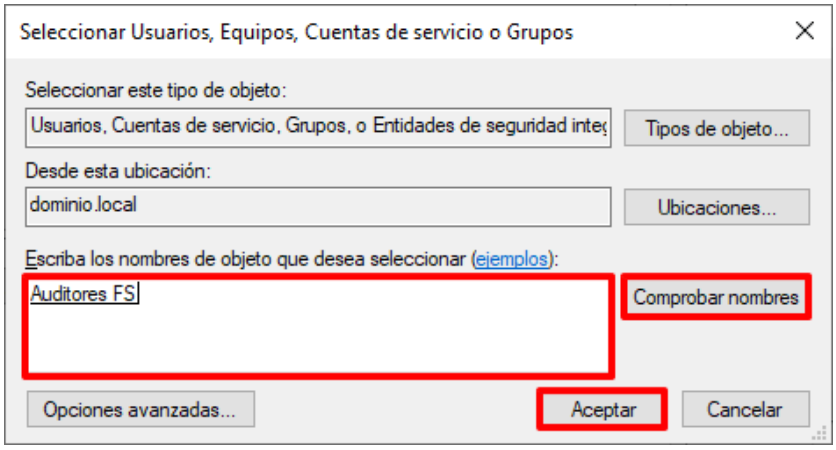
Paso	Descripción
153.	Pulse “Aplicar” y a continuación “Aceptar” para finalizar en la ventana “Propiedades: Auditores FS”. 
154.	A continuación, en el “Administrador del servidor”, en la parte superior derecha pulse sobre el botón “Herramientas” y seleccione “Administración de directivas de grupo”. 

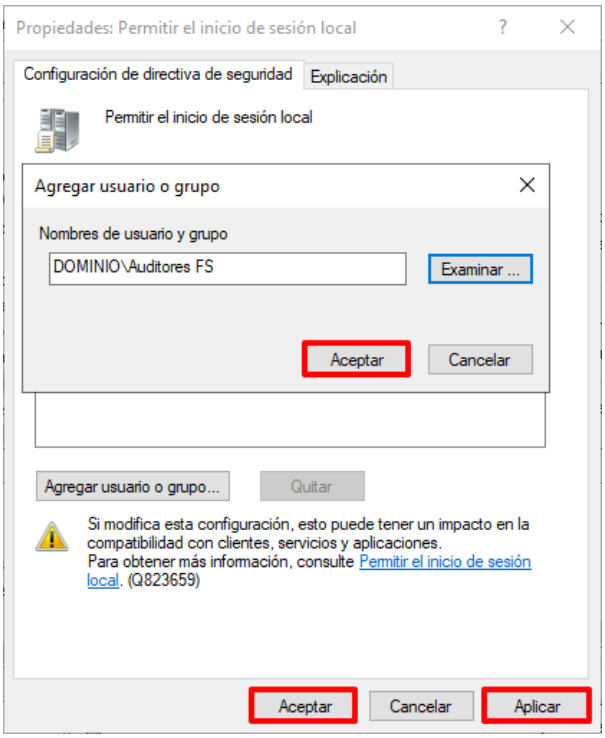
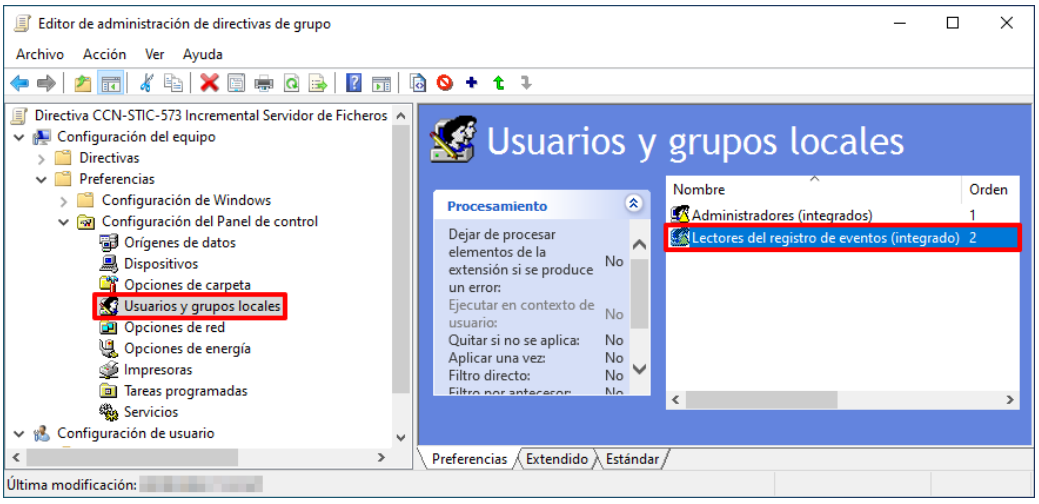
Paso	Descripción
155.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** Compruebe que realiza las tareas de administración sobre el dominio adecuado. Si no aparece su dominio en la ventana, utilice la opción "Mostrar dominios…" del menú contextual, marque los dominios que desea gestionar y pulse sobre "Aceptar" tal y como se indica a continuación. 

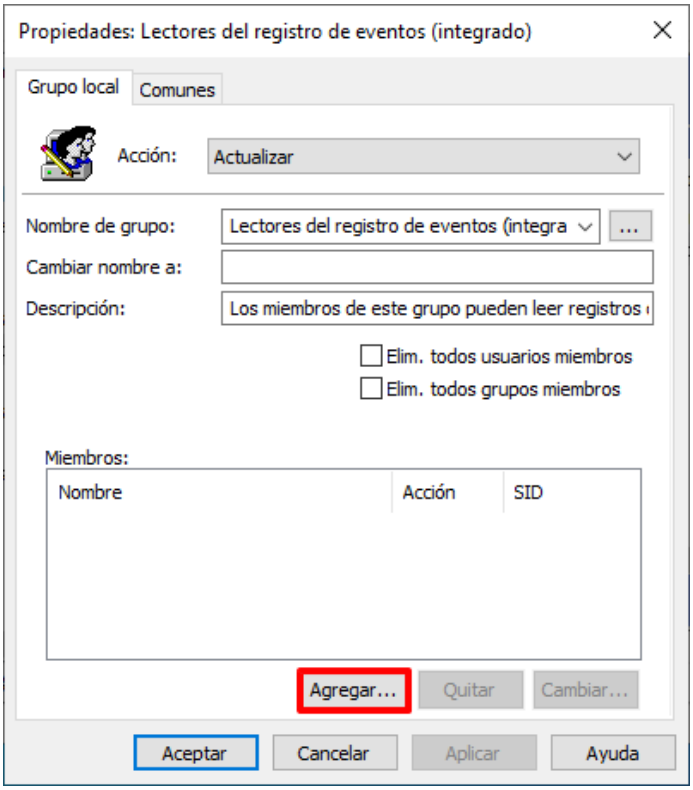
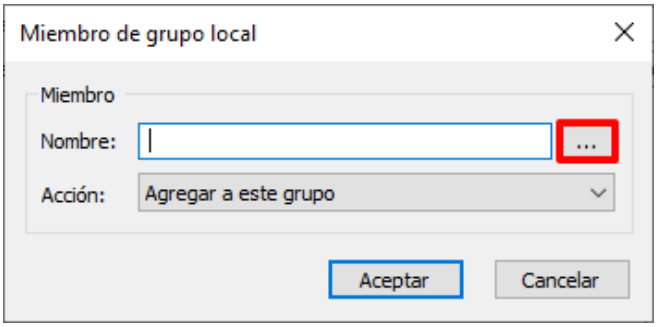
Paso	Descripción
156.	Seleccione con el botón derecho el objeto GPO “CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
157.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”**. A continuación, haga doble clic sobre la directiva **“Administrar registro de seguridad y auditoría”**. 

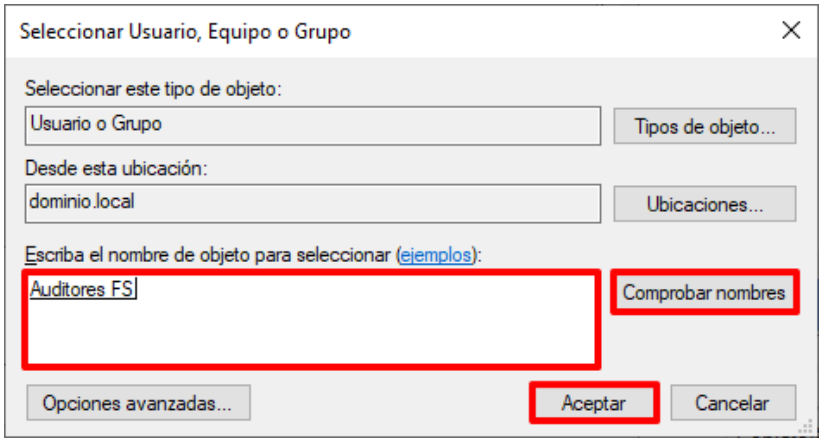
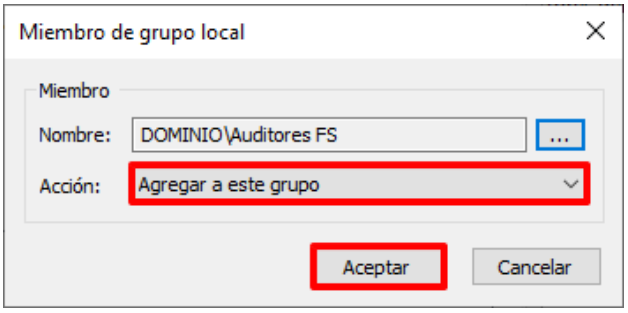
Paso	Descripción
158.	En la ventana emergente, pulse sobre “Agregar usuario o grupo…”. Pulse a continuación sobre “Examinar…”. 
159.	Introduzca el nombre del grupo “Auditores FS”, haga uso del botón “Comprobar nombres” para completar la información y pulse “Aceptar”.  **Nota:** El grupo “Auditores FS” habrá sido generado de forma automatizada si ha ejecutado previamente el script “CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual. Deberá adaptar esta configuración a las necesidades de su organización.

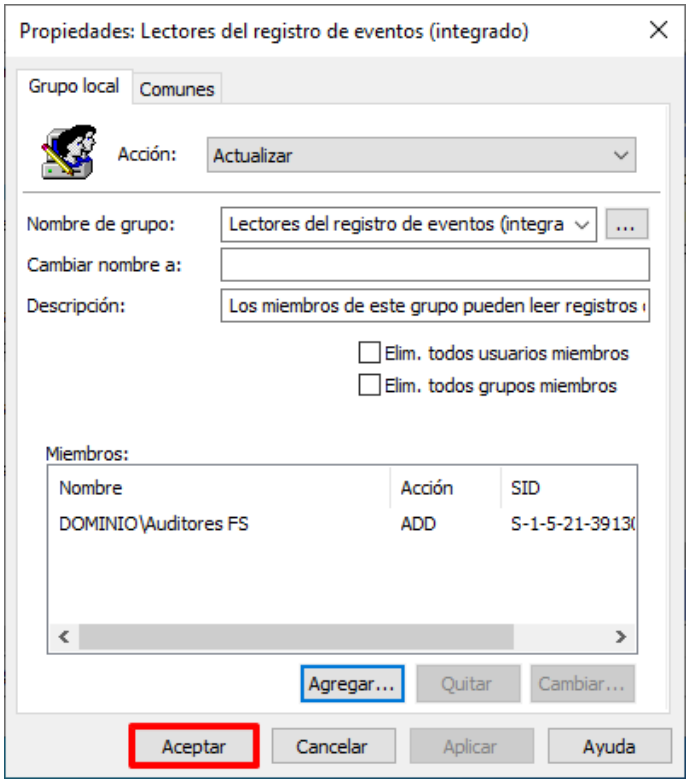
Paso	Descripción
160.	Pulse “Aceptar” en la ventana “Agregar usuario o grupo”. A continuación, pulse “Aplicar” y “Aceptar” y cierre el “Editor de administración de directivas de grupo”. 
161.	A continuación, haga doble clic sobre la directiva **“Permitir inicio de sesión local”**. 

Paso	Descripción
162.	En la ventana emergente, pulse sobre “Agregar usuario o grupo…”. Pulse a continuación sobre “Examinar…”. 
163.	Introduzca el nombre del grupo “Auditores FS”, haga uso del botón “Comprobar nombres” para completar la información y pulse “Aceptar”.  **Nota:** El grupo “Auditores FS” habrá sido generado de forma automatizada si ha ejecutado previamente el script “CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual. Deberá adaptar esta configuración a las necesidades de su organización.

Paso	Descripción
164.	Pulse “Aceptar” en la ventana “Agregar usuario o grupo”. A continuación, pulse “Aplicar” y “Aceptar” y cierre el “Editor de administración de directivas de grupo”. 
165.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) → Configuración del equipo → Preferencias → Configuración del Panel de control → Usuarios y grupos locales”**. En el panel derecho identifique el grupo “Lectores del registro de eventos (integrado)” y haga doble clic sobre el mismo. 

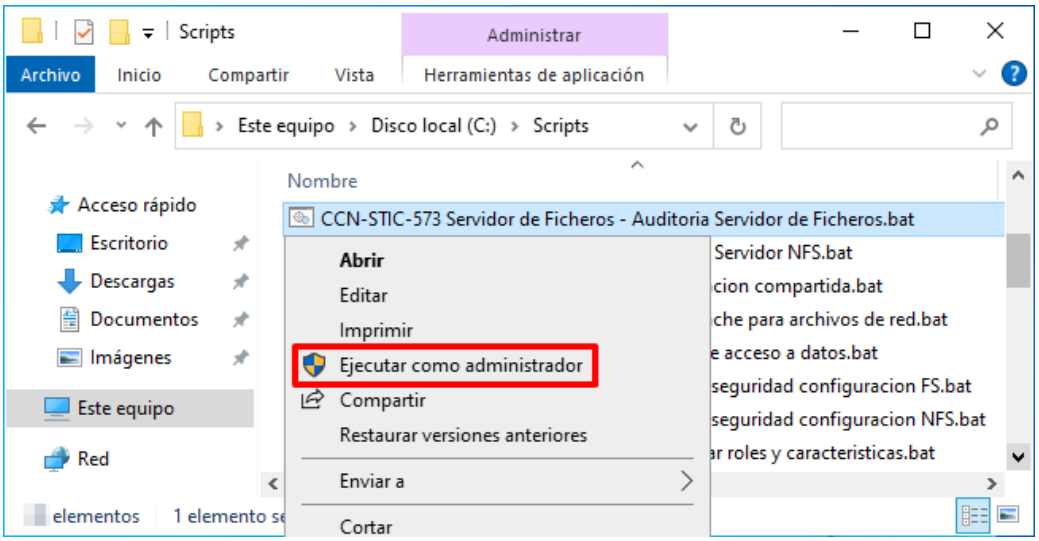
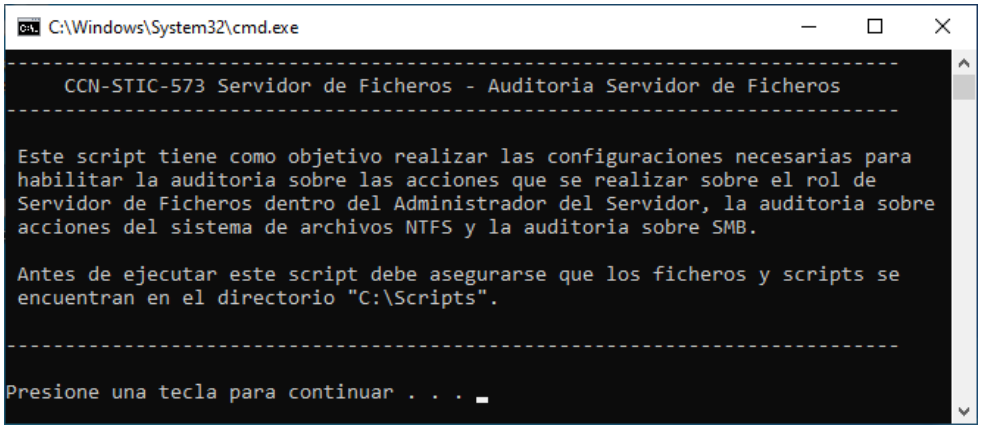
Paso	Descripción
166.	Pulse sobre el botón “Agregar…” para continuar. 
167.	En la nueva ventana emergente pulse sobre el botón “…”. 

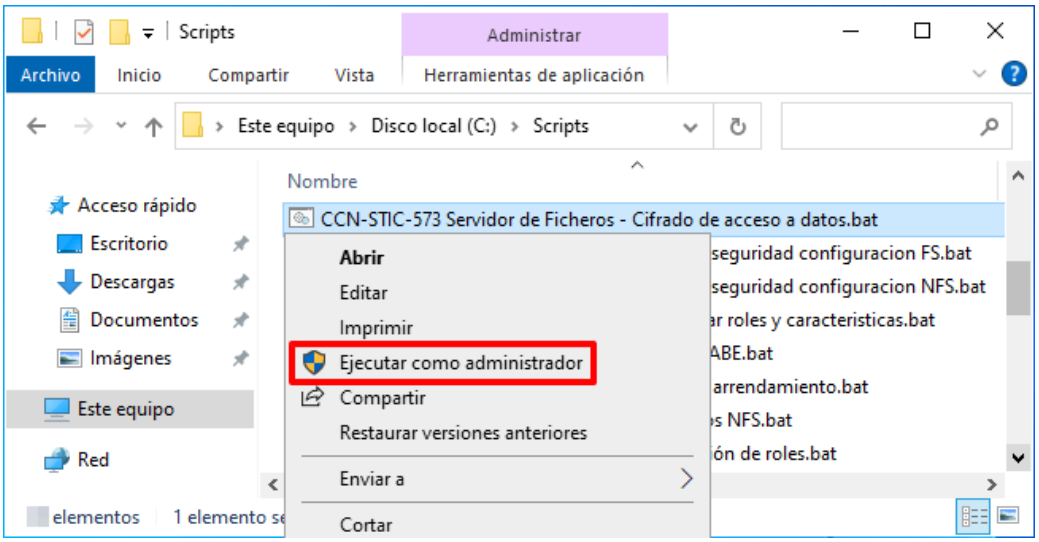
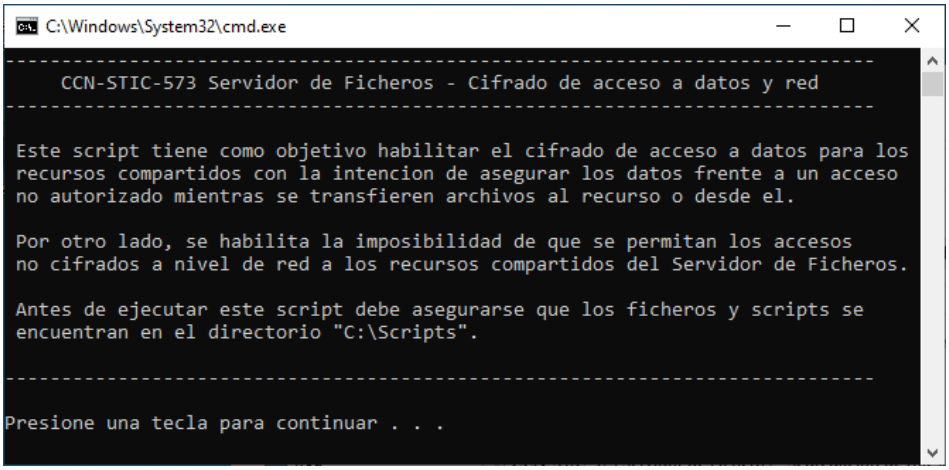
Paso	Descripción
168.	Escriba el nombre del grupo que desea incluir en el grupo integrado “Lectores del registro de eventos”. En este ejemplo, será el generado a través del script ejecutado en pasos anteriores (“Auditores FS”). Pulse sobre “Comprobar nombres” para completar el nombre y pulse “Aceptar”.  **Nota:** El grupo “Auditores FS” habrá sido generado de forma automatizada si ha ejecutado previamente el script “CCN-STIC-573 Servidor de Ficheros – Segregación de roles.bat”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual. Deberá adaptar esta configuración a las necesidades de su organización.
169.	En la anterior ventana emergente asegúrese de que la acción a realizar es “Agregar a este grupo” y pulse el botón “Aceptar”. 

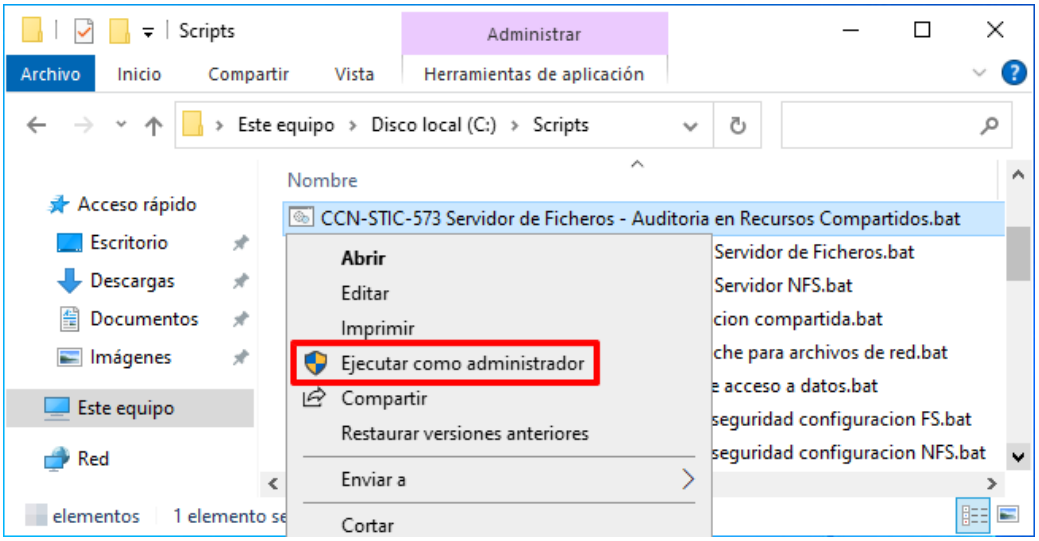
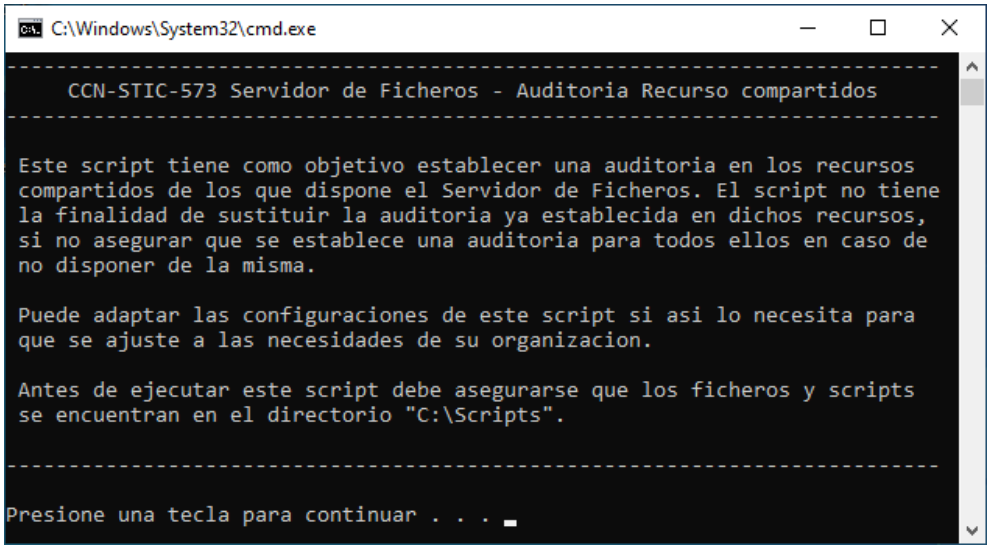
Paso	Descripción
170.	Para finalizar, pulse de nuevo sobre el botón “Aceptar”. 
171.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo el acceso los equipos de tipo Servidor de Ficheros para su gestión con privilegios para establecer configuraciones de auditoría sobre los recursos compartidos. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.

ANEXO A.2.6. MECANISMO DE AUTENTICACIÓN Y REGISTRO DE LA ACTIVIDAD

El presente punto tiene como objetivo ayudar a los administradores a complementar las opciones de auditoría ya implementadas dentro del sistema operativo Windows Server, centrándose en los recursos compartido que proporciona un equipo con el rol de Servidor de Ficheros.

Paso	Descripción
172.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
173.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Auditoria Servidor de Ficheros.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 
174.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

Paso	Descripción
175.	Ejecute ahora el script “CCN-STIC-573 Servidor de Ficheros - Cifrado de acceso a datos.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
176.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

Paso	Descripción
177.	Posteriormente ejecute el script “CCN-STIC-573 Servidor de Ficheros - Auditoria en Recursos Compartidos.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
178.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

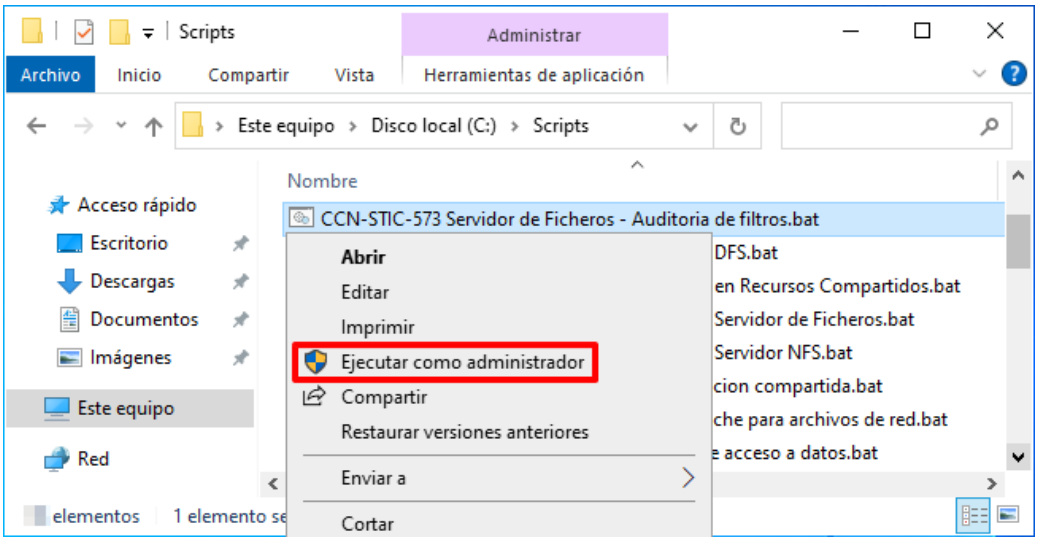
ANEXO A.2.6.1. REGISTRO DE LA ACTIVIDAD (USO OFICIAL – MATERIAS CLASIFICADAS)

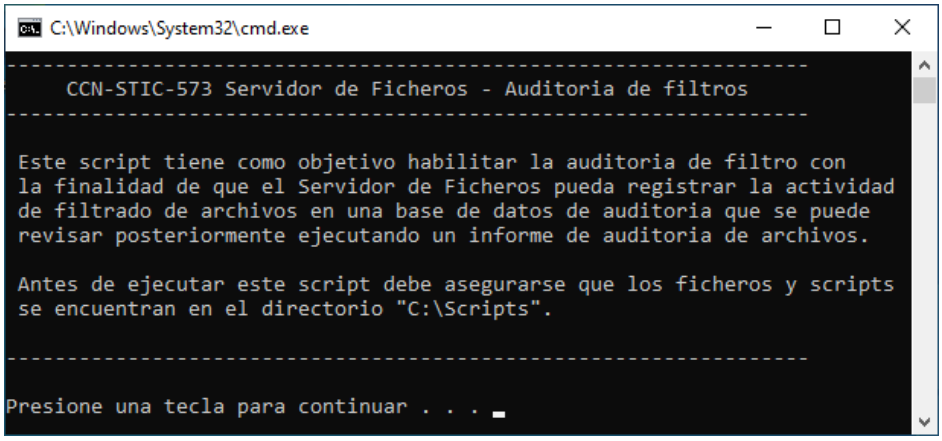
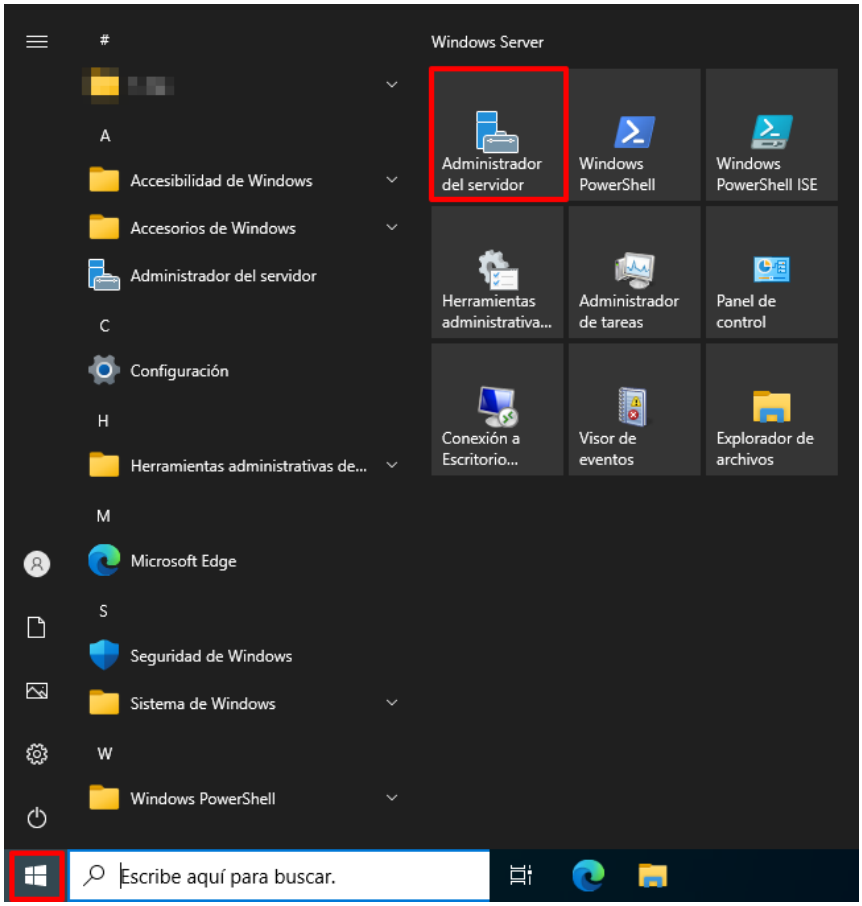
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

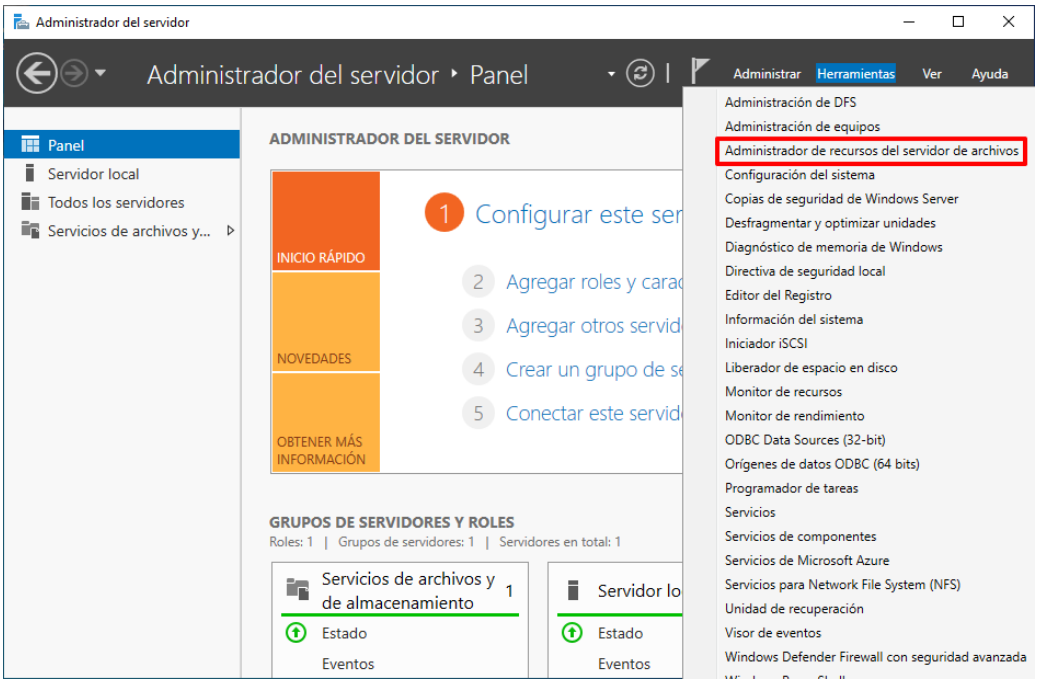
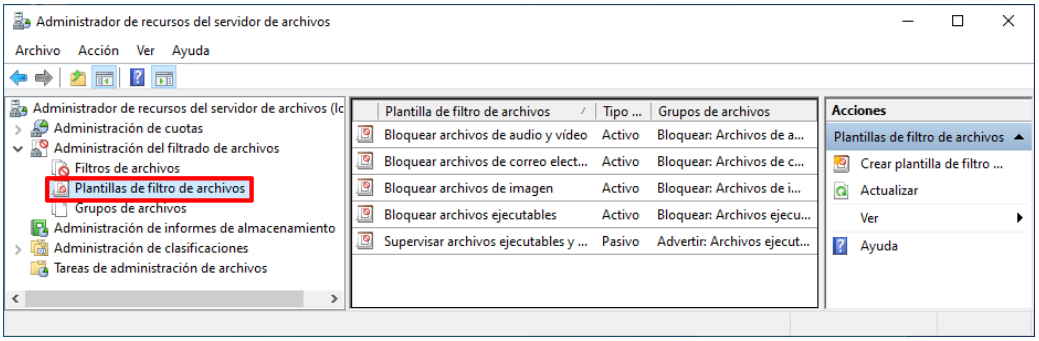
Nota: Deberá disponer del rol "Administrador de recursos del servidor de archivos" instalador para poder hacer uso de esta consola y sus servicios. Instale dicho rol en caso de no disponer del mismo.

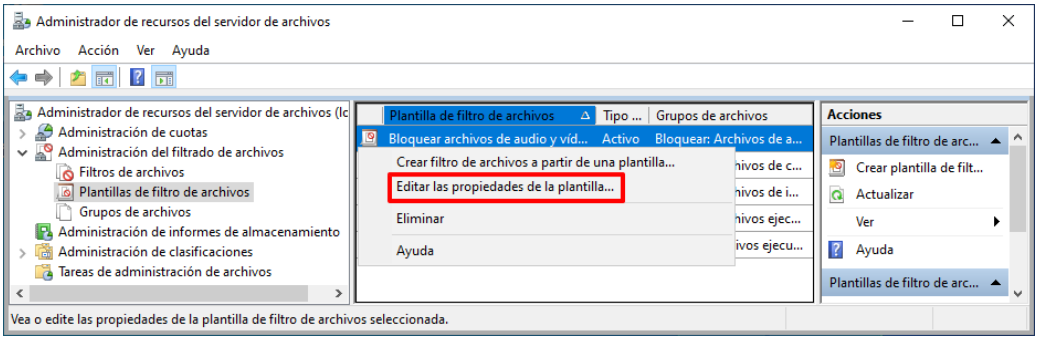
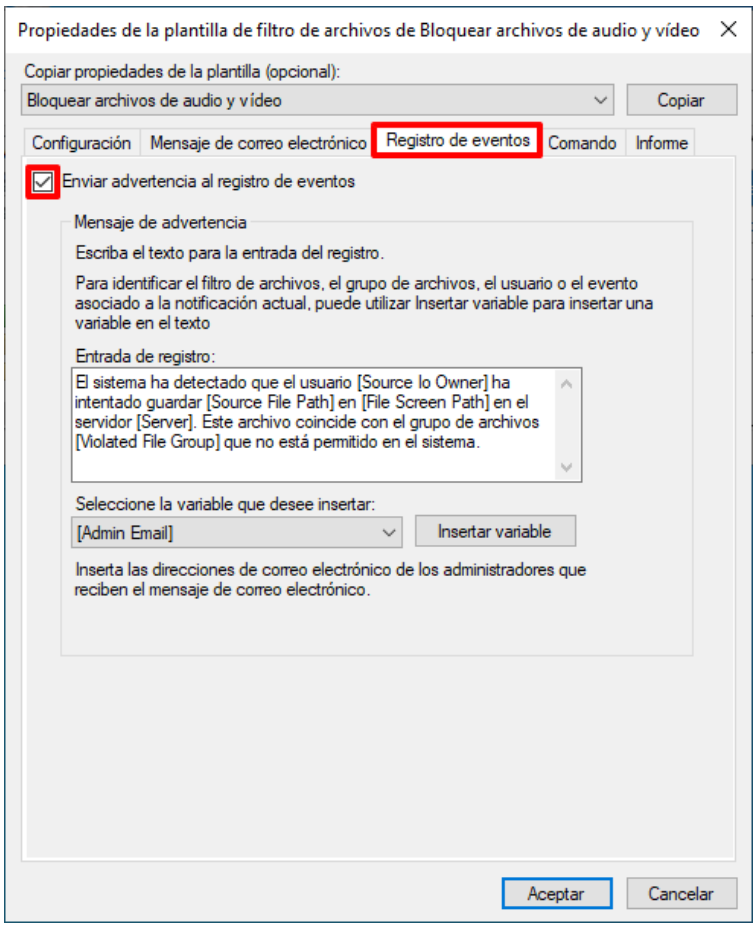
A continuación, se definirán los pasos que permitan establecer las configuraciones para registrar eventos adicionales relacionados con la inclusión de ficheros que pudieran nos estar autorizados a estar alojados en el servidor de ficheros.

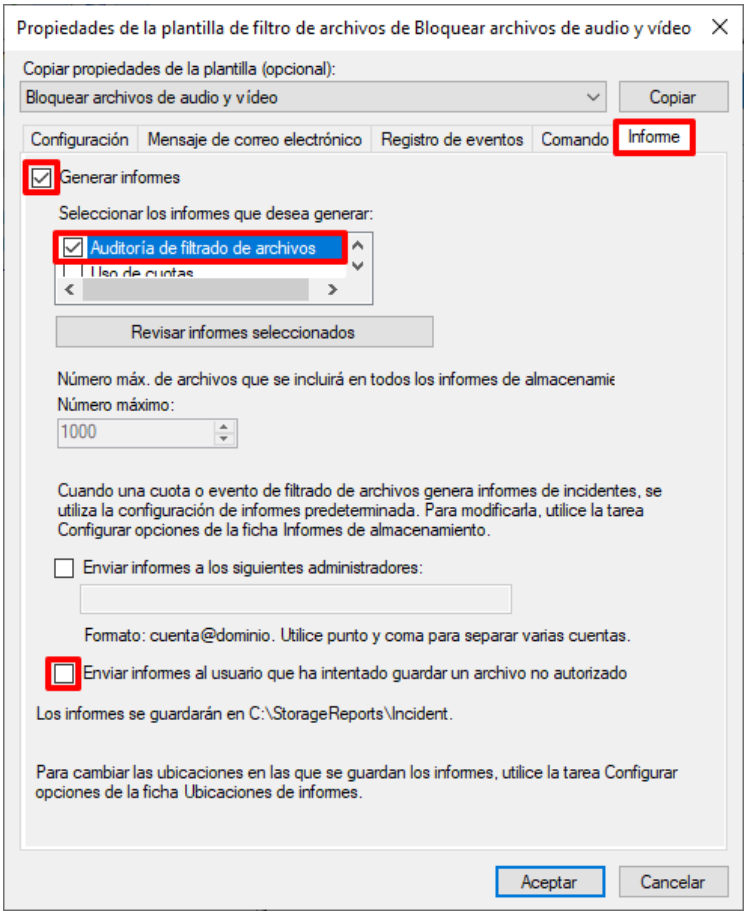
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

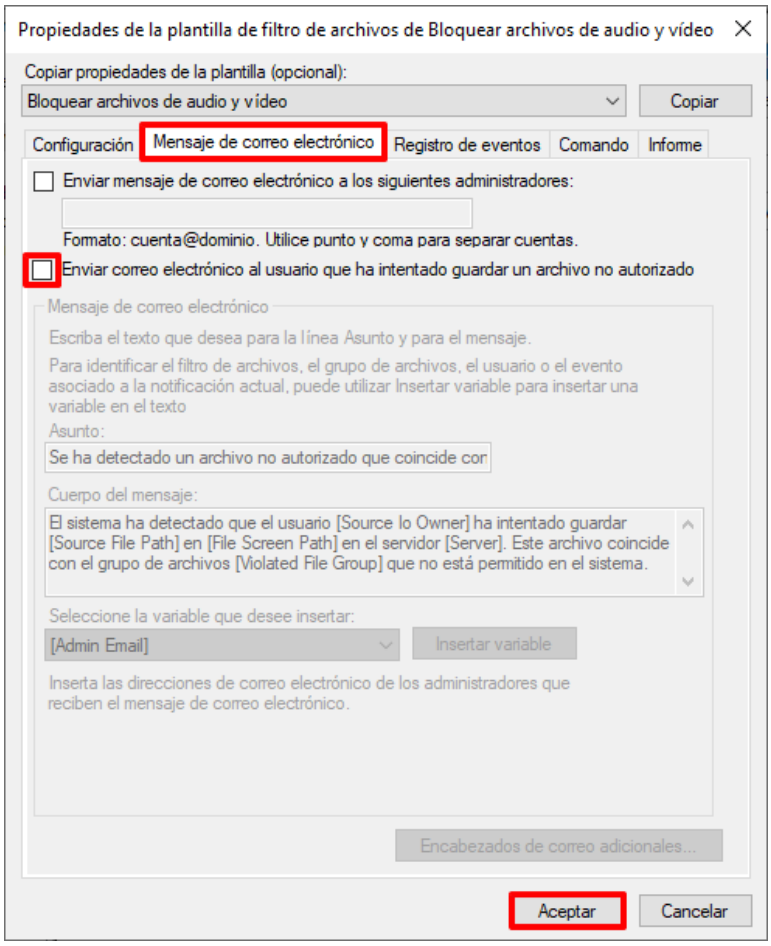
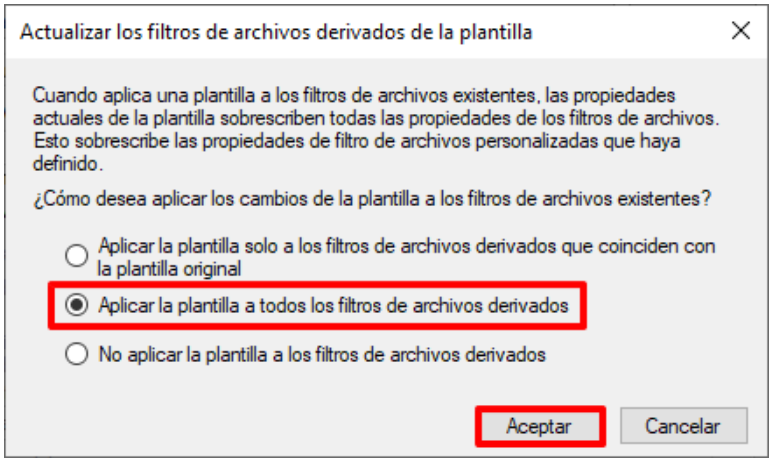
Paso	Descripción
179.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
180.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Auditoria de filtros.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 

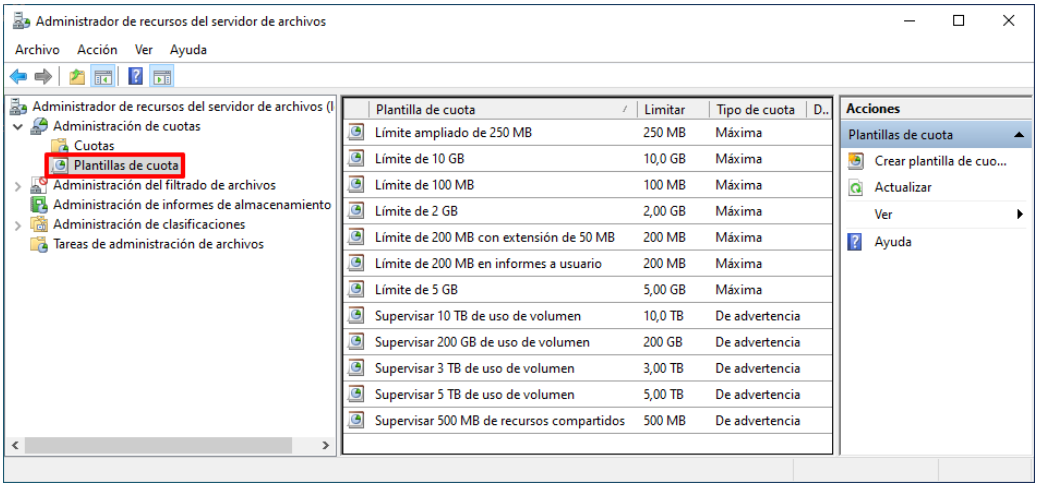
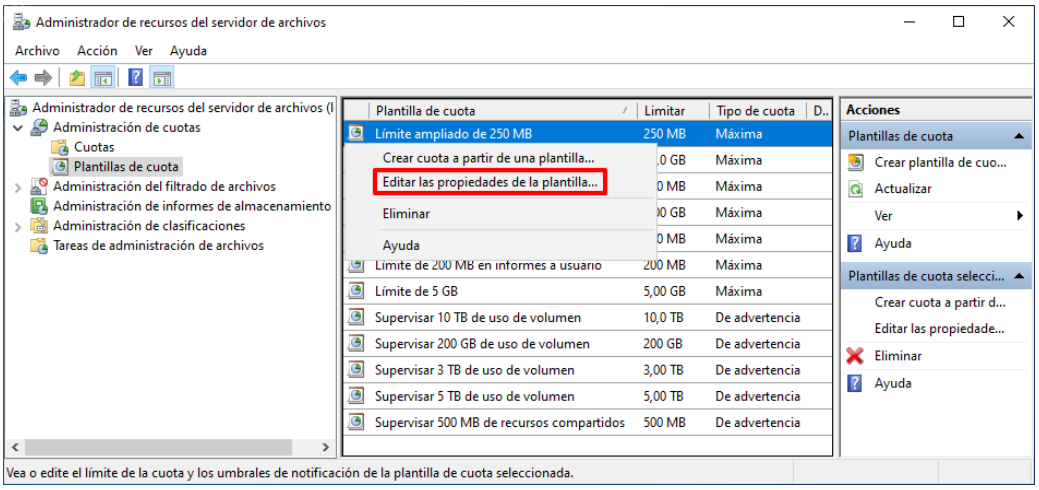
Paso	Descripción
181.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
182.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

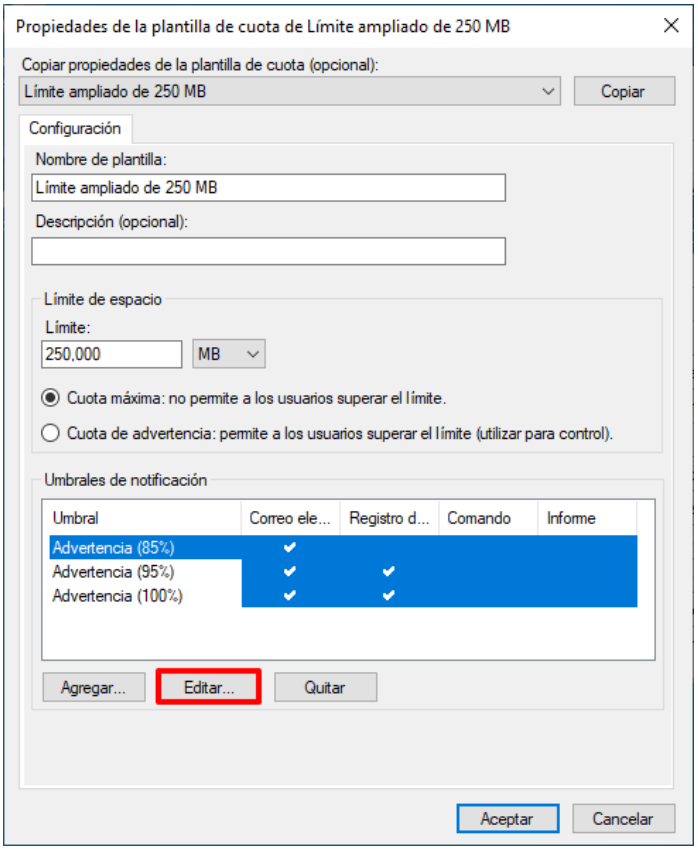
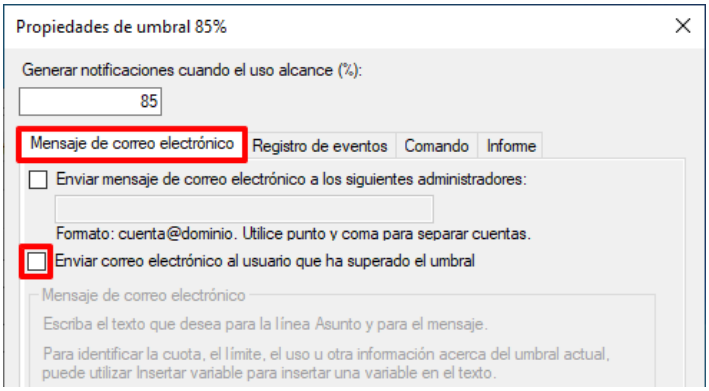
Paso	Descripción
183.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administrador de recursos del servidor de archivos”.  **Nota:** Deberá disponer del rol “Administrador de recursos del servidor de archivos” instalador para poder hacer uso de esta consola y sus servicios.
184.	Ahora diríjase al nodo “Administración del filtrado de archivos”, expándalo y seleccione el apartado “Plantillas de filtro de archivos”. 

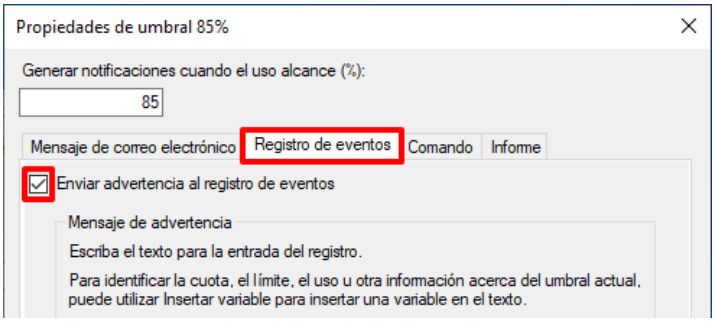
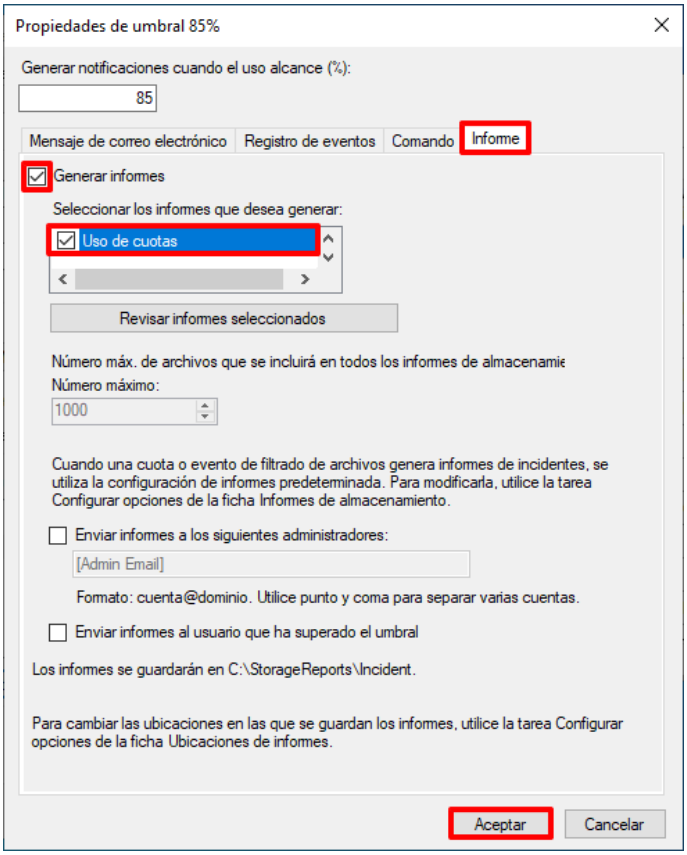
Paso	Descripción
185.	Haga clic derecho sobre una de las plantillas y seleccione la opción “Editar las propiedades de la plantilla…” del menú contextual.  **Nota:** Es indiferente la plantilla seleccionada dado que estas acciones deberán realizarse sobre todas las plantillas disponibles. Para este ejemplo se hace uso de la plantilla por defecto “Bloquear archivos de audio y vídeo”.
186.	Acceda a la pestaña “Registro de eventos” y verifique que se encuentra marcada la opción “Enviar advertencia al registro de eventos”.  **Nota:** Si lo desea puede editar el mensaje de entrada en el registro.

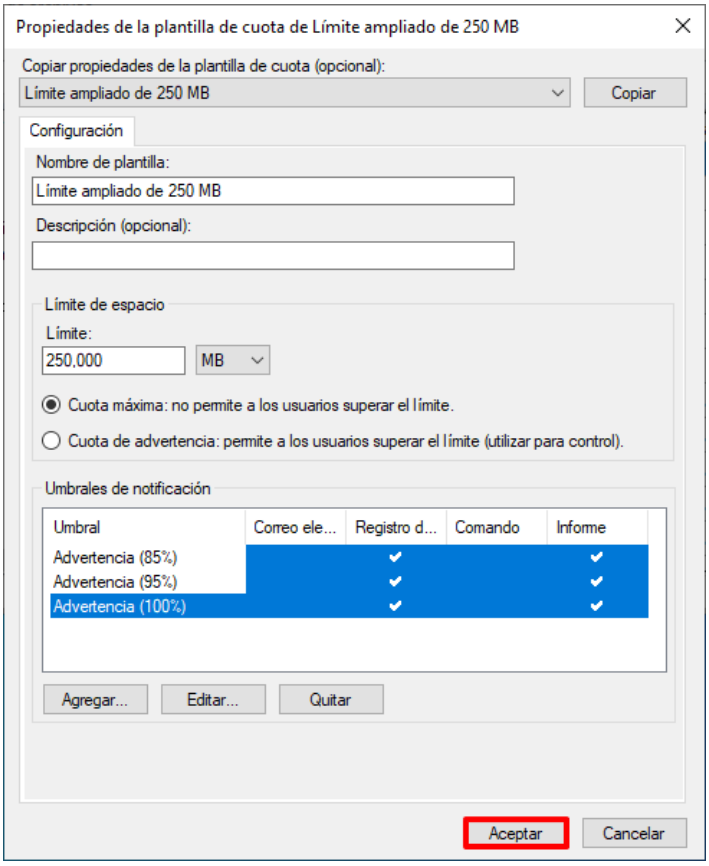
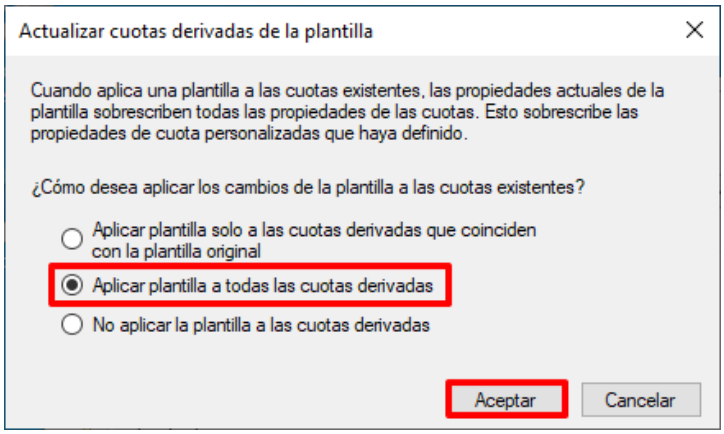
Paso	Descripción
187.	A continuación, diríjase a la pestaña “Informe”. Marque posteriormente la opción “Generar informes” y seleccione dentro del apartado “Seleccionar los informes que desea generar:” la opción “Auditoría de filtrado de archivos”. De igual modo asegúrese que se encuentra desmarcada la opción “Enviar informes al usuario que ha intentado guardar un archivo no autorizado.  **Nota:** Por defecto los informes se alojan en la ruta “C:\StorageReports\Incident”. De igual modo, dependiendo de la información que quiera o como la desee recopilar deberá seleccionar informes adicionales.

Paso	Descripción
188.	Por último, diríjase a la pestaña “Mensaje de correo electrónico” y desmarque la opción “Enviar correo electrónico al usuario que ha intentado guardar un archivo no autorizado”. Pulse “Aceptar” para finalizar. 
189.	En la ventana emergente que aparecerá marque la opción “Aplicar la plantilla a todos los filtros de archivos derivados” y pulse “Aceptar”. 

Paso	Descripción
190.	Realice de nuevo los pasos “185” a “189” para todas las plantillas de filtro de archivos disponibles.
191.	Despliegue ahora el nodo “Administración de cuotas” y seleccione el apartado “Plantillas de cuota”. 
192.	Haga clic derecho sobre una de las plantillas y seleccione la opción “Editar las propiedades de la plantilla…” del menú contextual.  **Nota:** Es indiferente la plantilla seleccionada dado que estas acciones deberán realizarse sobre todas las plantillas disponibles. Para este ejemplo se hace uso de la plantilla por defecto “Límite ampliado de 250 MB”.

Paso	Descripción
193.	En la nueva ventana emergente, dentro del apartado “Umbrales de notificación” seleccione uno de los umbrales y pulse sobre la opción “Editar…”.  **Nota:** Es indiferente el umbral seleccionado dado que estas acciones deberán realizarse sobre todos los umbrales definidos.
194.	En la pestaña “Mensaje de correo electrónico” desmarque la opción “Enviar correo electrónico al usuario que ha superado el umbral”. 

Paso	Descripción
195.	Diríjase ahora a la pestaña “Registro de eventos” y marque la opción “Enviar advertencia al registro de eventos”.  **Nota:** Si lo desea puede editar el mensaje de entrada en el registro.
196.	A continuación, diríjase a la pestaña “Informe”. Marque posteriormente la opción “Generar informes” y seleccione dentro del apartado “Seleccionar los informes que desea generar:” la opción “Uso de cuotas”. Pulse “Aceptar” para finalizar.  **Nota:** Por defecto los informes se alojan en la ruta “C:\StorageReports\Incident”. De igual modo, dependiendo de la información que quiera o como la desee recopilar deberá seleccionar informes adicionales.
197.	Repita los pasos “193” a “196” para cada uno de los umbrales definidos.

Paso	Descripción
198.	Cuando haya finalizado pulse sobre el botón “Aceptar”. 
199.	En la ventana emergente que aparecerá marque la opción “Aplicar plantilla a todas las cuotas derivadas” y pulse “Aceptar”. 
200.	Realice de nuevo los pasos “192” a “199” para todas las plantillas de filtro de archivos disponibles.

ANEXO A.2.7. CONFIGURACIÓN DE SEGURIDAD Y GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

En el presente apartado, se definirán los pasos y acciones que tienen como objetivo cumplir la regla de "mínima funcionalidad".

Para lograr el objetivo anterior se describen dos alternativas:

a) Por un lado, se facilitará un script que permita desinstalar aquellos roles y características consideradas no necesarias dentro de un equipo de tipo Servidor Miembro de un dominio que haga las veces de Servidor de Ficheros.

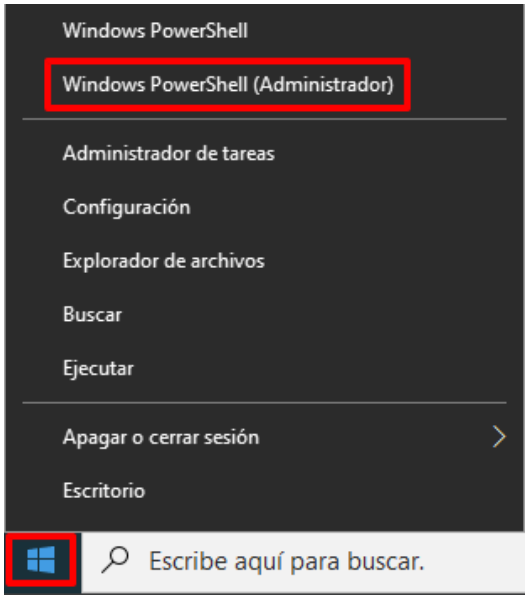
b) Por otra parte, se facilitará un paso a paso con información sobre como desinstalar roles y/o características de forma gráfica y manual.

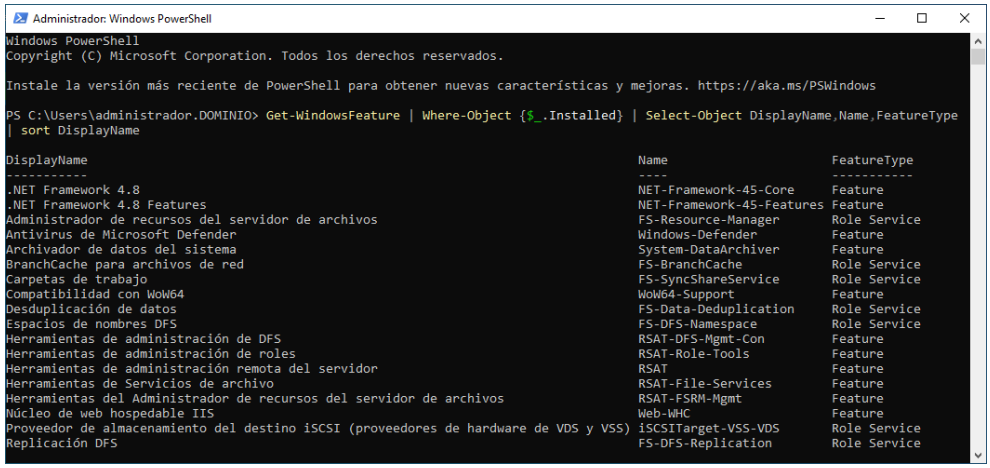
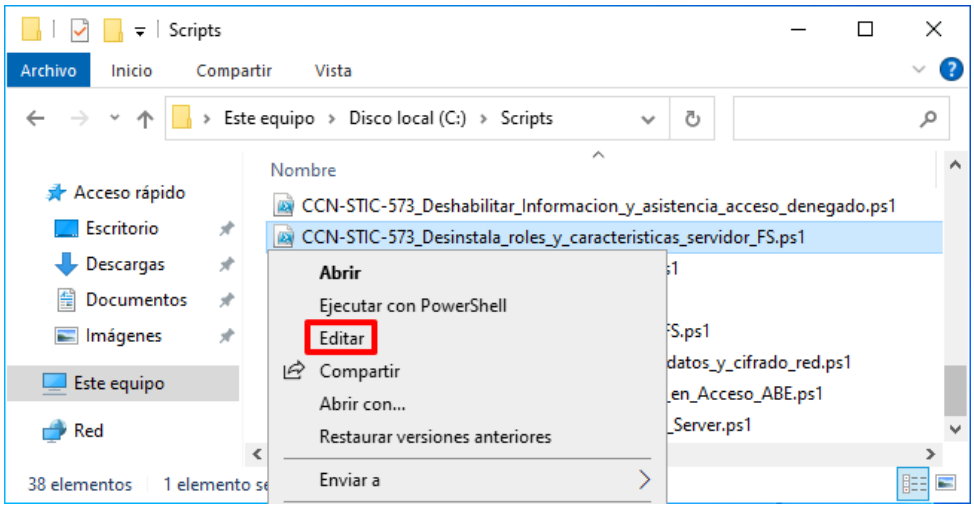
c) Por último, se aplicarán configuraciones de seguridad adicionales sobre el rol de Servidor de Ficheros con el objetivo de mejorar la seguridad en el mismo.

Por otro lado, se realizarán configuraciones adicionales asociadas a la gestión del servidor de ficheros.

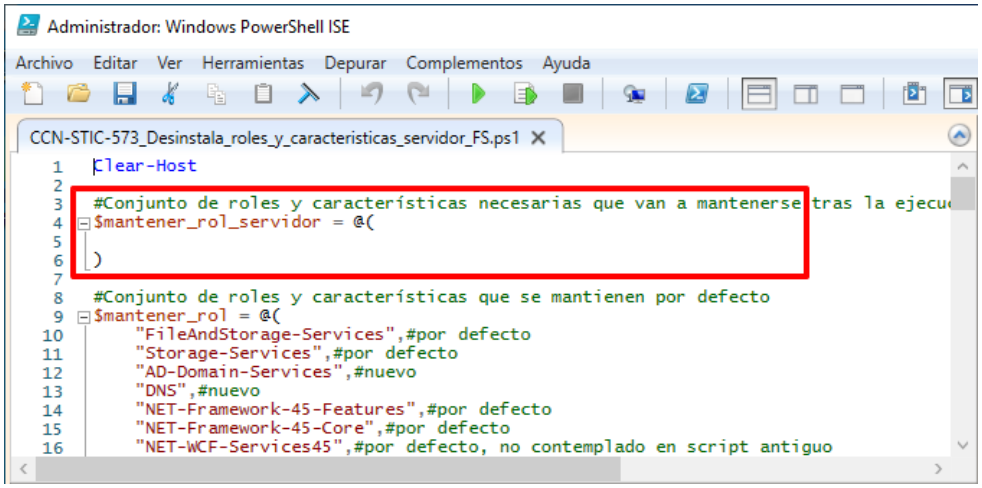
Nota: Si desea ejecutar esta acción de forma manual, vaya al "Paso 214" de este apartado.

Por otro lado, para continuar con las siguientes acciones relacionadas a la configuración de seguridad diríjase al "Paso 225".

Paso	Descripción
201.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
202.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Windows PowerShell (Administrador)". 

Paso	Descripción
203.	En la consola de PowerShell ejecute el siguiente comando para conocer aquellos roles y características instaladas en el equipo.
	> Get-WindowsFeature | Where-Object {$_.Installed} | Select-Object DisplayName,Name,FeatureType | Sort DisplayName
	 **Nota:** Puede redirigir la salida del comando a un fichero si lo desea con el objetivo de evaluar mejor la información mostrada. Para ello, ejecute el siguiente comando: Get-WindowsFeature | Where-Object {$_.Installed} | Select-Object DisplayName,Name,FeatureType | Sort DisplayName | Out-File "C:\[Ruta]\[Nombre_Fichero].txt
204.	A continuación, **EVALÚE** y **DETERMINE** aquellos roles y características **QUE NO SON NECESARIAS ELIMINAR** y anótelos. Deberá anotar los elementos ubicados en la columna "Name".
205.	Diríjase al directorio "C:\Scripts", haga clic derecho sobre el fichero "CCN-STIC-573_Desinstala_roles_y_caracteristicas_servidor_FS.ps1" y seleccione la opción del menú contextual "Editar". Con ello se abrirá una ventana de Windows PowerShell ISE. 

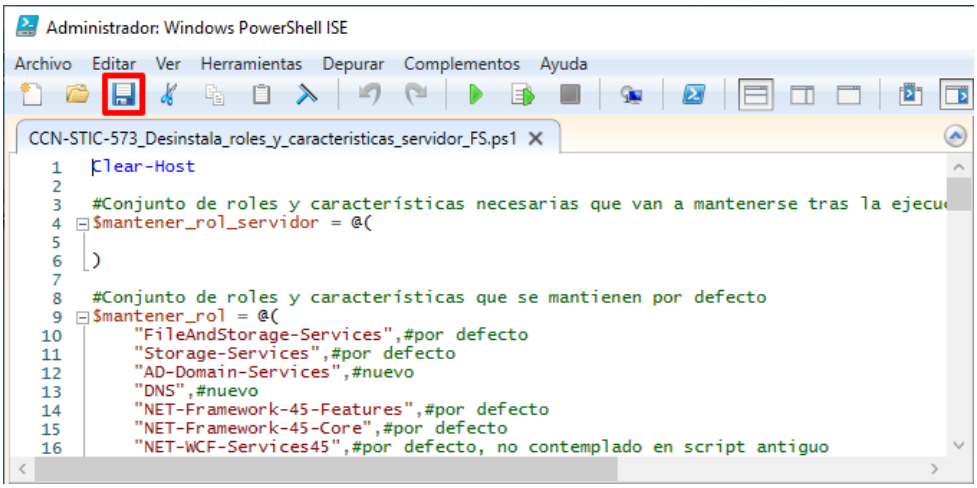
Paso	Descripción
206.	Dentro de la ventana de PowerShell ISE, al inicio del script identifique la línea donde se indica "$mantener_rol_servidor". Dentro de la citada línea deberá incluir aquellos roles y características anotadas en pasos anteriores. Deberá **incluir los nombres entre comillas ("") y separados por comas (,)**.

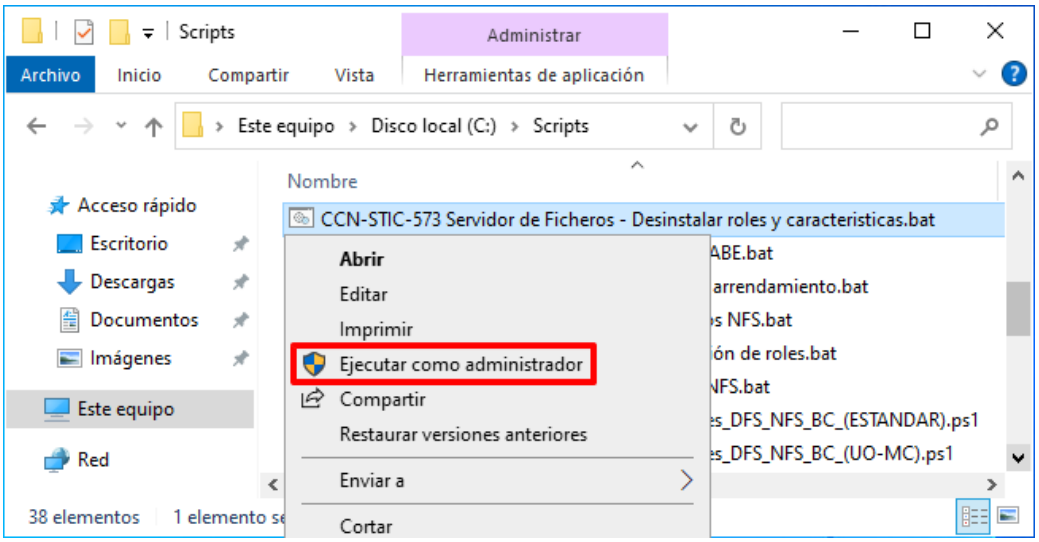
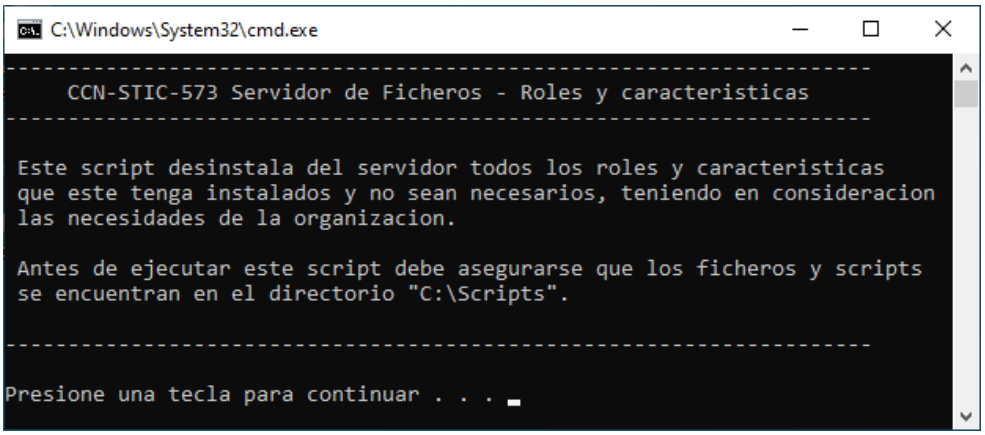


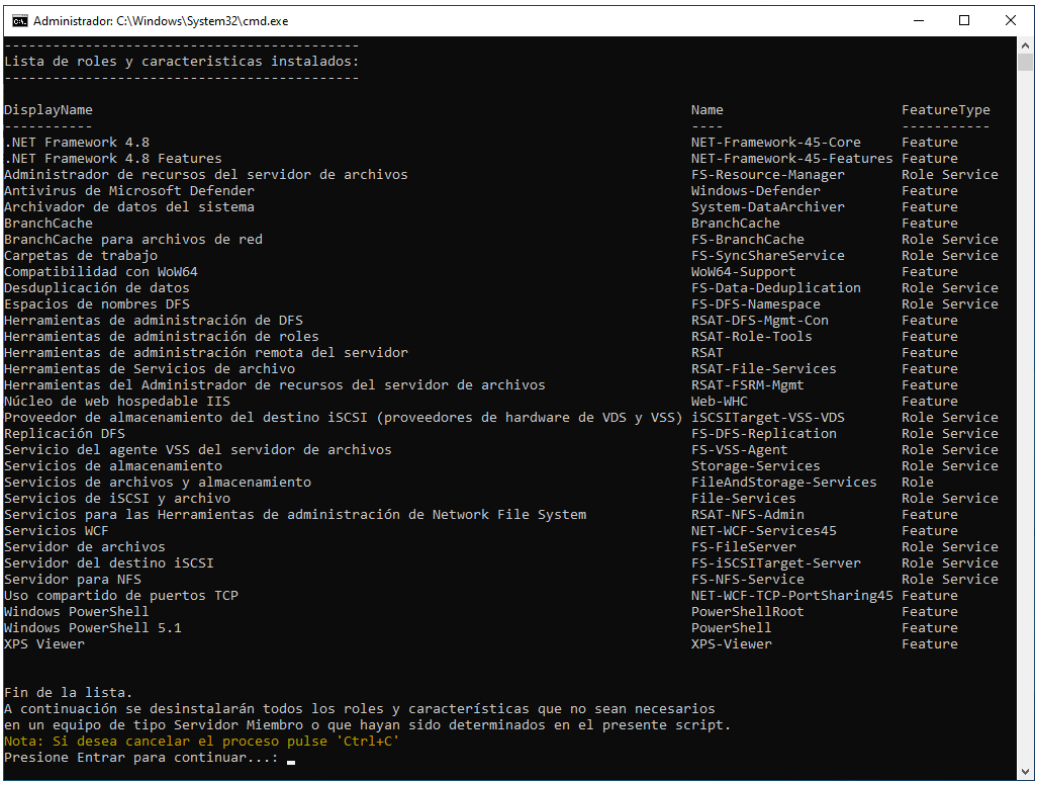
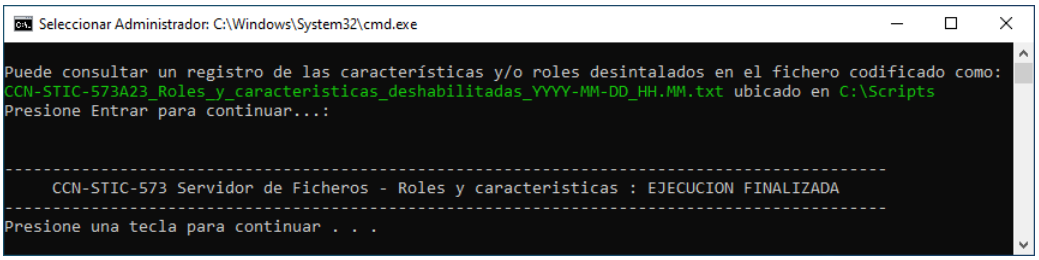
Nota: En este ejemplo se ha incluido la característica "XPS-Viewer".

Tenga en consideración que ya existen otros roles y/o características que ya han sido determinadas como necesarias y no se desinstalarán. Estos se encuentran definidos en la variable "$mantener_rol" y definidos según la funcionalidad asociada. Puede editar dichos valores si lo considera de necesidad.

207.	Cuando haya finalizado pulse sobre el botón "Guardar" en la parte superior izquierda.

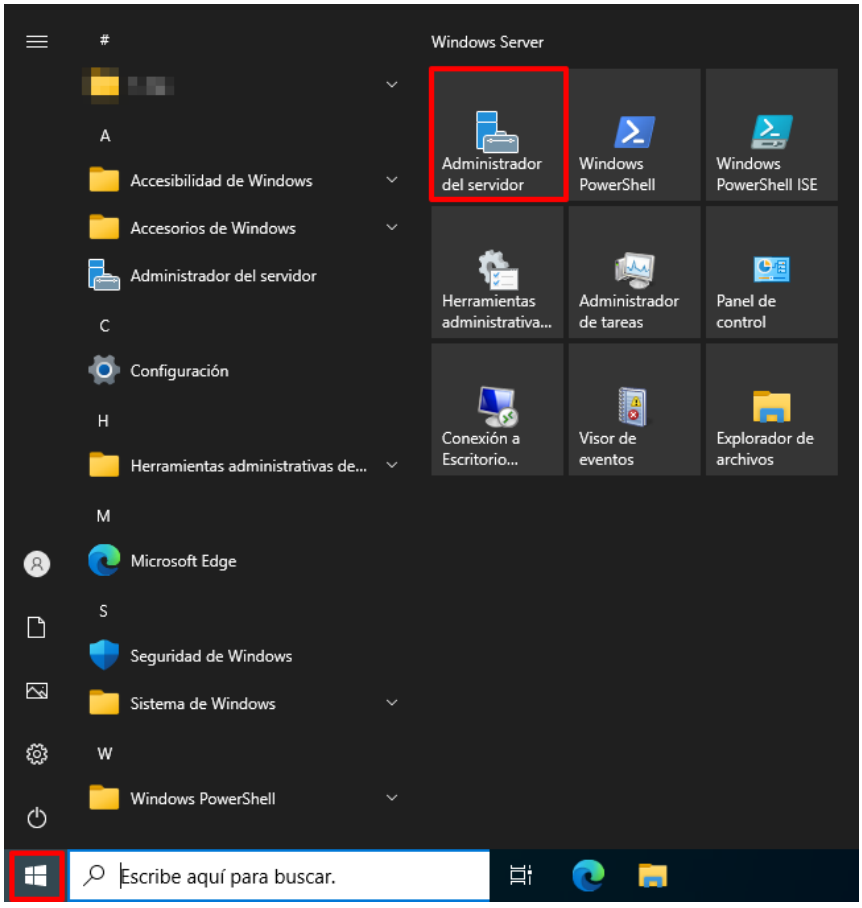


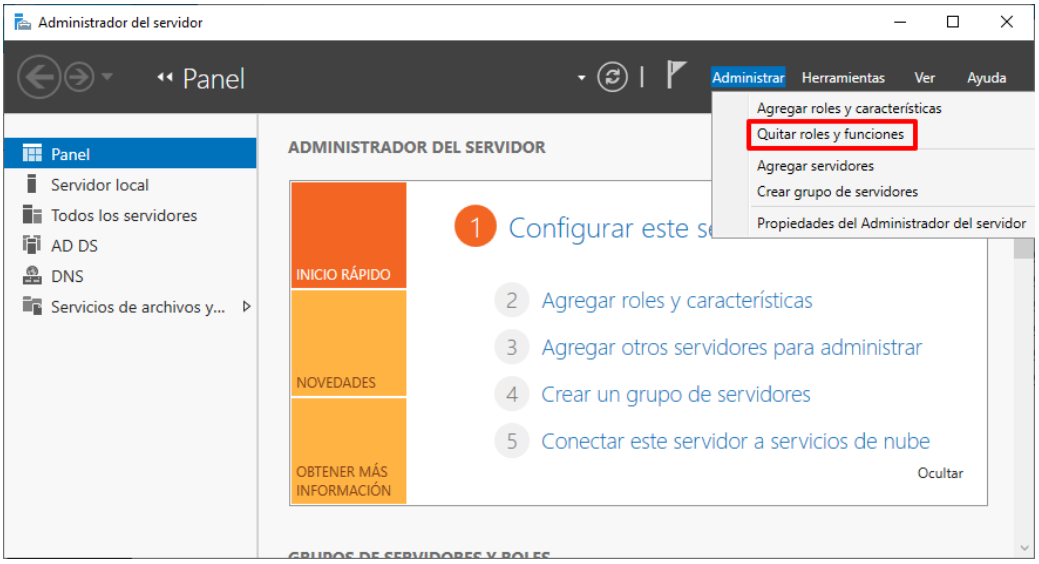
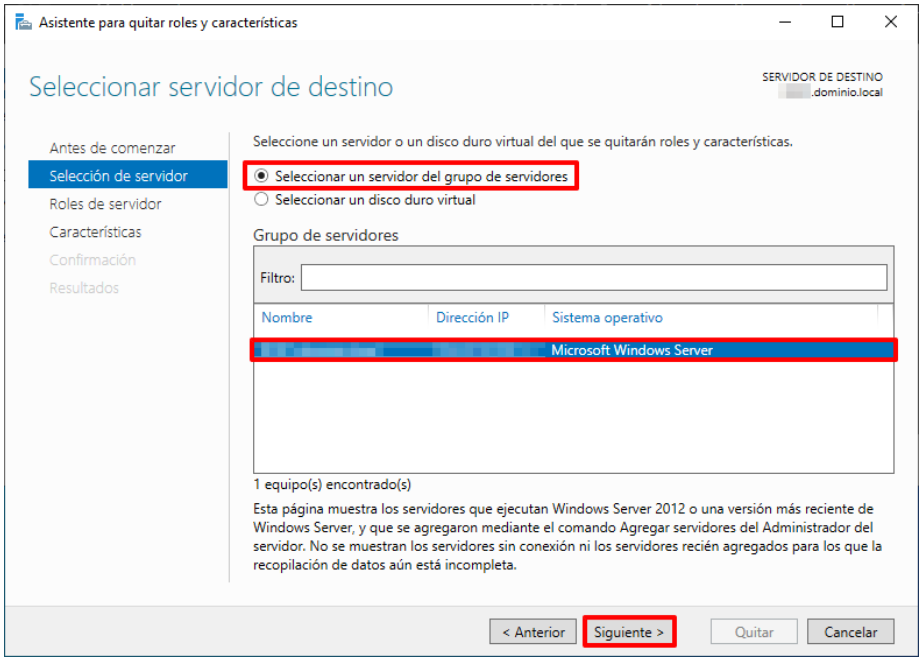
Paso	Descripción
208.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-573 Servidor de Ficheros - Desinstalar roles y caracteristicas.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
209.	Pulse cualquier tecla para continuar. 

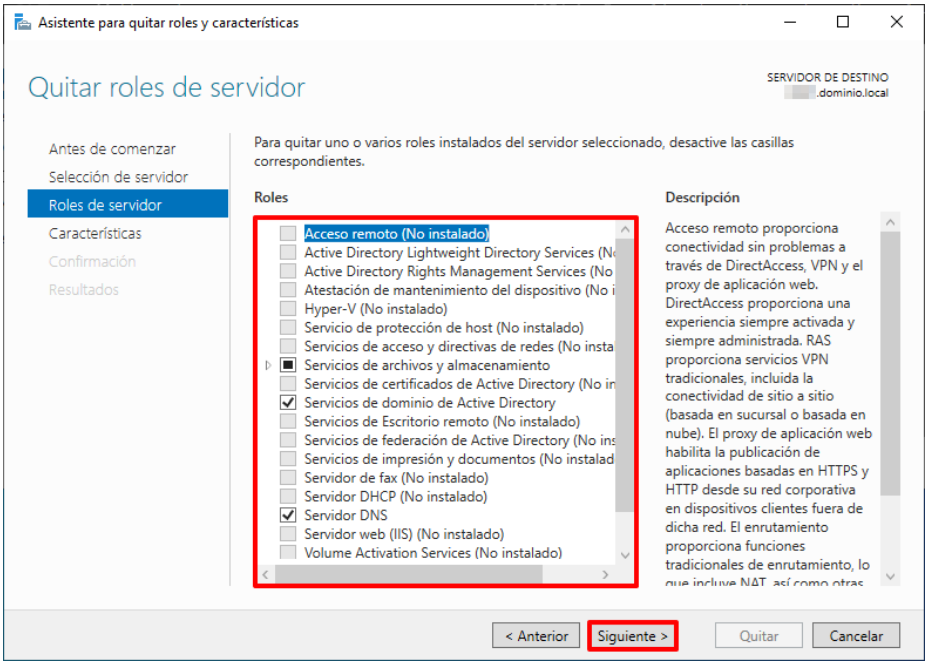
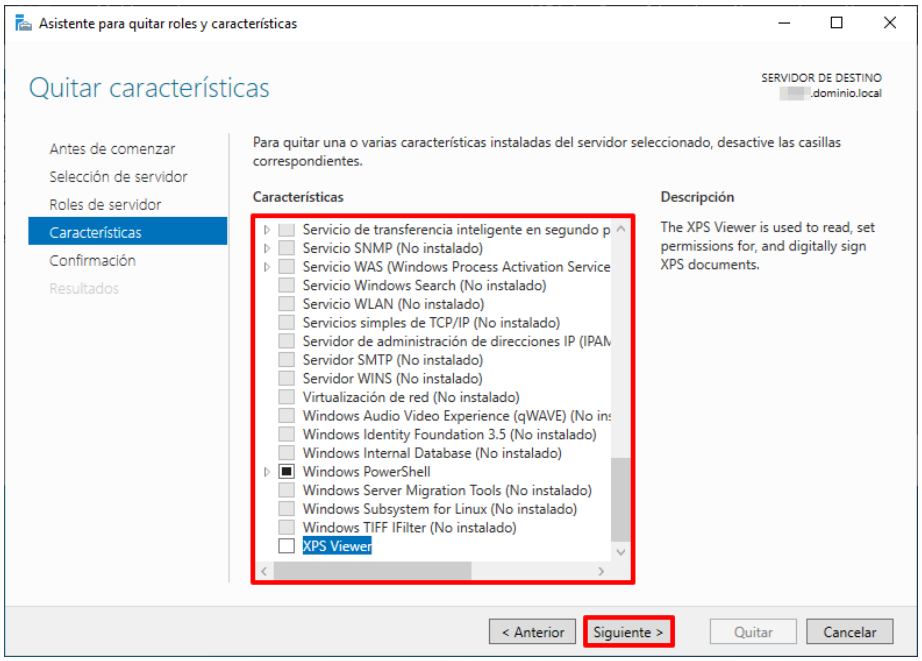
Paso	Descripción
210.	A continuación, se recopilará y mostrarán los roles y características instalados en el equipo. Deberá pulsar la tecla “Enter” para continuar y dar comienzo a la desinstalación de los roles y características no necesarias.  **Nota:** No tome de referencia los roles y características que se reflejan en la imagen ya que puede no coincidir con la configuración de su organización.
211.	Cuando el proceso haya finalizado, podrá evaluar las características y roles desinstalados. Pulse de nuevo la tecla “Enter” para continuar.
212.	El servidor se reiniciará a continuación para asegurar la adecuada desinstalación de roles y/o características. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
213.	Con esto se habrá finalizado la eliminación de roles y características no necesarias en un equipo de tipo Servidor Miembro que cumple con el rol de Servidor de Ficheros.

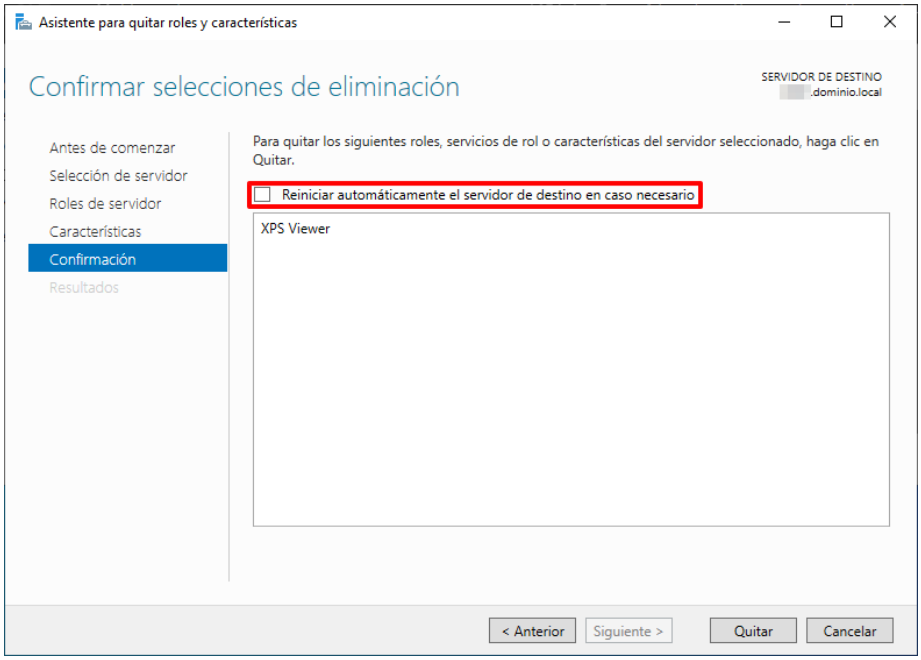
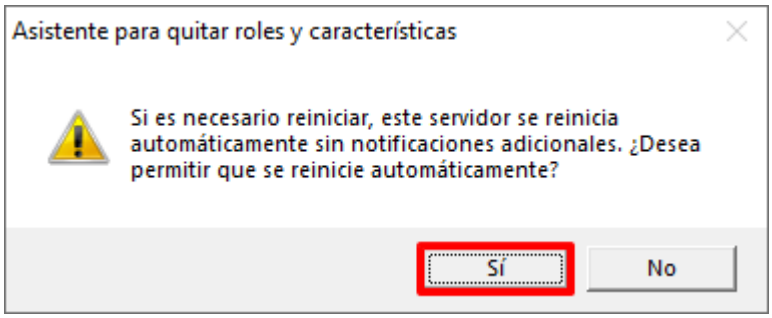
A continuación, se describen los pasos para realizar una desinstalación manual de roles y/o características implementadas en un equipo de tipo Servidor Miembro.

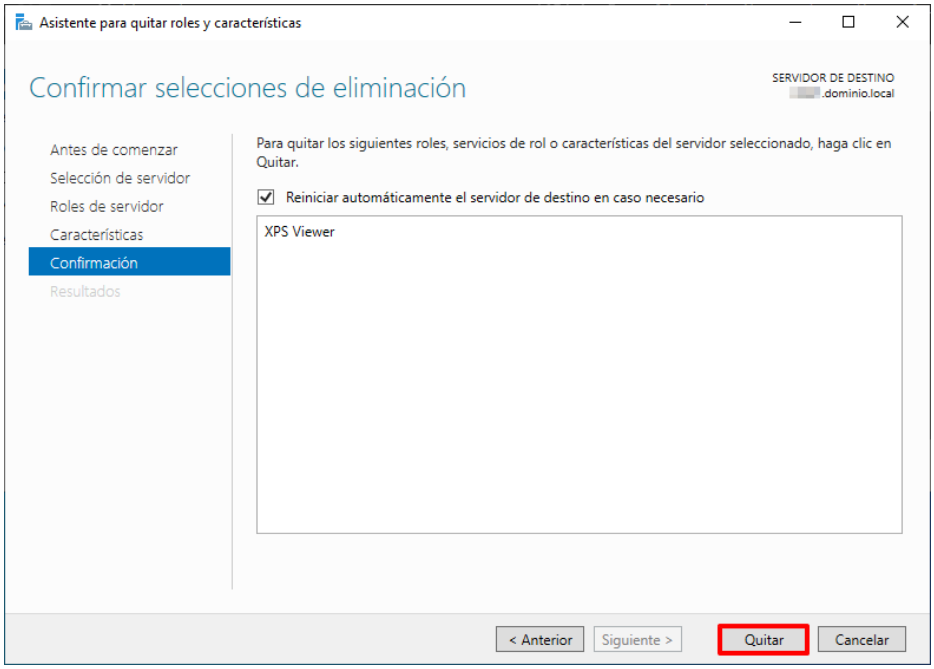
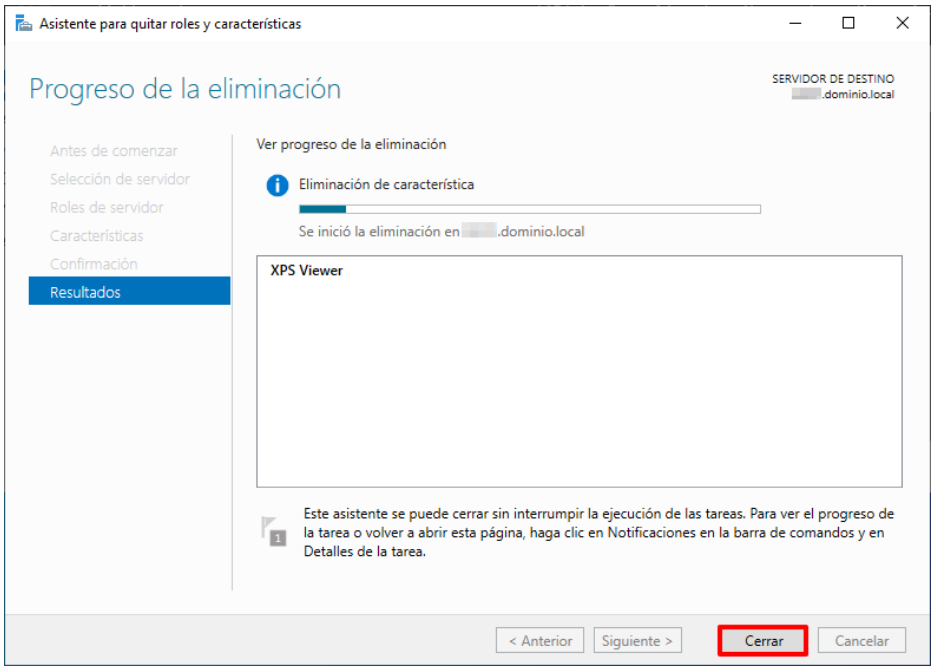
Nota: Para este ejemplo se desinstalará el visor XPS.
Si ya ejecutó los pasos anteriores por medio del script puede continuar en el "Paso 225".

Paso	Descripción
214.	Inicie sesión en un servidor miembro del dominio donde se va aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
215.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".

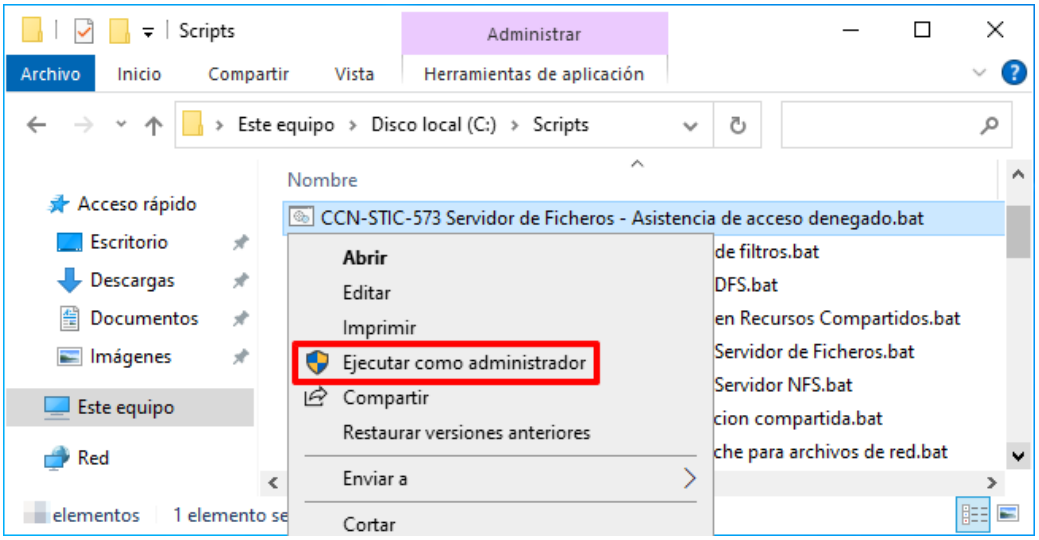
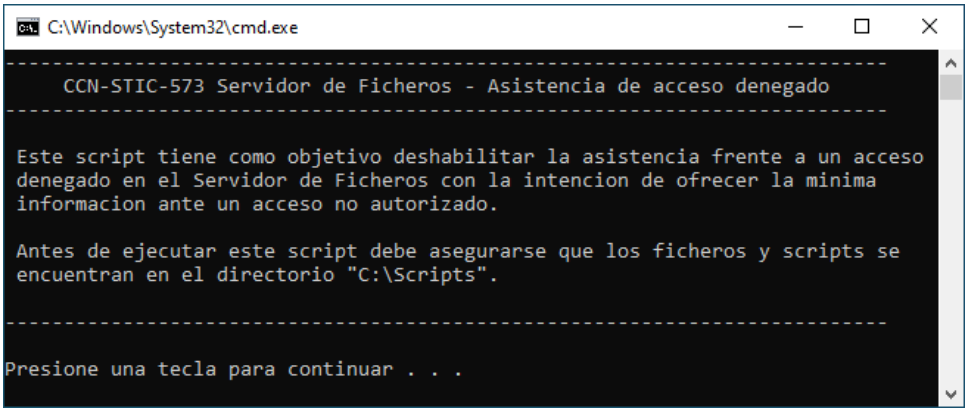
Paso	Descripción
216.	En la parte superior derecha de la ventana “Administrador del servidor” pulse sobre “Administrar → Quitar roles y funciones”. 
217.	En el asistente de instalación que se abrirá pulse “Siguiente >” en la primera ventana.
218.	A continuación, mantenga la opción “Seleccionar un servidor del grupo de servidores”, seleccione el equipo afectado en el apartado “Grupo de servidores” y pulse “Siguiente >”. 

Paso	Descripción
219.	En el siguiente apartado del asistente, “Roles de servidor”, identifique aquellos que no son necesarios y desmárquelos. Pulse “Siguiente >” para continuar. 
220.	Realice la misma acción que en el paso anterior, pero en el apartado del asistente “Características”. Si apareciera una ventana para eliminar roles o características dependientes deberá pulsar en dicha ventana sobre “Quitar características”. Pulse “Siguiente >” para continuar.  **Nota:** En este ejemplo se desinstala la característica “XPS Viewer”.

Paso	Descripción
221.	En la siguiente sección marque la opción “Reiniciar automáticamente el servidor de destino en caso necesario”. 
222.	Pulse “Sí” ante el mensaje de advertencia. 

Paso	Descripción
223.	Pulse sobre el botón “Quitar” para dar comienzo a la desinstalación. 
224.	A partir de ese momento el proceso dará comienzo. Pulse sobre el botón “Cerrar” cuando haya finalizado. En caso de ser necesario un reinicio el sistema advertirá de dicha necesidad. 

Durante los siguientes pasos se van a realizar las configuraciones que permitan definir configuraciones de seguridad adicionales relacionadas con el administrador de recursos del servidor de ficheros y el rol de Servidor de Ficheros.

Paso	Descripción
225.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
226.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Asistencia de acceso denegado.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 
227.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 

ANEXO A.2.7.1. CONFIGURACIÓN DE SEGURIDAD (USO OFICIAL – MATERIAS CLASIFICADAS)

El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

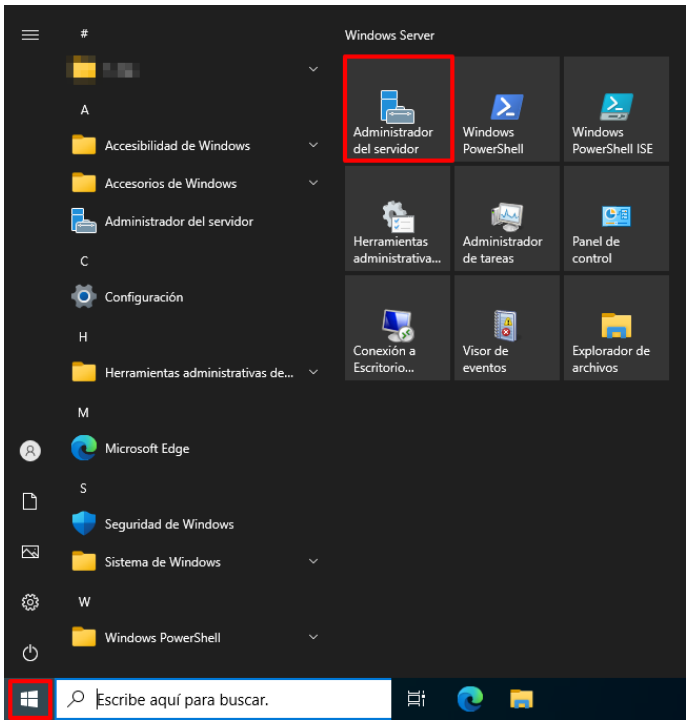
Nota: Deberá disponer del rol "Administrador de recursos del servidor de archivos" instalador para poder hacer uso de esta consola y sus servicios. Instale dicho rol en caso de no disponer del mismo.

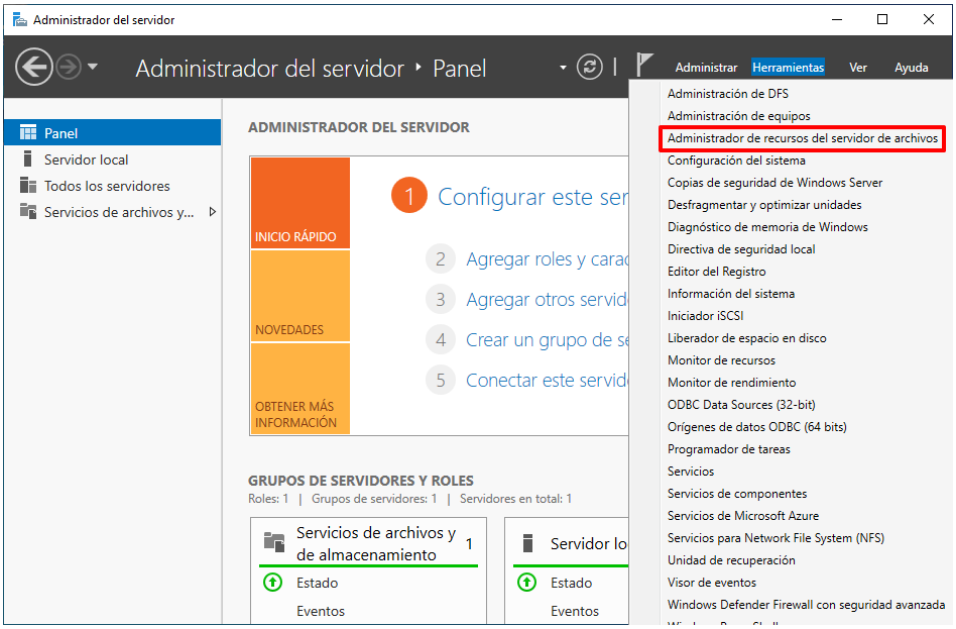
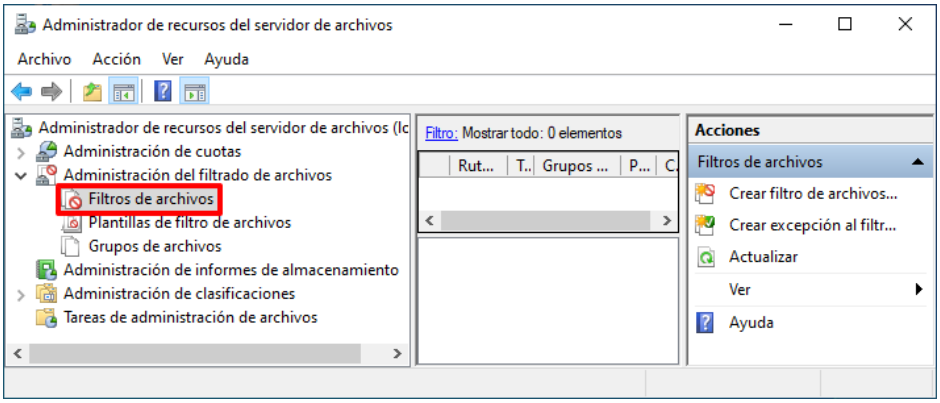
Ejecutadas las acciones anteriores, a continuación, se disponen los pasos que permitan realizar las siguientes acciones:

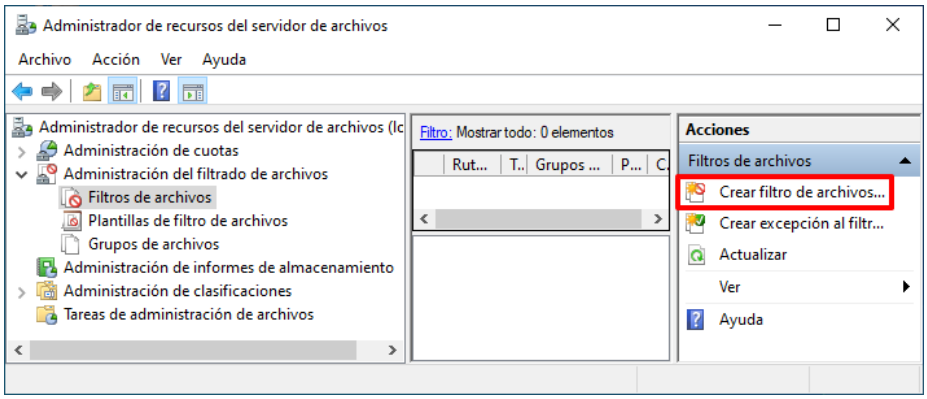
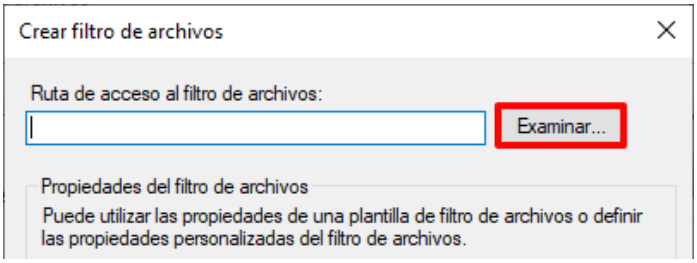
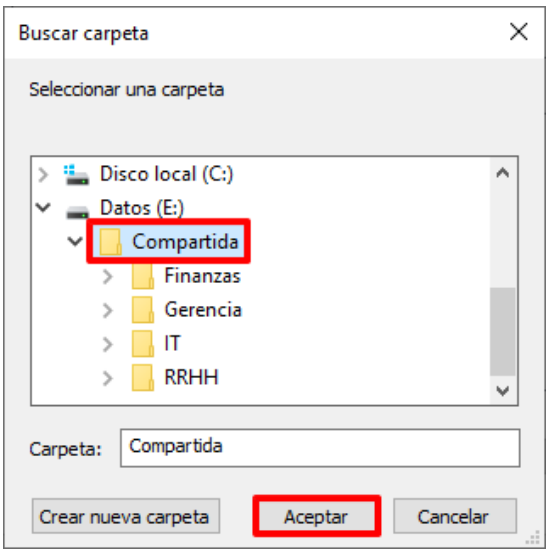
a) Se realizará un ejemplo para aplicar un filtrado de archivos a un recurso compartido.

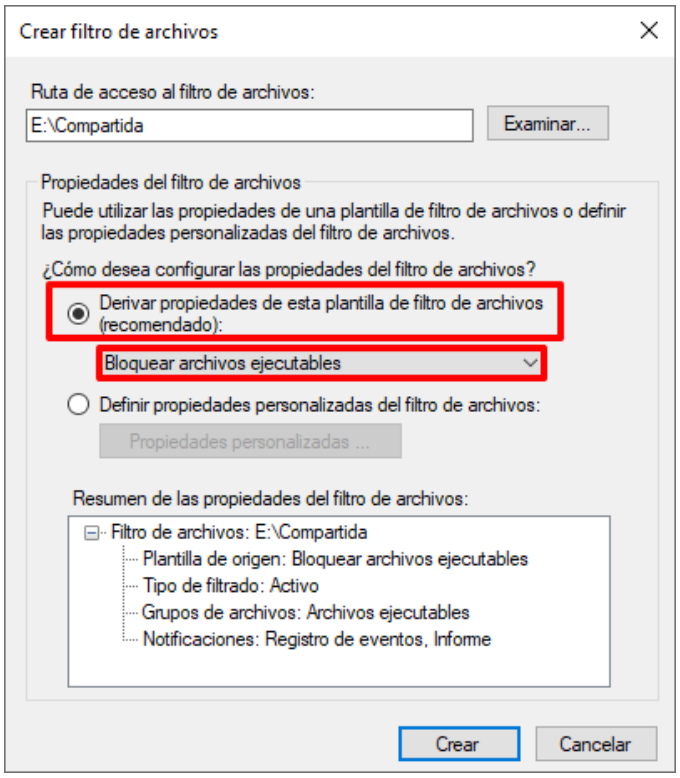
b) De definirá un ejemplo de cuota que limite superar un umbral de almacenamiento en un recurso compartido.

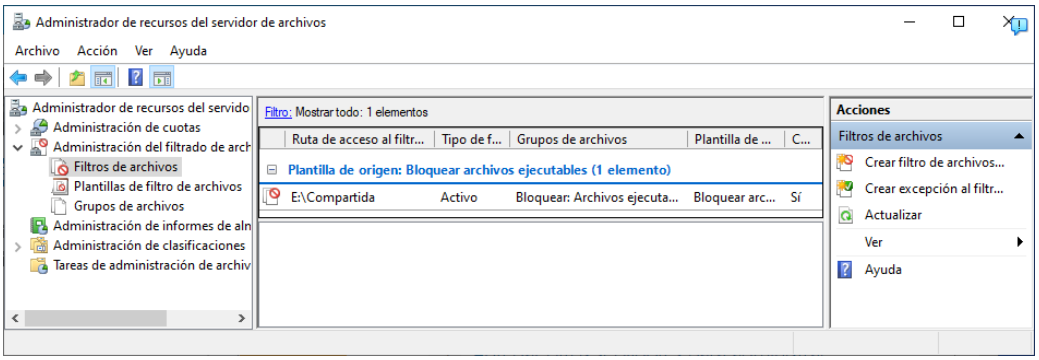
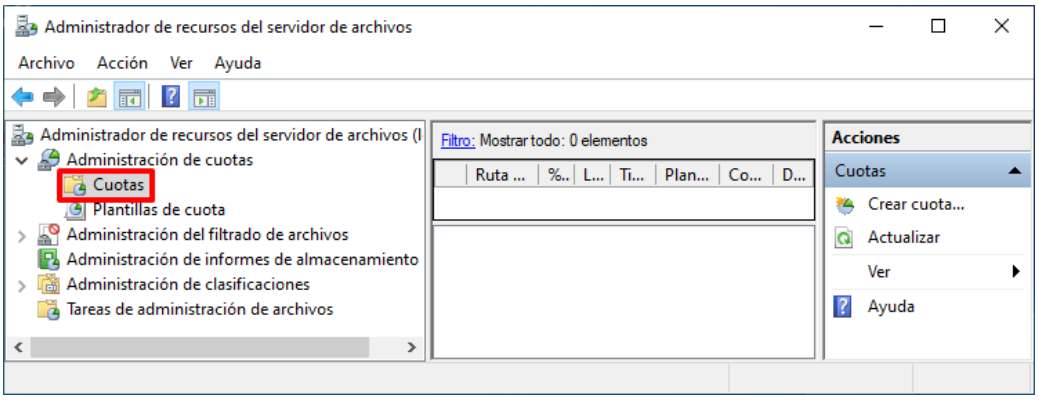
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

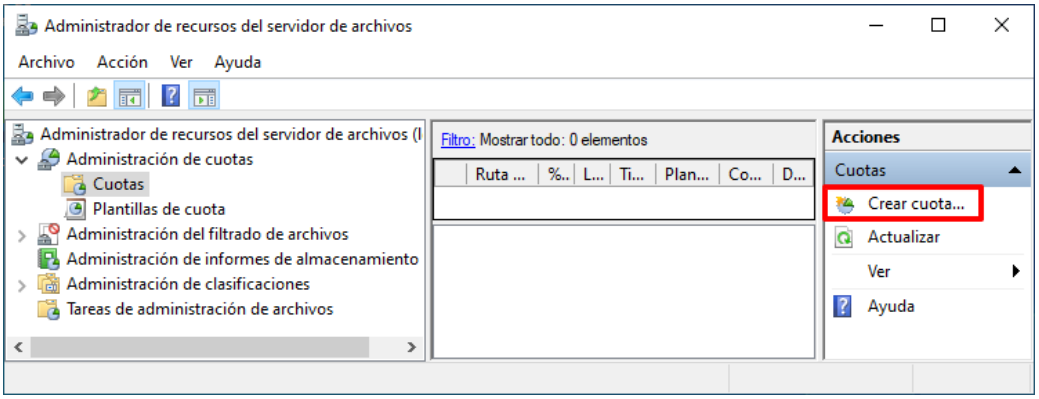
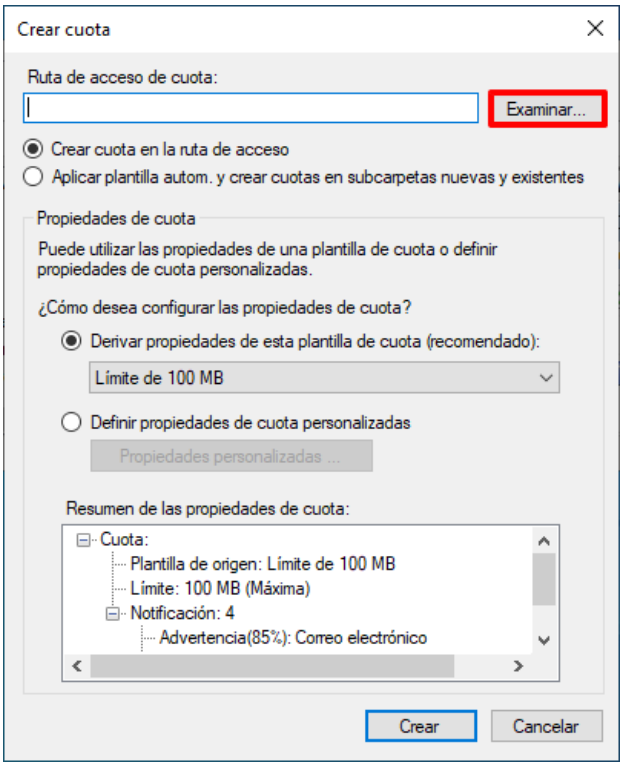
Paso	Descripción
228.	A continuación, ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".

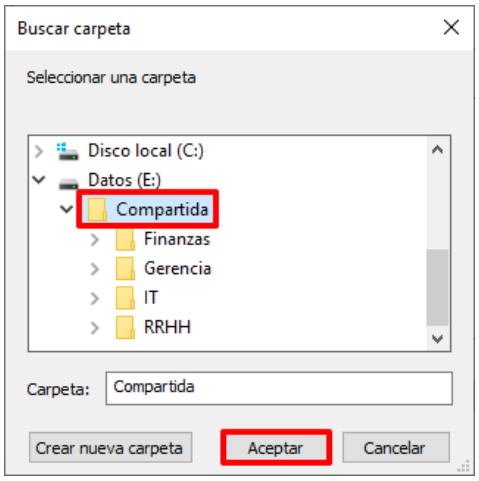
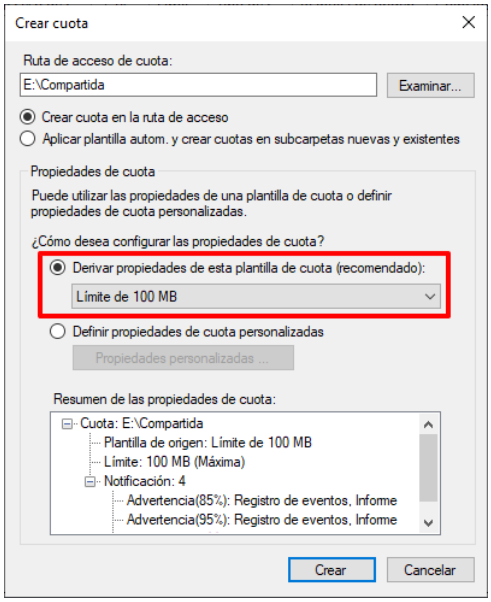
Paso	Descripción
229.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administrador de recursos del servidor de archivos”.  **Nota:** Deberá disponer del rol “Administrador de recursos del servidor de archivos” instalador para poder hacer uso de esta consola y sus servicios.
230.	Diríjase al nodo “Administración del filtrado de archivos”, expándalo y seleccione el apartado “Filtros de archivos”. 

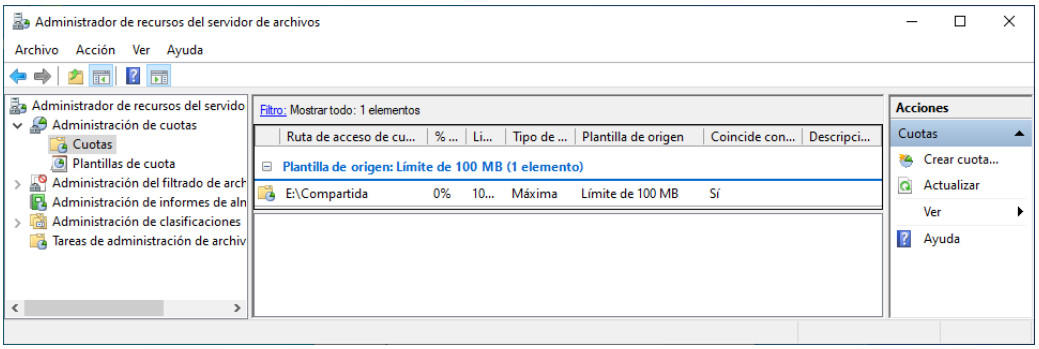
Paso	Descripción
231.	Se va a generar y aplicar un filtrado de archivos que impida a los usuarios alojar información que no esté aceptada en el servidor de ficheros con el objetivo de evitar posibles ataques por medio de la inclusión de ficheros maliciosos. Pulse ahora en el panel derecho sobre “Crear filtro de archivos…”. 
232.	En la ventana emergente pulse sobre el botón “Examinar…”. 
233.	En la ventana emergente, deberá seleccionar el recurso compartido sobre el que desea realizar un filtrado de archivos. Pulse “Aceptar” para continuar.  **Nota:** En este ejemplo se hace uso del recurso compartido de ejemplo denominado “Compartida”. Deberá adaptar los pasos según las necesidades de su organización.

Paso	Descripción
234.	Posteriormente, mantenga marcada la opción “Derivar propiedades de esta plantilla de filtro de archivos (recomendado)”. De igual modo seleccione una de las plantillas de filtro de archivos definidas.  **Nota:** Para este ejemplo se define que no es posible alojar, dentro del recurso compartido creado para este paso a paso, ficheros de tipo ejecutable. En caso de no disponer de una plantilla acorde a las necesidades de su organización y los tipos de ficheros que se deben bloquear, deberá crear previamente dicha plantilla (apartado “Plantillas de filtro de archivos”). Deberá tener en consideración de igual modo los grupos de archivos que se incluyen por cada tipo y que se asocian a las plantillas. En este caso, si tampoco se encontrara alineados se deberá generar un grupo de archivos específico (apartado “Grupos de archivos”). No es objeto de esta guía la creación, parametrización y gestión de estos componentes dado que deben adaptarse a las necesidades de cada organización y se conciben como tareas administrativas.
235.	Pulse el botón “Crear” para finalizar.

Paso	Descripción
236.	Podrá ver el filtro activo en el panel central del "Administrador de recursos del servidor de archivos". En este punto los usuarios no podrán alojar ficheros de tipo ejecutable en el servidor de ficheros. 
237.	Ejecute los pasos "231" a "235" para incluir restricciones adicionales de filtrado de archivos sobre el mismo recurso compartido si así lo necesitará y **aplique de igual modo criterios de restricción de ficheros sobre el resto de recursos compartidos del servidor**. Tenga en consideración que puede establecer configuraciones como "Filtrado pasivo" en las plantillas de filtro de archivos, lo que le permitirá comprender que tipos de ficheros alojan los usuarios antes de realizar un bloqueo directo.
238.	Despliegue ahora el nodo "Administración de cuotas" y seleccione el apartado "Cuotas". 

Paso	Descripción
239.	Se va a generar y aplicar una cuota que limite la inclusión de datos de manera ilimitada sobre el servidor de ficheros con el objetivo de evitar ataques que colapsen el almacenamiento máximo del servidor e impidan el uso del servicio. Pulse ahora en el panel derecho sobre “Crear cuota…”. 
240.	En la nueva ventana emergente pulse sobre el botón “Examinar…”. 

Paso	Descripción
241.	En la ventana emergente, deberá seleccionar el recurso compartido sobre el que desea establecer una cuota de almacenamiento. Pulse "Aceptar" para continuar.  **Nota:** En este ejemplo se hace uso del recurso compartido de ejemplo denominado "Compartida". Deberá adaptar los pasos según las necesidades de su organización.
242.	A continuación, seleccione la plantilla de cuota a utilizar para el recurso compartido. Pulse sobre el botón "Crear" para finalizar.  **Nota:** Para este ejemplo se define que no es posible alojar, dentro del recurso compartido creado para este paso a paso, ficheros de más de 100MB. En caso de no disponer de una plantilla acorde a las necesidades de su organización y las cuotas a aplicar, deberá crear previamente dicha plantilla (apartado "Plantillas de cuota"). No es objeto de esta guía la creación, parametrización y gestión de estos componentes dado que deben adaptarse a las necesidades de cada organización y se conciben como tareas administrativas.

Paso	Descripción
243.	Pulse el botón “Crear” para finalizar.
244.	Podrá ver la cuota activa en el panel central del “Administrador de recursos del servidor de archivos”. En este punto los usuarios no podrán almacenar más de 100MB en el servidor de ficheros. 
245.	Ejecute los pasos “239” a “243” para incluir cuotas adicionales el mismo recurso compartido si así lo necesitará y **aplique de igual modo criterios de cuotas de almacenamiento sobre el resto de recursos compartidos del servidor**. Tenga en consideración que puede establecer configuraciones como “Cuota de advertencia” en las plantillas de cuotas, lo que le permitirá comprender como se utiliza el almacenamiento y utilizar advertencias que permitan superar el límite definido en el uso del almacenamiento.

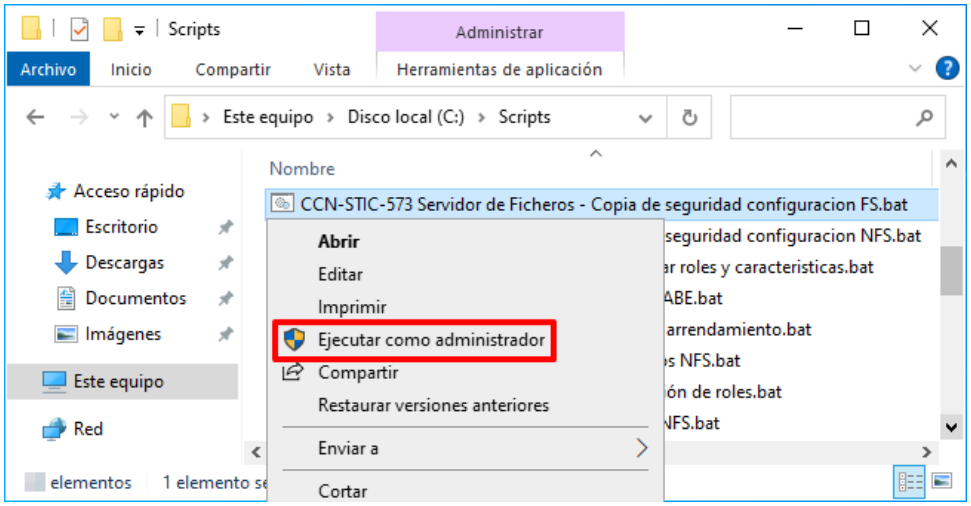
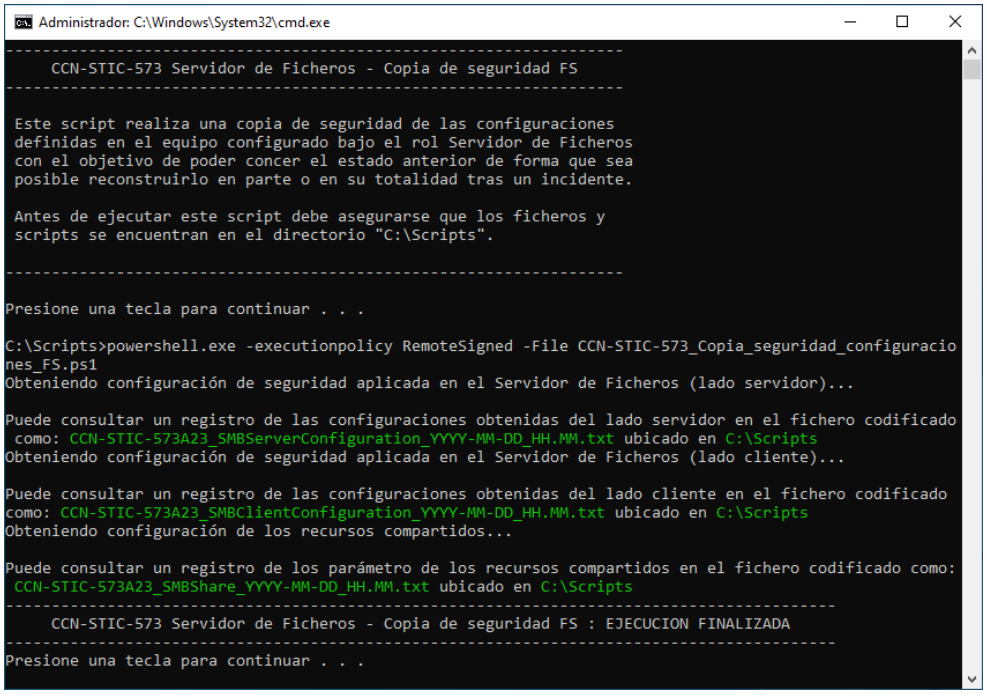
ANEXO A.2.7.2. GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD (USO OFICIAL – MATERIAS CLASIFICADAS)

El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

A continuación, se definen las acciones para realizar una copia de seguridad de la configuración del rol de Servidor de Ficheros de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

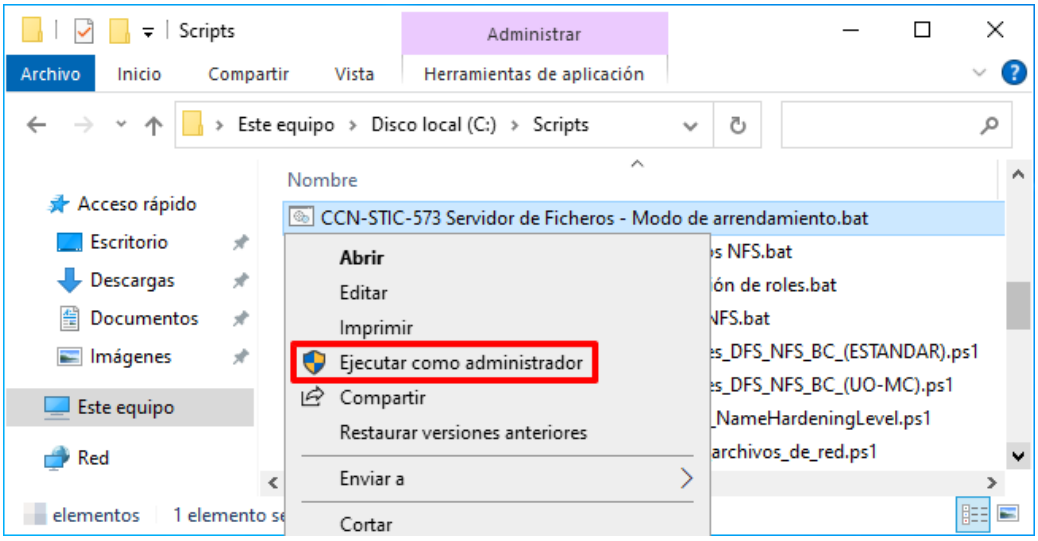
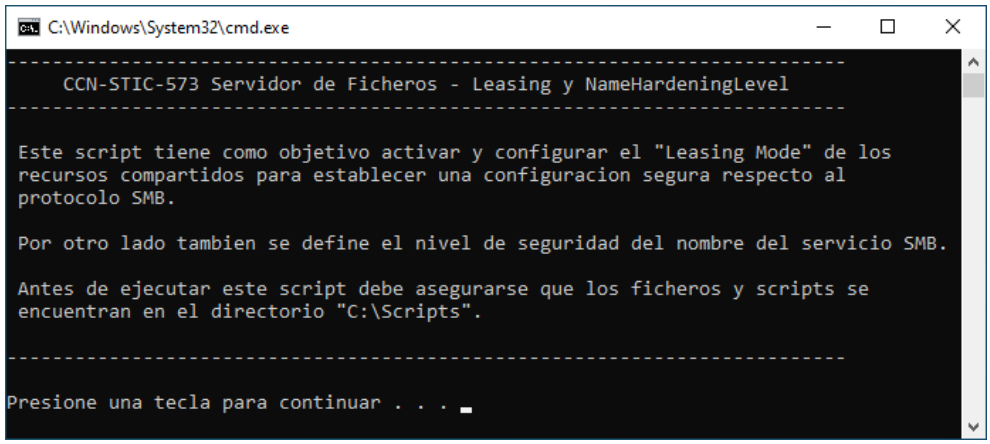
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

Paso	Descripción
246.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.

Paso	Descripción
247.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Copia de seguridad configuracion FS.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
248.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
249.	Recoja y aloje la información resultante del script en un sitio adecuado.

ANEXO A.2.8. PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD

A continuación, se establecen las configuraciones necesarias para cumplir con los algoritmos y parámetros de comunicación necesarios dentro de los sistemas operativos Windows Server y aplicable sobre los equipos de tipo Servidor de Ficheros.

Paso	Descripción
250.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
251.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Modo de arrendamiento.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
252.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
253.	Reinicie el equipo para asegurar que se aplican todos los cambios.

ANEXO B. CONFIGURACIONES ADICIONALES

El presente apartado describe una serie de configuraciones, las cuales su aplicación depende las necesidades de la organización. Cuando se haga uso de las herramientas o elementos descritos bajo el siguiente anexo deberá configurarse la tecnología tal y como se expone a continuación.

ANEXO B.1. REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

A continuación, se definirán las acciones para disponer de un adecuado control de acceso sobre los diferentes recursos compartidos que se encuentren alojados en un equipo bajo el rol Servidor de Ficheros cuando este haga uso del rol NFS.

Nota: Si en su organización no hace uso de estos elementos puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

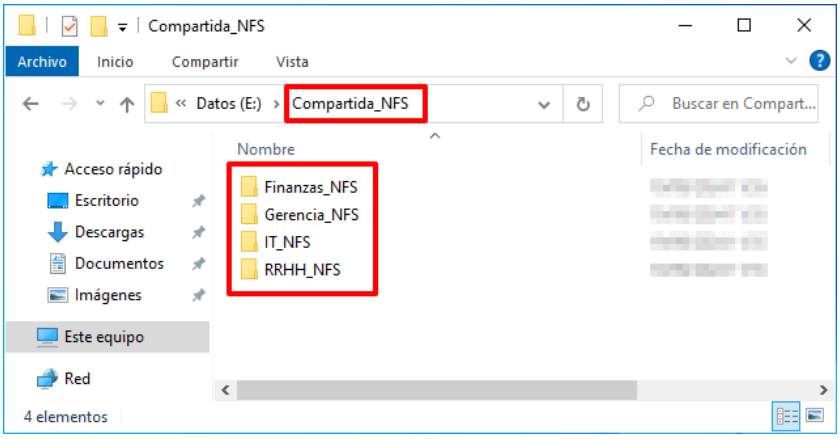
Los pasos descritos a continuación son un ejemplo de cómo asignar accesos a usuarios, sin rechazar o validar la gestión por medio de consolas o herramientas adicionales que una organización pudiera disponer. Cada organización deberá adaptar los pasos descritos en el presente apartado en función de las necesidades de la misma.

Para la elaboración de este paso a paso, se ha definido **un escenario a modo de ejemplo** que pretenda reflejar las acciones que deben llevarse a cabo. Para ello se define la siguiente información:

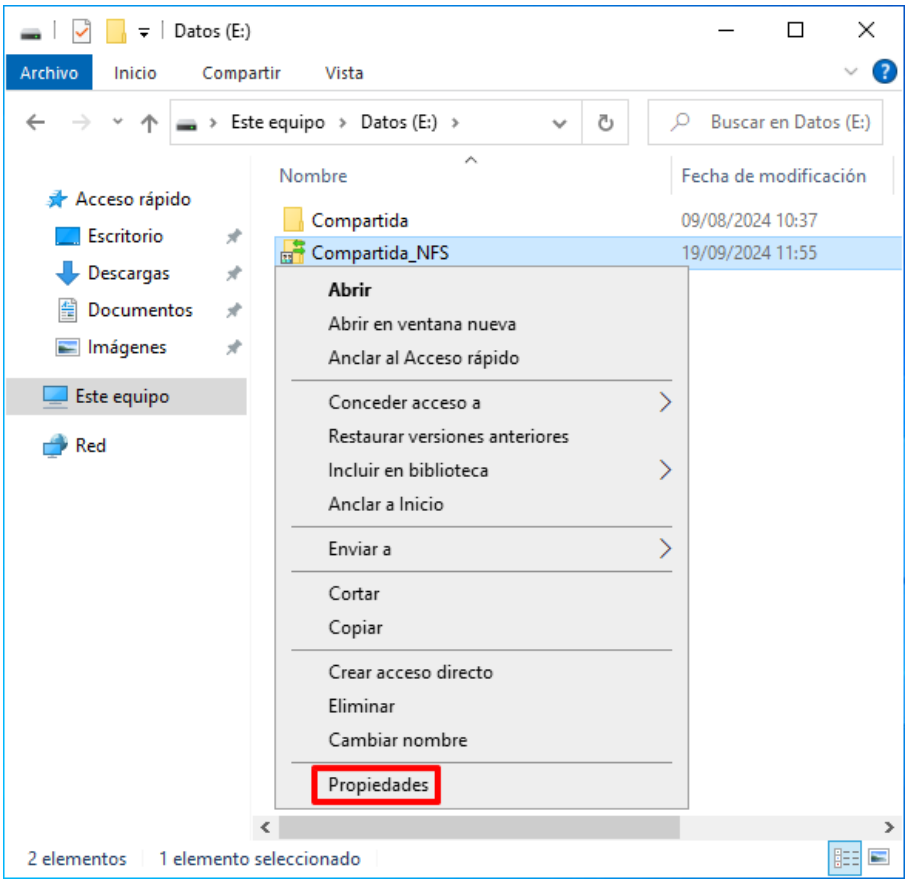
Nota: No es objeto de esta guía de seguridad definir o mostrar cómo se realizan las acciones de creación de recursos compartidos, usuarios y/o grupos de seguridad debido a que estas se conciben como labores de administración.

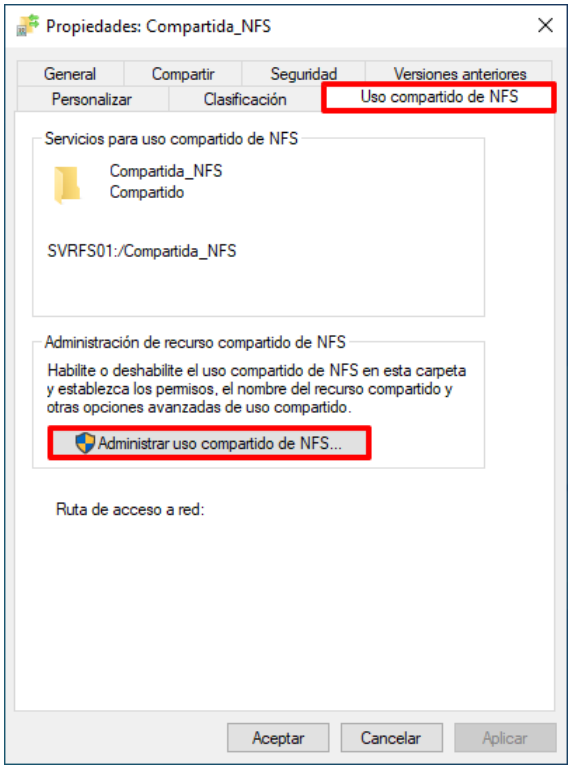
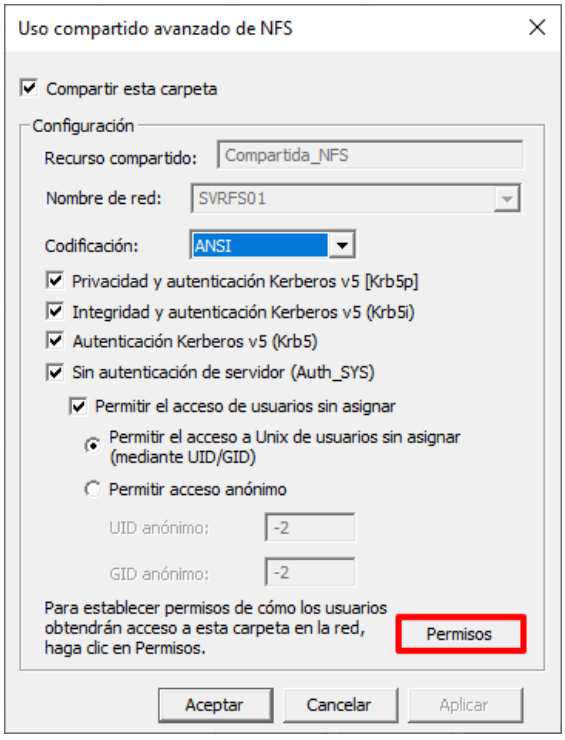
a) Equipos para facilitar acceso: Se hará uso de los equipos del entorno generado para la elaboración de esta guía de seguridad con el objetivo de definir la gestión de acceso.

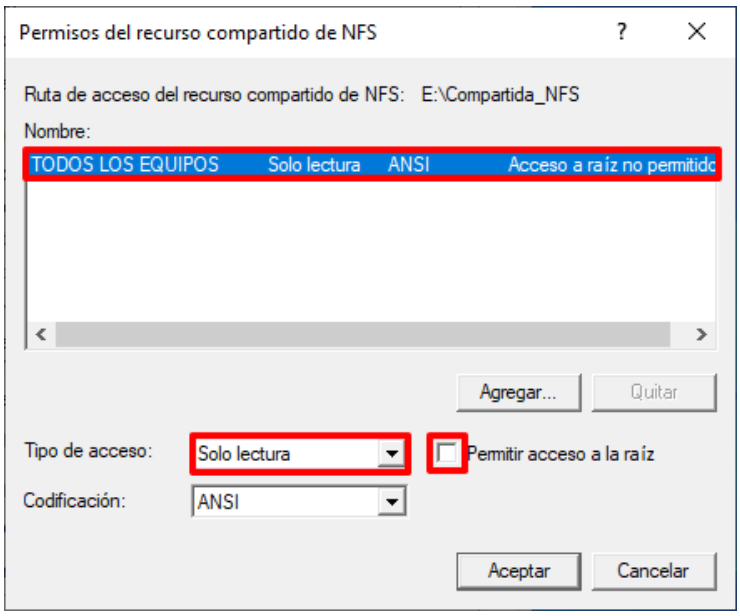
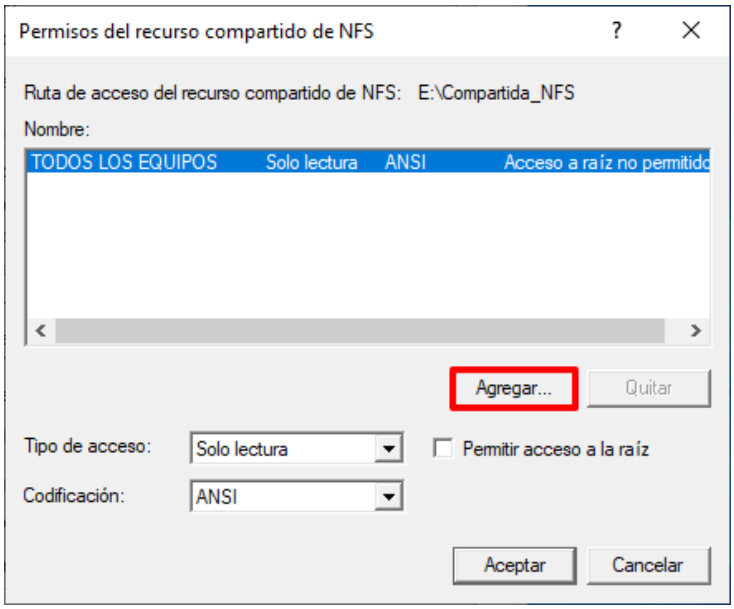
b) Recursos compartidos: En línea con la información anterior se ha generado un recurso compartido con diferentes directorios y ficheros de ejemplo en un almacenamiento dedicado para el servicio el cual permitan ejemplificar las acciones asociadas a este apartado, y que permita cumplir con los requisitos de acceso.

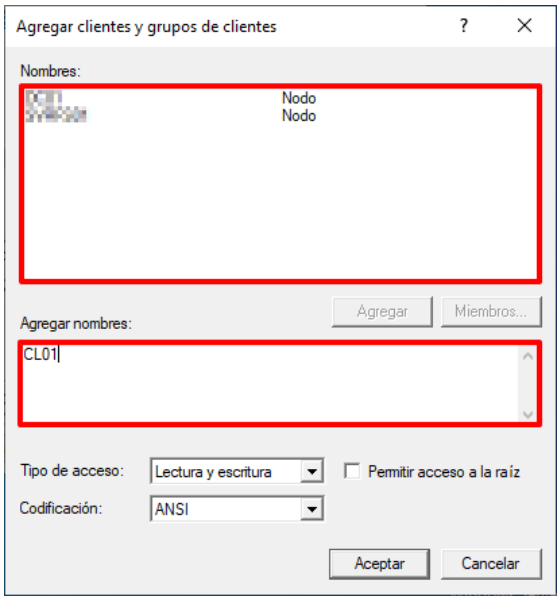
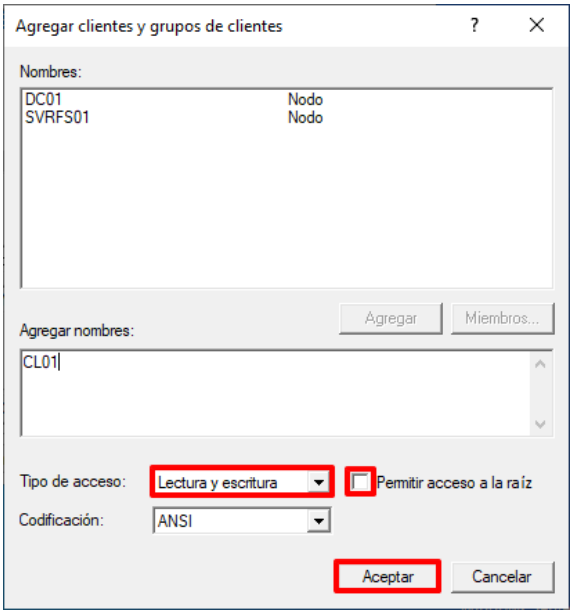


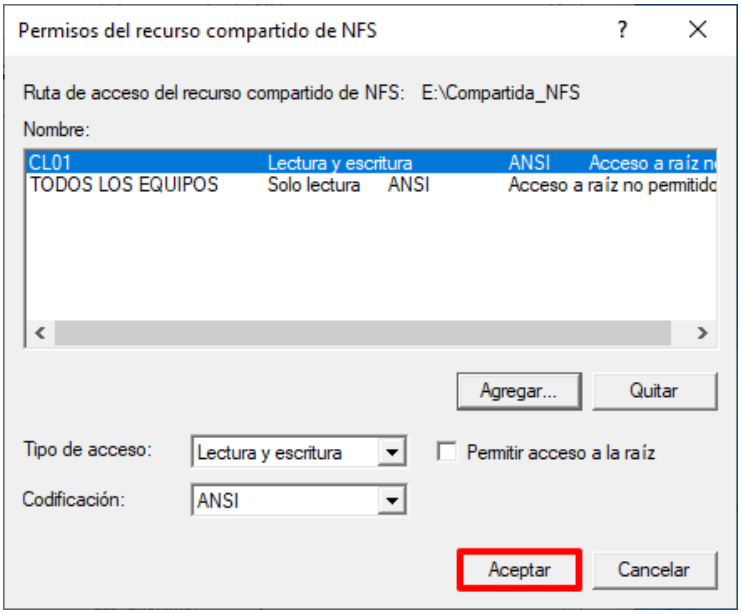
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
2.	Diríjase a la ubicación donde se encuentran los recursos compartidos bajo NFS. deberá acceder a las opciones de permisos haciendo clic derecho sobre el directorio de Windows y seleccionando “Propiedades” del menú contextual.  **Nota:** En este ejemplo se hace uso del recurso compartido denominado “Compartida_NFS” Adapte estos pasos a las necesidades de su organización. Puede realizar estas mismas acciones bajo la consola “Administrador del servidor” en su apartado “Recurso compartidos”.

Paso	Descripción
3.	En la nueva ventana emergente seleccione la pestaña “Uso compartido NFS” y a continuación pulse sobre “Administrar uso compartido de NFS”. 
4.	En la nueva ventana “Uso compartido avanzado de NFS” pulse sobre el botón “Permisos”. 

Paso	Descripción
5.	En la nueva ventana que aparecerá, evalúe si se encuentra definido el grupo “TODOS LOS EQUIPOS”. En el caso de que estuviera como entrada, selecciónelo y asegúrese que la configuración “Tipo de acceso:” se encuentra en “Solo lectura” y que se encuentra desmarcada la opción “Permitir acceso a la raíz”. 
6.	Posteriormente se deberá otorgar permiso a aquellas entidades que requieran del correspondiente requisito de acceso. Para ello, al igual que se realizó en pasos anteriores haga clic de nuevo sobre el botón “Agregar…”. 

Paso	Descripción
7.	En el apartado “Agregar nombres” defina el nombre o nombres de equipos a los que desea permitir el acceso. Si ya agregó antes un equipo dispondrá de una lista en la sección “Nombres:” y podrá añadirlo por medio del botón “Agregar”.  **Nota:** En este ejemplo se hace uso del equipo denominado “CL01”. Deberá adaptar esta configuración a las necesidades de su organización. Tenga en consideración que puede incluir más de un equipo a la vez separando el nombre de estos por punto y coma (;).
8.	A continuación, defina el “Tipo de acceso:” y si no es imprescindible no marque la opción “Permitir acceso a la raíz”. Pulse “Aceptar” cuando haya finalizado.  **Nota:** En este ejemplo se hace uso del acceso “Lectura y escritura”. Deberá adaptar esta configuración a las necesidades de su organización.

Paso	Descripción
9.	Si fuera necesario eliminar alguna entidad para denegar el acceso bastará con seleccionar dicha entidad en la ventana “Permisos del recurso compartido de NFS” y pulsar sobre el botón “Quitar”.
10.	Pulse de nuevo “Aceptar” en la ventana “Permisos del recurso compartido de NFS” y de nuevo “Aceptar” sobre la ventana “Uso compartido avanzado de NFS. 
11.	Repita los pasos “2” a “10” sobre cada uno de los recursos compartidos NFS de los que disponga su infraestructura y de igual modo sobre cada uno de los subrecursos según las necesidades de acceso de su organización. Recuerde que **los equipos que se den de alta solo deben disponer de acceso y capacidad sobre aquellos directorios o recursos que así se determine**, no disponiendo de accesos adicionales. De igual modo se deberá **limitar los permisos de las entidades de tipo equipo a los estrictamente necesarios, no otorgando permisos adicionales** a la entidad seleccionada.

ANEXO B.2. MECANISMO DE AUTENTICACIÓN Y REGISTRO DE LA ACTIVIDAD

El objetivo de la siguiente sección es definir los mecanismos de registro y auditoría para elementos adicionales relacionados con la compartición de ficheros por medio de los elementos nativos de Windows. En este caso se hace referencia a los roles DFS y NFS.

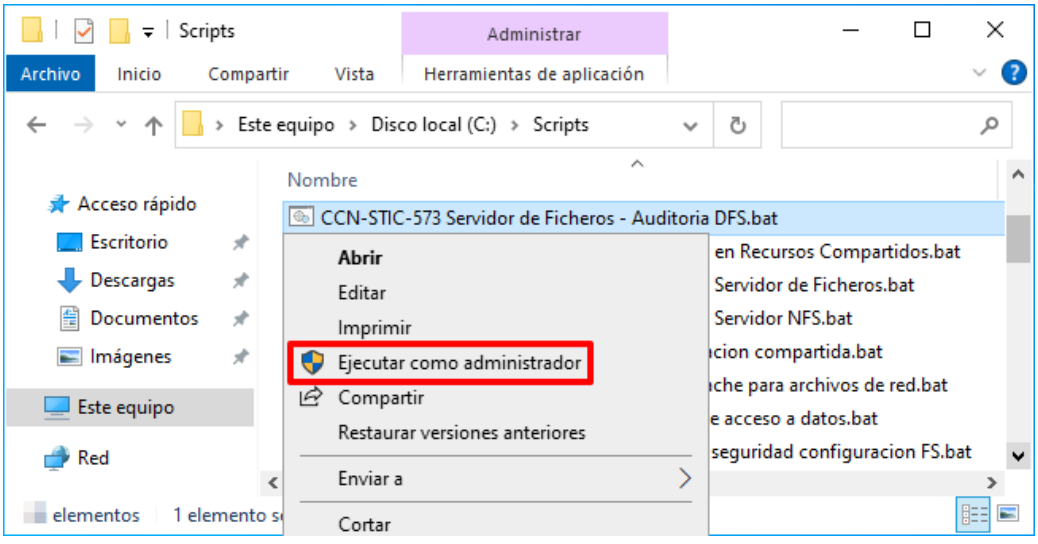
a) Diríjase al "Paso 1" para la configuración de DFS.

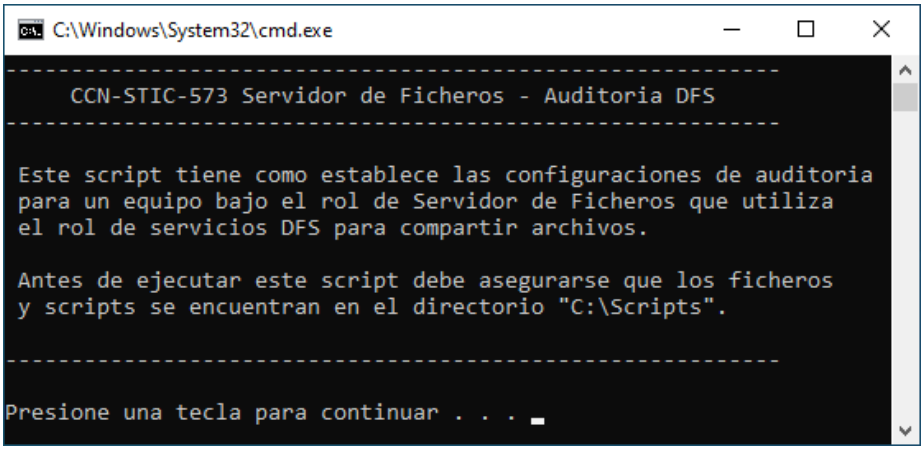
b) Diríjase al "Paso 5" para la configuración de NFS.

Nota: Si en su organización no hace uso de estos elementos puede ignorar el siguiente paso a paso y continuar en el siguiente punto. Si solo hace uso de alguno de los elementos definidos ejecute los pasos relacionados al rol específico (DFS o NFS).

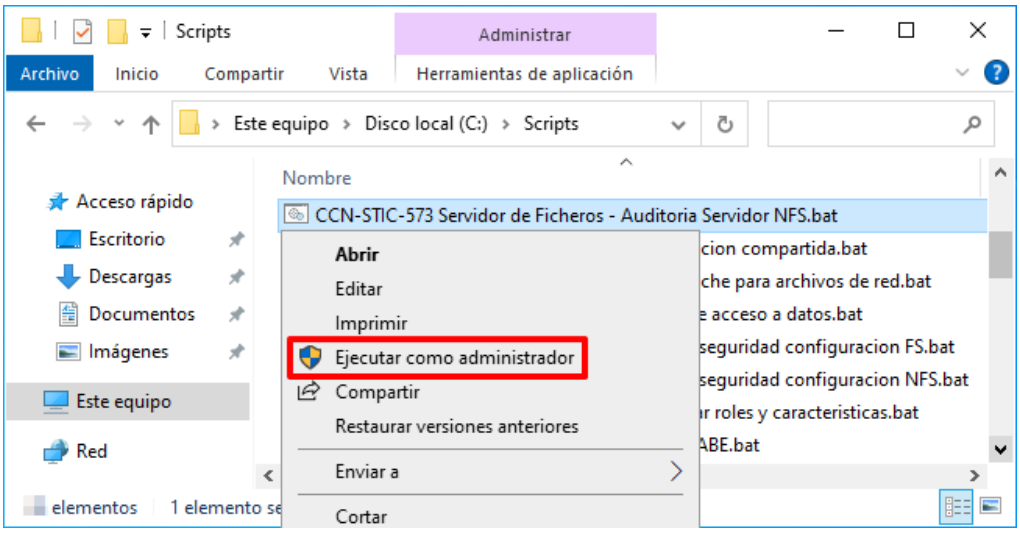
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

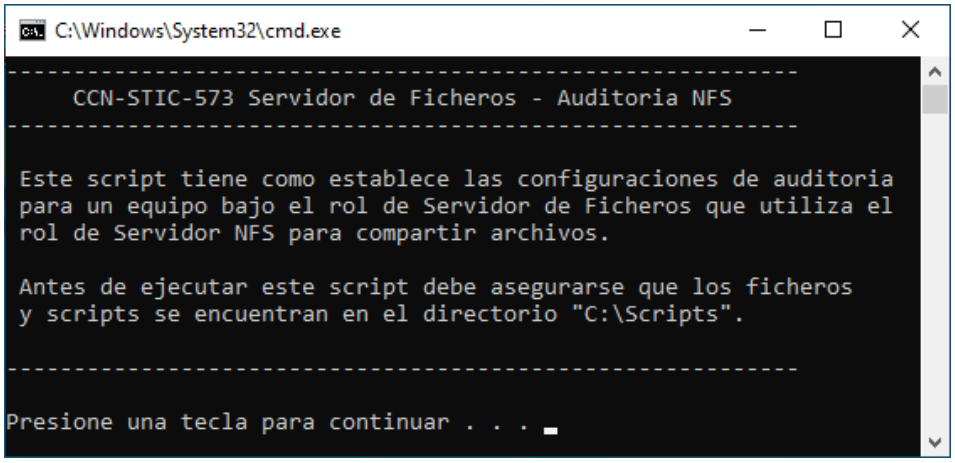
A continuación, se aplicarán las configuraciones para la auditoría DFS.

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
2.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Auditoria DFS.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 

Paso	Descripción
3.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
4.	Reinicie el equipo para asegurar que se aplican todos los cambios.

A continuación, se aplicarán las configuraciones para la auditoría NFS.

Paso	Descripción
5.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
6.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Auditoria Servidor NFS.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 

Paso	Descripción
7.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
8.	Reinicie el equipo para asegurar que se aplican todos los cambios.

ANEXO B.3. CONFIGURACIÓN DE SEGURIDAD Y GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

A través de la siguiente sección y su paso a paso se establecen las configuraciones de seguridad necesarias para la compartición de ficheros por medio de los elementos nativos de Windows. En este caso se hace referencia a los roles BranchCache y NFS.

a) Diríjase al "Paso 1" para la configuración de BrachCache.

Nota: Las configuraciones asociadas a BranchCache son aquellas que se encuentran ligadas al rol de Servidor de Ficheros y a la compartición de archivos (BrachCache para archivos de red), no a la característica específica definida como BranchCache.

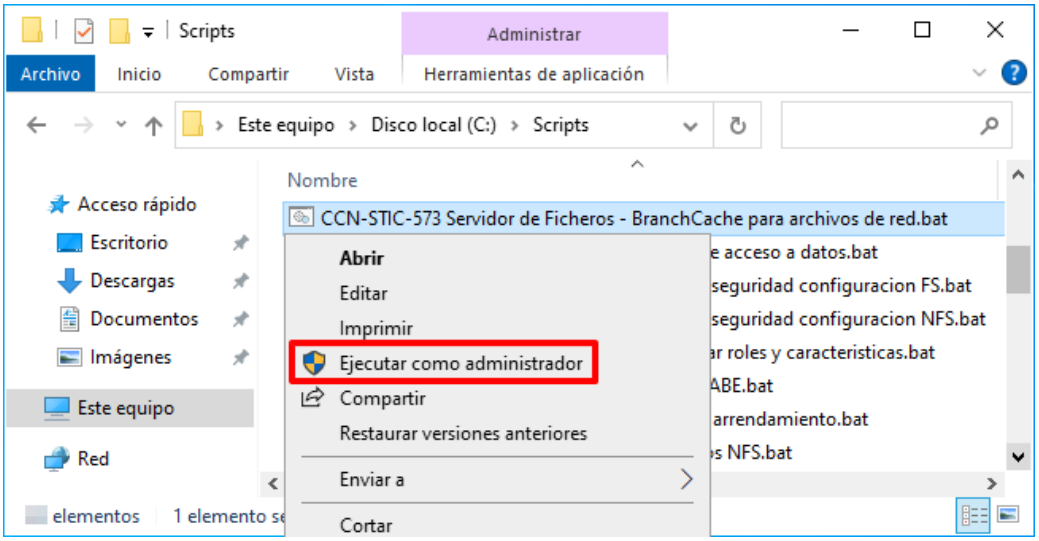
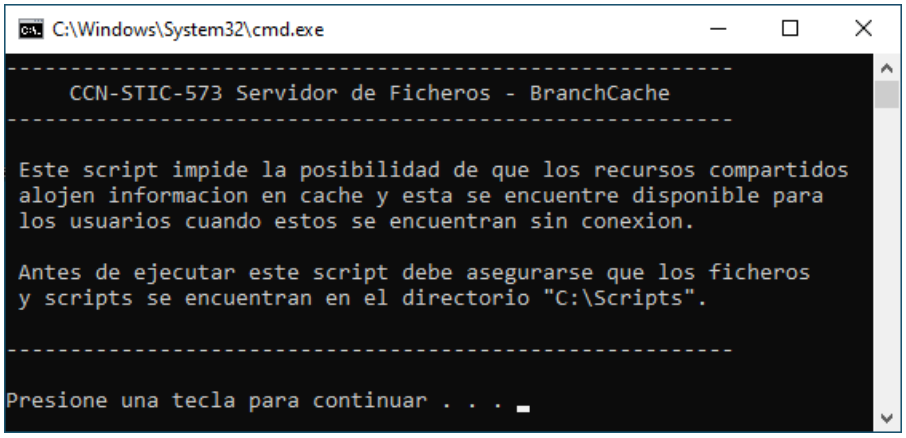
b) Diríjase al "Paso 5" para la configuración de NFS.

Nota: Si en su organización no hace uso de estos elementos puede ignorar el siguiente paso a paso y continuar en el siguiente punto. Si solo hace uso de alguno de los elementos definidos ejecute los pasos relacionados al rol específico (BrachCache o NFS).

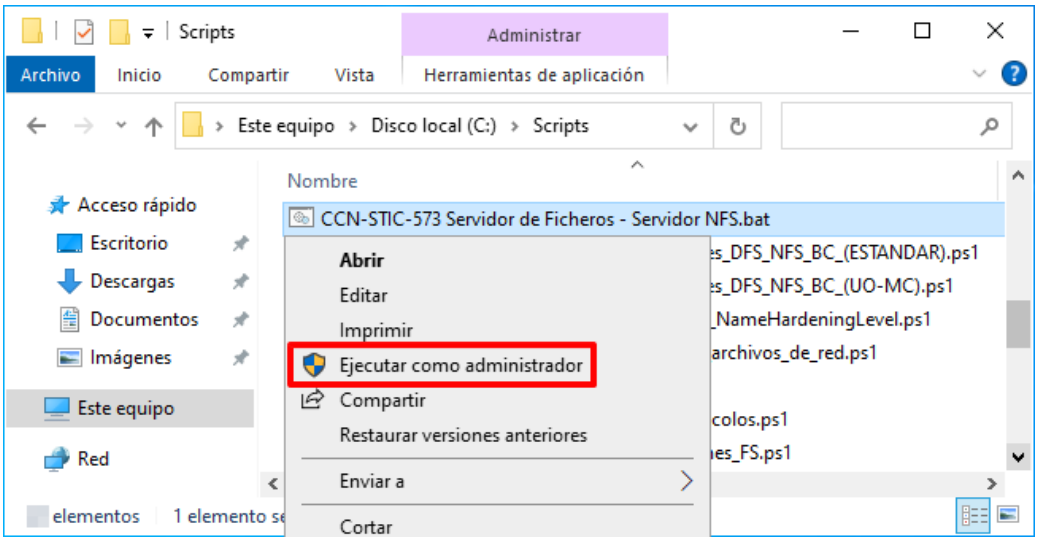
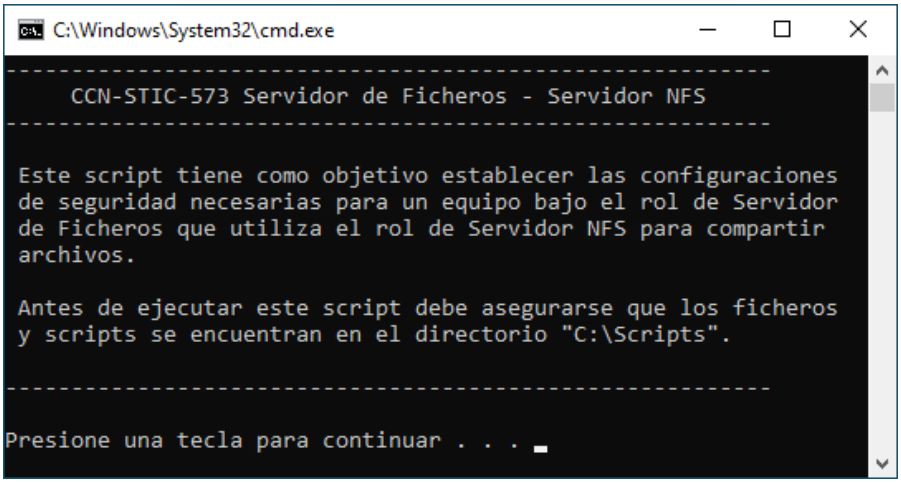
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

A continuación, se aplicarán las configuraciones de seguridad para BranchCache para archivos de red.

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.

Paso	Descripción
2.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - BranchCache para archivos de red.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
3.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
4.	Reinicie el equipo para asegurar que se aplican todos los cambios.

A continuación, se aplicarán las configuraciones de seguridad para NFS.

Paso	Descripción
5.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
6.	Diríjase al directorio "C:\Scripts" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Servidor NFS.bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá. 
7.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
8.	Reinicie el equipo para asegurar que se aplican todos los cambios.

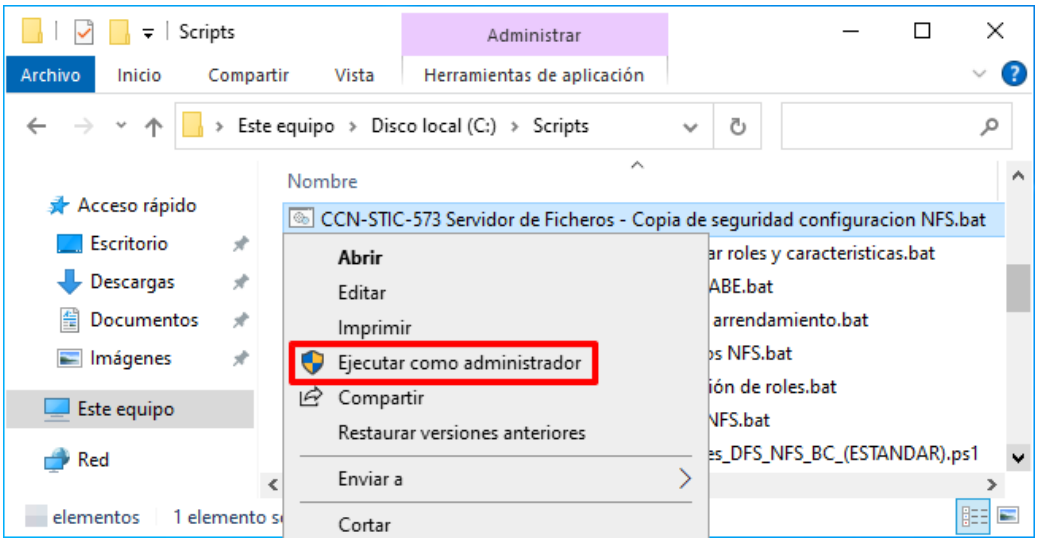
ANEXO B.3.1. GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD (USO OFICIAL – MATERIAS CLASIFICADAS)

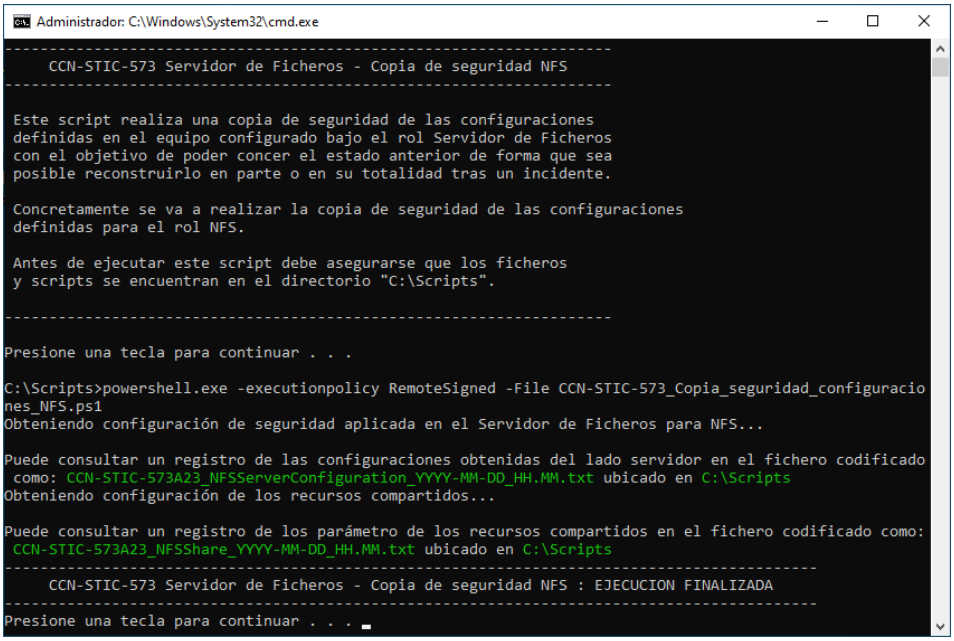
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

A continuación, se definen las acciones para realizar una copia de seguridad de la configuración del rol de Servidor de Ficheros, cuando este haga uso de servicios adicionales de compartición de ficheros nativos de Windows. Se hace referencia en este caso a NFS. Esto permitirá restaurar, si es necesario, la configuración de dichos servicios en parte o en su totalidad tras un incidente.

Nota: Si en su organización no hace uso de estos elementos o bien realiza la copia de seguridad por otros medios puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
2.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Copia de seguridad configuracion NFS.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 

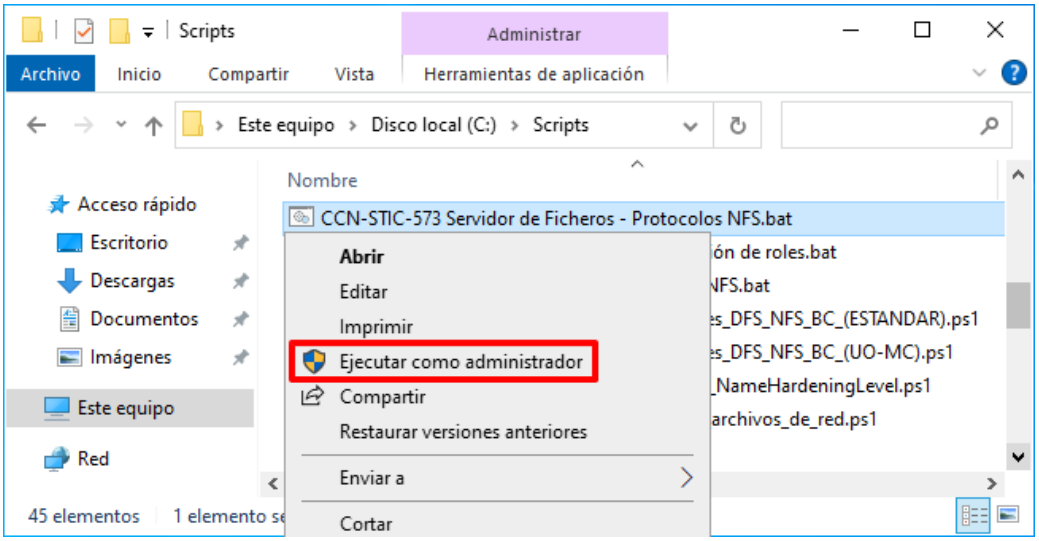
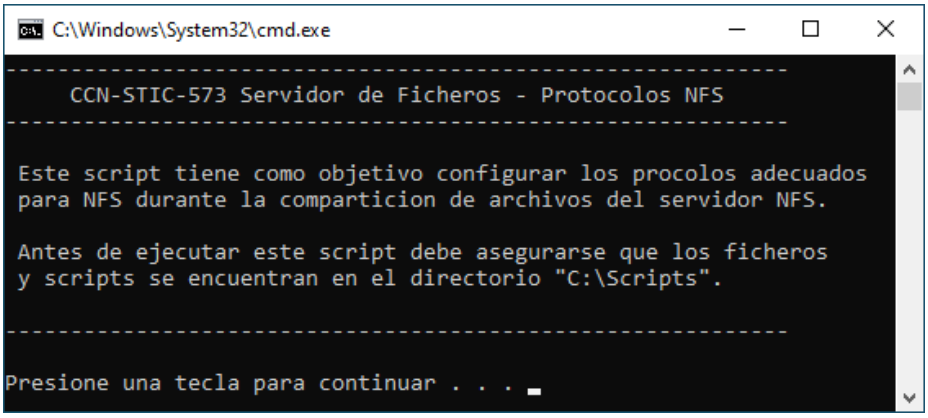
Paso	Descripción
3.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
4.	Reinicie el equipo para asegurar que se aplican todos los cambios.

ANEXO B.4. PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD

A continuación, se establecen las configuraciones necesarias para cumplir con los algoritmos y parámetros de comunicación necesarios dentro de los sistemas operativos Windows Server y aplicable sobre los equipos de tipo Servidor de Ficheros cuando se hace uso del rol NFS.

Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.

Paso	Descripción
2.	Diríjase al directorio “C:\Scripts” copiado en apartados anteriores y ejecute el script “CCN-STIC-573 Servidor de Ficheros - Protocolos NFS.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
3.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
4.	Reinicie el equipo para asegurar que se aplican todos los cambios.

ANEXO B.5. COPIAS DE SEGURIDAD

Los pasos definidos a continuación tienen como objetivo definir las acciones para disponer de un mecanismo que permita recuperar datos perdidos, accidental o intencionadamente.

Nota: Si en su organización ya dispone de un elemento que realice copias de seguridad puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

Antes de continuar tenga en consideración los siguientes aspectos:

a) Deberá disponer de un espacio adicional donde alojar las copias realizadas.

b) La característica "Copias de seguridad de Windows Server" deberá encontrarse implementada en los equipos donde se desea realizar la copia de seguridad.

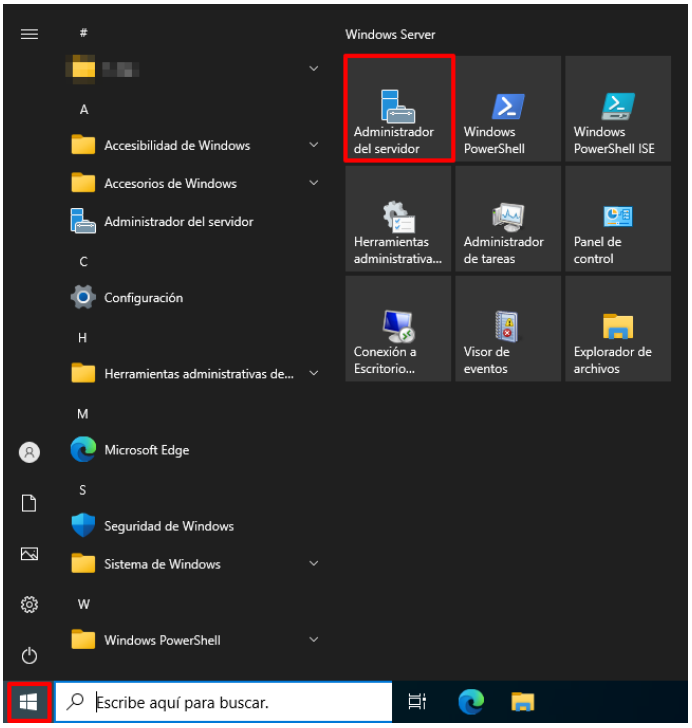
c) El uso de esta herramienta es de uso local por lo que no podrá utilizarse como mecanismo central de gestión de copias, aunque existe la posibilidad de programar dichas copias y alojarlas todas en una misma ubicación remota, de modo que estas se encuentren centralizadas.

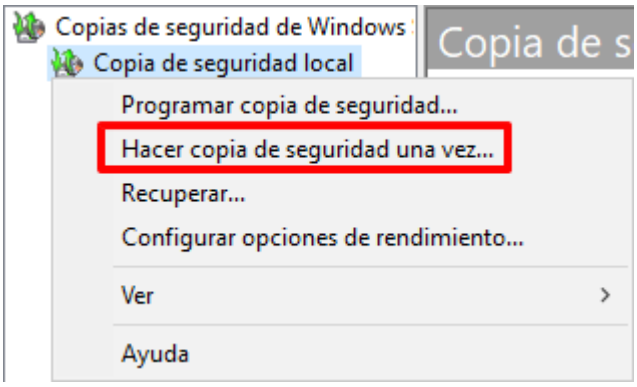
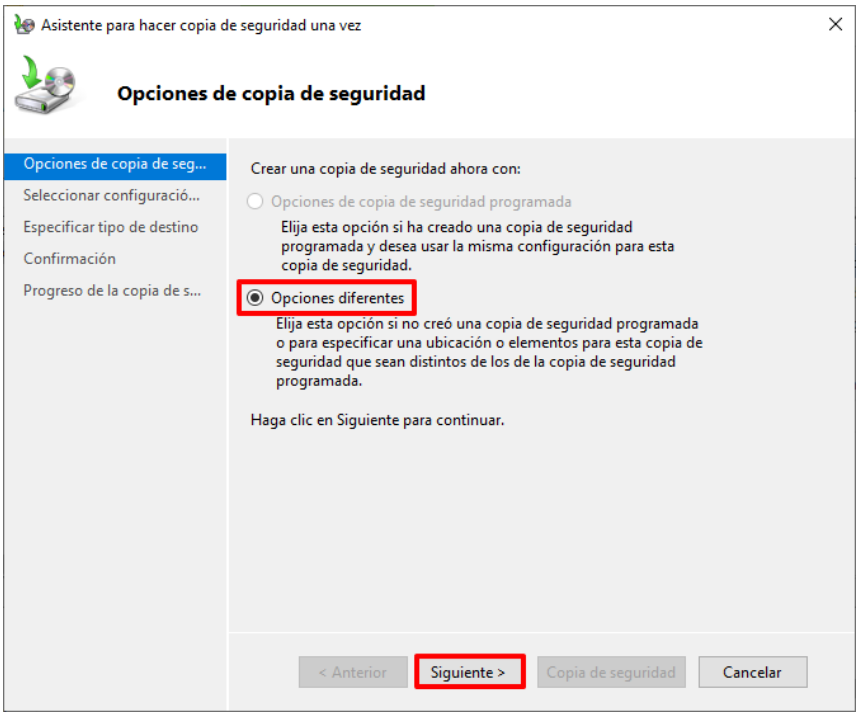
d) Si previamente ha seguido los pasos de Requisitos de Acceso presentes en la guía, codificada como "CCN-STIC-570A23", para ejecutar de forma correcta los pasos indicados a continuación deberá deshabilitar temporalmente el objeto GPO "CCN-STIC-570A23 Incremental Control Dispositivos" en las Unidades Organizativas donde se haya vinculado, o incluir los identificadores necesarios al objeto GPO indicado.

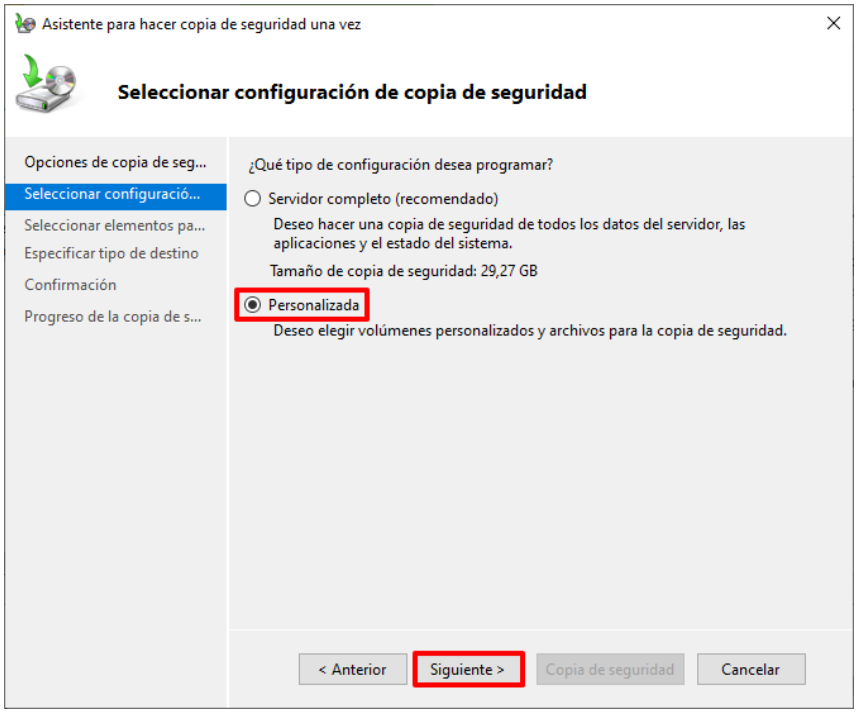
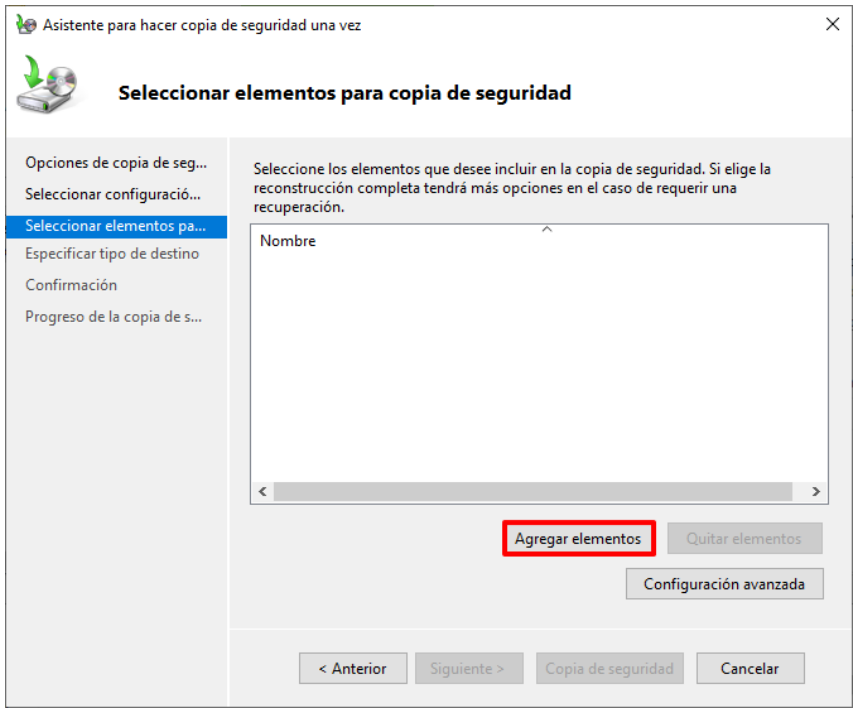
Nota: En este ejemplo se va a realizar una copia de seguridad puntual en el tiempo de una carpeta de datos alojada en un equipo de tipo Servidor Miembro que hace las veces de Servidor de Ficheros.

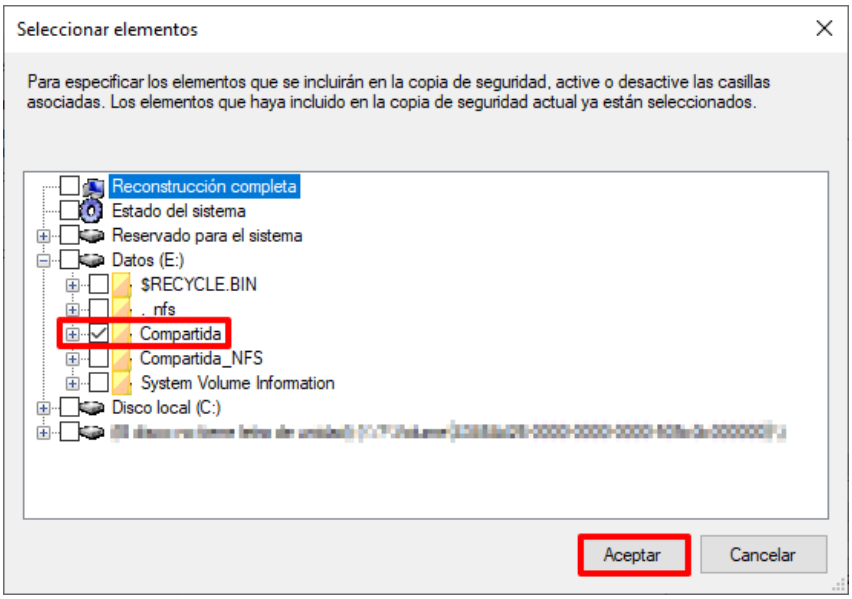
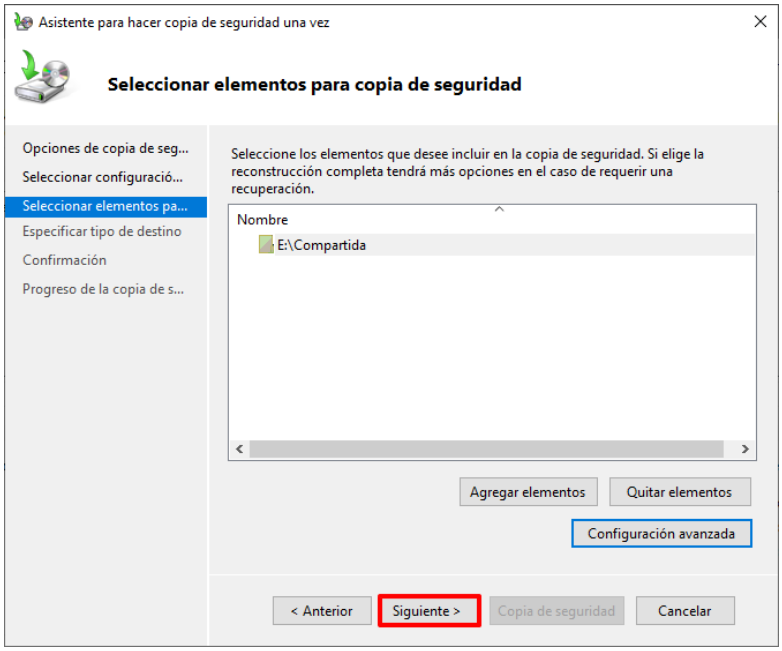
Se recomienda establecer una copia de seguridad programada con el objetivo de que esta se realice de una forma periódica acorde a las políticas de la organización, tomando en consideración su configuración (Completa, Incremental, etc.).

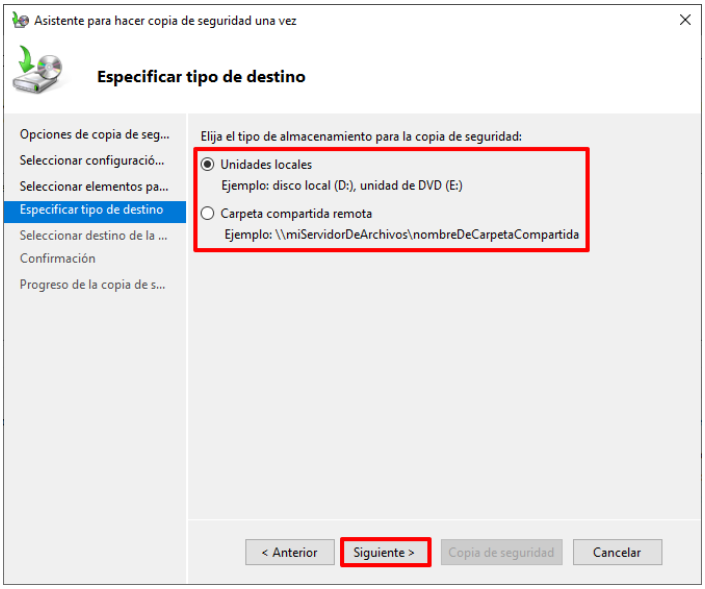
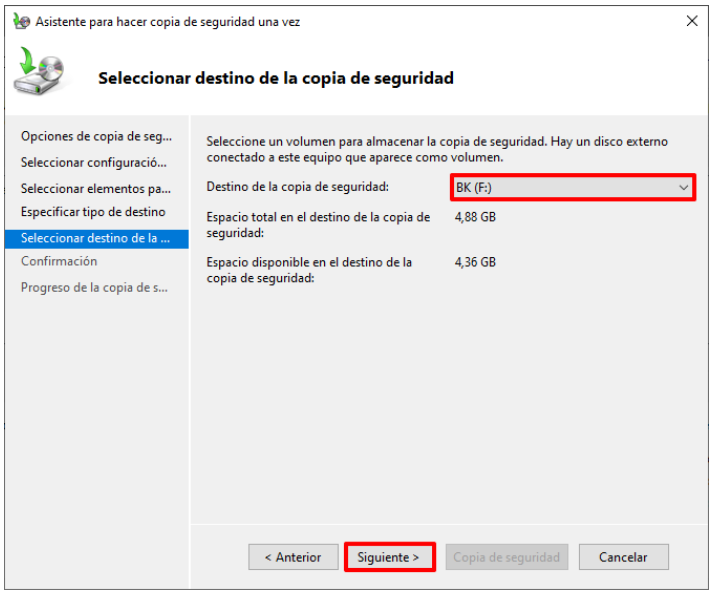
Paso	Descripción
1.	Inicie sesión en el equipo donde desea realizar la copia de seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

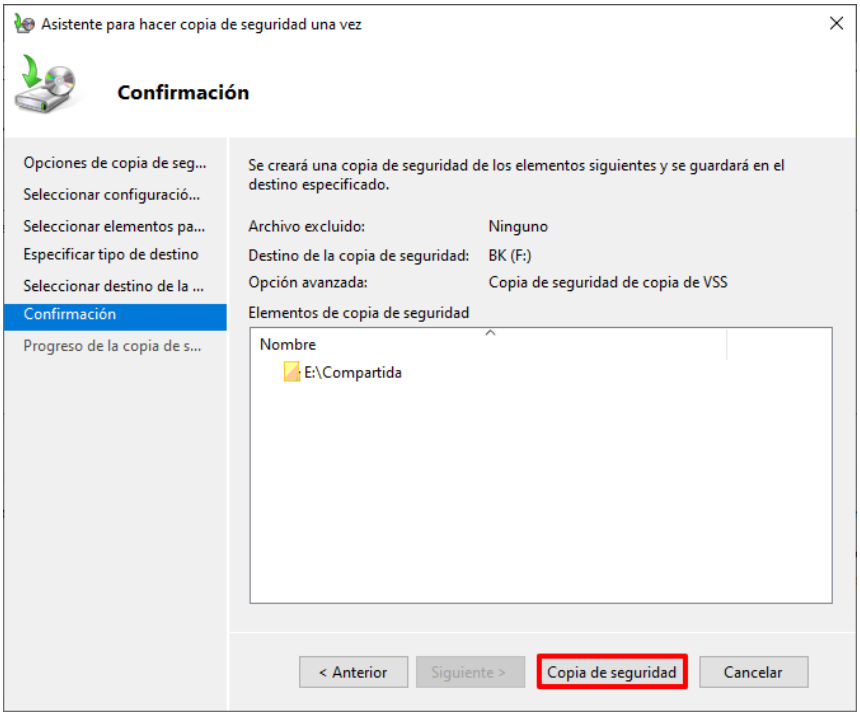
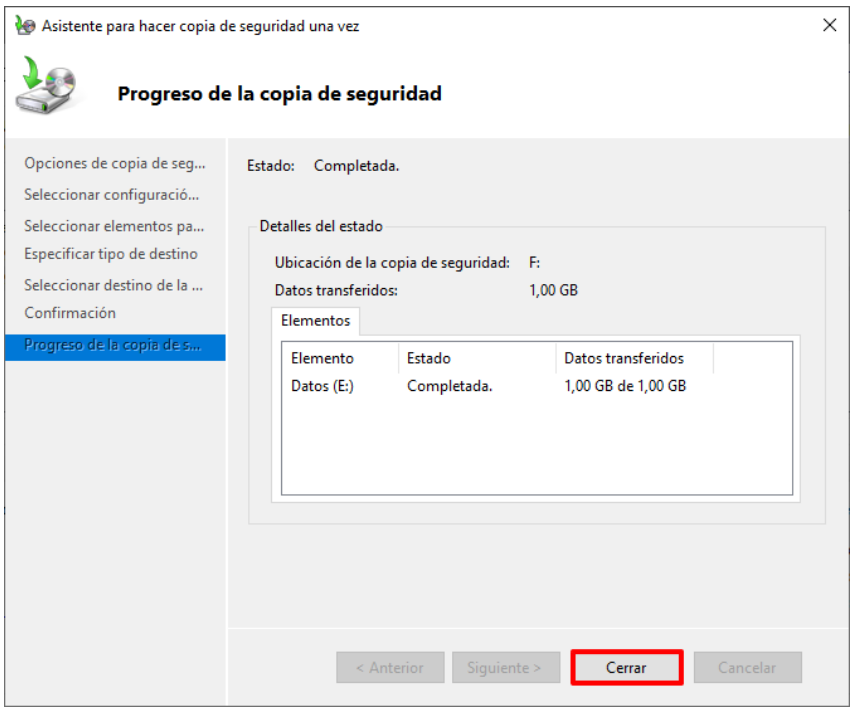
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.
3.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Copias de seguridad de Windows Server”. 

Paso	Descripción
4.	En la consola que se abrirá, haga clic derecho sobre “Copia de seguridad local” y seleccione la opción del menú contextual “Hacer copia de seguridad una vez…”. 
5.	En la primera ventana del asistente mantenga seleccionada la opción “Opciones diferentes” y pulse “Siguiente >”. 

Paso	Descripción
6.	En la siguiente ventana del asistente seleccione la opción “Personalizada” y pulse “Siguiente >” para continuar. 
7.	Pulse en la siguiente ventana del asistente sobre “Agregar elementos”. 

Paso	Descripción
8.	En la nueva ventana emergente deberá seleccionar los recursos compartidos de los que desee realizar la copia de seguridad. Pulse "Aceptar" cuando haya finalizado.  **Nota:** En este ejemplo se ha seleccionado el directorio E:\Compartida.
9.	Pulse "Siguiente >" en la ventana "Seleccionar elementos para copia de seguridad".  **Nota:** Puede hacer uso del botón "Configuración avanzada" para añadir exclusiones a la información seleccionada.

Paso	Descripción
10.	Seleccione el tipo de almacenamiento para la copia de seguridad y pulse “Siguiente >”.  **Nota:** En este ejemplo se hace uso de la opción “Unidades locales”. Dependiendo de la configuración o ubicación donde se desea alojar la copia de seguridad deberá adaptar este paso a sus necesidades.
11.	En la opción “Destino de la copia de seguridad” seleccione la unidad donde desea alojar la copia de seguridad y pulse “Siguiente >”.  **Nota:** En este ejemplo se selecciona la unidad “F:” dedicada a la realización de copias de seguridad. Si en la sección previa (Especificar el tipo de destino) hubiera seleccionado la opción “Carpeta compartida remota” deberá definir en este paso la ruta compartida donde se alojará la copia de seguridad.

Paso	Descripción
12.	Pulse ahora sobre el botón “Copia de seguridad” de la siguiente ventana. 
13.	A continuación, comenzará el proceso de copia de seguridad, cuando finalice podrá evaluar el estado de la ejecución de dicha copia. Pulse “Cerrar” para cerrar el asistente. 

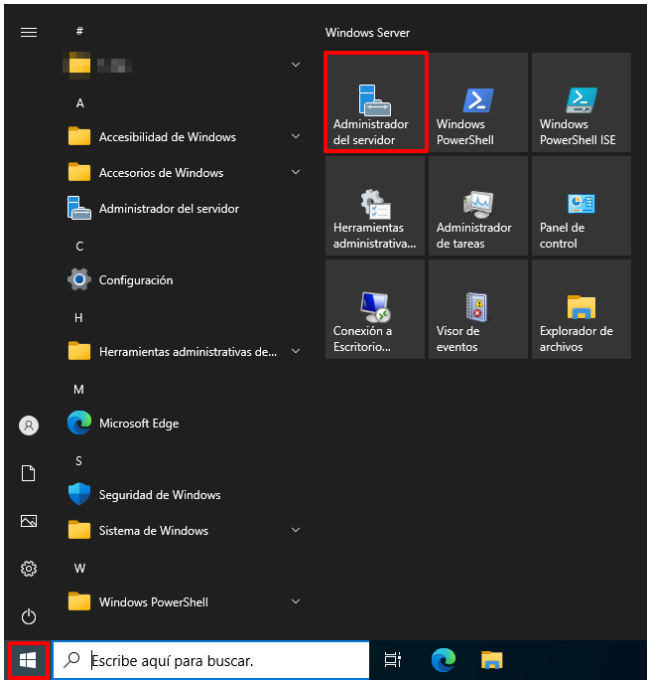
ANEXO C. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

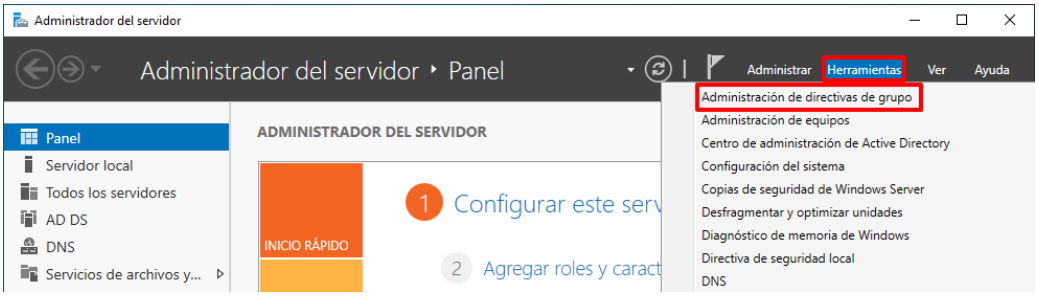
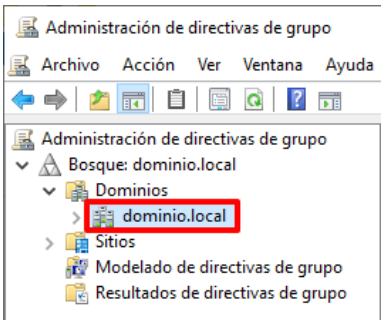
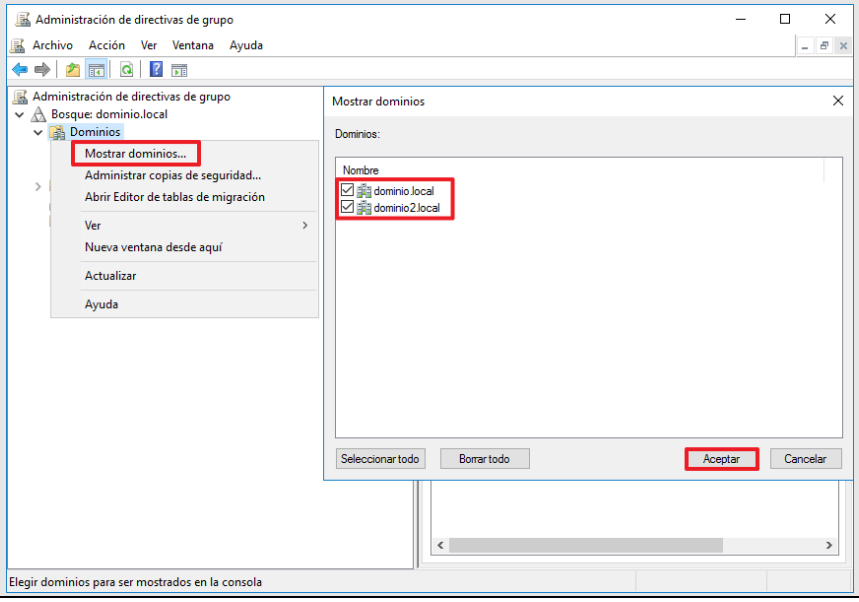
ANEXO C.1. RETENCIÓN DE REGISTROS DE ACTIVIDAD

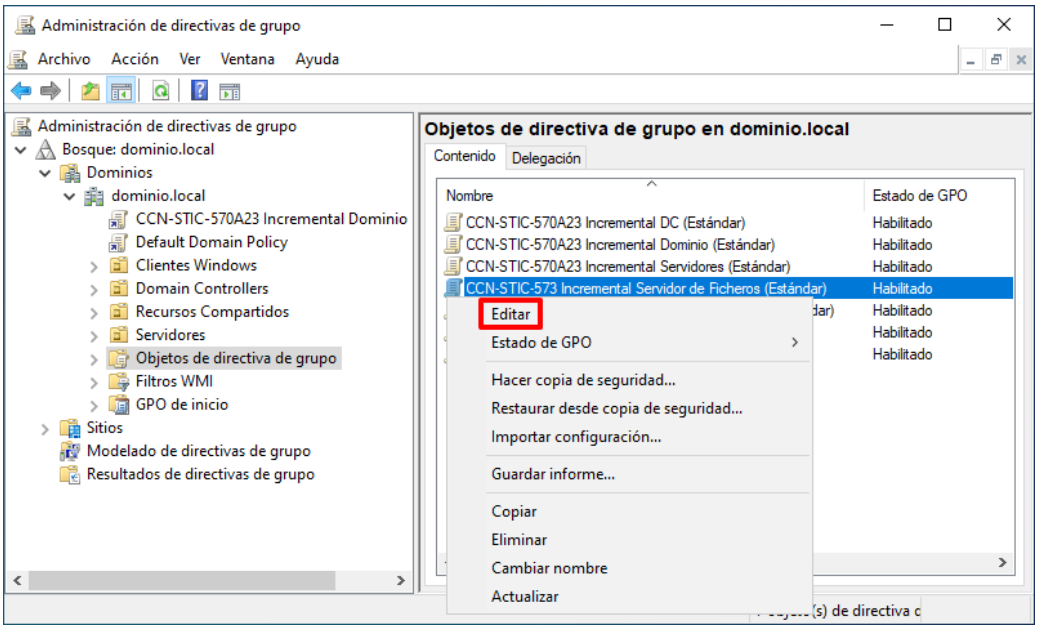
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a los registros de actividad y conforme a lo descrito en su refuerzo número tres (3), es necesario realizar una retención de los eventos auditados antes de que estos sean eliminados.

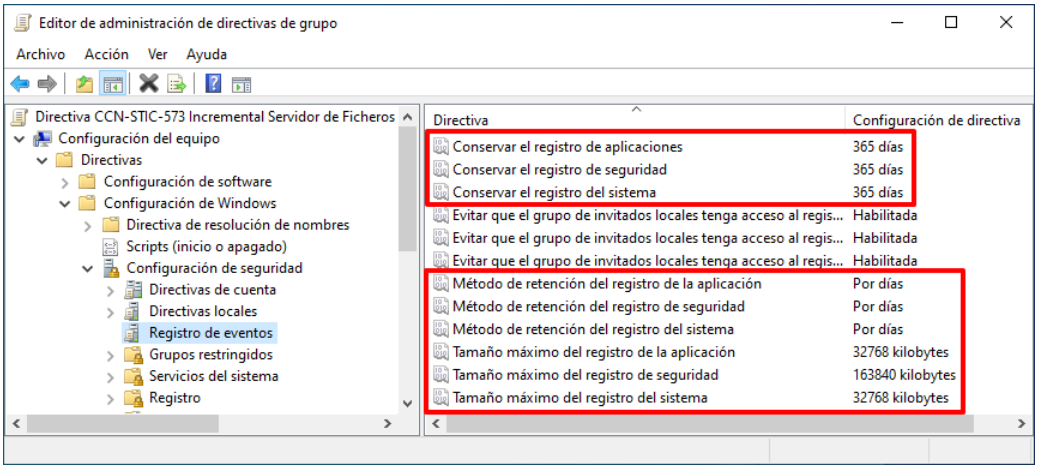
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a modificar y/o adaptar la configuración establecida en los apartados anteriores del presente documento.

Tenga en consideración que **cuando el registro de eventos de Windows se llena, se impide que usuarios sin privilegios de administrador puedan iniciar sesión sobre el equipo**. Para evitar esta situación, **se requiere vaciar el registro de forma manual** para retornar el funcionamiento a un estado normal.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.

Paso	Descripción
3.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
4.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** Compruebe que realiza las tareas de administración sobre el dominio adecuado. Si no aparece su dominio en la ventana, utilice la opción “Mostrar dominios…” del menú contextual, marque los dominios que desea gestionar y pulse sobre “Aceptar” tal y como se indica a continuación. 

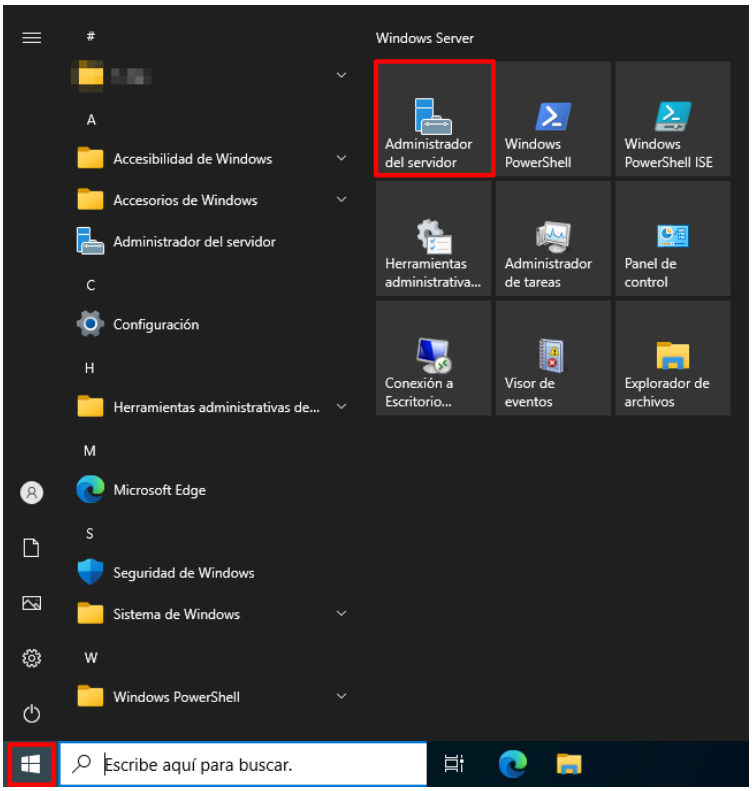
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de retención: – CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO incremental que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-573 Incremental Servidor de Ficheros (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-573 Incremental Servidor de Ficheros ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”**.

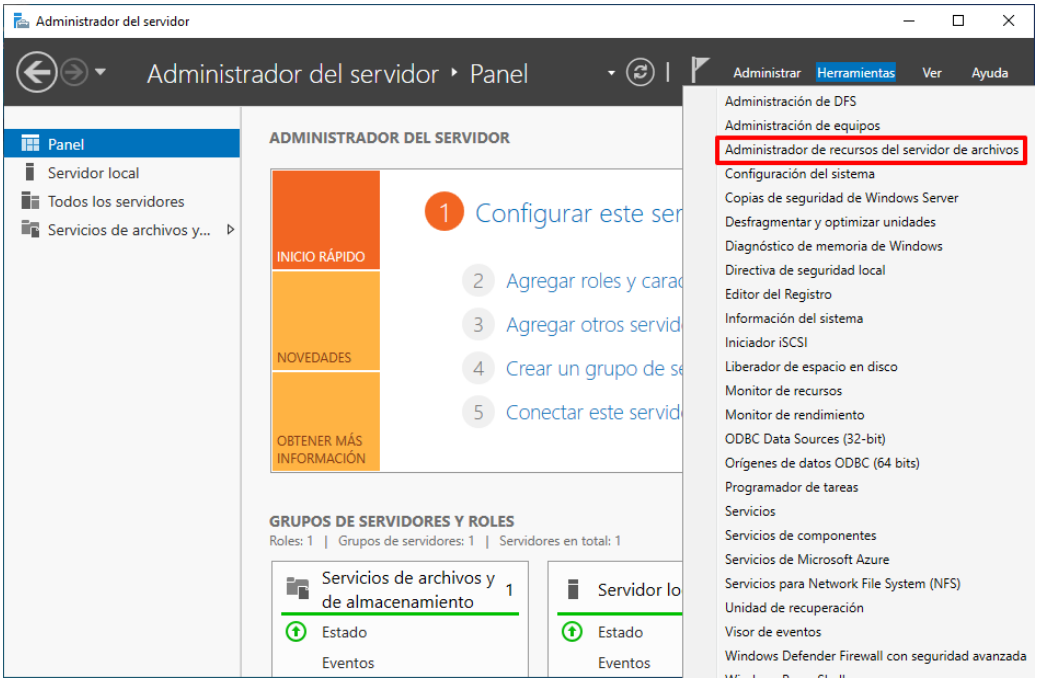
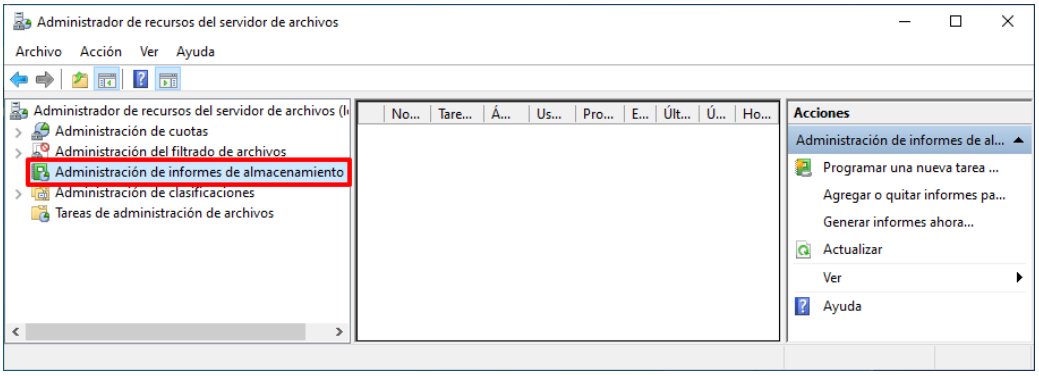
Paso	Descripción
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Conservar el registro de aplicaciones – Conservar el registro de seguridad – Conservar el registro del sistema – Método de retención del registro de la aplicación – Método de retención del registro de seguridad – Método de retención del registro del sistema – Tamaño máximo del registro de la aplicación – Tamaño máximo del registro de seguridad – Tamaño máximo del registro del sistema 
9.	La configuración establecida en las directivas anteriores asegura que los apartados de eventos de aplicaciones, seguridad y sistema se roten a intervalos de un (1) año. En este sentido se ha establecido el máximo tiempo permitido por las configuraciones definidas por el fabricante. De igual modo, en caso de mantener este tiempo de rotación deberá asegurar que el tamaño establecido en sendos registros, permite alojar todos los eventos generados para evitar la pérdida de información. En cualquiera de los casos, deberá adaptar las configuraciones en función de su necesidad tomando en consideración que la configuración actual puede suponer un inconveniente en cuanto al almacenamiento si el sistema no se encuentra correctamente dimensionado. **Nota:** Es posible establecer configuraciones para almacenar todos los eventos o que estos se sobrescriban. En ambos casos será necesario realizar una rotación manual de los registros para evitar un colapso en el almacenamiento del sistema o evitar la pérdida de registros respectivamente.

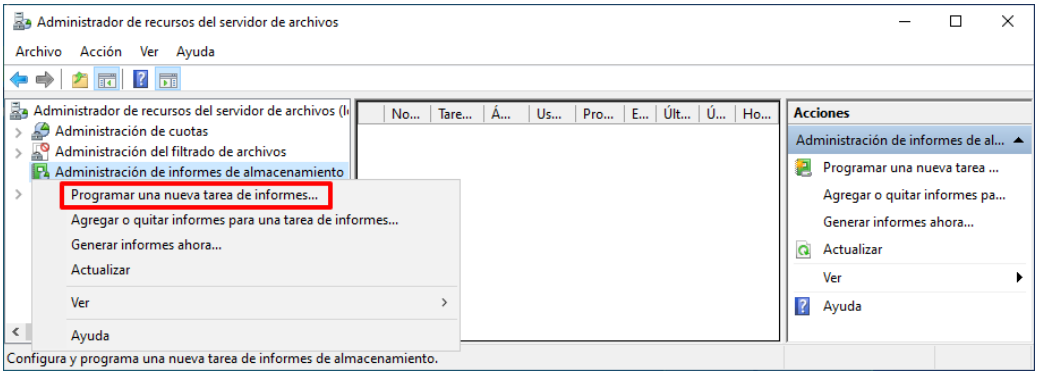
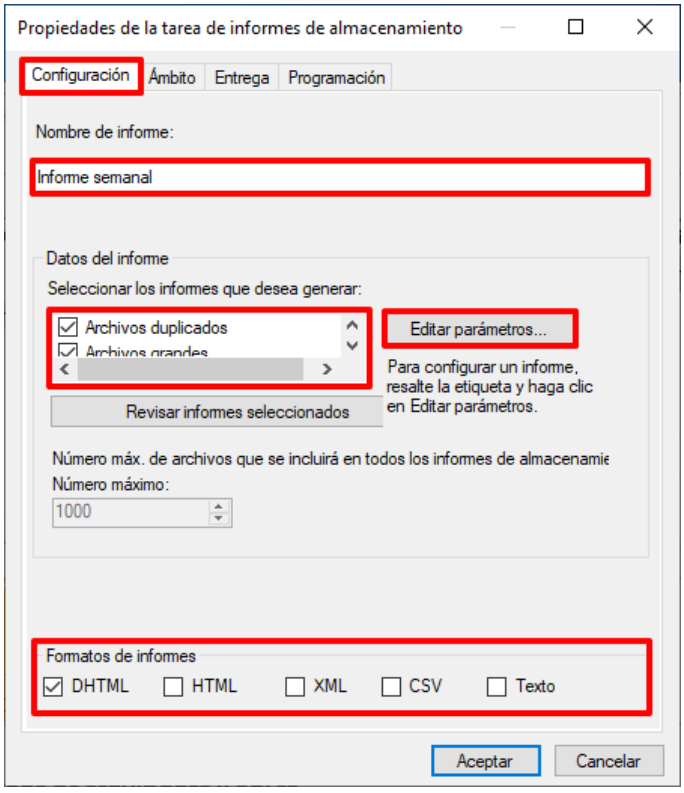
ANEXO C.2. INFORMES DE ALMACENAMIENTO

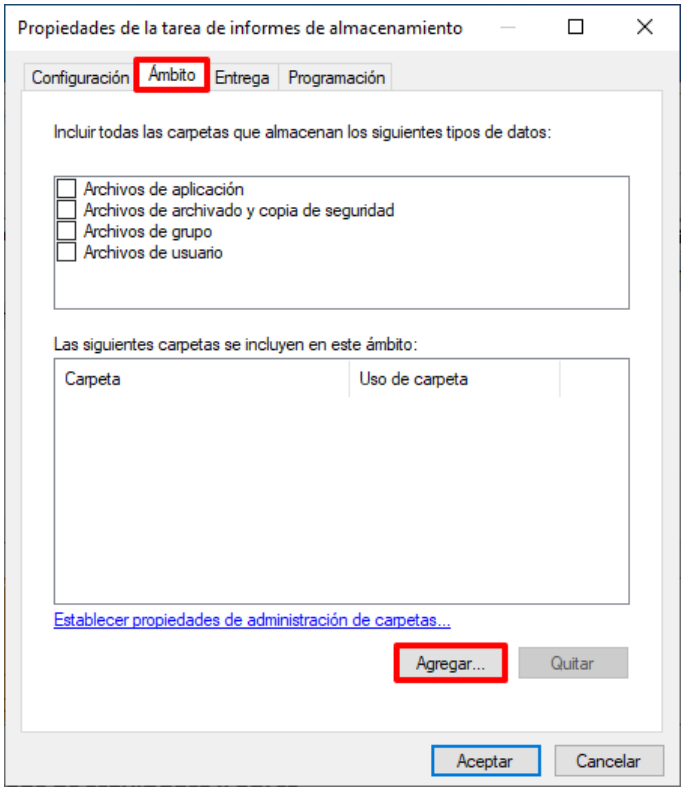
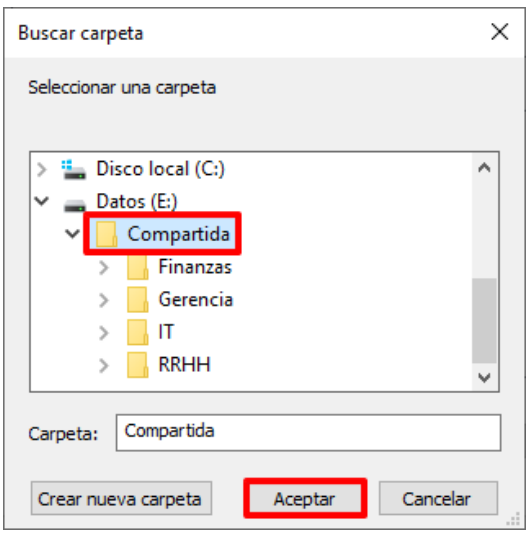
Con el objetivo de la mejora y conocimiento sobre la información alojada en el equipo con el rol Servidor de Ficheros, es posible la configuración de los informes de almacenamiento para disponer de un control más exhaustivo sobre la información alojada en este.

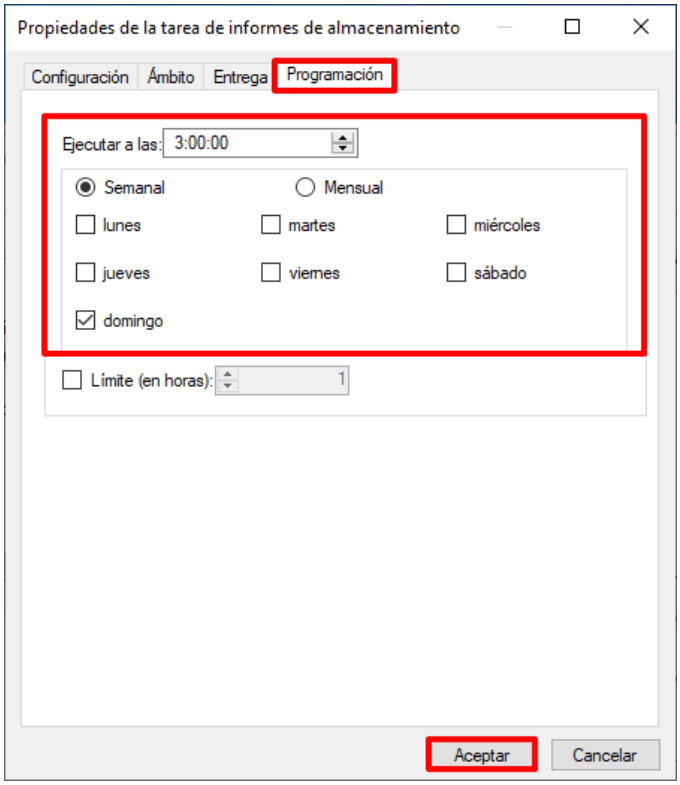
Nota: Deberá disponer del rol "Administrador de recursos del servidor de archivos" instalador para poder hacer uso de esta consola y sus servicios. Instale dicho rol en caso de no disponer del mismo si desea realizar el siguiente paso a paso.

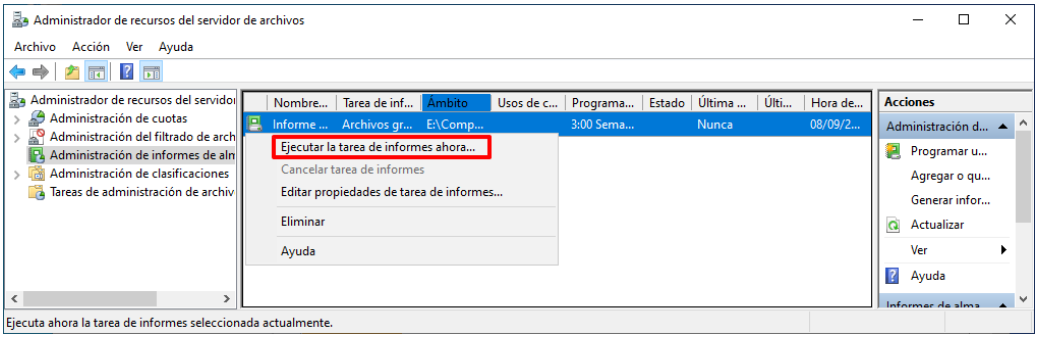
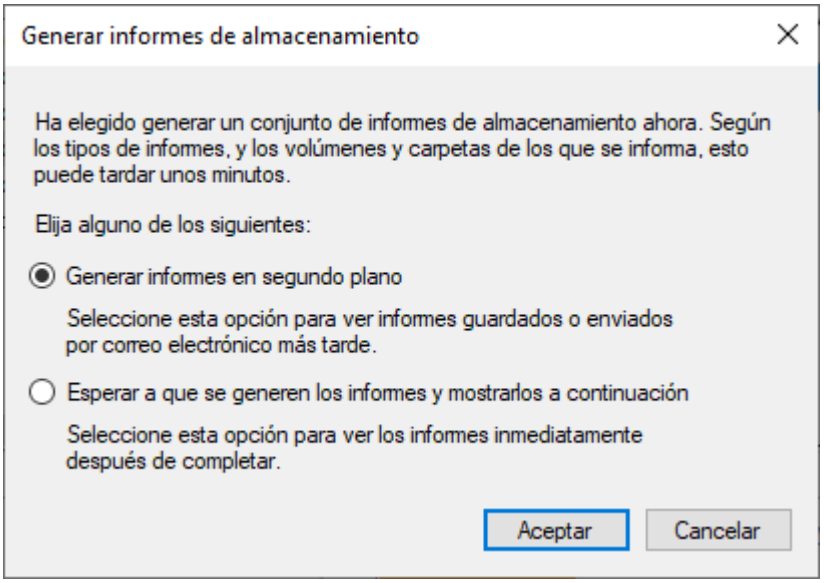
Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
2.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".

Paso	Descripción
3.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administrador de recursos del servidor de archivos”.  **Nota:** Deberá disponer del rol “Administrador de recursos del servidor de archivos” instalador para poder hacer uso de esta consola y sus servicios.
4.	En el “Administrador de recursos del servidor de archivos” diríjase al nodo “Administración de informes de almacenamiento”. 

Paso	Descripción
5.	Haga clic derecho sobre el nodo y seleccione la opción del menú contextual “Programar una nueva tarea de informes…”. 
6.	En la nueva ventana que aparecerá sitúese sobre la pestaña “Configuración” y defina un nombre para el informe. Posteriormente defina los datos que ha de contener el informe y si es necesario edite alguno de dichos datos por medio del botón “Editar parámetros…”. Por último, defina el formato de informe que más se ajuste a sus necesidades.  **Nota:** En este ejemplo se hace uso del nombre de informe “Informe semanal” y la configuración por defecto. Deberá adaptar estos pasos según las necesidades de su organización.

Paso	Descripción
7.	A continuación, diríjase a la pestaña “Ámbito” y pulse sobre el botón “Agregar…”. 
8.	En la ventana emergente, deberá seleccionar el recurso compartido sobre el que desea obtener el informe. Pulse “Aceptar” para continuar.  **Nota:** En este ejemplo se hace uso del recurso compartido de ejemplo denominado “Compartida”. Deberá adaptar los pasos según las necesidades de su organización.

Paso	Descripción
9.	Incluya según se ha especificado en los pasos “7” y “8” todos los recursos compartidos disponibles en el servidor.
10.	Diríjase ahora a la pestaña “Programación” y defina la periodicidad de ejecución del informe. Por último, pulse “Aceptar”.  **Nota:** En este ejemplo se realiza una ejecución semanal del informe a una hora determinada. Deberá adaptar los pasos según las necesidades de su organización.

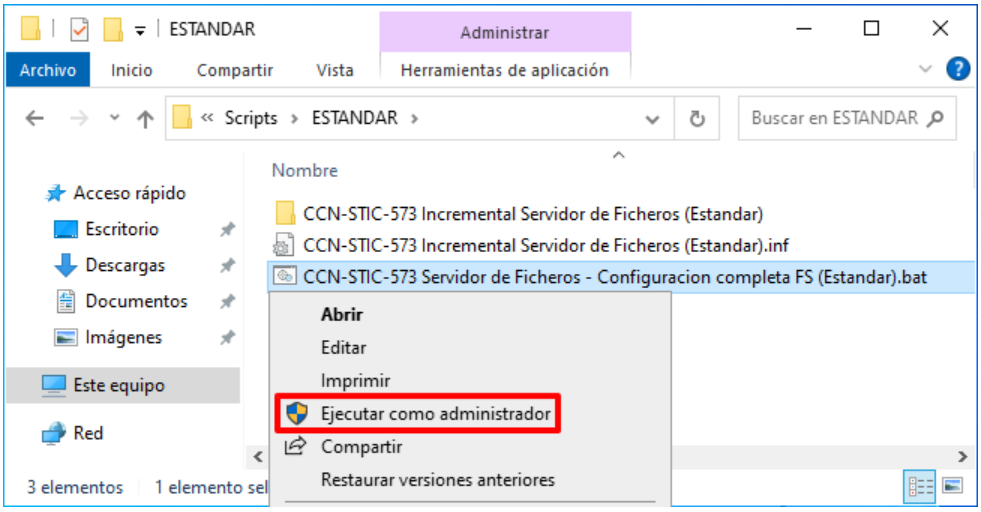
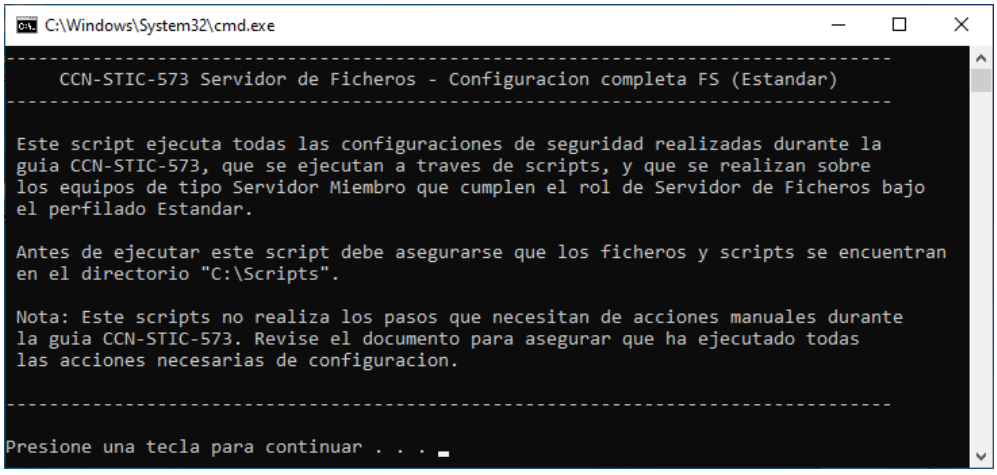
Paso	Descripción
11.	Aparecerá creada la tarea en el panel central. Podrá ejecutar esta tarea a demanda si lo desea haciendo clic derecho sobre la tarea y seleccionando la opción “Ejecutar la tarea de informes ahora…”. En dicho caso deberá además decidir si la tarea se ejecuta en segundo plano o se espera a que se generen los informes para mostrarlos tras su ejecución. Pulse “Aceptar” para continuar.   **Nota:** Por defecto los informes se alojan en la ruta “C:\StorageReports\Scheduled”.

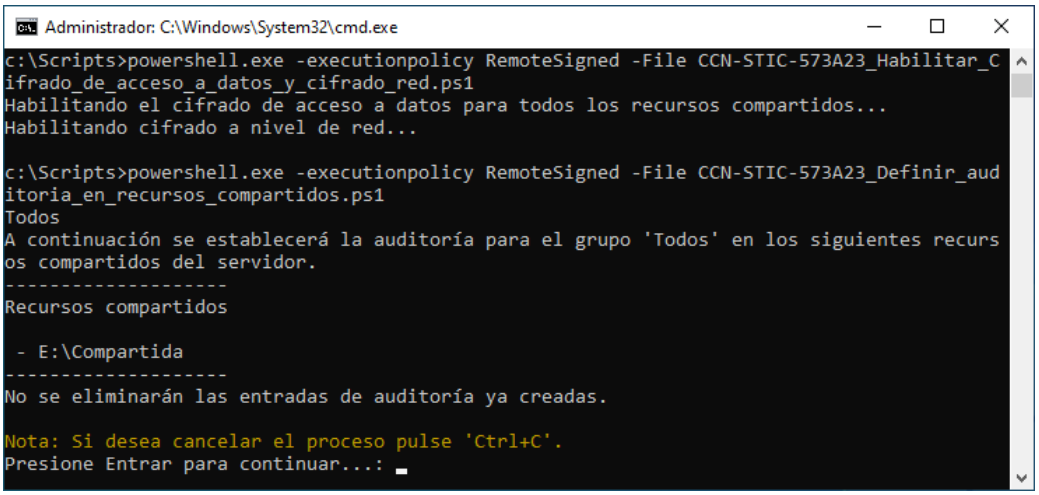
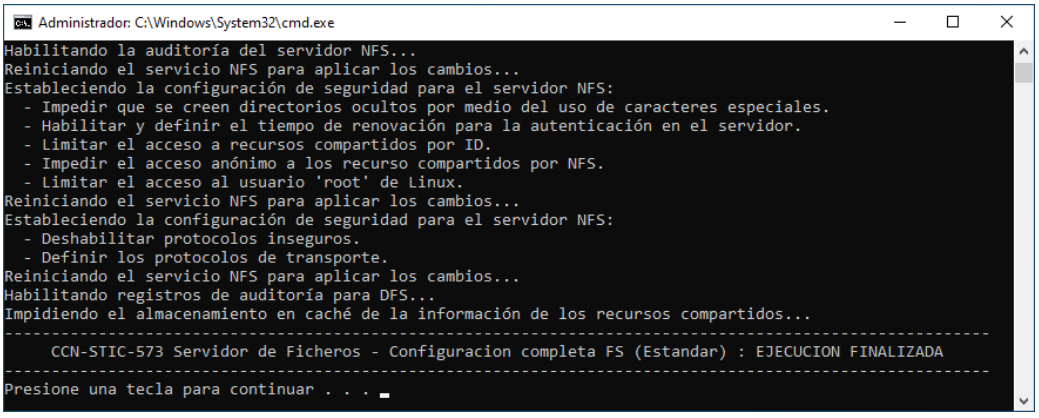
ANEXO C.3. APLICACIÓN DE CONFIGURACIONES COMPLETAS

El siguiente anexo tiene como objetivo ayudar a los administradores a aplicar las configuraciones sobre los Servidores Miembro de la organización que hagan uso del rol de Servidor de Ficheros. Para ello, se han generado diversos scripts que aúnan a otros de modo que es posible ejecutar de forma masiva todos los scripts facilitados en el presente documento.

Tenga en consideración que el script tendrá presente la existencia de ciertos roles instalados para determinar o no la aplicación de dicha configuración sobre estos. Se hace referencia a los roles DFS, NFS y BrachCache para archivos de red.

Nota: La ejecución de este apartado no exime revisar y ejecutar el resto de apartados de la guía debido a que se ejecutan pasos manuales y necesidades adicionales, como las configuraciones a aplicar en el Controlador de Dominio o la configuración de permisos sobre los recursos compartidos. Por ello, una vez realizado este apartado regrese al "ANEXO A.2.3 IDENTIFICACIÓN" para realizar el resto de configuraciones manuales.

Paso	Descripción
1.	Inicie sesión en un servidor miembro del dominio que disponga del rol Servidor de Ficheros donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio o Administrador del Servidor.
2.	Diríjase al directorio "C:\Scripts\[TIPO DE PERFILADO]" copiado en apartados anteriores y ejecute el script "CCN-STIC-573 Servidor de Ficheros - Configuracion completa FS (TIPO DE PERFILADO).bat". Para ello, haga clic derecho sobre el script y seleccione la opción "Ejecutar como Administrador" del menú contextual que aparecerá.  **Nota:** En este ejemplo se hace uso del perfil de configuración "Estándar".
3.	Pulse cualquier botón para iniciar la ejecución del script. 

Paso	Descripción
4.	Verá a continuación como se van ejecutando los scripts necesarios. Pulse "Enter" cuando se lo solicite el script tras la visualización de los recursos compartidos del servidor. 
5.	Pulse cualquier botón para finalizar la ejecución del script. 

Paso	Descripción
6.	Tras la ejecución del script anterior será necesario que ejecute los pasos manuales de cada sección correspondiente teniendo en cuenta el perfil que está aplicando: – ANEXO A.2.4 REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO → Pasos "60" a "105". – ANEXO A.2.5 SEGREGACIÓN DE FUNCIONES Y TAREAS • ESTÁNDAR: Pasos "111" a "140". • USO OFICIAL O MATERIAS CLASIFICADAS: Pasos "111" a "140" y pasos "146" a "171". – ANEXO A.2.6.1 REGISTRO DE LA ACTIVIDAD (USO OFICIAL – MATERIAS CLASIFICADAS) → Pasos "182" a "200". – ANEXO A.2.7 CONFIGURACIÓN DE SEGURIDAD Y GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD • ESTÁNDAR: Pasos "214" a "224". • USO OFICIAL o MATERIAS CLASIFICADAS: Pasos "214" a "224" y pasos "228" a "245".
7.	Reinicie el equipo para asegurar que se aplican todos los cambios.
8.	Según los roles o elementos de compartición de ficheros adicionales instalados en los equipos que realizan estas tareas deberá seguir los pasos manuales descritos a continuación: – ANEXO B.1 REQUISITOS DE ACCESO Y PROCESO DE GESTIÓN DE DERECHOS DE ACCESO → Pasos "1" a "11". – ANEXO B.5 COPIAS DE SEGURIDAD → Pasos "1" a "13".
9.	Reinicie el equipo para asegurar que se aplican todos los cambios.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL