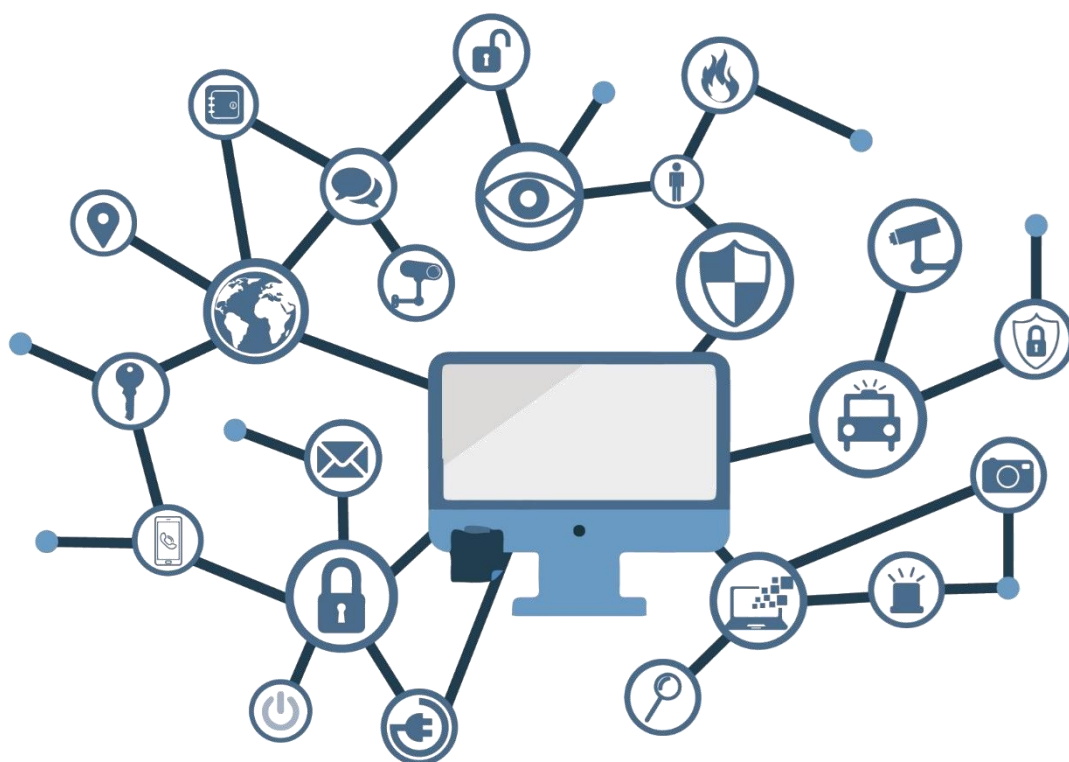


CCN-STIC-573A21

IMPLEMENTACIÓN DE SEGURIDAD EN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2019



JULIO 2022



MINISTERIO DE DEFENSA



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-203-5

Fecha de Edición: julio de 2022

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

cpage.mpr.gob.es

ÍNDICE

1. INTRODUCCIÓN	4
2. OBJETO.....	4
3. ALCANCE	5
4. DESCRIPCIÓN DEL USO DE ESTA GUÍA.....	6
5. DECLARACIÓN DE RIESGOS.....	8
5.1 RIESGOS ASOCIADOS A UN SERVIDOR DE FICHEROS EN WINDOWS SERVER 2019	9
5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO	10
5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO	10
5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA	11
6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES.....	12
7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS	13
ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD PARA UN SERVIDOR DE FICHEROS SOBRE WINDOWS SERVER 2019.....	15
ANEXO A.1. PREPARACIÓN DEL DOMINIO	16
ANEXO A.2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD	27
ANEXO A.3. CONFIGURACIONES ADICIONALES	30
ANEXO A.3.1. CONFIGURACIÓN DE LOS ESPACIOS DE ALMACENAMIENTO	30
ANEXO A.3.2. USO DE LISTAS DE CONTROL DE ACCESO.	38
ANEXO A.3.3. LIMITACIÓN DE USO DE ESPACIO EN DISCO.....	42
ANEXO A.3.4. VISIBILIDAD DE LA ESTRUCTURA DE CARPETAS DE FICHEROS DE DATOS.	48
ANEXO A.3.5. FILTRADO DE ARCHIVOS.	52
ANEXO A.3.6. SEGREGACIÓN DE ROLES.	57
ANEXO A.3.7. COPIAS DE SEGURIDAD.	61
ANEXO A.3.8. AUDITORIA DE ARCHIVOS.	65
ANEXO A.3.9. ELIMINACIÓN DE DATOS DUPLICADOS.....	73
ANEXO A.3.10. MEDIDAS ANTI-RANSOMWARE HABILITADAS.....	78
ANEXO A.3.11. DISCOS DE DATOS CIFRADOS.....	83

1. INTRODUCCIÓN

Esta guía forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en las tecnologías y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación en el cumplimiento del Esquema Nacional de Seguridad (ENS) y para los sistemas que manejen información clasificada.

La serie CCN STIC 500 se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán sucesivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté configurando.

2. OBJETO

El propósito de esta guía es proporcionar los procedimientos para aplicar un perfilado de seguridad, en base a un análisis de riesgos preceptivo, en sistemas que implementen servidores Windows Server 2019 y que actúen como servidor de ficheros.

La configuración que se aplica a través de la presente guía se ha diseñado para adaptarse a las características específicas de cada entorno, en función de los resultados obtenidos del análisis de riesgos preceptivo. 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 por el análisis de riesgos preceptivo de cada escenario, la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- b) Se tendrán en cuenta los avances tecnológicos y el estado de arte más reciente en ciberseguridad.
- c) Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca utilizando la Declaración de Aplicabilidad como elemento fundamental sobre el que vertebrar la seguridad en base a responsabilidad compartida.
- d) La Declaración de Aplicabilidad (conjunto de medidas a implementar) utilizarán de base los niveles del Esquema Nacional de Seguridad validados por el análisis de riesgos preceptivo utilizando de base una categorización de ENS MEDIO.
- e) Las medidas de seguridad se podrán aplicar a sistemas ya implementados o nuevos sistemas, minimizando el impacto en el entorno de producción.
- f) Las guías se revisarán y se actualizarán según las nuevas amenazas y estado de arte tecnológico en ciberseguridad.

Este marco de aplicación basado en un perfilado de seguridad tiene en consideración la diversidad de escenarios que se pueden dar, con sus particularidades, riesgos y amenazas, por lo que será cada organización que implementa las medidas de seguridad la que deba determinar qué medidas serán de aplicación, compensadas o complementadas, en función de sus condiciones específicas asumiendo una responsabilidad compartida en la puesta en operación del sistema.

Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación:

- a) Alcance básico.
- b) Alcance intermedio.
- c) Alcance avanzado.

Para la elaboración de esta guía, se ha hecho un esfuerzo de revisión exhaustiva de las distintas configuraciones de seguridad disponibles en Windows Server 2019, alineándolas y clasificándolas en función de los riesgos que cada una de ellas mitigan o abordan individualmente.

De esta forma, se pretende dar mayor coherencia al conjunto de medidas resultantes o perfilado de seguridad, siendo necesario aplicar únicamente aquellas medidas que realmente atienden a un riesgo declarado en función de los niveles de alcance señalados anteriormente.

Se trata de implementar medidas con un criterio claro, conociendo los riesgos, el contexto de la amenaza y la superficie de exposición de cada sistema en particular, y adaptando las medidas de seguridad a aplicar en función de ello.

3. ALCANCE

Para ayudar a las organizaciones a identificar los riesgos de seguridad y por lo tanto realizar el perfilado correspondiente para cada uno de sus sistemas, se ha incorporado a esta guía un apartado denominado declaración de riesgos donde se identifican y se explican los principales riesgos del producto o tecnología de que trata la guía.

Esta guía se ha elaborado con el objetivo de proporcionar información específica sobre los riesgos y las medidas de mitigación recomendadas para los escenarios planteados. En particular, se incluirá la configuración para aplicar un perfilado de seguridad de un servidor con “Windows Server 2019”, instalado en español con la versión completa del producto, bien actuando con el rol de servidor de ficheros.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

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 pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

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

Este documento incluye:

- a) Descripción de uso de esta guía. Breve explicación acerca de los pasos a seguir para identificar, seleccionar y aplicar las medidas de seguridad recomendadas.
- b) Declaración de riesgos. En esta sección se identifican los principales riesgos asociados al producto o tecnología del que trata la guía CCN-STIC. Por ejemplo, un servicio web puede tener riesgos relacionados con el acceso remoto, mientras que un controlador de dominio puede tener riesgos relacionados con los procesos de autenticación. La organización podrá hacer uso de los riesgos identificados en este punto y añadir los que considere necesarios para su escenario en particular.
- c) Identificación de valor de riesgo. En esta sección se muestran una serie de tablas o mapas de calor, con tres (3) niveles de superficie de exposición y los valores de riesgo resultantes de la intersección de los niveles de impacto y probabilidad. Se trata de una muestra de cómo alterando alguna de estas variables (superficie de exposición, impacto y probabilidad), los resultados del riesgo de adecúan a cada realidad.
- d) Perfilado de seguridad. En este punto se establecen las medidas de seguridad que se deberán aplicar al producto o tecnología del que trata la guía. Su clasificación se realiza en tres (3) niveles, cada uno de ellos asociado a un conjunto de niveles de riesgos.

4. DESCRIPCIÓN DEL 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) **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. Para ello, se han identificado una serie de riesgos inherentes al producto o tecnología, los cuales deberán ser completados con los riesgos particulares del sistema que se vaya a implementar.

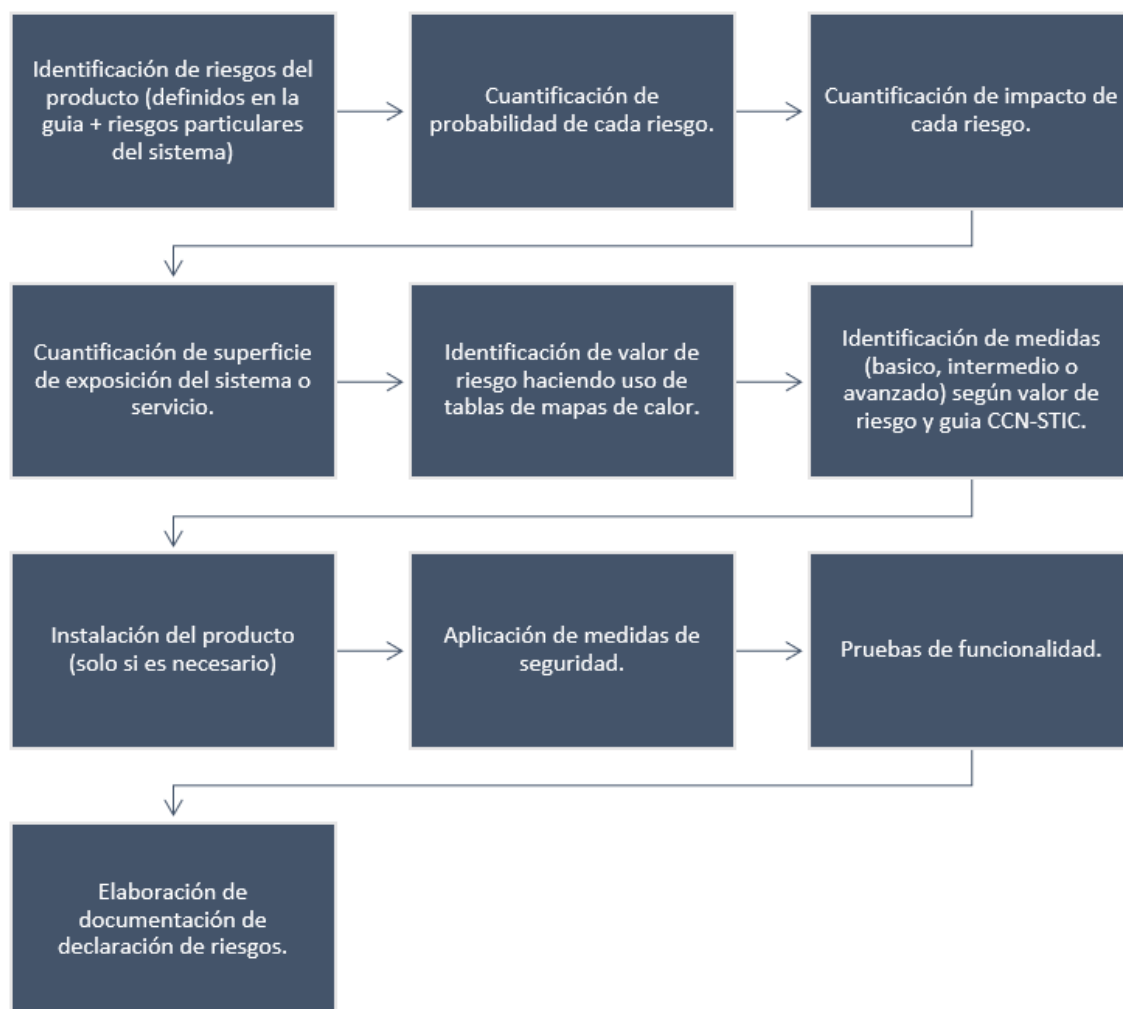
Para la identificación inicial de riesgos, se ha empleado la metodología MAGERIT y la herramienta PILAR, sobre un escenario basado en un sistema operativo Windows Server 2019 con las características de servidor de ficheros habilitadas.

- b) **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.
- c) **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.
- d) **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).

- e) **Identificación de valor de riesgo haciendo uso de tablas de mapas de calor.** Para cada guía, se han desarrollado una serie de tablas de mapas de calor, permitiendo calcular e identificar dónde se sitúa cada uno de los riesgos identificados en los primeros pasos. Una vez identificado el nivel de riesgo, en el siguiente paso se procederá a aplicar la medida correspondiente para mitigar dicho nivel de riesgo.
- f) **Identificación de medidas (básico, intermedio o avanzado) según valor de riesgo y guía CCN-STIC.** La lista de medidas de seguridad está agrupada en categorías y ordenada según el nivel de riesgo resultante de los cálculos anteriores. Es importante señalar que cada categoría puede conllevar la necesidad de aplicar una o varias medidas de seguridad que, a su vez, se pueden traducir en distintas configuraciones, directivas de seguridad o la instalación de software de protección.

Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de adaptación al entorno a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta guía de seguridad se identifican qué medidas de seguridad serán necesarias aplicar, pero el cómo aplicarlas se deja a responsabilidad de las propias organizaciones.

- g) **Instalación del producto (en nuevas instalaciones).** Una vez conocidos los riesgos y las medidas de mitigación de éstos, se procederá a la instalación del sistema operativo en el caso de nuevas implementaciones. En caso de que el sistema ya se encuentre instalado, se puede saltar este paso.
- h) **Aplicación de medidas de seguridad.** En este paso, se aplicarán las medidas de seguridad recomendadas según el nivel de riesgo resultante para hacer efectiva la mitigación, reducción o eliminación del riesgo. Es lo que se denomina perfilado de seguridad. Cada organización puede tener un perfilado distinto, como se ha indicado anteriormente, se deberán aplicar las medidas de seguridad en función de dicho perfilado.
- i) **Pruebas de funcionalidad.** Se recomienda diseñar y ejecutar un plan de pruebas de funcionalidad posterior a la aplicación de medidas, dado que alguna de ellas 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.
- j) **Elaboración de documentación de declaración de riesgos.** Se recomienda elaborar un documento de declaración de riesgos donde se establezca claramente cada uno de los riesgos identificados y las medidas de seguridad aplicadas.



5. DECLARACIÓN DE RIESGOS

Se trata del primer paso a realizar para la aplicación de las medidas de seguridad acordes a la realidad y condiciones donde estará operando el sistema.

Con motivo de la aparición de nuevas versiones y cambios en el software de base, como los sistemas operativos, es altamente recomendable contar con unas medidas de seguridad y de evaluación constantes que puedan detectar, de forma proactiva y previa a su aplicación, cualquier vulnerabilidad, amenaza o riesgo.

El análisis de riesgos permitirá elaborar un perfilado para la aplicabilidad de medidas acorde a los resultados obtenidos, minimizando los vectores de ataque, brechas o malas configuraciones de seguridad sobre los activos, e intentando también que estas medidas no afecten a la funcionalidad o usabilidad del sistema y sus objetivos.

Esta guía de seguridad tiene como uno de sus objetivos ayudar a la implementación de las medidas de seguridad, por lo tanto, para la elaboración de la propia guía se ha realizado un análisis de riesgos específico para un sistema basado en Windows Server 2019 con el rol implementado de Servidor de Ficheros.

Para la ejecución del presente Análisis de Riesgos, se han definido dos (2) escenarios base, los cuales se consideran esenciales y estándar de uso del sistema operativo.

- a) El primer escenario será un sistema aislado en red, quiere decir que estará conectando a elementos de red internos dentro de una organización o entidad, pero no realizará conexiones externas hacia redes no seguras como Internet.
- b) El segundo escenario será un sistema conectado a redes no seguras como puede ser Internet, quiere decir que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

5.1 RIESGOS ASOCIADOS A UN SERVIDOR DE FICHEROS EN WINDOWS SERVER 2019

A continuación, se identifican los resultados de este análisis, los cuales forman parte de la declaración de riesgos y constituye, como ya se ha indicado, el primer paso a realizar en la implementación de esta guía de seguridad. Estos riesgos se deberán tener en consideración cuando la organización diseñe y elabore su propio análisis de riesgos.

Para facilitar la tarea de identificar, cuantificar y valorar cada uno de los riesgos, se ha elaborado la siguiente tabla de control, donde se podrán ir registrando, en cada caso, los niveles de probabilidad e impacto asociados a cada riesgo para un equipo en concreto.

EXP	NOMBRE DEL EQUIPO			
	SISTEMA OPERATIVO		BUILD	
	FUNCION PRINCIPAL		FECHA DE AA.RR.	
NUM	RIESGOS	APLICA (S/N)	PROBABILIDAD [1...5]	IMPACTO [1...5]
1.	[A.3] Manipulación de los registros de actividad (log)			
2.	[A.5] Suplantación de la identidad			
3.	[A.6] Abuso de privilegios de acceso			
4.	[A.11] Acceso no autorizado			
5.	[A.13] Repudio (negación de actuaciones)			
6.	[A.24] Denegación de servicio			
7.	[A.25] Robo de equipos			

5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO

El siguiente paso será cuantificar la probabilidad de cada uno de los riesgos. Los valores de probabilidad podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) muy poco probable y cinco (5) muy probable.

- a) **Probabilidad 1:** Es muy poco probable que se materialice el riesgo, ya sea por las condiciones específicas del sistema en la organización o porque existan salvaguardas ya implementadas que hagan que el riesgo prácticamente desaparezca.
- b) **Probabilidad 2:** Es poco probable que se materialice el riesgo, aunque se puede materializar.
- c) **Probabilidad 3:** Es probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- d) **Probabilidad 4:** Es bastante probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- e) **Probabilidad 5:** Es muy probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización o porque no existen salvaguardas que reduzcan la probabilidad de materialización del riesgo. Las medidas de seguridad a aplicar cuando se da este nivel pueden ser más estrictas que en niveles inferiores.

5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO

Al igual que sucede con la cuantificación de la probabilidad, se deberá cuantificar el grado de impacto en el servicio o negocio en el supuesto caso de que el riesgo se materialice. Los valores de impacto podrán ir desde el valor 1 hasta el valor 5, siendo 1 cuando no tiene un impacto conocido o es muy pequeño y 5 cuando el impacto es muy importante.

- a) **Impacto 1:** El riesgo, en el caso de que se materialice, no tiene un impacto conocido o es muy pequeño, prácticamente despreciable. Los datos y el servicio no se ven comprometidos y el sistema funciona correctamente. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- b) **Impacto 2:** El riesgo, en el caso de que se materialice, tiene un impacto pequeño. No se han comprometidos los datos ni el servicio, sin embargo, es posible que, si no se corrige, el sistema se vuelva inestable o pueda existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- c) **Impacto 3:** El impacto en el sistema es preocupante. No se han comprometido los datos, sin embargo, el servicio puede continuar de forma limitada y, a corto plazo, podría haber una degradación de la seguridad del sistema. Si no se aplican las medidas necesarias puede existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención, pero también medidas de corrección.

- d) **Impacto 4:** El impacto en el sistema es importante. Es posible que algunos datos hayan sido comprometidos y los servicios se hayan visto afectados. También es posible que el sistema se haya vuelto inestable o comience a ser vulnerable. Se debe actuar lo antes posible para restablecer el correcto funcionamiento.
- e) **Impacto 5:** El impacto en el sistema es muy importante. Afecta directamente a la disponibilidad del servicio, imposibilitando el acceso a la información. El sistema ha sido comprometido y algunos o todos los datos han sido comprometidos. Un atacante externo puede haber obtenido acceso privilegiado y puede estar controlando el sistema. Se deben aplicar medidas de recuperación de forma inmediata.

5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA

Por último, se deberá tener en cuenta el nivel o grado de exposición del sistema a las amenazas y riesgos externos. Este valor actuará como modulador a la hora de calcular el valor final de cada uno de los riesgos.

Por ejemplo, ante un riesgo cuyo impacto y probabilidad son altos o muy altos, si el sistema se encuentra en un nivel de superficie de exposición bajo, es lógico pensar que el valor final del riesgo se vea atenuado, en parte, por las condiciones de exposición en las que encuentra el sistema. Por el contrario, si un riesgo tiene unos niveles de impacto y probabilidad bajos, ante un nivel de superficie de exposición alto, es lógico pensar que el valor final del riesgo se vea incrementado por este mismo motivo.

Es evidente que pueden existir multitud de escenarios y configuraciones de red, siendo prácticamente imposible reflejar todas ellas en una sola guía de seguridad. Sin embargo, para una mejor comprensión y simplificación de las medidas que se deberán adoptar, se han agrupado en tres (3) niveles las distintas opciones de superficie de exposición.

- a) **Nivel de superficie de exposición 1:** representa aquellos sistemas que no están expuestos a riesgos externos procedentes de redes interconectadas o redes no confiables como Internet. En este nivel se encuentran los sistemas aislados, sin ningún tipo de comunicación con otras redes.
- b) **Nivel de superficie de exposición 2:** representa aquellos sistemas que tienen algún tipo de conexión de red local o de interconexión con otras redes. Estos sistemas se conectan únicamente con redes confiables. En este nivel, se encuentran los sistemas compuestos por más de un equipo conectado a través de una red local (LAN) o varios sistemas que están interconectados entre sí, a través de otros medios, pero que no son accesibles desde Internet o redes no confiables.
- c) **Nivel de superficie de exposición 3:** representa aquellos sistemas accesibles desde o con conexión directa o indirecta con Internet y otras redes. Dado que Internet se considera una red no confiable, el riesgo de explotación de vulnerabilidades de ejecución remota es mucho mayor que en los niveles inferiores. En este nivel se encuentra la mayoría de los sistemas en producción de las organizaciones.

6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES

Una vez identificados los distintos riesgos inherentes al sistema y después de calcular los valores de probabilidad, impacto y superficie de exposición de cada uno de ellos, el siguiente paso será determinar el valor final de cada riesgo. Tal y como ya se ha indicado, este valor variará en función de cada una de las tres (3) variables que se han tenido en cuenta.

Para facilitar su cálculo, se han elaborado las siguientes tablas con un diseño de mapas de calor, que varían según la superficie de exposición que tendrá el sistema. Cada una de ellas servirá como referencia para determinar el valor final del riesgo, el cual se podrá anexar a la tabla de riesgos del punto “5.1 RIESGOS ASOCIADOS A UN SERVIDOR DE FICHEROS EN WINDOWS SERVER 2019”.

SUPERFICIE DE EXPOSICIÓN		1			
PROBABILIDAD	NIVEL DE RIESGO				
5	5	6	7	7	8
4	4	5	6	7	7
3	3	4	5	6	7
2	2	3	4	5	6
1	2	2	3	4	5
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		2			
PROBABILIDAD	NIVEL DE RIESGO				
5	6	7	7	8	9
4	5	6	7	7	8
3	4	5	6	7	7
2	3	4	5	6	7
1	2	3	4	5	6
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		3			
PROBABILIDAD	NIVEL DE RIESGO				
5	7	7	8	9	10
4	6	7	7	8	9
3	5	6	7	7	8
2	4	5	6	7	7
1	3	4	5	6	7
IMPACTO	1	2	3	4	5

7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS

A continuación, se muestran las categorías o agrupación de medidas de seguridad que deberán ser aplicadas a Windows Server 2019, en función de los resultados obtenidos por el análisis de riesgos y la cuantificación de cada uno de éstos.

Para una mejor comprensión, se han agrupado las medidas en tres (3) alcances de implementación, cada uno de ellos asociado a un grupo de niveles de riesgos.

- a) Alcance básico.
- b) Alcance intermedio.
- c) Alcance avanzado.

Una vez obtenido el nivel de riesgo de cada uno de los riesgos identificados, se aplicará la siguiente tabla para determinar las medidas necesarias en cada nivel.

Esta tabla indica que, si se ha obtenido un valor menor o igual a 3, se deberán aplicar las categorías de perfilado de seguridad de alcance BÁSICO. Si el valor obtenido para un riesgo determinado está entre 4 y 6, se deberán aplicar las categorías de perfilado de seguridad de alcance INTERMEDIO. Por último, si el valor obtenido es 7 o superior, se deberán aplicar las categorías de perfilado de alcance AVANZADO.

NIVEL DE RIESGO	ALCANCE		
	(B)ÁSICO	(I)INTERMEDIO	(A)VANZADO
9	SI	SI	SI
8	SI	SI	SI
7	SI	SI	SI
6	SI	SI	
5	SI	SI	
4	SI	SI	
3	SI		
2	SI		
1	SI		

En la siguiente tabla se muestra la asociación entre los riesgos identificados en el primer paso de esta guía y las categorías de perfilado de seguridad que mitigan, controlan o reducen dicho riesgo.

Como se puede observar, pueden existir categorías de perfilado de seguridad que actúen sobre uno o varios riesgos. Por lo tanto y para una mejor identificación, se han codificado cada una de las categorías, asociándolas al primer riesgo que mitigan, obteniendo la siguiente nomenclatura de categorías.

- a) A.3: corresponde con el código de riesgo que especifica la herramienta PILAR.
- b) SEC-FS1: corresponde con la categoría de seguridad 1 para dicho riesgo. El número se incrementará en uno para cada nueva categoría que se haya identificado.

La siguiente tabla define qué conjunto de medidas de seguridad deben ser aplicadas, en función de los niveles de riesgo obtenidos.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019 FILES SERVER	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log)	[A.3.SEC-FS1] Se encuentra habilitada la auditoría sobre los recursos del servidor.			
	[A.3.SEC-FS2] Se audita la creación, modificación y eliminación de ficheros de datos.			
	[A.3.SEC-FS3] Se audita la descarga/copia de ficheros de datos.			
	[A.3.SEC-FS4] Se audita el uso de copias de seguridad y restauración.			
	[A.3.SEC-FS5] Se controla la visibilidad de la estructura de carpetas de ficheros de datos.			
[A.5] Suplantación de la identidad	[A.5.SEC-FS1] Se comprueba la configuración de los sistemas de archivos.			
	[A.5.SEC-FS2] Se definen permisos sobre los directorios y ficheros.			
	[A.5.SEC-FS3] Se controlan las ACL			
	[A.3.SEC-FS2] Se audita la creación, modificación y eliminación de ficheros de datos.			
[A.6] Abuso de privilegios de acceso	[A.6.SEC-FS1] Se controla el uso de consolas de administración del espacio de almacenamiento.			
	[A.6.SEC-FS2] Se controla quién puede hacer copias de seguridad.			
	[A.3.SEC-FS2] Se audita la creación, modificación y eliminación de ficheros de datos.			
	[A.5.SEC-FS2] Se definen permisos sobre los directorios y ficheros.			
[A.11] Acceso no autorizado	[A.11.SEC-FS1] Se ha reforzado el uso del protocolo SMB.			
	[A.3.SEC-FS2] Se audita la creación, modificación y eliminación de ficheros de datos.			
	[A.5.SEC-FS2] Se definen permisos sobre los directorios y ficheros.			
[A.13] Repudio (negación de actuaciones)	[A.13.SEC-FS1] Se dispone de medidas anti Ransomware habilitadas.			
[A.24] Denegación de servicio	[A.24.SEC-FS1] Configuración de cuotas de disco.			
	[A.24.SEC-FS2] Se controla quien puede iniciar/detener los servicios del sistema.			
	[A.24.SEC-FS3] Activar desduplicación de archivos.			
[A.25] Robo de equipos	[A.25.SEC-FS1] Discos de datos cifrados.			
	[A.25.SEC-FS2] Se hace uso de TPM para cifrado de disco.			

ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD PARA UN SERVIDOR DE FICHEROS SOBRE WINDOWS SERVER 2019

En el presente anexo, se incluye una línea base de seguridad para la aplicación de medidas de seguridad en un servidor Windows Server 2019 con el rol de servidor de ficheros y unido a un dominio Windows mediante la guía “CCN-STIC-570A21 - Guía de aplicación de perfilado de seguridad para Windows Server 2019” previamente aplicada, atendiendo a los aspectos definidos en cada uno de los puntos anteriores de este documento.

Esta configuración se ofrece a modo de referencia o ejemplo de aplicabilidad de medidas en función de unos resultados concretos del análisis de riesgos ejecutado. Es posible que en otros escenarios y con otra superficie de exposición, el perfilado de aplicación de medidas sea diferente.

Es necesario remarcar que la línea base de seguridad establecida dentro del presente anexo corresponde con un **perfilado intermedio**.

Nota: En caso de que el perfilado de seguridad y superficie de exposición obtenidos, en base al análisis realizado, requieran de una **configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad**. Por el contrario, en caso de que el resultado de dicho análisis indique que la necesidad de configuración solo deba establecerse según el perfilado básico, será posible evitar ciertas medidas de seguridad de las establecidas en el presente anexo.

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

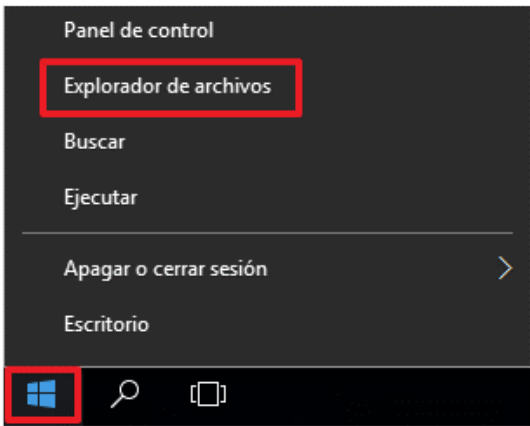
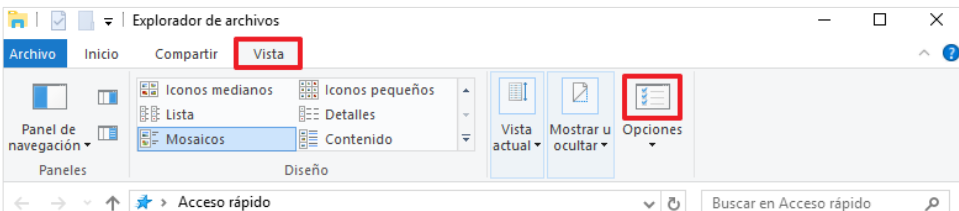
- a) Aplicación de seguridad en el entorno de Servidor de Ficheros sobre Microsoft Windows Server 2019 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de la misma. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.
- b) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 311/2022 y que se encontrarán implementados con Microsoft Windows Server 2019 mediante el seguimiento de la guía CCN-STIC-570A21 – Guía de aplicación de perfilado de seguridad para Windows Server 2019.

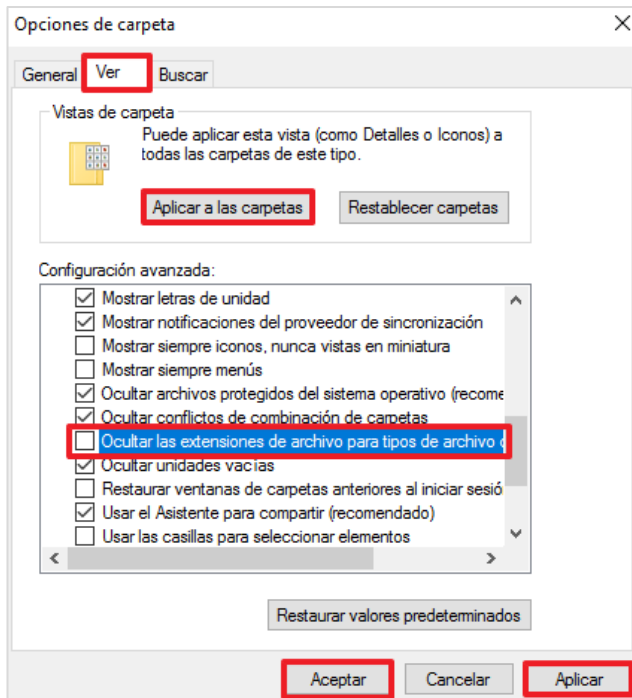
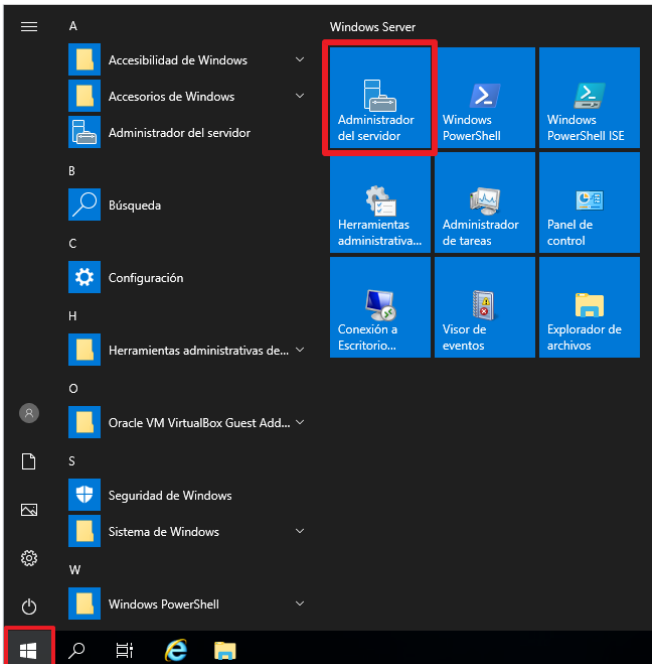
Por otro lado, es necesario indicar que ciertas categorías de seguridad no puedan ser aplicadas por medio de objetos GPO o configuraciones exactas a nivel de Windows, por ello se ha dedicado un apartado específico que permita establecer ejemplos de configuración sobre este tipo de categorías las cuales deberán ser adaptadas por cada organización.

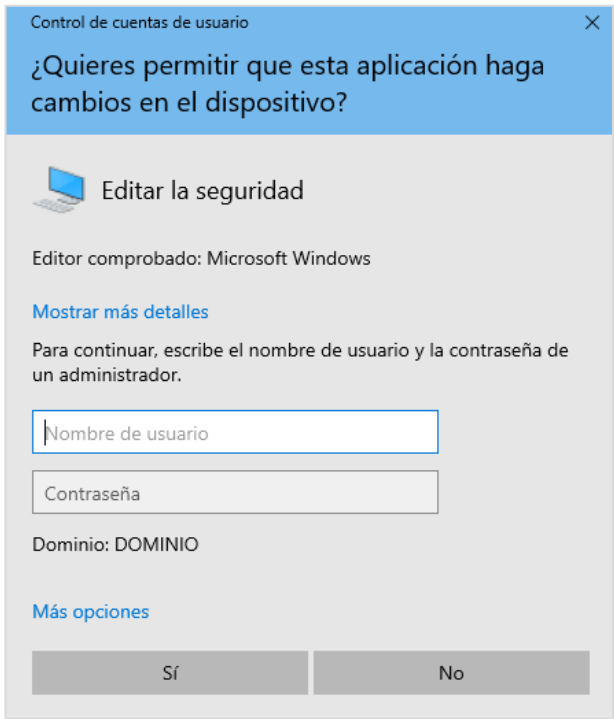
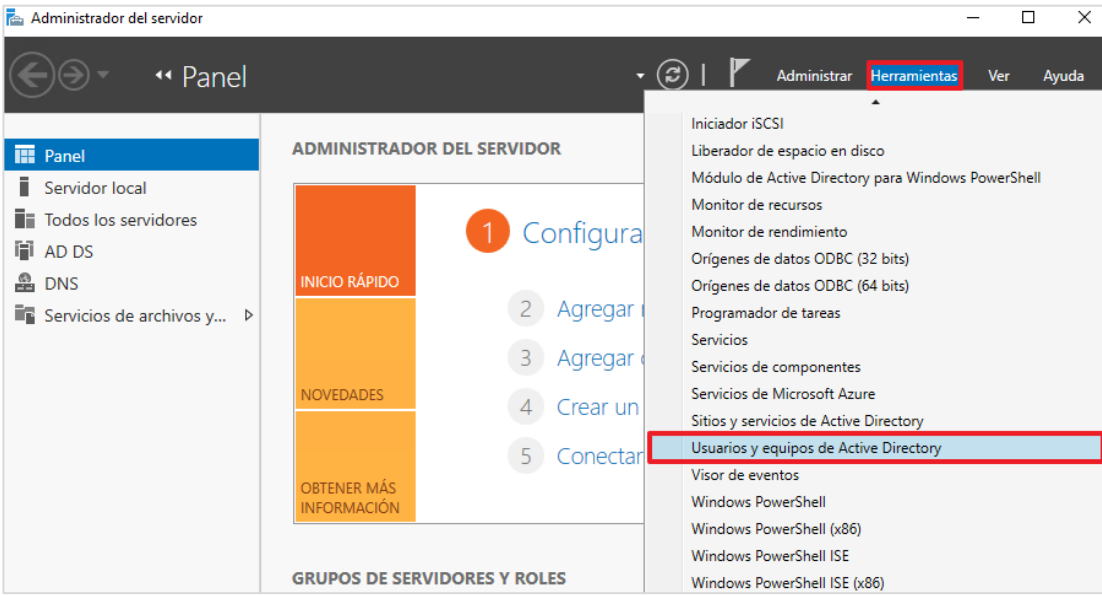
Debe tenerse en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

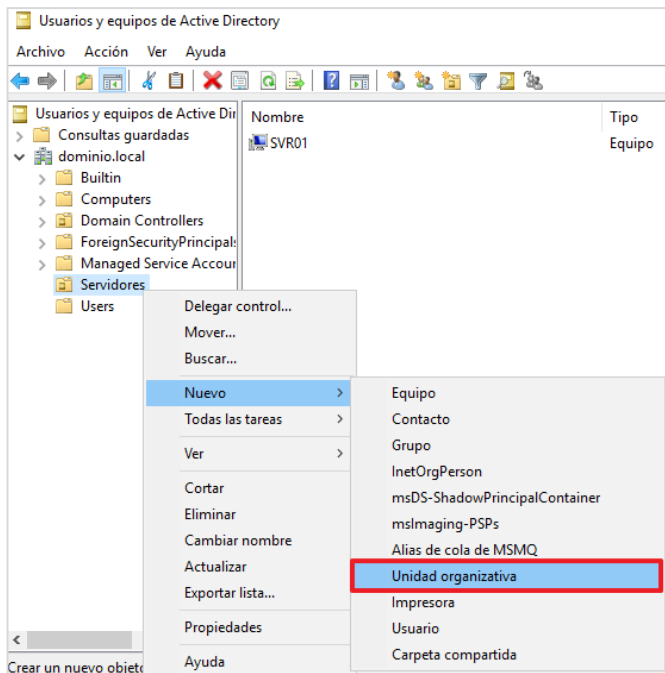
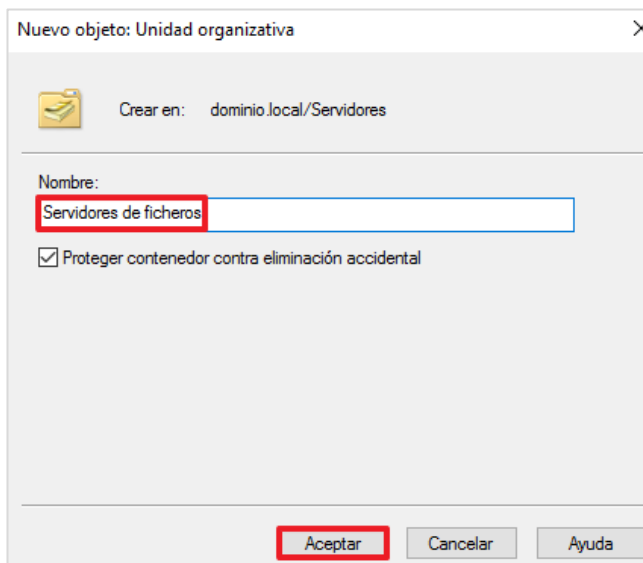
ANEXO A.1. PREPARACIÓN DEL DOMINIO

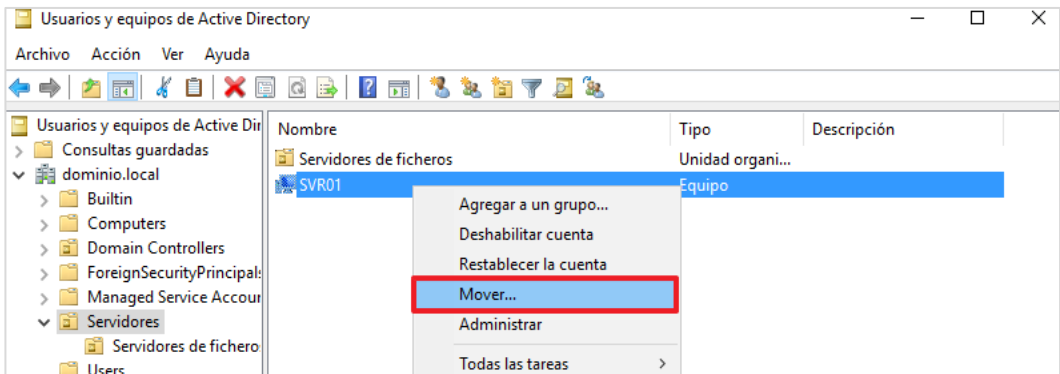
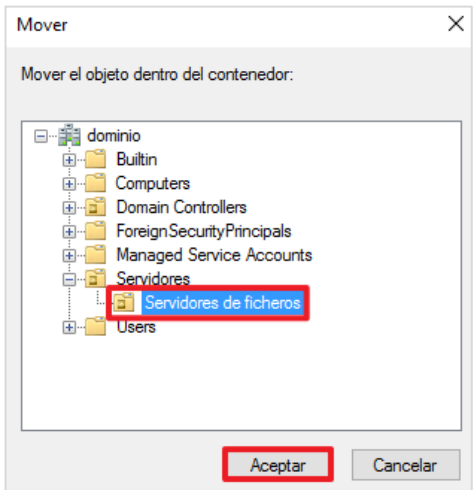
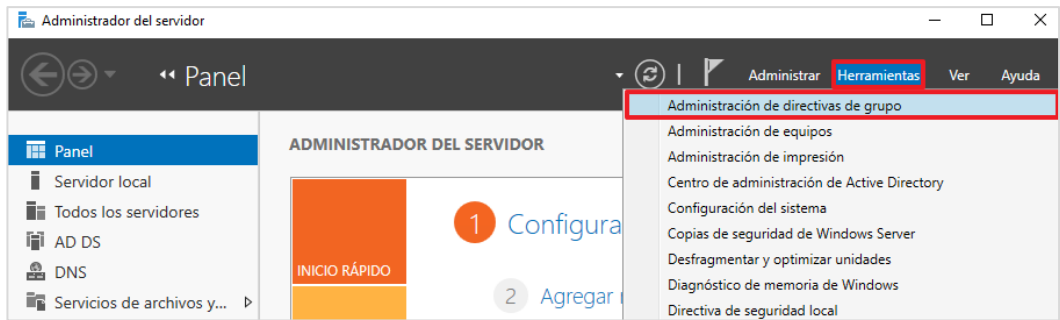
Los pasos que se describen a continuación se realizarán sobre un equipo Controlador de Dominio del dominio al que va a pertenecer el Servidor de ficheros que se está asegurando.

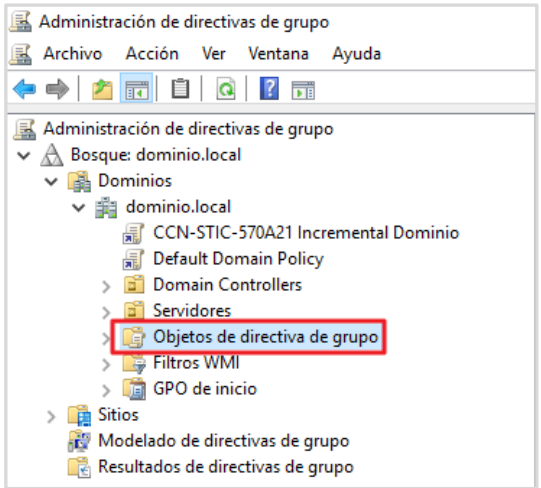
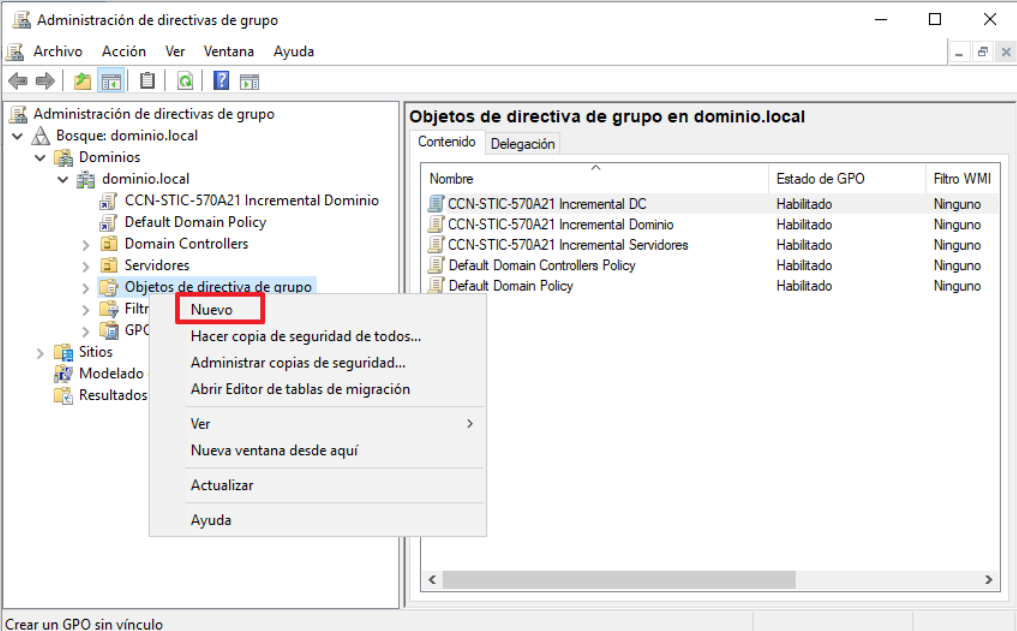
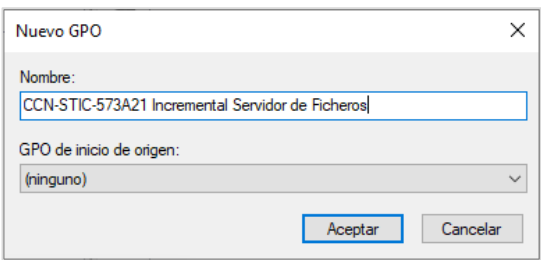
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad para el Servidor de ficheros.  Nota: Inicie sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\" .
3.	Copie los scripts y plantillas de seguridad asociados a esta guía en el directorio "C:\Scripts" .
4.	Configure el "Explorador de archivos" para que muestre las extensiones de los archivos ya que, por defecto, el "Explorador de archivos" oculta las extensiones conocidas y este hecho dificulta su identificación. 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". 

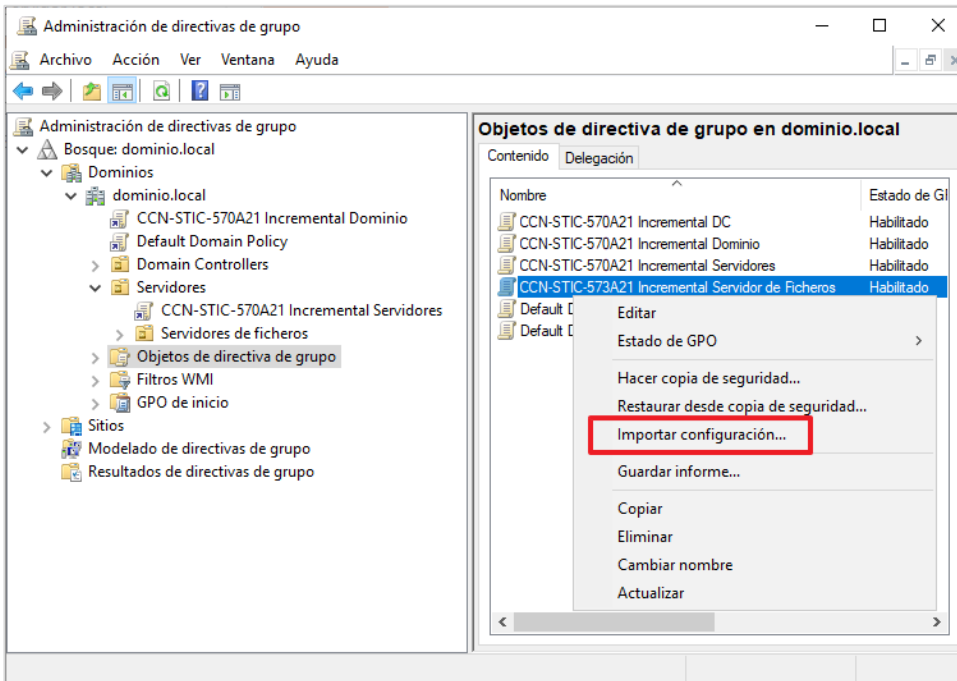
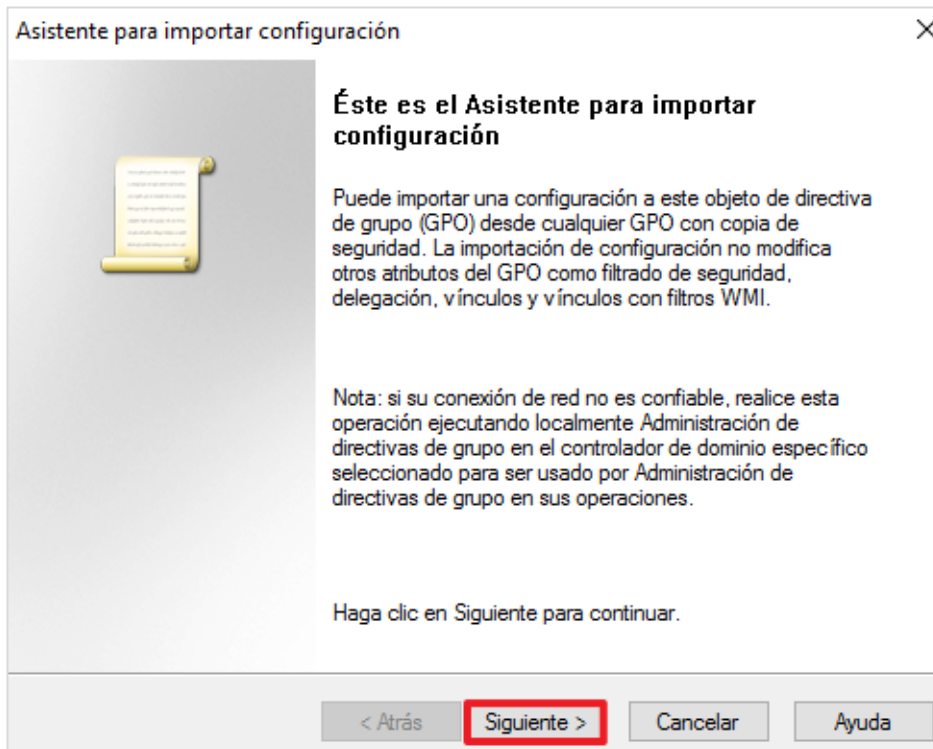
Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” pulse “Sí” ante el mensaje de confirmación y, por último, pulse “Aceptar”. 
7.	A continuación, abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

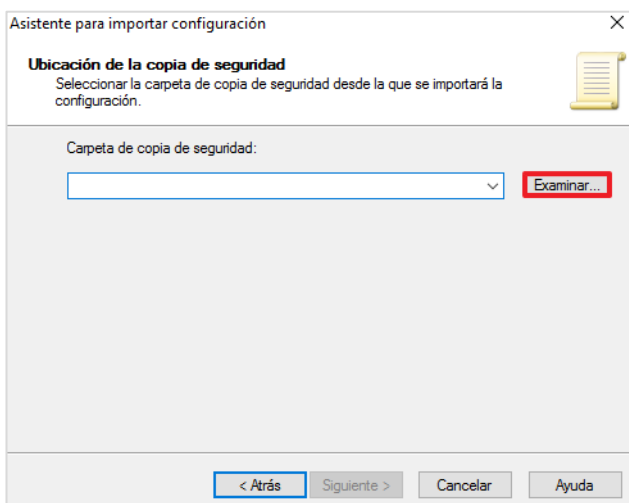
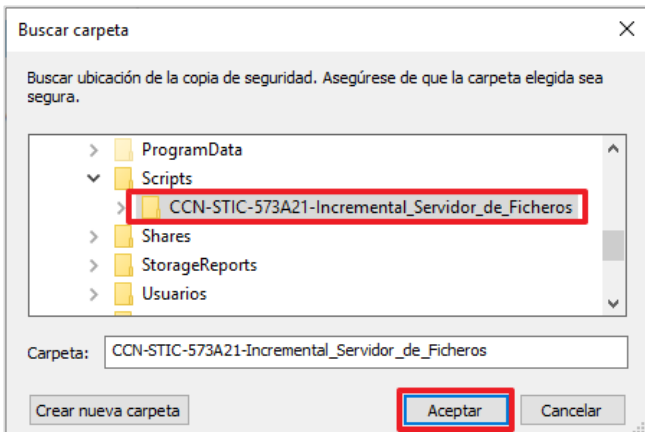
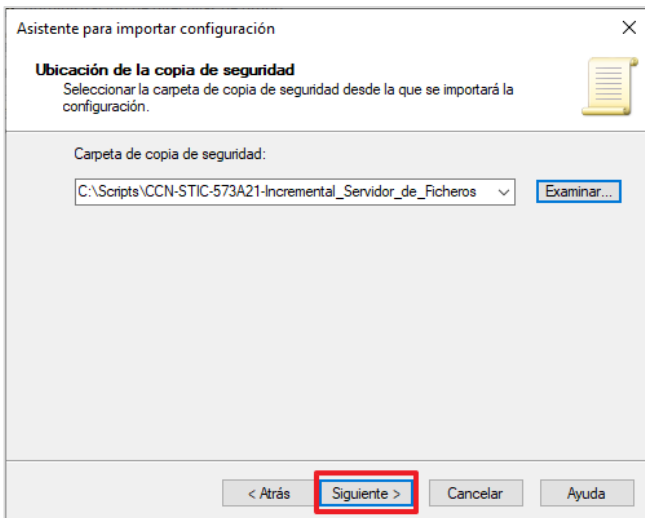
Paso	Descripción
8.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales necesarias para continuar. 
9.	A continuación, inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta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

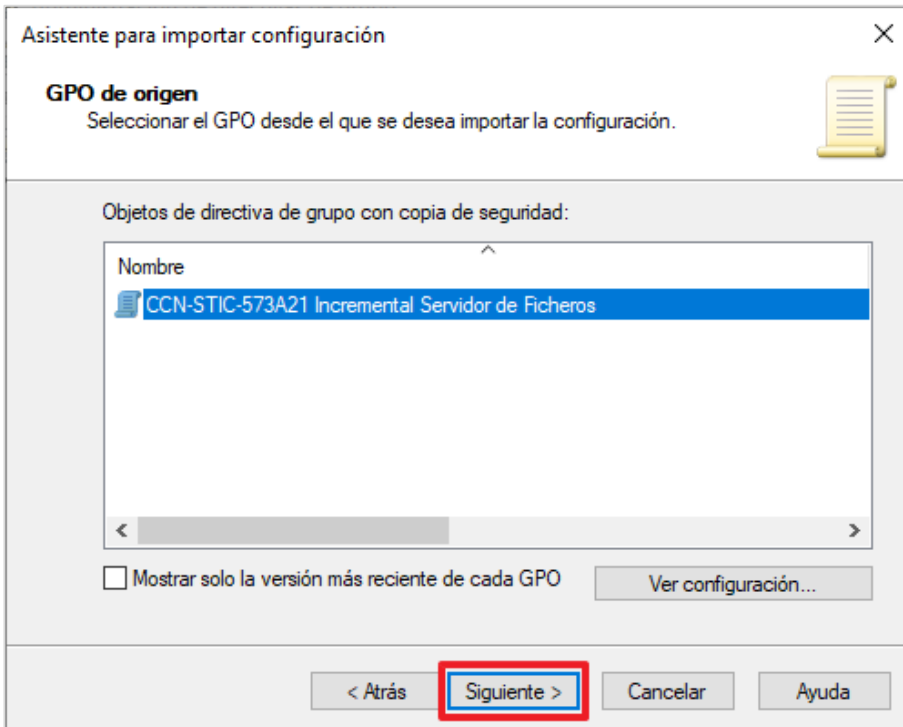
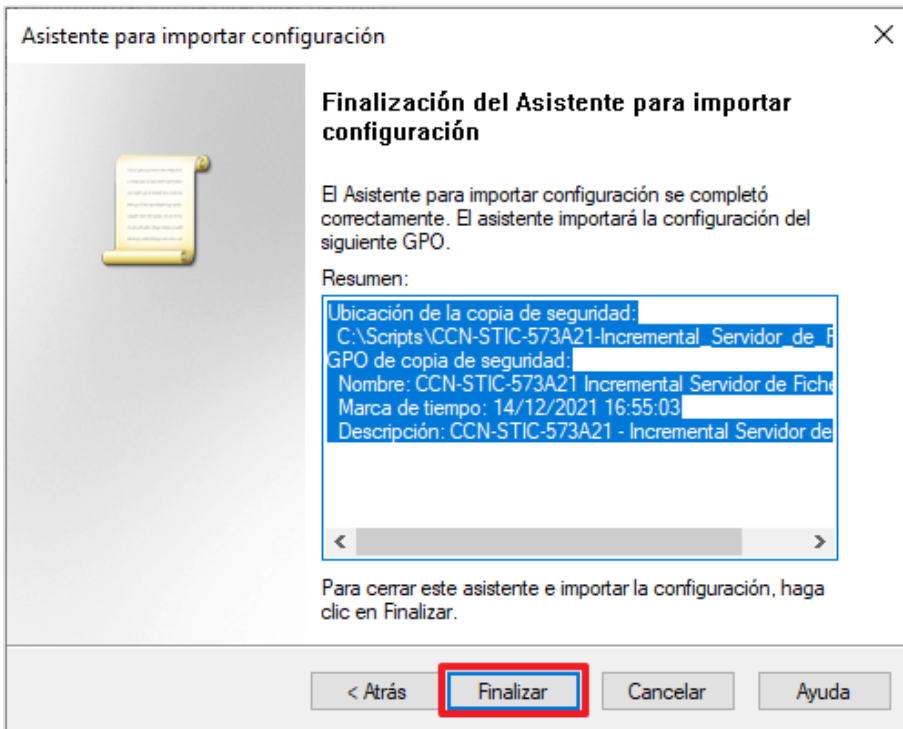
Paso	Descripción
10.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la Guía CCN-STIC-570A21 – IMPLEMENTACIÓN DE SEGURIDAD EN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2019. Para ello, seleccione el nodo “<<Dominio>> → <<unidad organizativa>>” y, desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo → Unidad organizativa”.  Nota: En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local / Servidores”.
11.	Introduzca el nombre “Servidores de ficheros” tal y como se muestra en la imagen y pulse sobre “Aceptar”. 

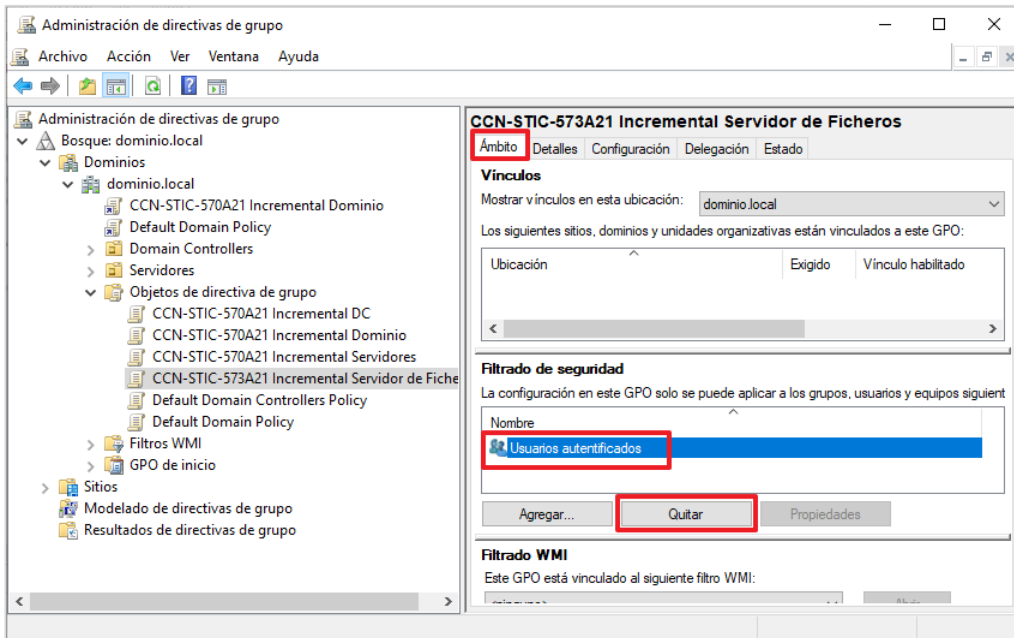
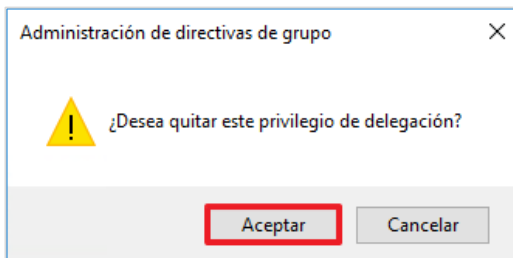
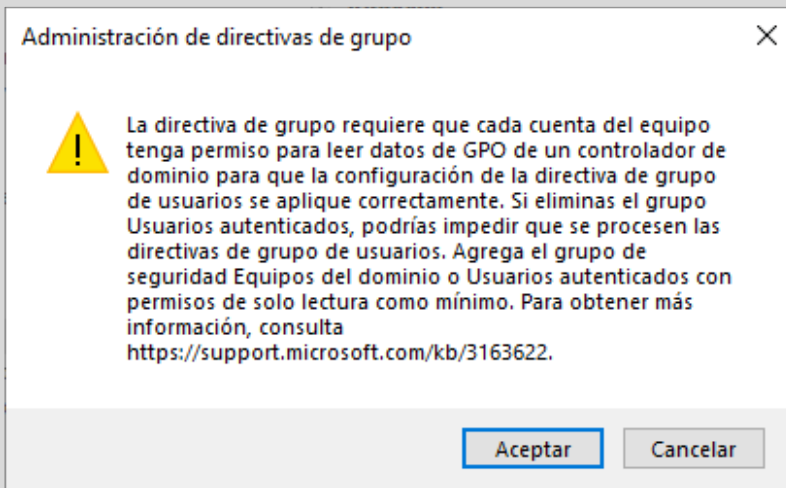
Paso	Descripción
12.	Una vez creada la nueva unidad organizativa, se deberán mover los servidores de ficheros a la unidad organizativa “Servidores de ficheros”. Para ello, se deberá hacer clic con el botón derecho sobre el servidor y seleccionar la opción “Mover...” en el servidor que desee ubicar en la nueva unidad organizativa. 
13.	A continuación, seleccione la unidad organizativa “Servidores de ficheros” y pulse sobre “Aceptar”. 
14.	Cierre la herramienta de “ Usuarios y equipos de Active Directory ”.
15.	A continuación, abra el “ Administrador del servidor ”.
16.	Inicie la consola “Administración de directivas de grupo”. Para ello, pulse sobre el botón “Herramientas → Administración de directivas de grupo”. 

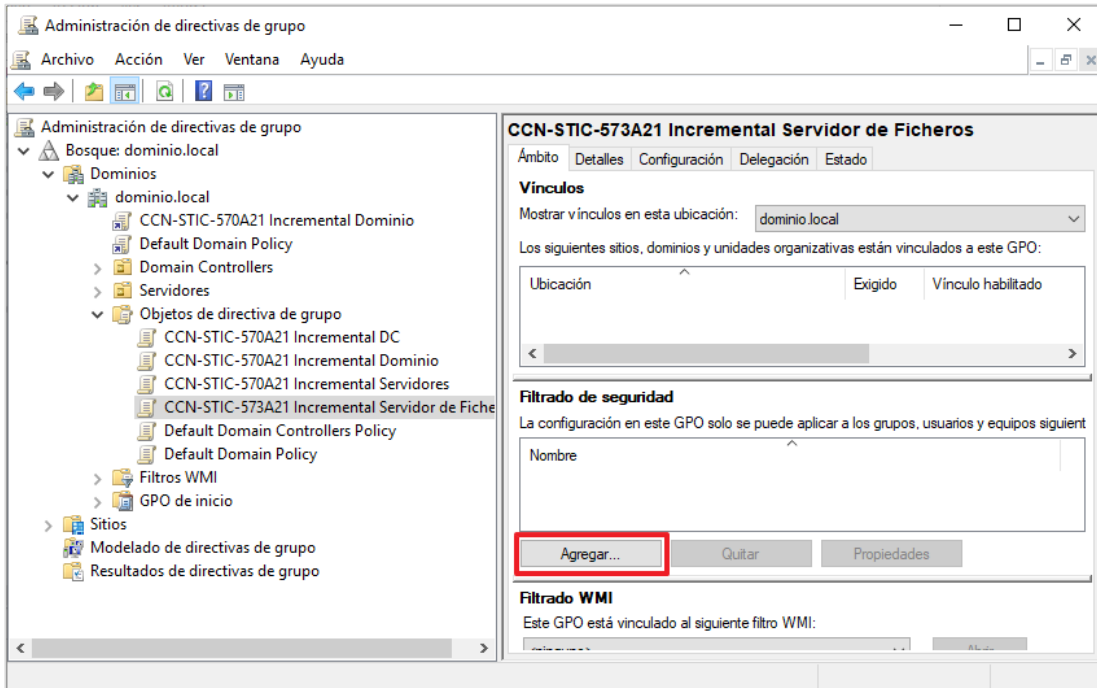
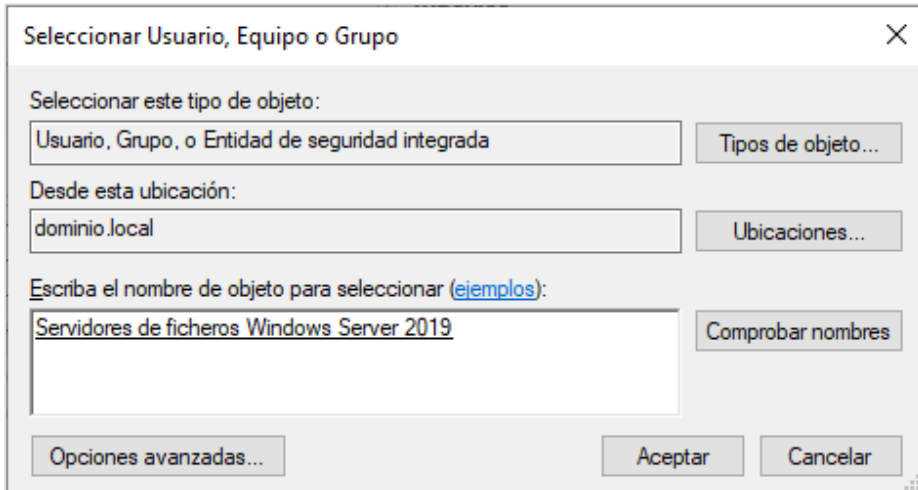
Paso	Descripción
17.	Ubíquese sobre el nodo “Objetos de directiva de grupo” situado en “Bosque:<Su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”. 
18.	Pulse, con el botón derecho, sobre “Objetos de directiva de grupo” y seleccione la opción “Nuevo” del menú contextual. 
19.	Establezca, para la nueva, GPO el nombre “CCN-STIC-573A21 Incremental Servidor de Ficheros” y pulse “Aceptar”. 

Paso	Descripción
20.	A continuación, pulse con el botón derecho sobre la GPO recién creada y seleccione la opción “Importar configuración” en el menú contextual. 
21.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
22.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.

Paso	Descripción
23.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
24.	Seleccione la carpeta “CCN-STIC-573A21-Incremental_Servidor_de_Ficheros” que encontrará en el directorio “C:\Scripts” y pulse el botón “Aceptar”. 
25.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

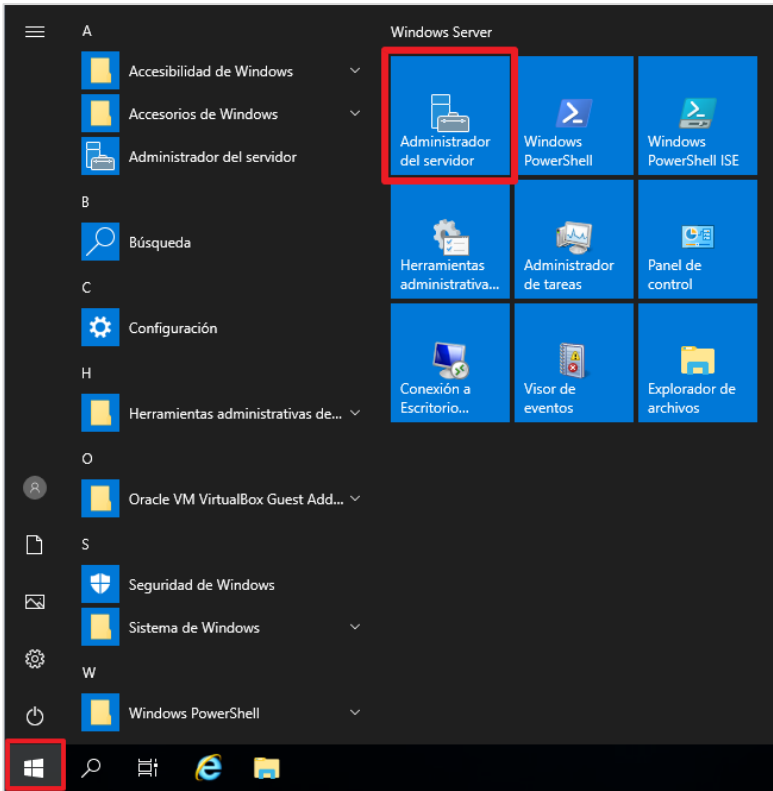
Paso	Descripción
26.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-573A21 Incremental Servidor de Ficheros” y pulse el botón “Siguiente >”. 
27.	Para completar el asistente, pulse el botón “Finalizar”. 
28.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración y continúe con el siguiente paso.

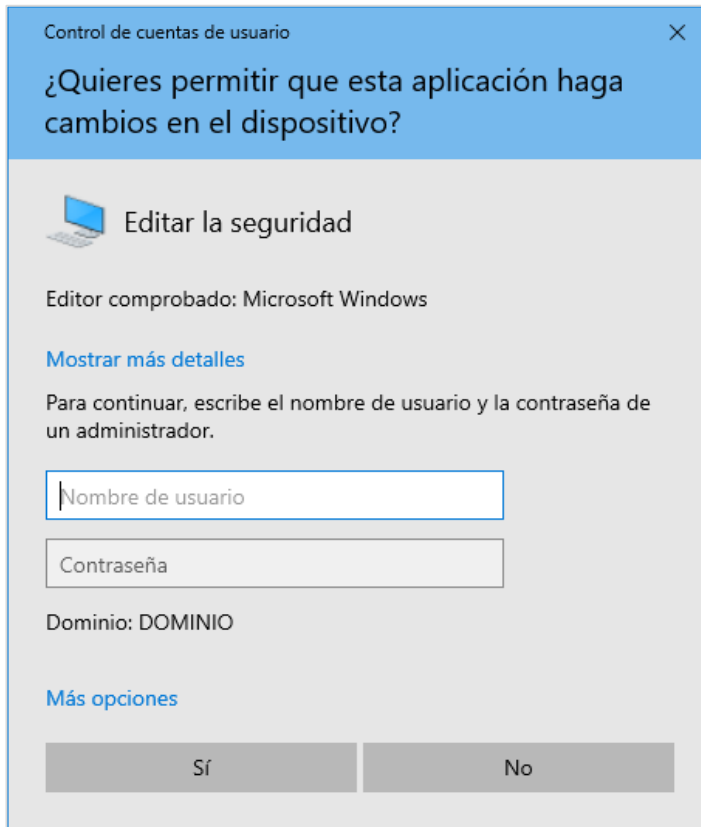
Paso	Descripción
29.	Seleccione la GPO recién configurada y acceda a la pestaña “Ámbito”. Localice el apartado “Filtrado de seguridad” y dentro del él seleccione el grupo “Usuarios autenticados”. Pulse sobre el botón “Quitar”. 
30.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio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

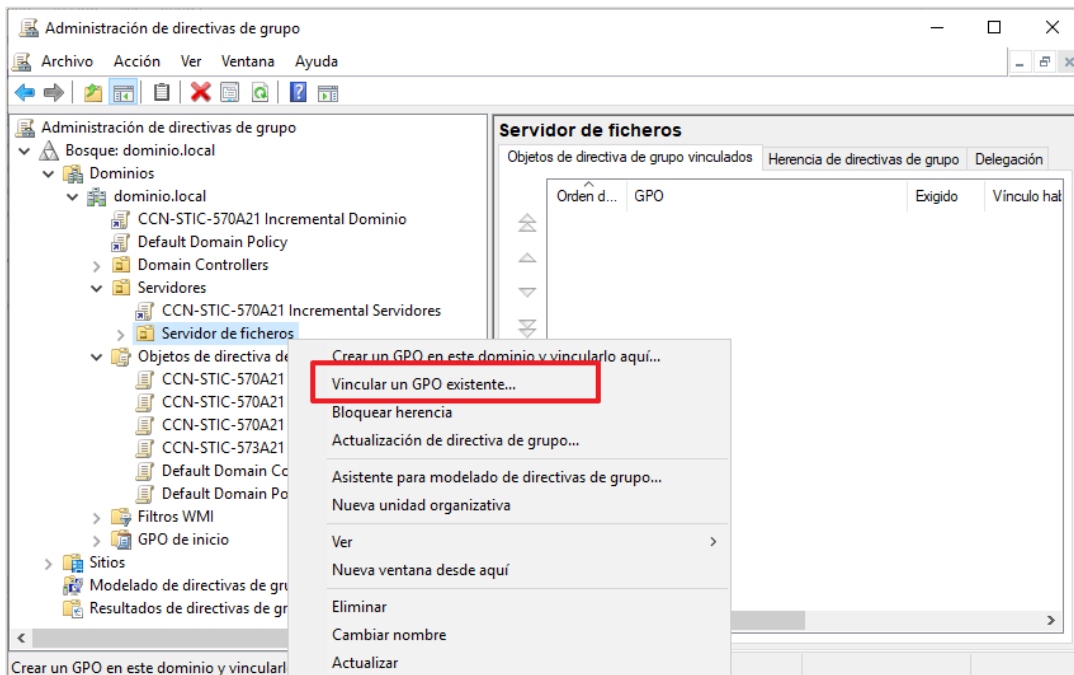
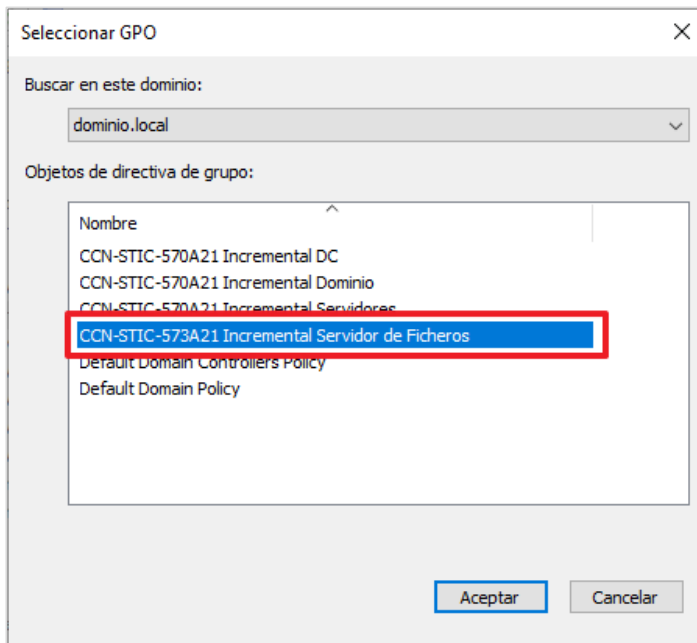
Paso	Descripción
31.	A continuación, pulse sobre el botón “Agregar...”. 
32.	Agregue los grupos de usuarios que contengan los equipos con el rol “Servidores de ficheros Windows Server 2019” y pulse “Aceptar” para finalizar.  Nota: Para este ejemplo se utiliza el grupo “Servidores de ficheros Windows Server 2019” que contiene el servidor con el rol “Servidor de ficheros”.
33.	Cierre la consola “Administración de directivas de grupo” y elimine la carpeta “C:\Scripts”.

ANEXO A.2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El siguiente punto establece la aplicación de las políticas de seguridad una vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
34.	Inicie sesión en el servidor “Controlador de Dominio” donde se va a aplicar seguridad para el “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Dominio.
35.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

Paso	Descripción
36.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales necesarias para continuar. 
37.	Inicie la consola “Administración de directivas de grupo”. Para ello, pulse sobre el botón “Herramientas → Administración de directivas de grupo”. 
38.	A continuación, despliegue el nodo “Bosque: <<Nombre de bosque>> → Dominios → <<Nombre de dominio>> → Servidores → Servidores de ficheros”. Nota: En este ejemplo, el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de ficheros”.

Paso	Descripción
39.	Seleccione con el botón derecho la unidad organizativa y pulse sobre la opción del menú contextual “Vincular GPO existente...”. 
40.	A continuación, localice la GPO configurada anteriormente, “CCN-STIC-573A21 Incremental Servidor de Ficheros”, y pulse “Aceptar”. 

ANEXO A.3. CONFIGURACIONES ADICIONALES

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

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

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

Nota: Las diferentes configuraciones ofrecidas en este anexo son una referencia de las múltiples soluciones que se pueden encontrar para cada uno de los riesgos identificados, es decir, la misma funcionalidad aquí presentada para la mitigación del riesgo puede ser aplicada mediante otros procedimientos, software, o configuraciones. No deben tomarse estas configuraciones como métodos únicos de mitigación.

ANEXO A.3.1. CONFIGURACIÓN DE LOS ESPACIOS DE ALMACENAMIENTO

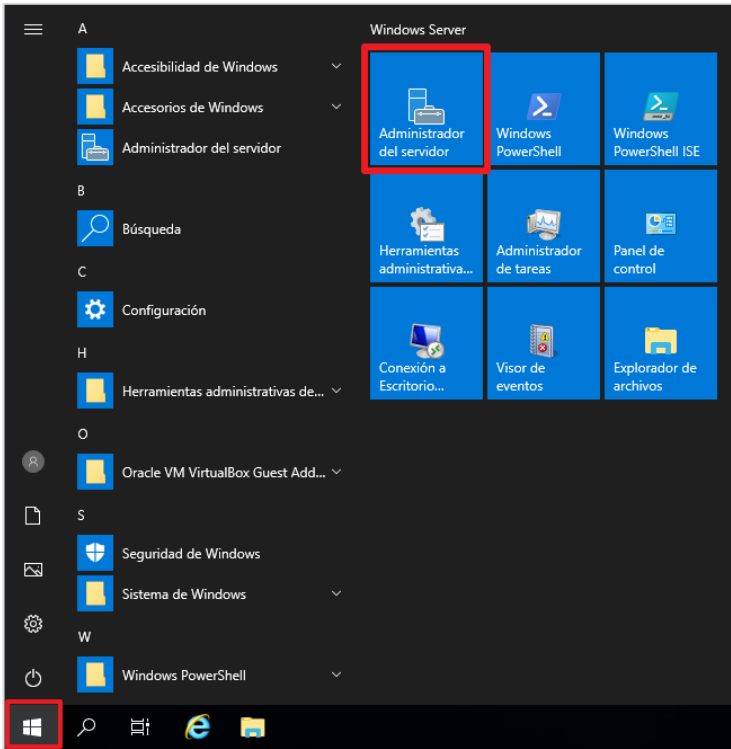
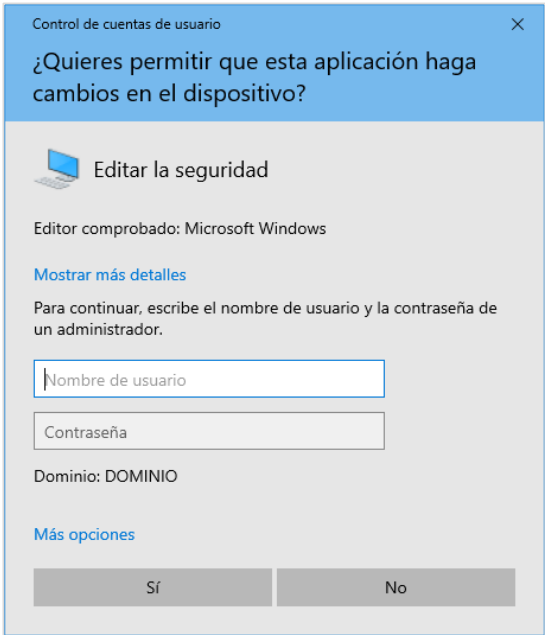
Dependiendo de qué recursos se compartan en el servidor de ficheros, pueden generarse accesos indeseados a los datos. Por tanto, se recomienda que los recursos compartidos en el Servidor de ficheros estén alojados en una ubicación distinta al disco de sistema operativo y que ésta solo se utilice para el alojamiento de recursos evitando, con ello, exponer más información de la estrictamente necesaria.

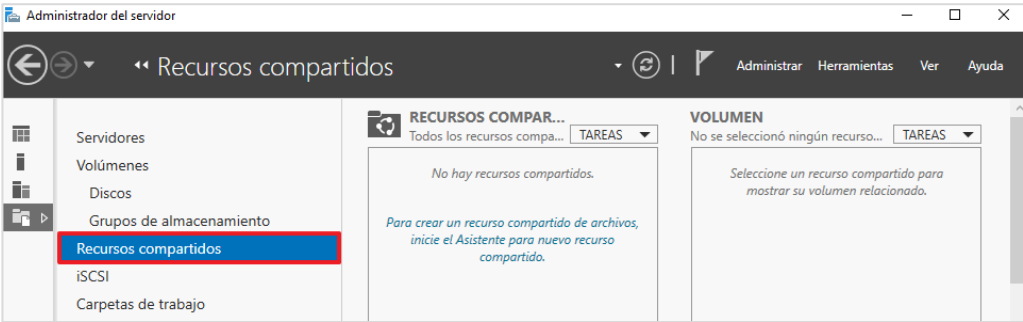
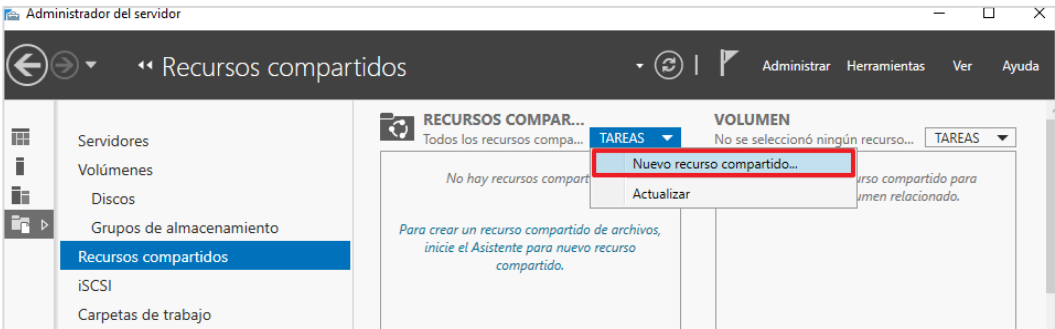
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

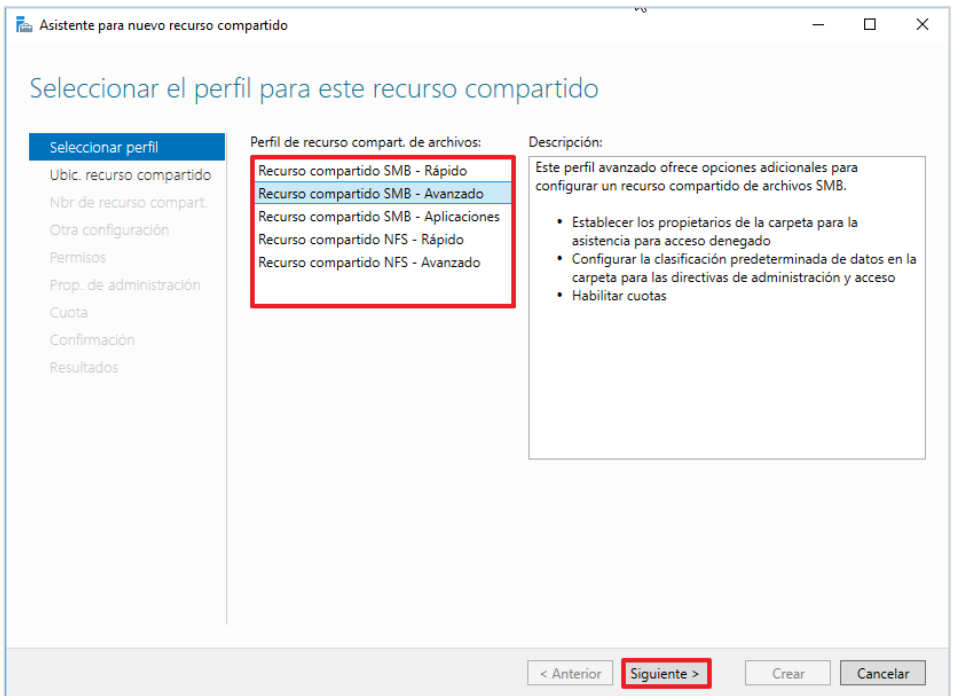
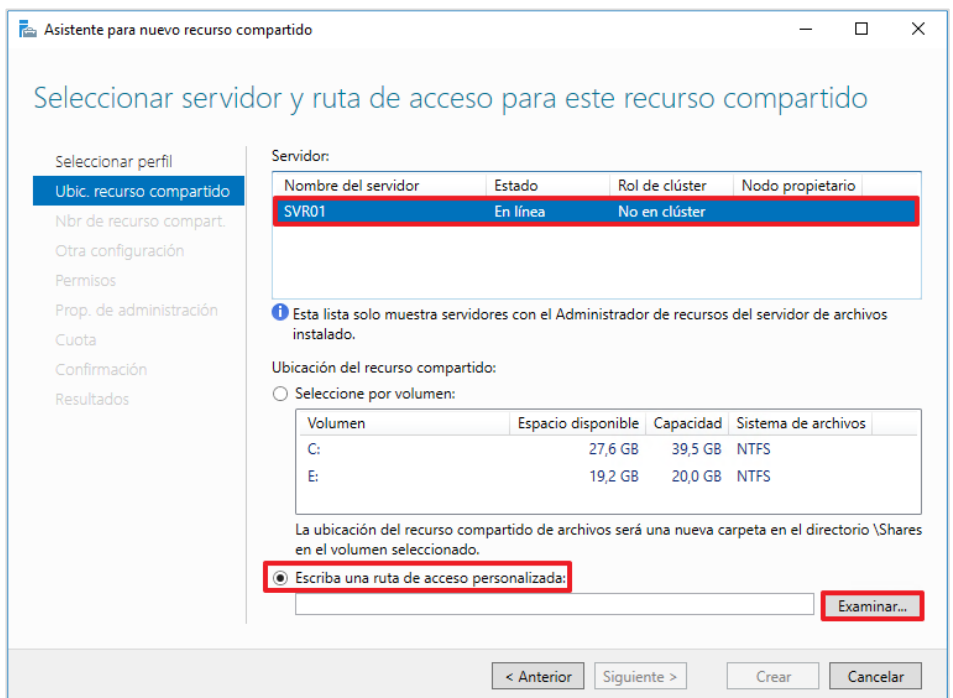
- a) **[A.3.SEC-FS2]** Se audita la creación, modificación y eliminación de ficheros de datos.
- b) **[A.3.SEC-FS3]** Se audita la descarga y/o copia de ficheros de datos.

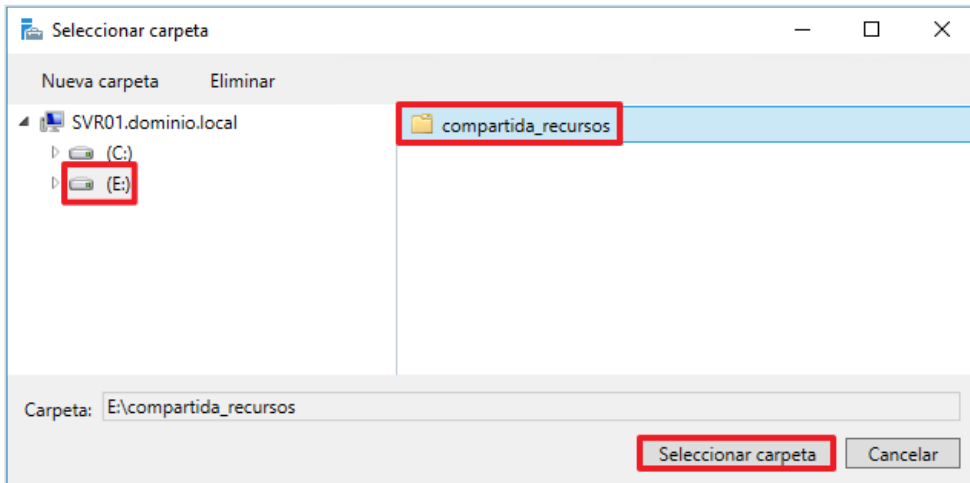
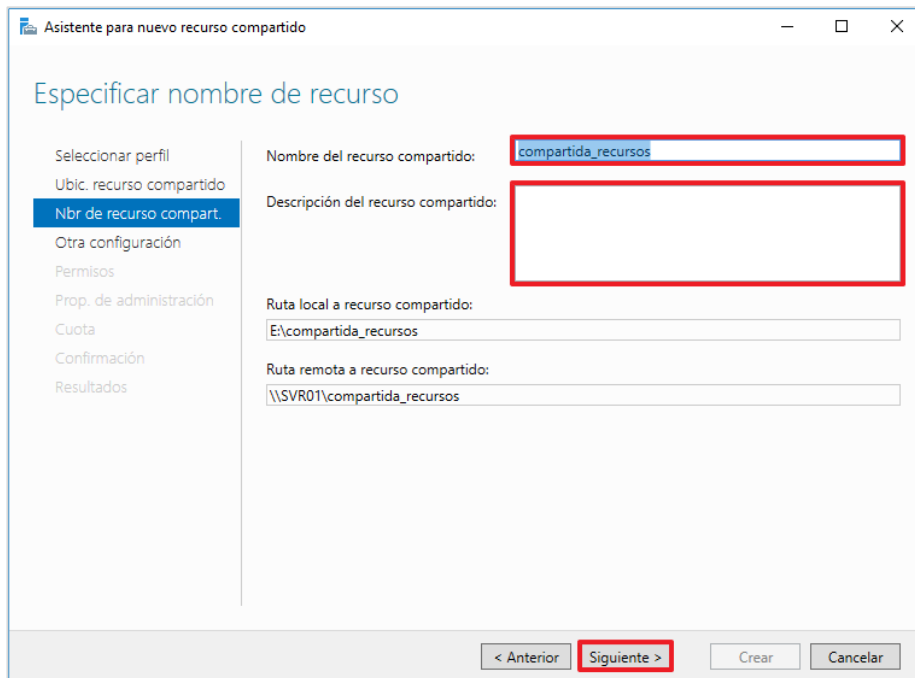
En este apartado, se determinará la gestión de los recursos que son compartidos a través del Servidor de ficheros.

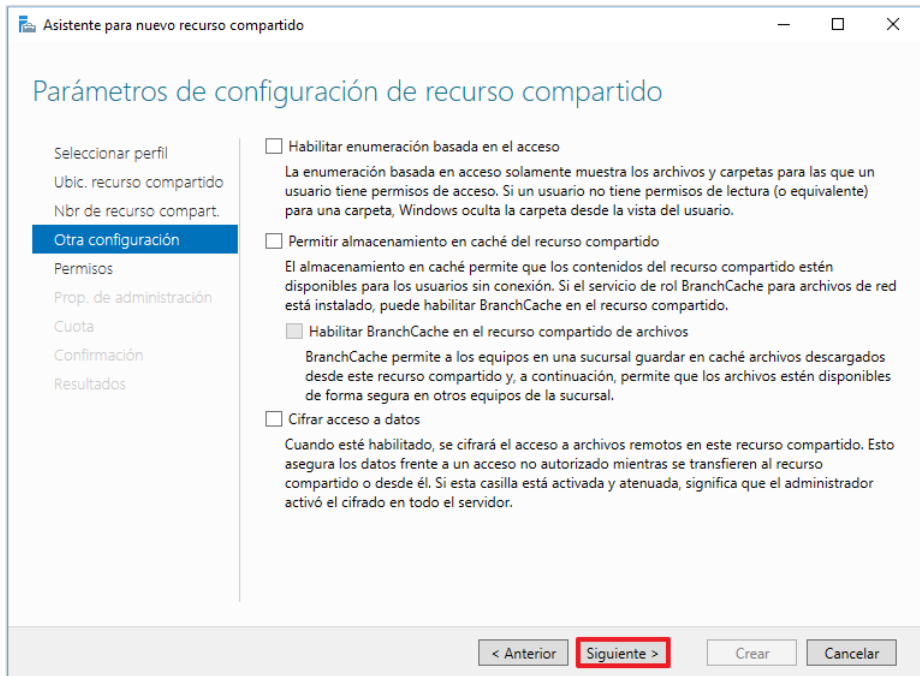
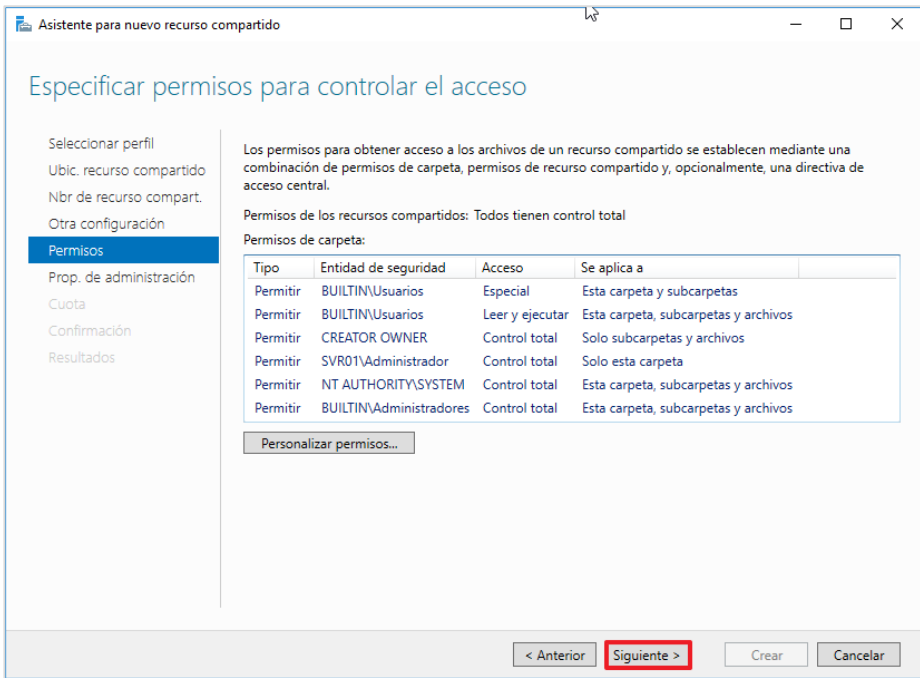
Paso	Descripción
41.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.

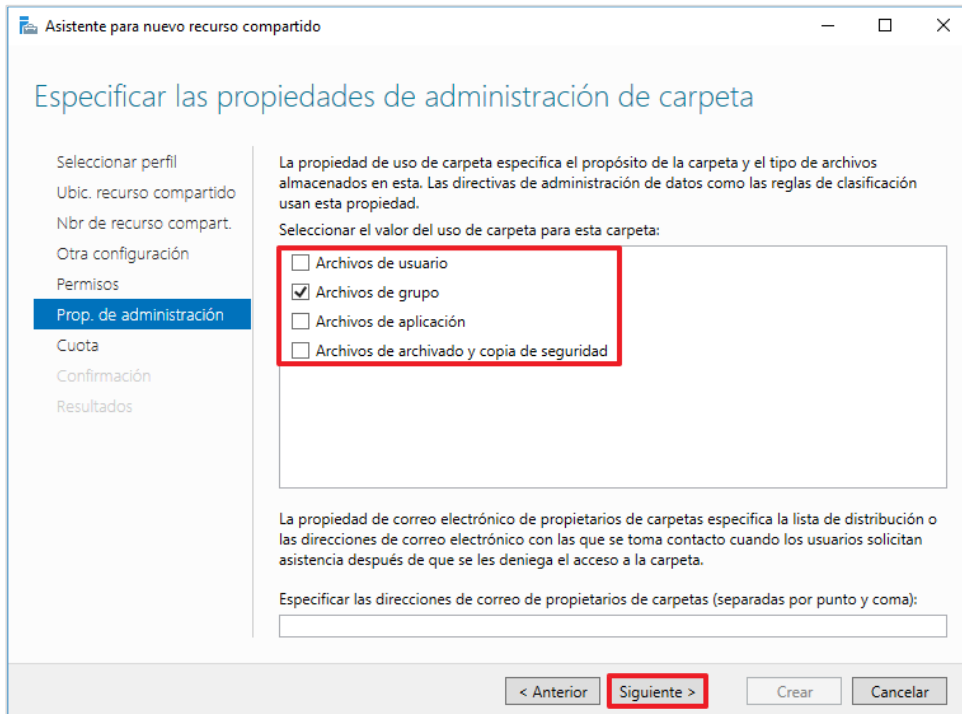
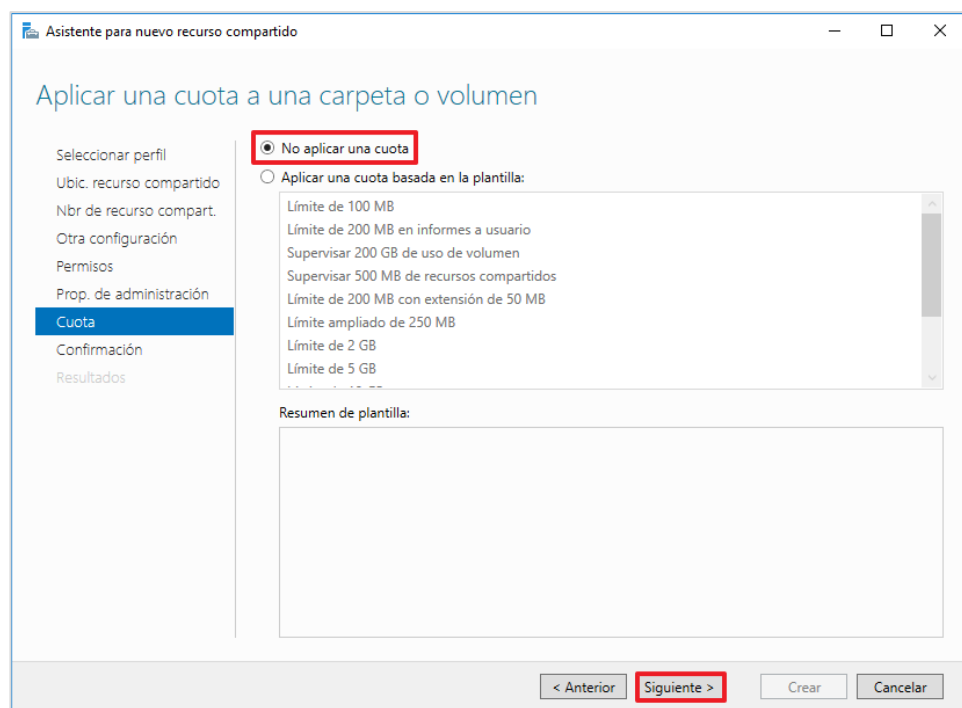
Paso	Descripción
42.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 
43.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 

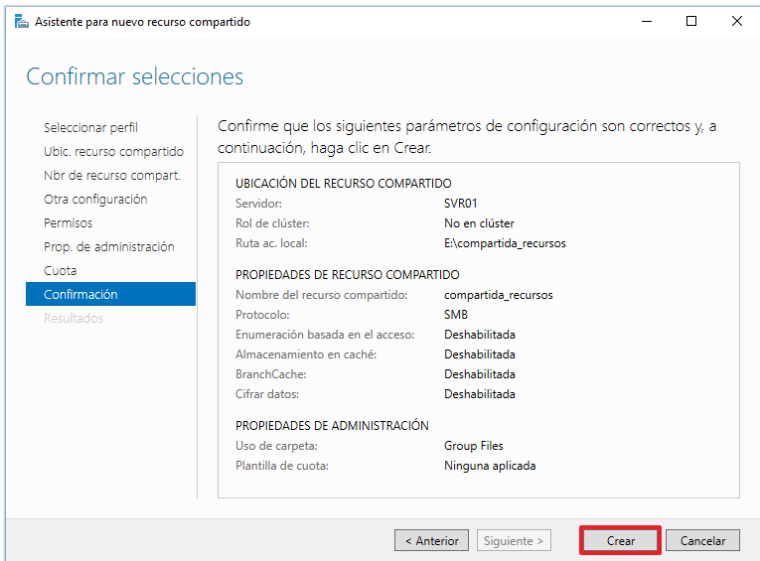
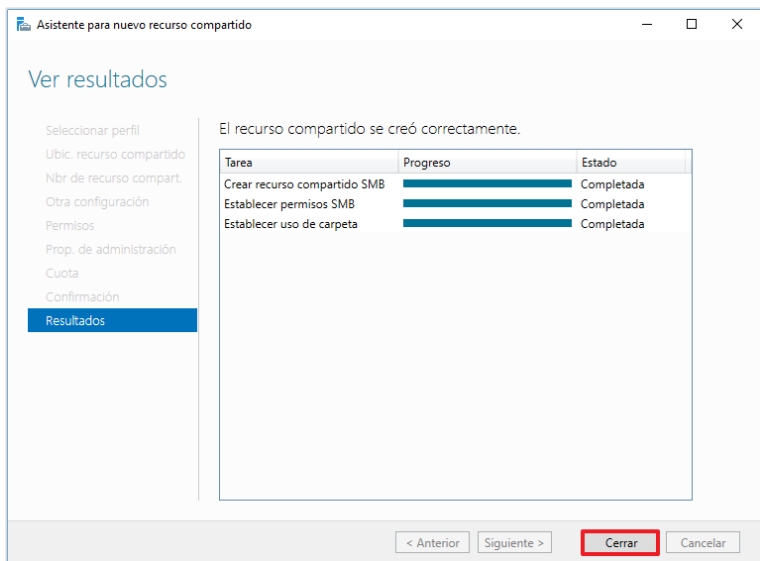
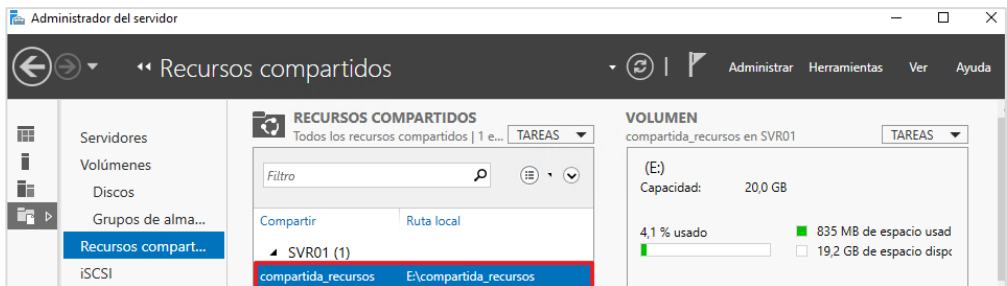
Paso	Descripción
44.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
45.	Seleccione la sección “Recursos compartidos”. 
46.	En el apartado “Recursos compartidos”, pulse sobre el desplegable “TAREAS” y seleccione la opción “Nuevo recurso compartido...”. 

Paso	Descripción
47.	Se iniciará el asistente para añadir un nuevo recurso compartido. En el apartado “Seleccionar perfil”, seleccione un perfil de recurso compartido de archivos y pulse “Siguiente >”.  Nota: Para este ejemplo, se utiliza la opción “Recurso compartido SMB – Avanzado”.
48.	Seleccione el servidor sobre el que desea crear el recurso compartido. A continuación, seleccione la opción “Escriba una ruta de acceso personalizada:” y pulse sobre el botón “Examinar...”. 

Paso	Descripción
49.	Ante la ventana emergente, navegue y seleccione el recurso que desea compartir. Pulse sobre “Seleccionar carpeta” para continuar.  Nota: Para este ejemplo, se comparte un directorio creado previamente denominado “compartida_recursos” en una ubicación dedicada a recursos compartidos denominada “Datos (E:)”. Ajuste esta configuración a las necesidades de su organización.
50.	A continuación, pulse sobre “Siguiete >” para continuar con el asistente.
51.	En el apartado “Nbr. de recurso compart.”, establezca un nombre para el recurso y una descripción del mismo, si lo desea, y pulse sobre “Siguiete >”.  Nota: En este ejemplo, se mantiene el nombre del recurso seleccionado en el apartado anterior del asistente.

Paso	Descripción
52.	En el apartado “Otra configuración”, seleccione los parametros de configuración de recurso compartido que precise y pulse “Siguiente >”.  Nota: Para este ejemplo no se ha seleccionado ninguna configuración adicional.
53.	Pulse “Siguiente >” en el apartado “Permisos”.  Nota: Los permisos de acceso a los archivos del recurso compartido se deben configurar posteriormente. En el siguiente punto, se explica la creación de listas de acceso (ACLs).

Paso	Descripción
54.	Seleccione en el apartado “Prop. de administración” una categoría para el recurso compartido, si lo desea, y pulse el botón “Siguiente >”.  Nota: Para este ejemplo, se utiliza la categorización “Archivos de grupo”. Adapte esta configuración a su entorno.
55.	Pulse “Siguiente >” en el apartado “Cuota”.  Nota: En este ejemplo, se deja marcada la opción por defecto “No aplicar una cuota”.

Paso	Descripción
56.	En el apartado “Confirmación”, pulse sobre el botón “Crear”. 
57.	En el apartado “Resultados”, se mostrará el proceso de creación del recurso. Cuando el proceso finalice pulse sobre “Cerrar”. 
58.	Podrá comprobar, desde el “Administrador del servidor”, el recurso que se acaba de compartir. 

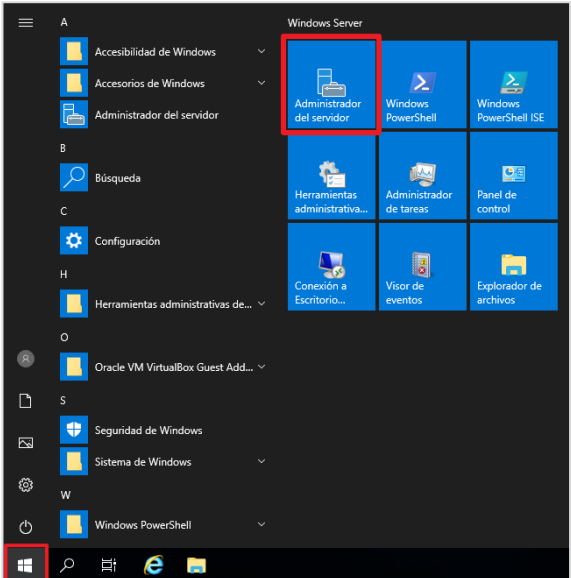
ANEXO A.3.2. USO DE LISTAS DE CONTROL DE ACCESO.

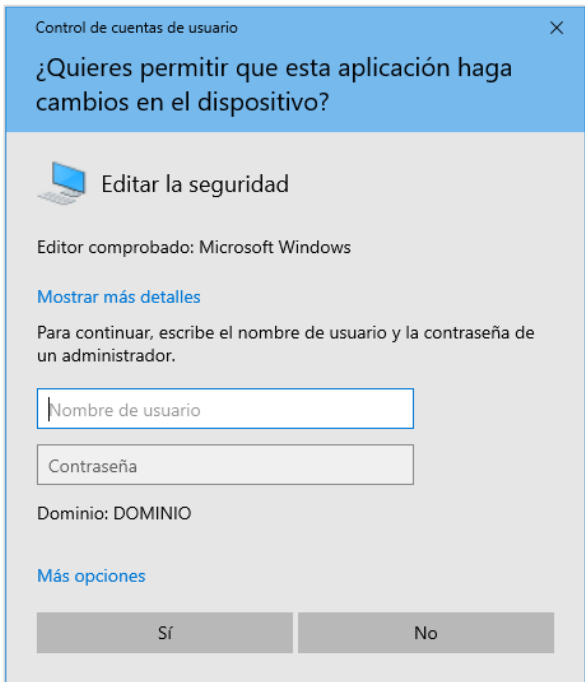
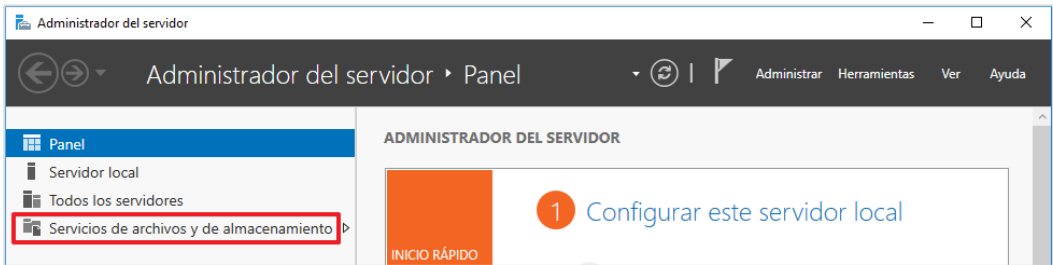
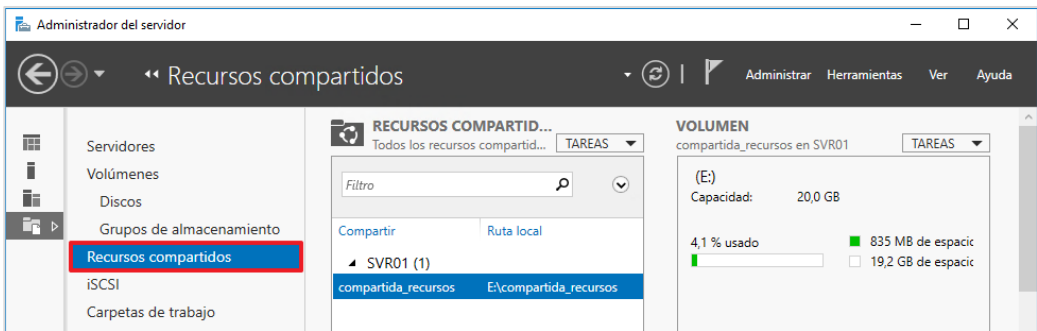
En este apartado, se tendrán en consideración la gestión y administración del acceso a los recursos del servidor de ficheros según el marco operacional de perfilado intermedio establecido por el ENS para, de este modo, controlar el acceso a directorios con información sensible de ser sustraída y limitar el número de usuarios con acceso a la misma.

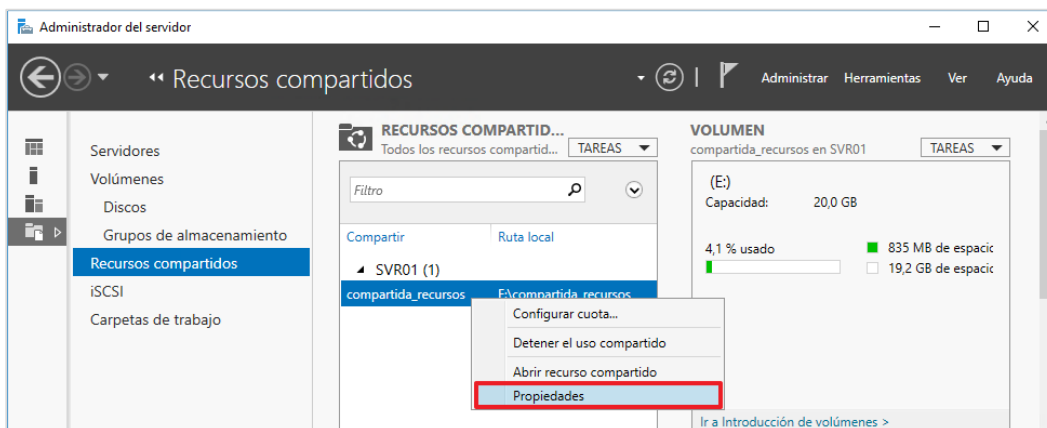
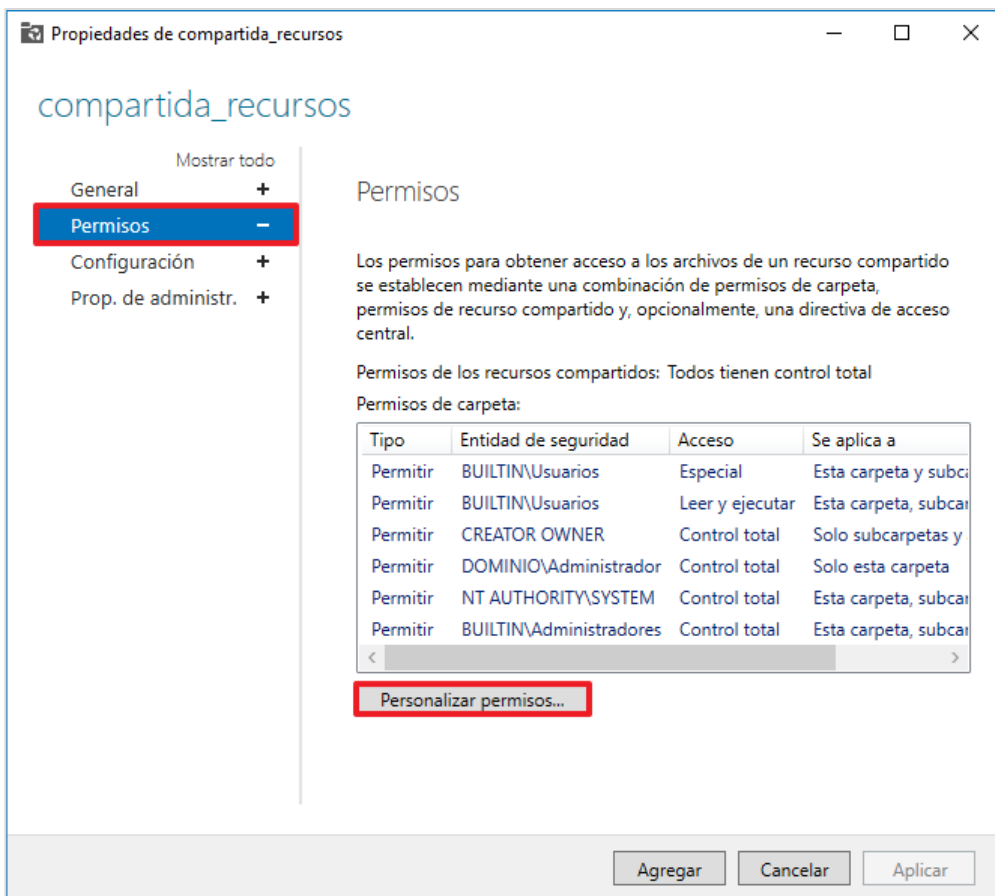
Una lista de control de acceso (ACL) del sistema de archivos contiene reglas que otorgan o deniegan el acceso a archivos y/o directorios. A continuación, se procederá a indicar dónde y cómo se deben configurar dichas ACLs.

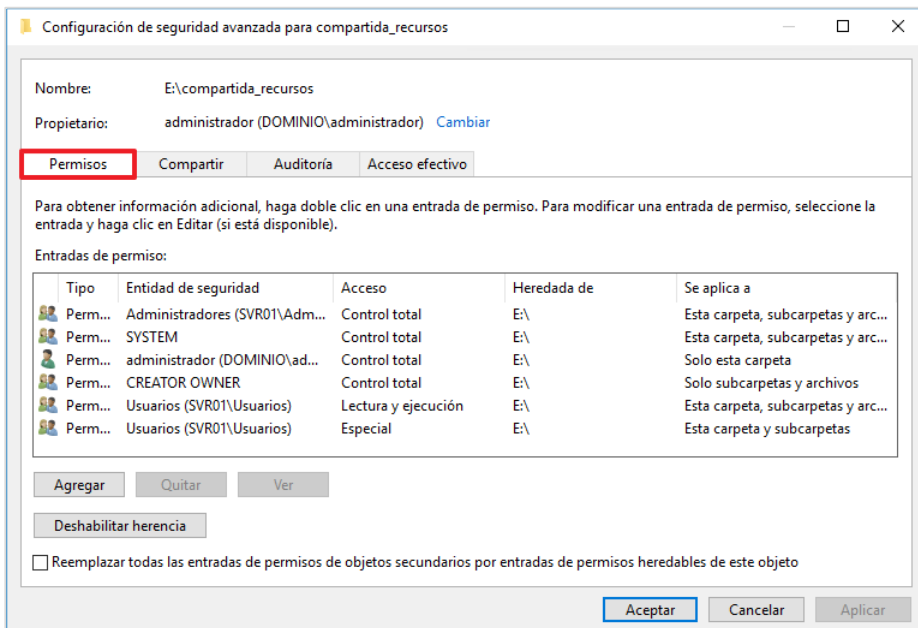
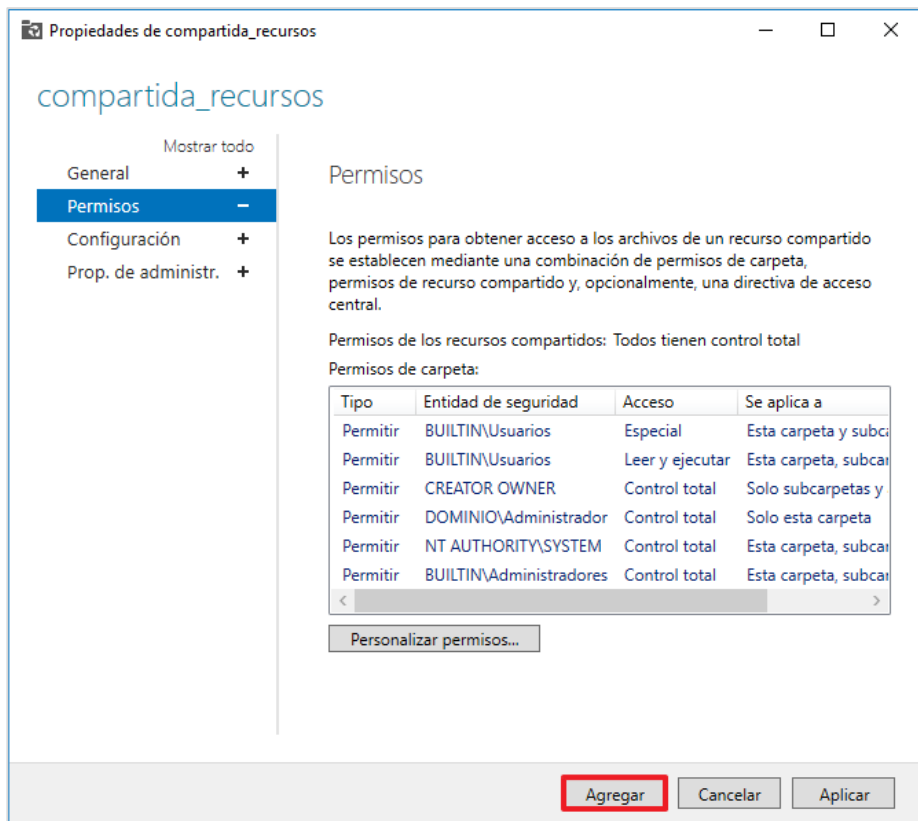
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.5.SEC-FS1]** Se comprueba la configuración de los sistemas de archivos.
- b) **[A.5.SEC-FS2]** Se definen permisos sobre los directorios y ficheros.
- c) **[A.5.SEC-FS3]** Se controlan las ACL.

Paso	Descripción
59.	Inicie sesión en el servidor miembro que tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.
60.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

Paso	Descripción
61.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 
62.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
63.	Seleccione la sección “Recursos compartidos”. 

Paso	Descripción
64.	Seleccione, con el botón derecho, el recurso sobre el que desea modificar los permisos y pulse la opción “Propiedades”.  Nota: En este ejemplo, se editan las propiedades del recurso denominado “compartida_recursos”.
65.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos...”. 

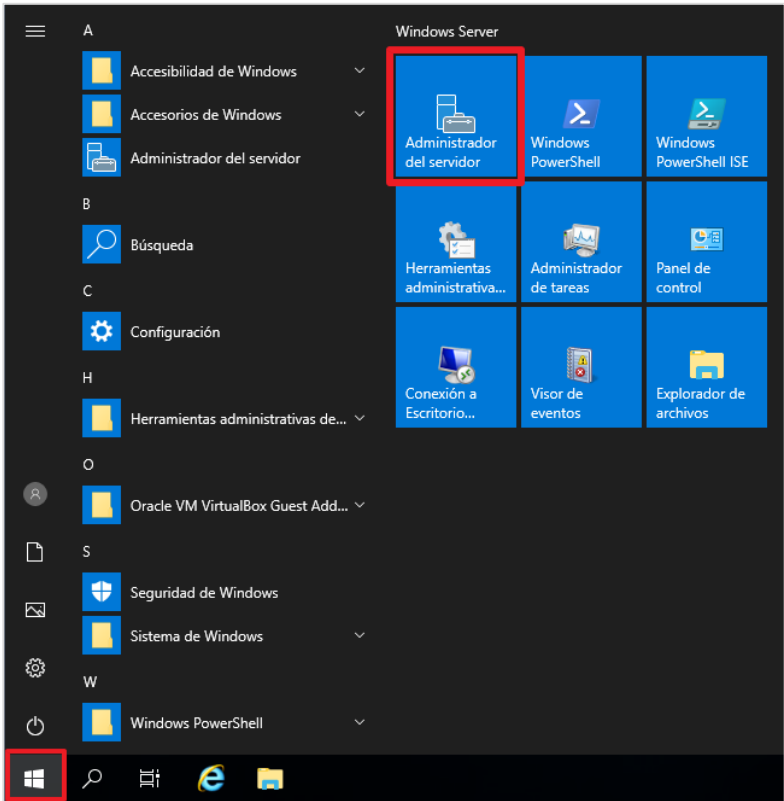
Paso	Descripción
66.	A continuación, en la pestaña “Permisos”, edite los permisos que desee para el recurso compartido.  Nota: Tenga en consideración que, por seguridad, deberá eliminar el grupo “Todos” de cualquier recurso que este compartido.
67.	Para finalizar, pulse sobre “Aceptar” y, después, sobre el botón “Agregar” para hacer efectivos los cambios. 

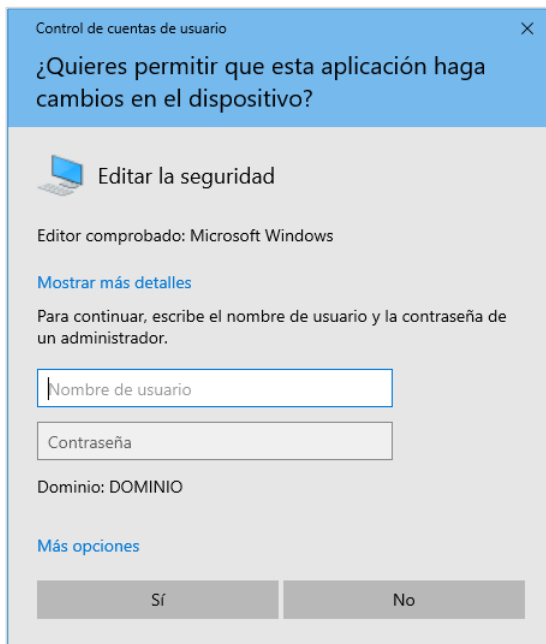
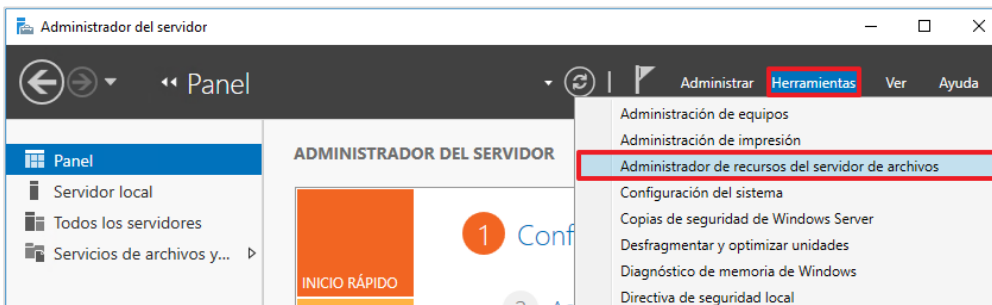
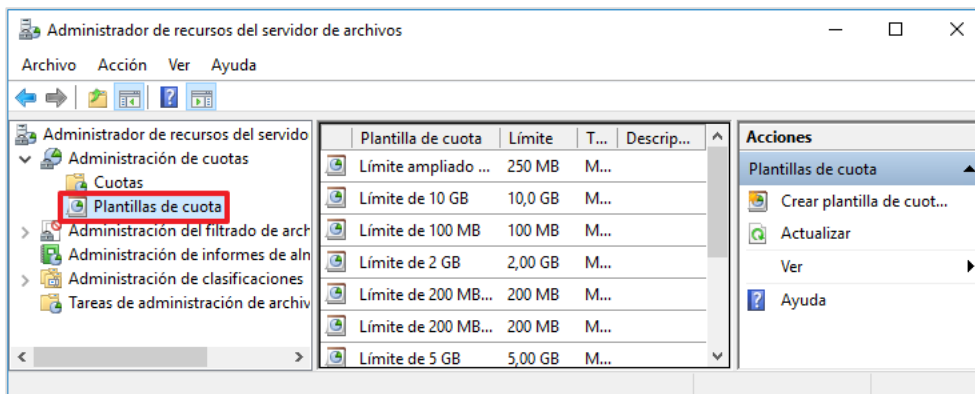
ANEXO A.3.3. LIMITACIÓN DE USO DE ESPACIO EN DISCO.

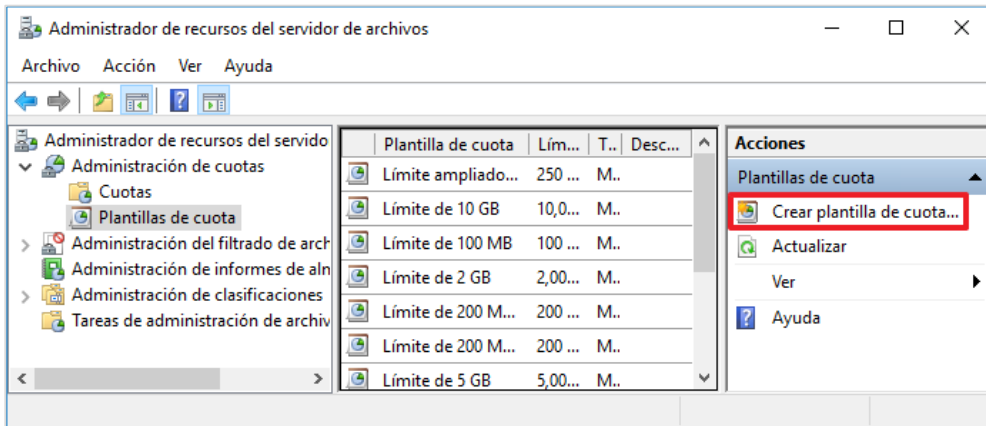
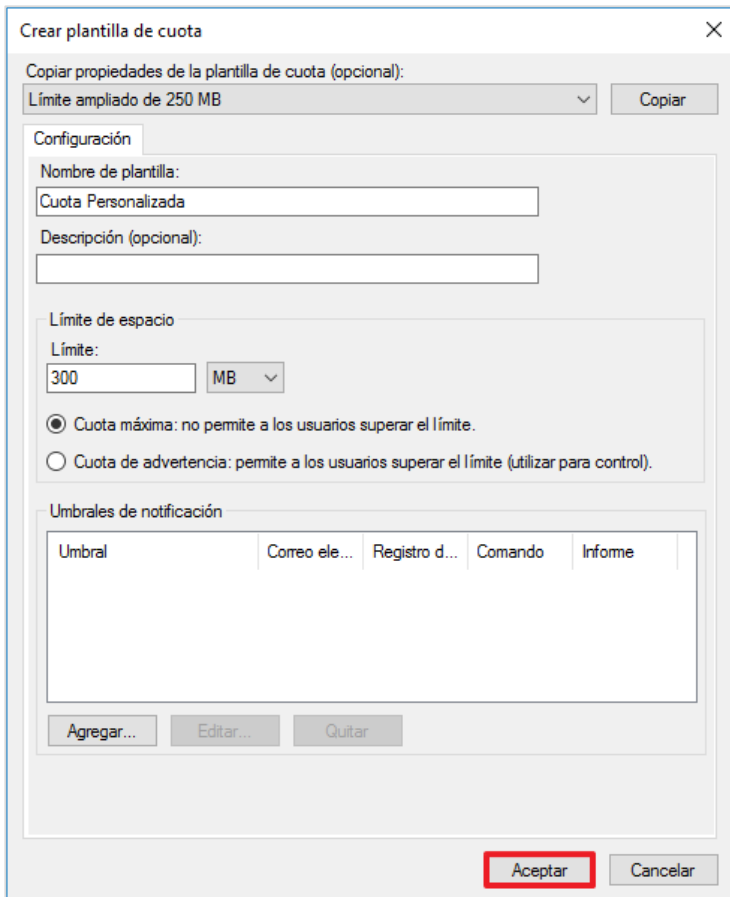
Para cumplir con el perfilado intermedio del ENS, será necesario configurar la limitación al usuario en cuanto al uso del espacio en disco para así prevenir un uso excesivo de los recursos y poder reaccionar frente a los incidentes que se puedan provocar.

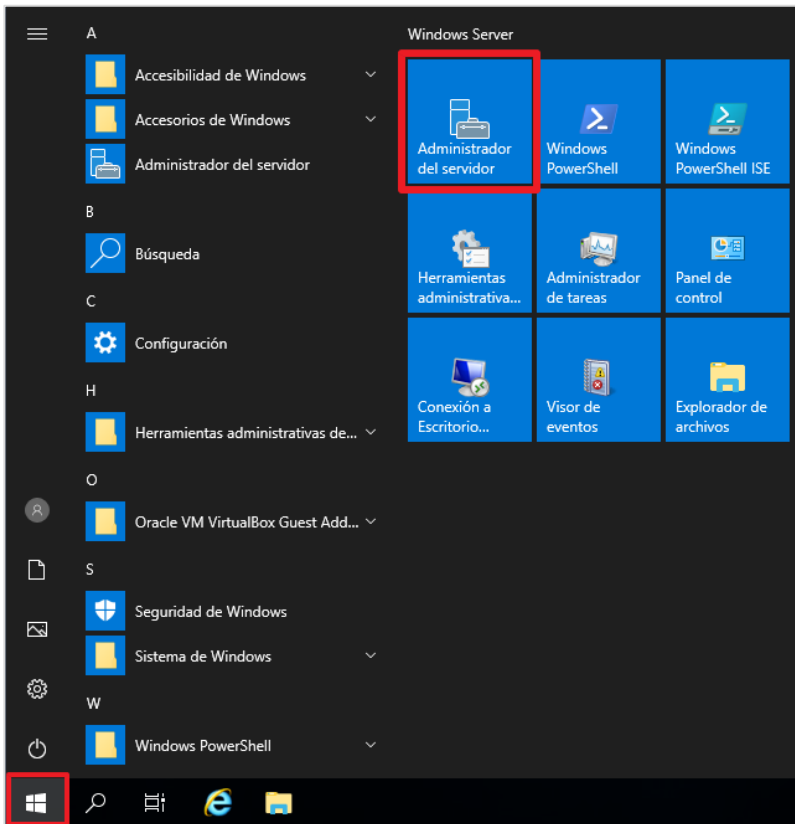
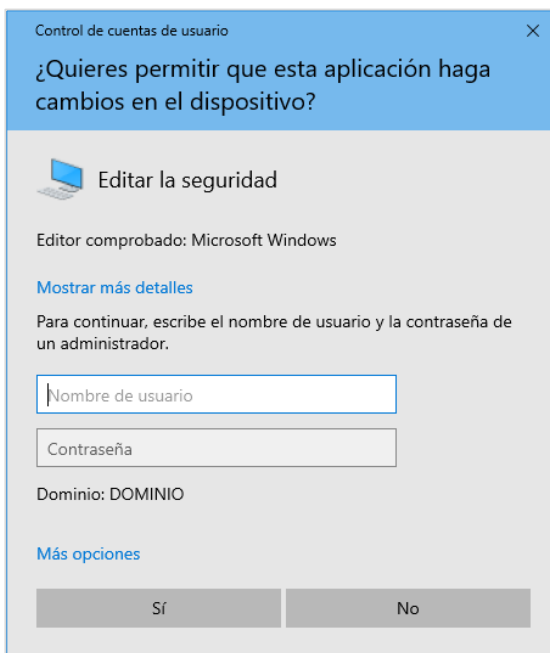
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

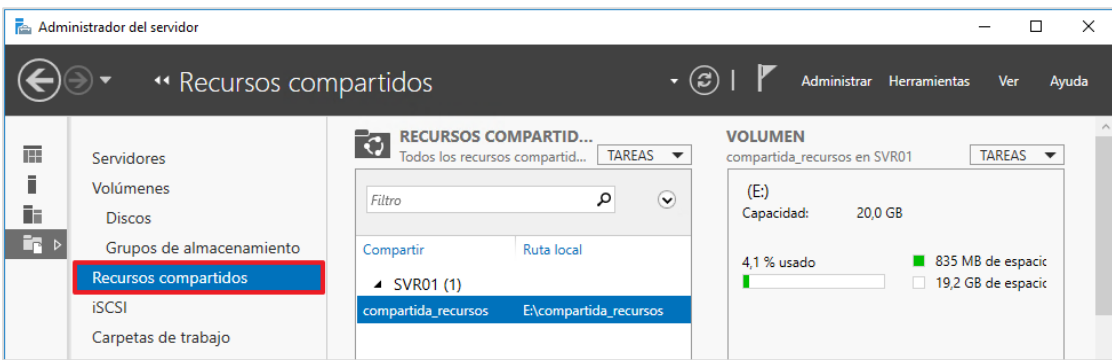
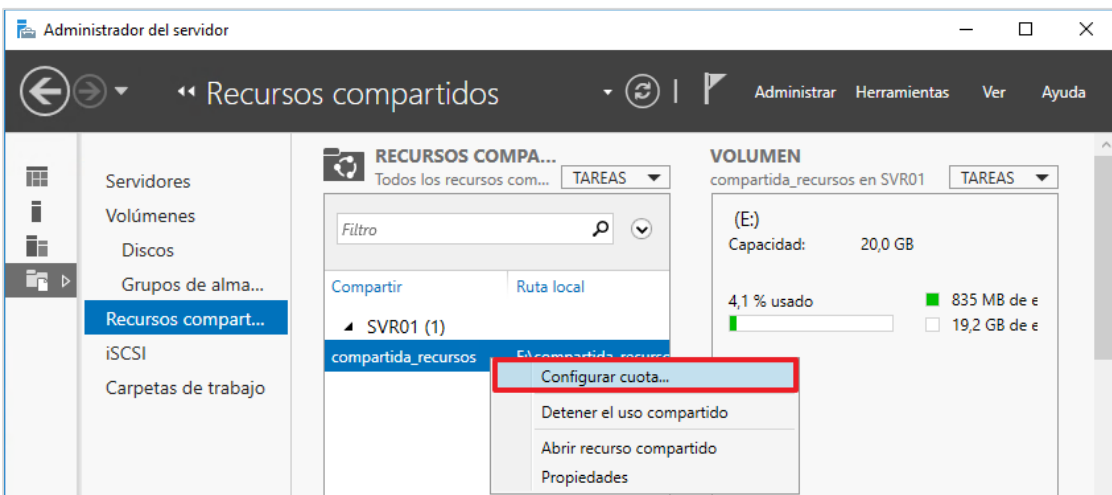
a) [A.24.SEC-FS1] Cuotas de disco.

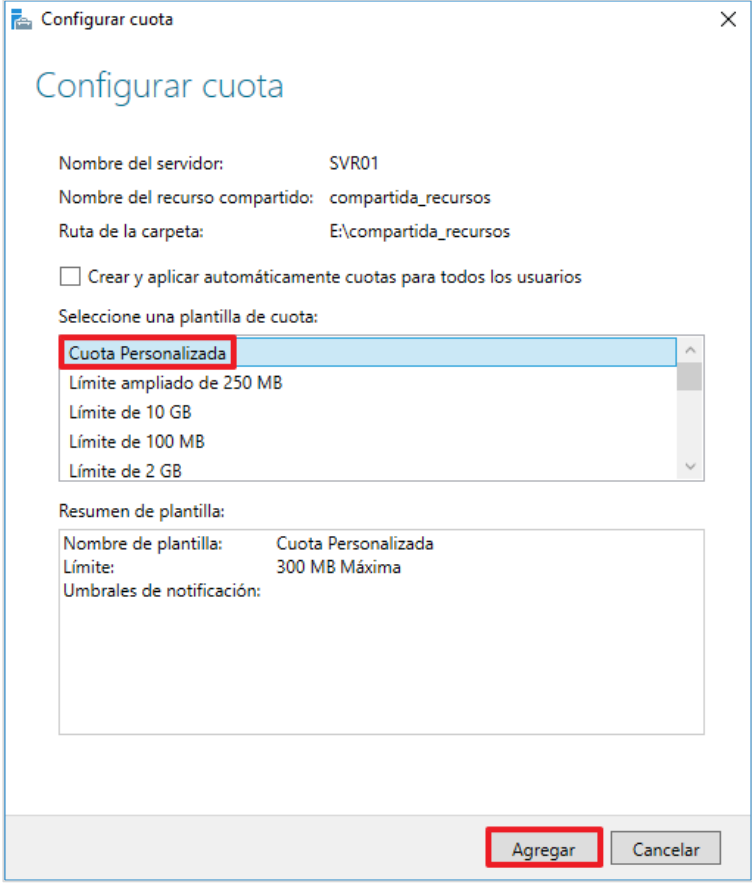
Paso	Descripción
68.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.
69.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

Paso	Descripción
70.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 
71.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
72.	Expanda el nodo “Plantillas de cuota” desde la ruta “Administrador de recursos del servidor de archivos (local) → Administración de cuotas → Plantillas de cuota” tal y como se muestra a continuación. 

Paso	Descripción
73.	En el panel “Acciones”, seleccione “Crear plantilla de cuota...”. 
74.	En la nueva ventana emergente, establezca la configuración deseada para la cuota y pulse “Aceptar” para completar su creación.  Nota: En este ejemplo, se utiliza el nombre “Cuota Personalizada” y se da un valor límite de 300MB.

Paso	Descripción
75.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 
76.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 

Paso	Descripción
77.	Pulse sobre “Servicios de archivos y de almacenamiento”. 
78.	Seleccione la sección “Recursos compartidos”. 
79.	Seleccione, con el botón derecho, el recurso sobre el que desea aplicar la cuota configurada anteriormente y pulse la opción “Configurar cuota...”. 

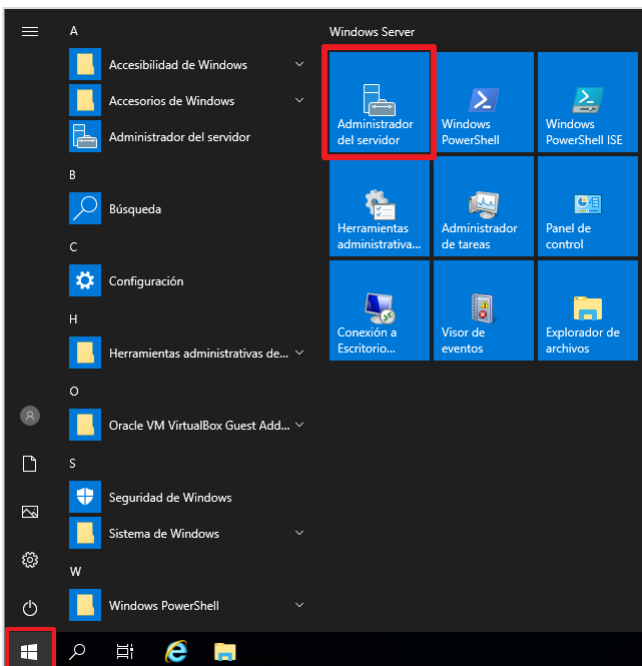
Paso	Descripción
80.	En la nueva ventana emergente, seleccione una cuota creada por defecto por el sistema o una cuota creada específicamente para el recurso compartido. Pulse “Agregar” para finalizar.  Nota: En este ejemplo se aplica la cuota denominada “Cuota Personalizada”, creada anteriormente. Si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

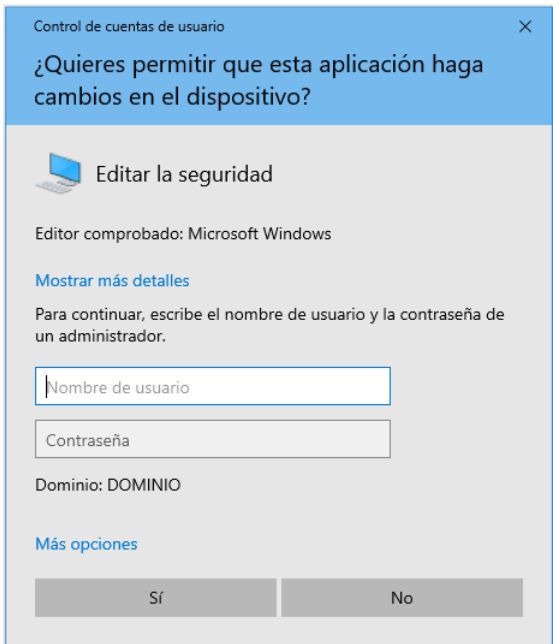
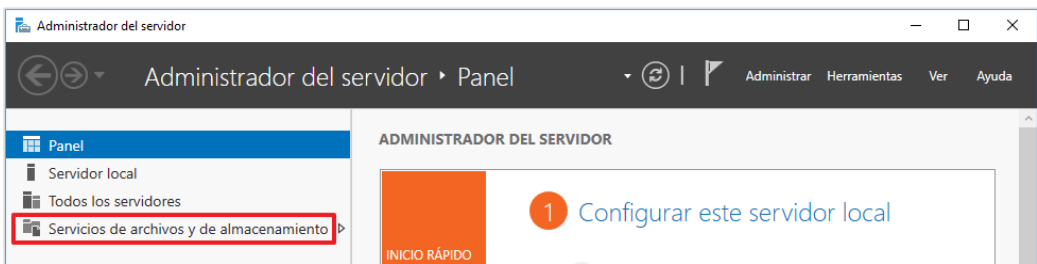
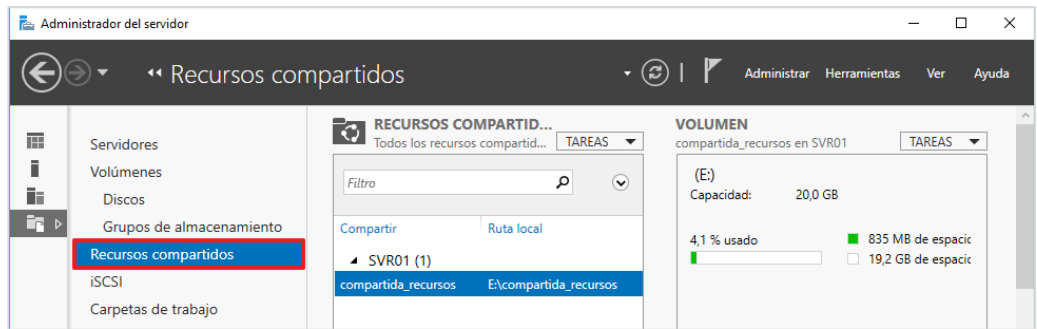
ANEXO A.3.4. VISIBILIDAD DE LA ESTRUCTURA DE CARPETAS DE FICHEROS DE DATOS.

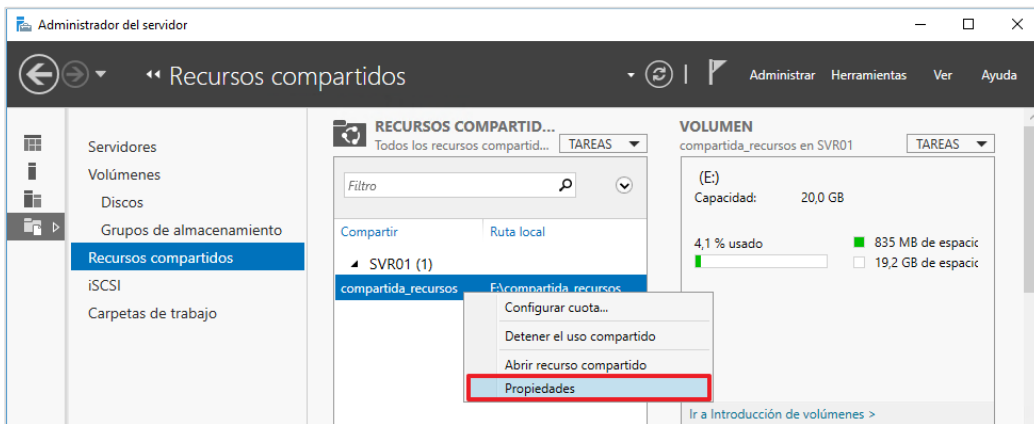
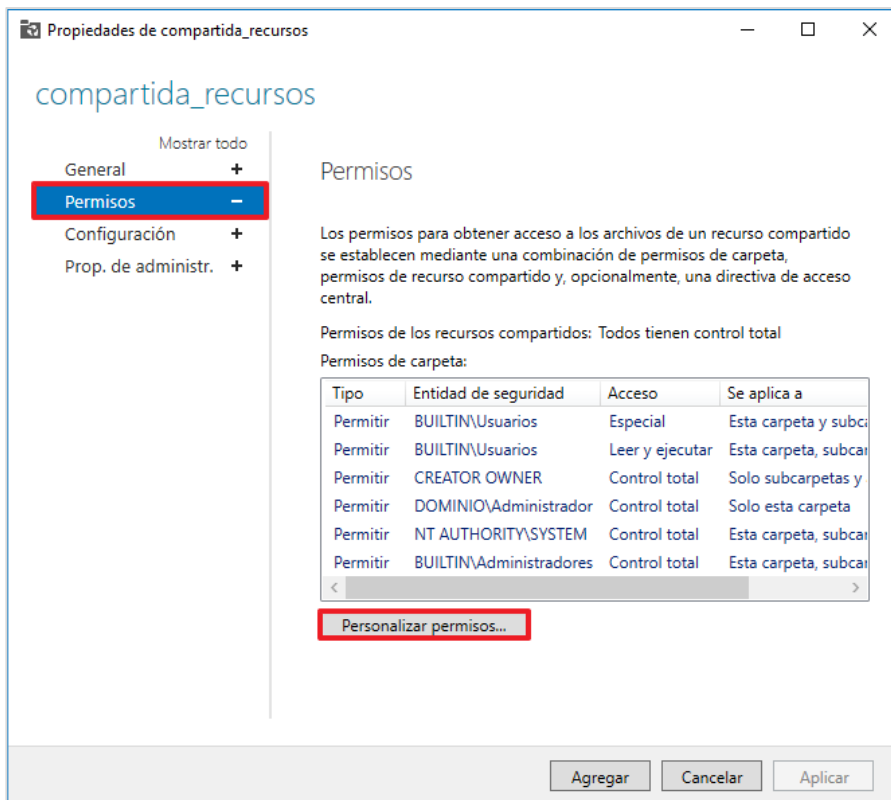
De forma predeterminada, los permisos se heredan del directorio raíz de la unidad y se conceden permisos de lectura al grupo DOMINIO\Usuarios. Como resultado, incluso después de habilitar la enumeración basada en acceso, todas las carpetas del espacio de nombres permanecen visibles para todos los usuarios del dominio. En el siguiente “paso a paso”, se describe como evitar la enumeración de carpetas a las que el usuario no tiene acceso.

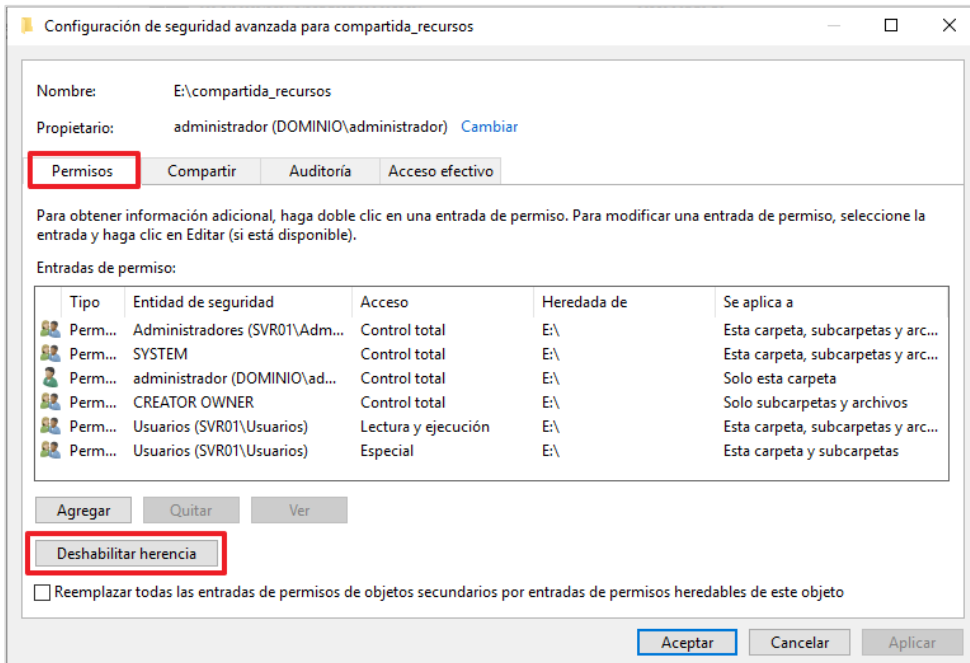
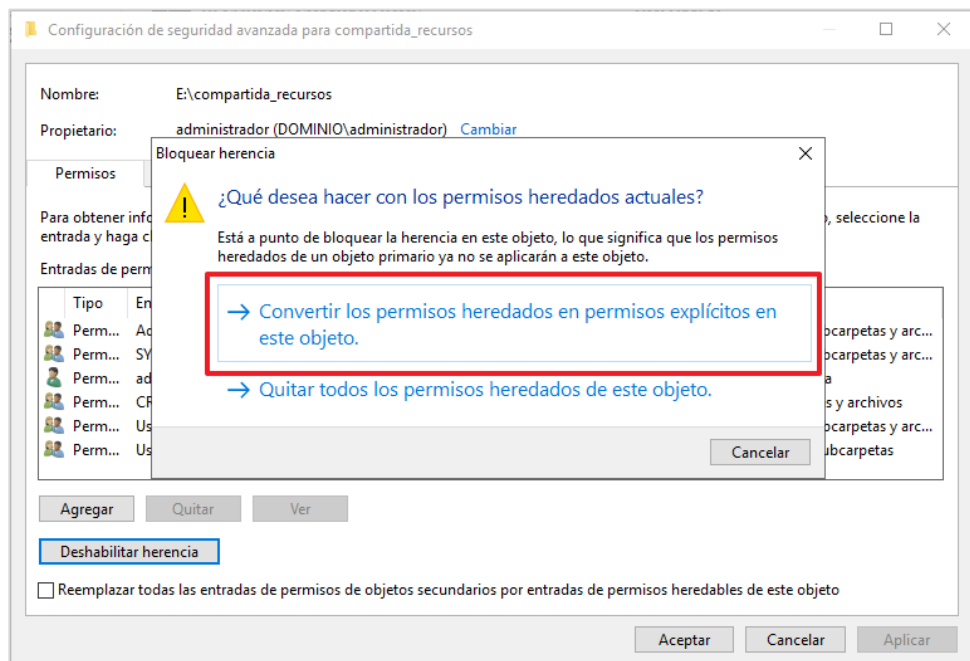
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.3.SEC-FS5]** Se controla la visibilidad y acceso de la estructura de carpetas de ficheros de datos.

Paso	Descripción
81.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.
82.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

Paso	Descripción
83.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 
84.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
85.	Seleccione la sección “Recursos compartidos”. 

Paso	Descripción
86.	Seleccione, con el botón derecho, el recurso sobre el que desea modificar los permisos y pulse la opción “Propiedades”.  Nota: En este ejemplo se editan las propiedades del recurso denominado “compartida_recursos”.
87.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos...”. 

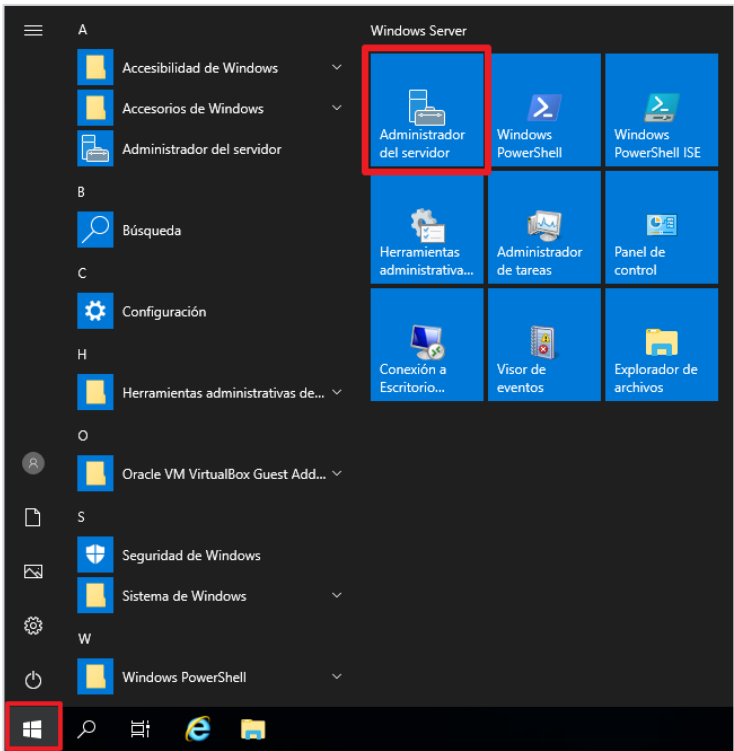
Paso	Descripción
88.	A continuación, en la pestaña “Permisos”, pulse sobre “deshabilitar herencia” para que el recurso no herede los permisos de la carpeta raíz y, de ese modo, poder eliminar o mantener los usuarios o grupos que sean de aplicación: 
89.	En la ventana emergente, seleccione “Convertir los permisos heredados en permisos explícitos en este objeto”. 

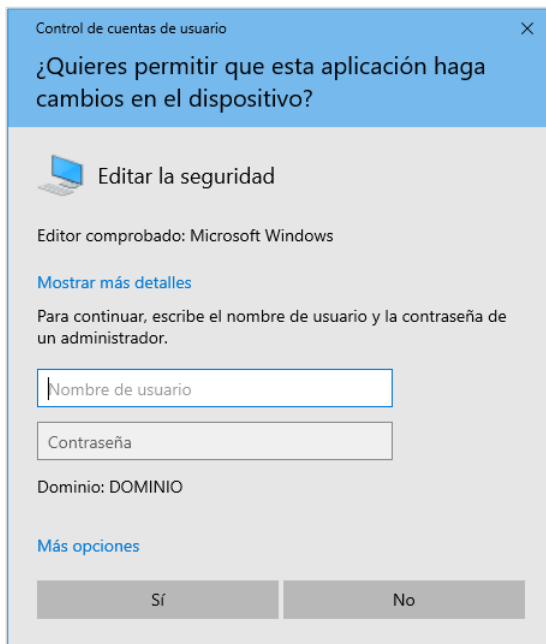
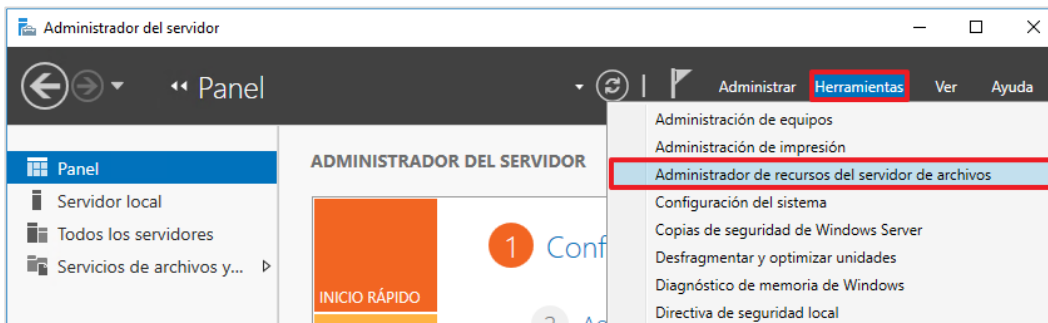
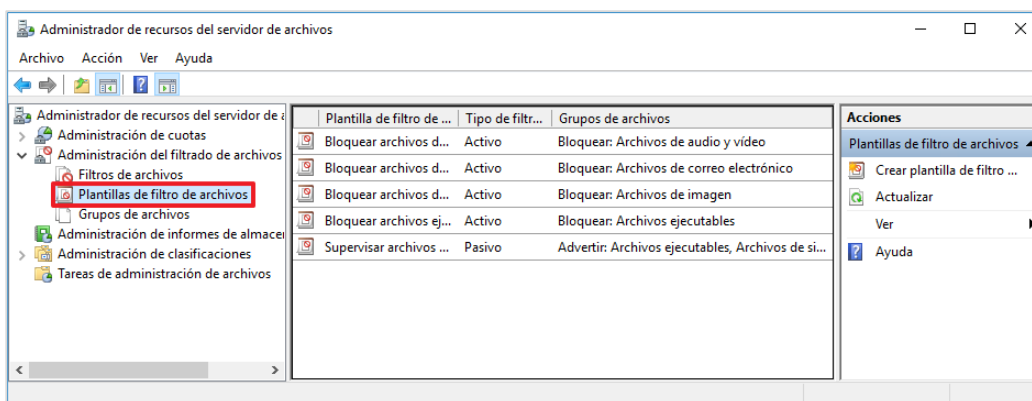
ANEXO A.3.5. FILTRADO DE ARCHIVOS.

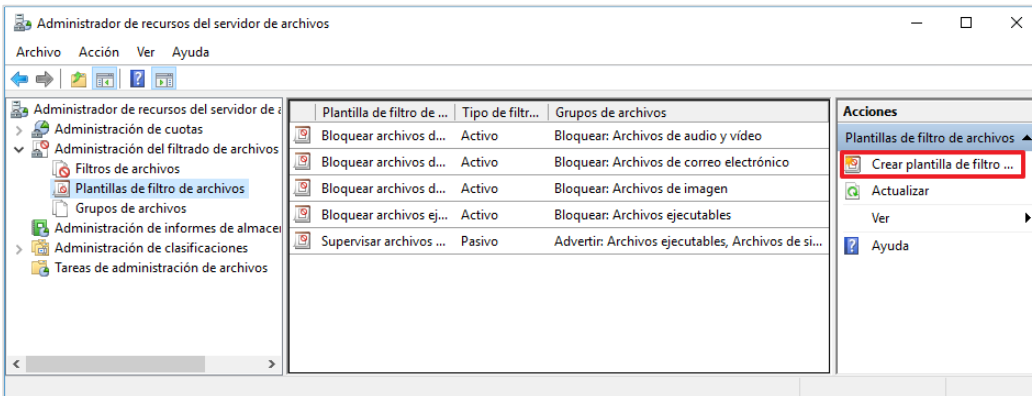
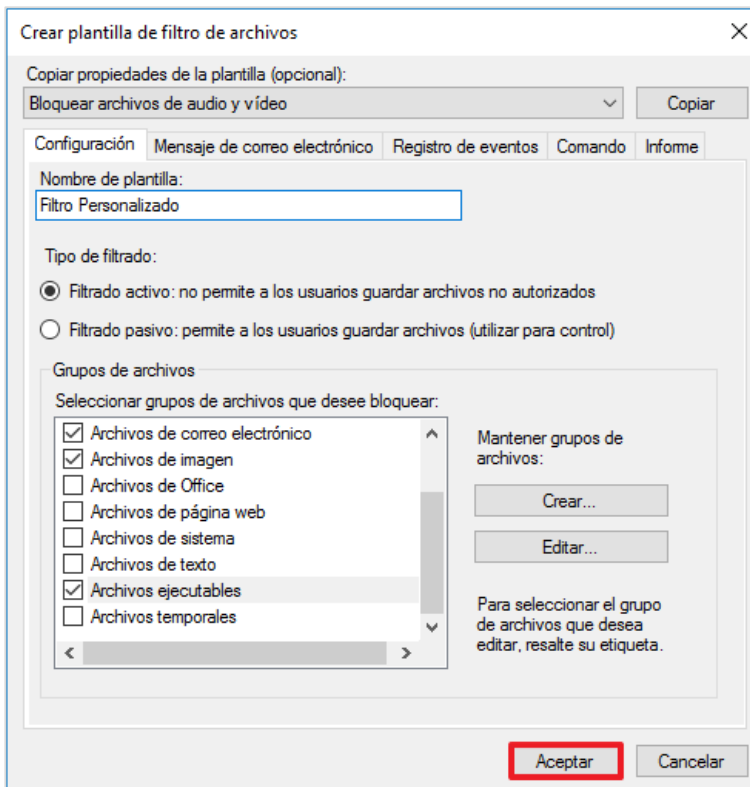
Según lo establecido en el marco operacional para equipos “Servidor de ficheros” que les sea de aplicación el perfilado intermedio de ENS, será necesario configurar el filtrado de archivos para prevenir la introducción de archivos indeseados en el servidor o archivos que puedan poner en riesgo la seguridad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

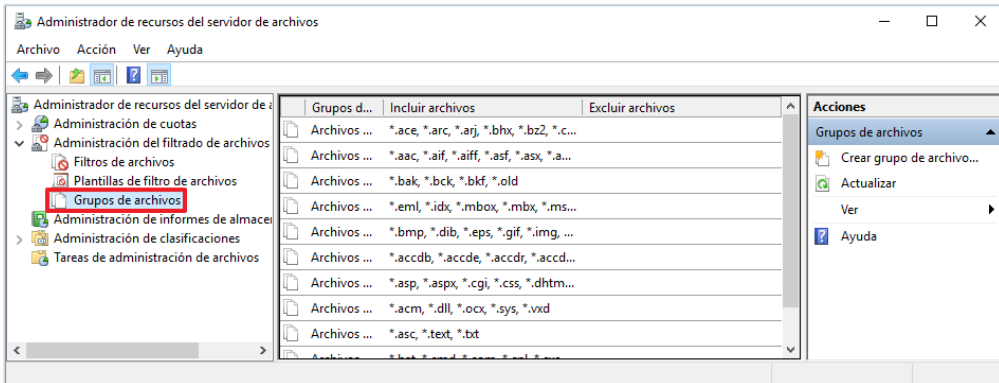
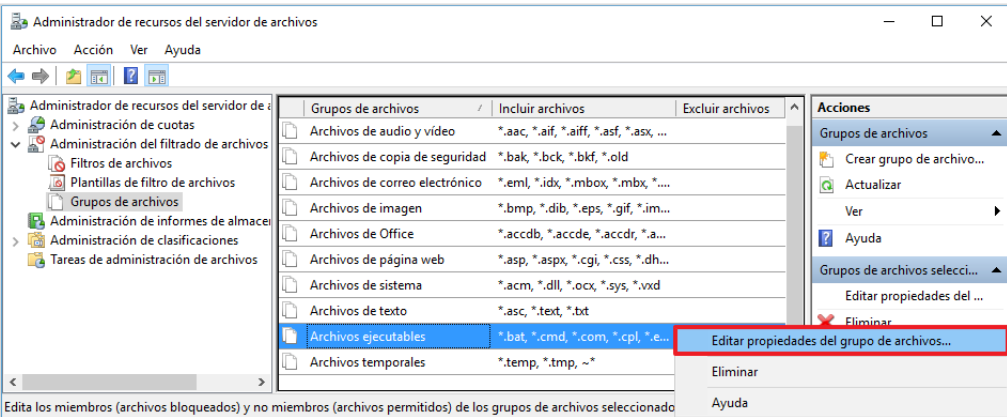
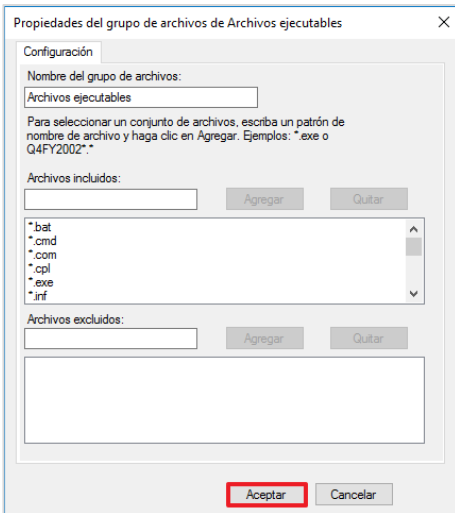
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

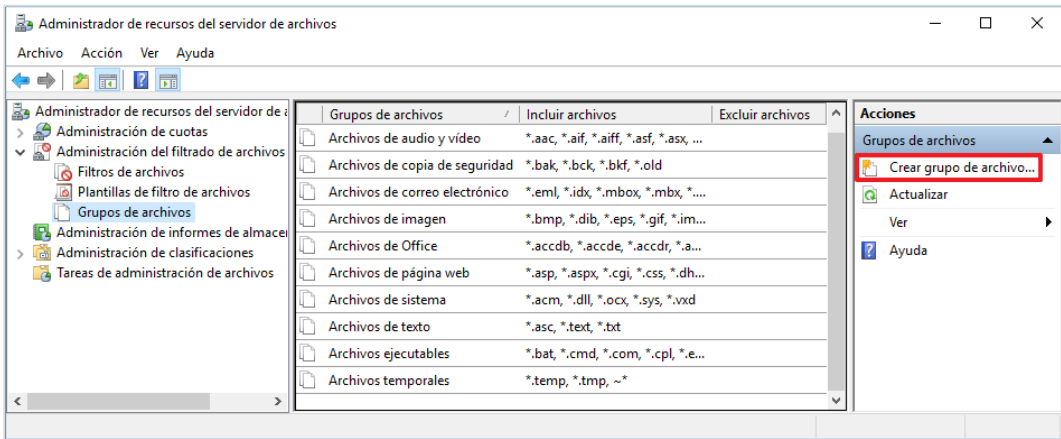
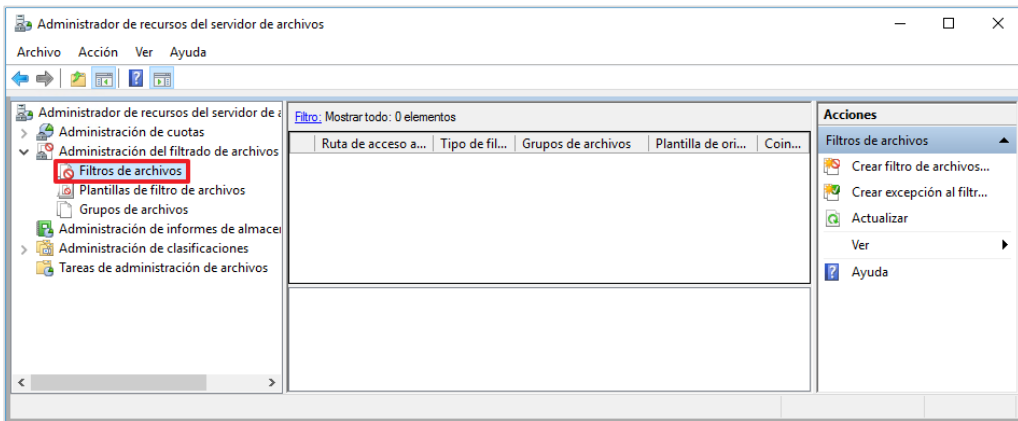
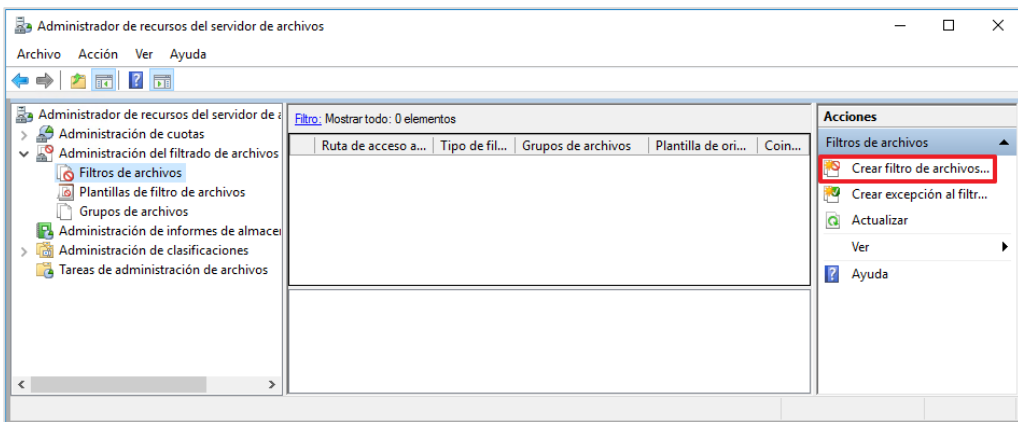
- a) **[A.3.SEC-FS3]** Se audita la descarga y/o copia de ficheros de datos.

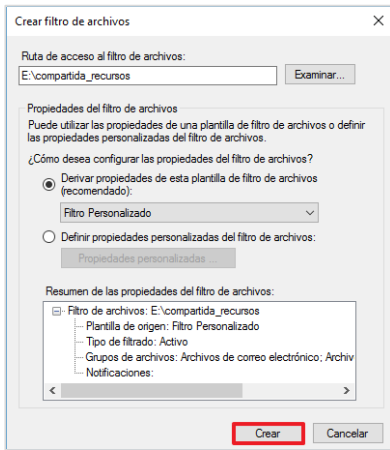
Paso	Descripción
90.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.
91.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

Paso	Descripción
92.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 
93.	Acceda al apartado “Herramientas” y seleccione “Administrador de recursos del servidor de archivos”. 
94.	Expanda el nodo “Plantillas de filtro de archivos” desde la ruta “Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Plantillas de filtro de archivos” tal y como se muestra a continuación. 

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

Paso	Descripción
97.	Expanda el nodo “Grupos de archivos” desde la ruta “Administrador de recursos del servidor de archivos (local) → Administración del filtrado de archivos → Grupos de archivos” tal y como se muestra a continuación. 
98.	Seleccione cualquier grupo de archivos con el botón derecho y pulse sobre la opción del menú contextual “Editar propiedades del grupo de archivos...”.  Nota: Para este ejemplo se edita el grupo de archivos “Archivos ejecutables”.
99.	En la ventana emergente, configure los tipos de archivos que se bloquean y cuales están excluidos. Pulse “Aceptar” para finalizar. 

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

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

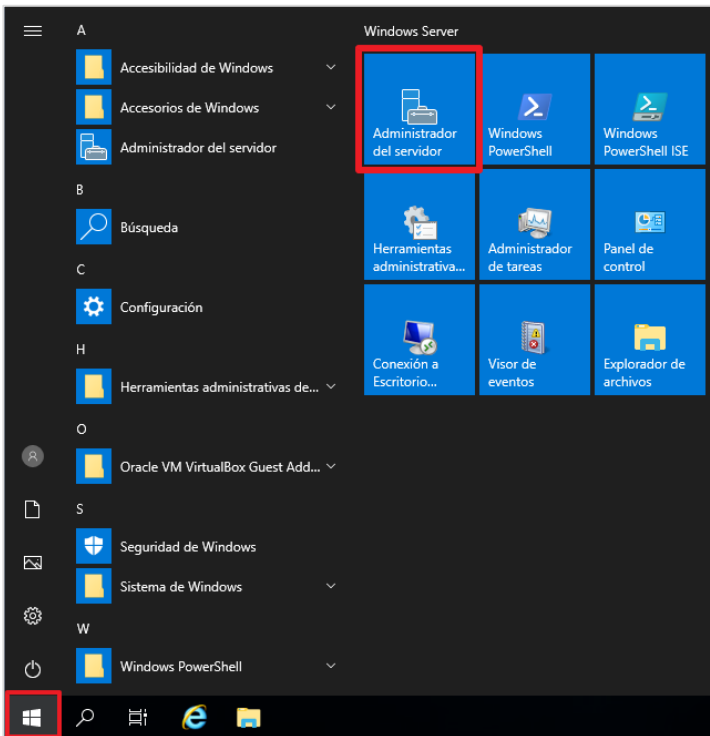
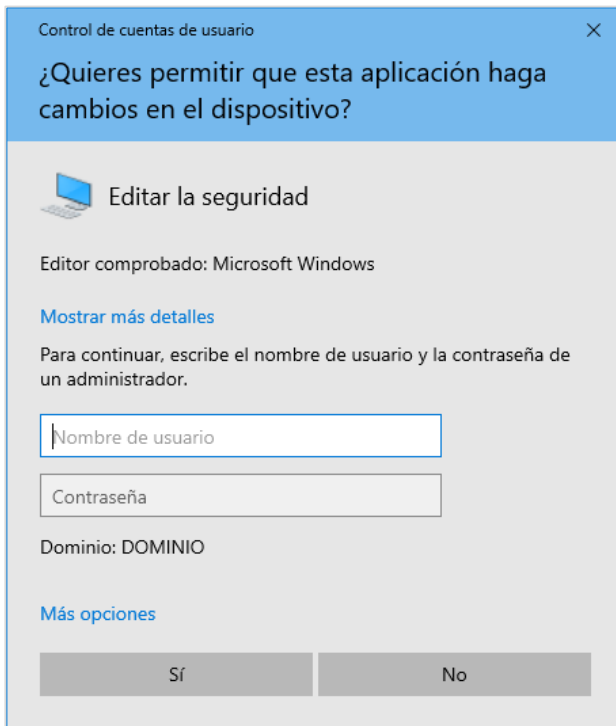
ANEXO A.3.6. SEGREGACIÓN DE ROLES.

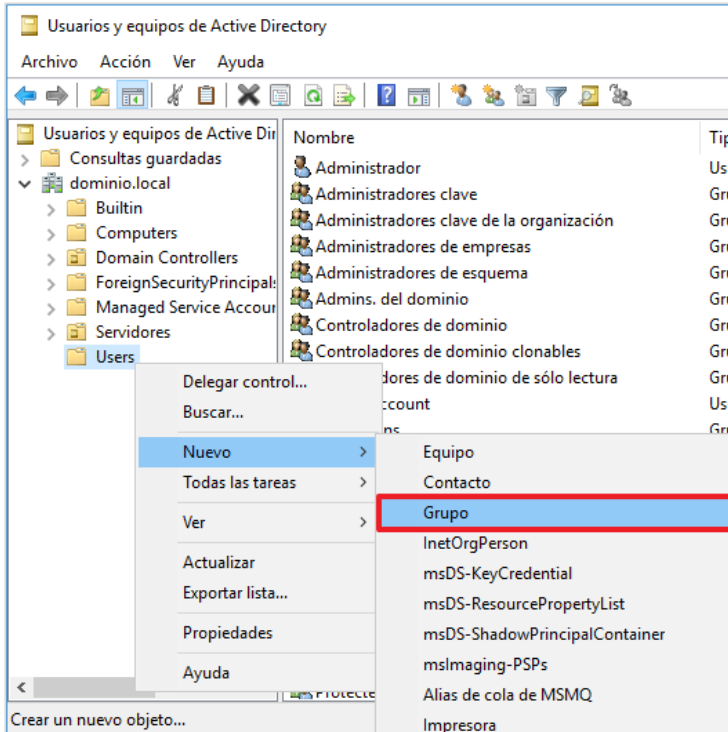
Con la aplicación del perfilado intermedio de ENS sobre el Servidor de ficheros, será necesario crear grupos de usuarios para conceder o denegar permisos sobre los recursos, así como para la administración del Servidor de ficheros.

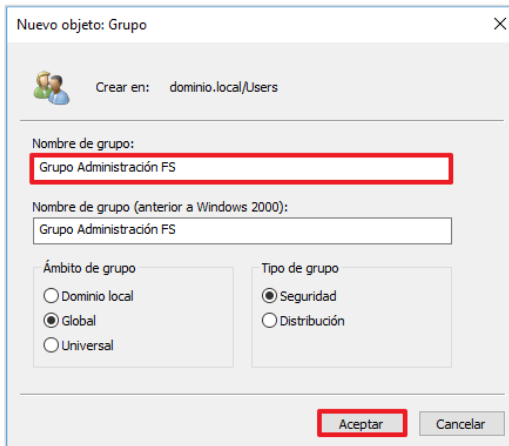
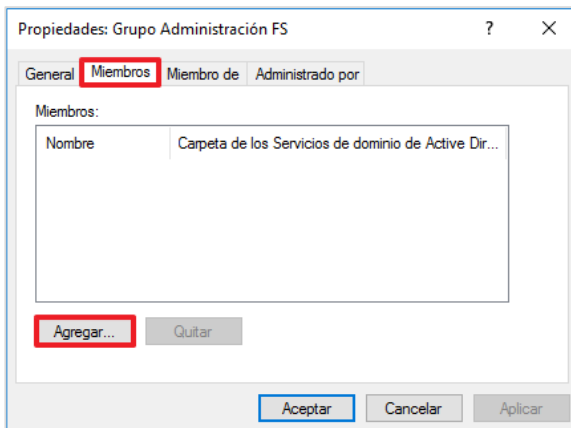
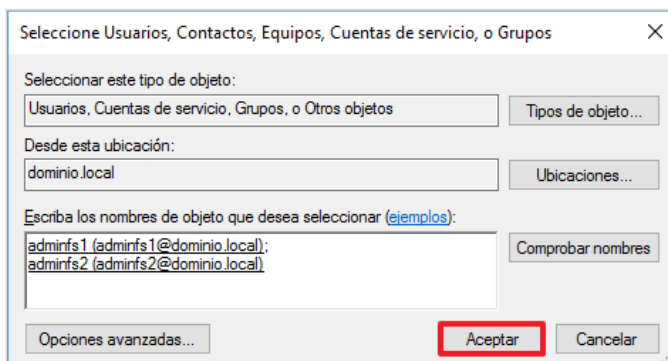
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- [A.6.SEC-FS1]** Se controla el uso de consolas de administración del espacio de almacenamiento.
- [A.24.SEC-FS2]** Iniciar/detener los servicios del sistema.

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

Paso	Descripción
105.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 
106.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 

Paso	Descripción
107.	Acceda al apartado “Herramientas” y seleccione “Usuarios y Equipos de Active Directory”. 
108.	Despliegue el nodo “<Su dominio> → Users”. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual “Nuevo → Grupo”. 

Paso	Descripción
109.	Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.  Nota: En este ejemplo, se utiliza el nombre “Grupo Administración FS”.
110.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar...” para añadir usuarios al grupo. 
111.	Añada los usuarios que desee al grupo y pulse “Aceptar”.  Nota: En este ejemplo se añaden los usuarios “adminfs1” y “adminfs2” utilizados para la creación de esta guía.”

ANEXO A.3.7. COPIAS DE SEGURIDAD.

Por defecto, los “Administradores” y los “Operadores de copia de seguridad” son los usuarios capacitados para realizar las copias de seguridad en los servidores pertenecientes al Dominio de Windows.

Asignar el permiso de “Hacer copias de seguridad de archivos y directorios” a un usuario, es similar a conceder los siguientes permisos al usuario o grupo en cuestión en todos los archivos y carpetas del sistema:

- a) Atravesar carpeta o ejecutar archivo
- b) Mostrar carpeta o leer datos
- c) Leer atributos
- d) Leer atributos extendidos
- e) Leer permisos

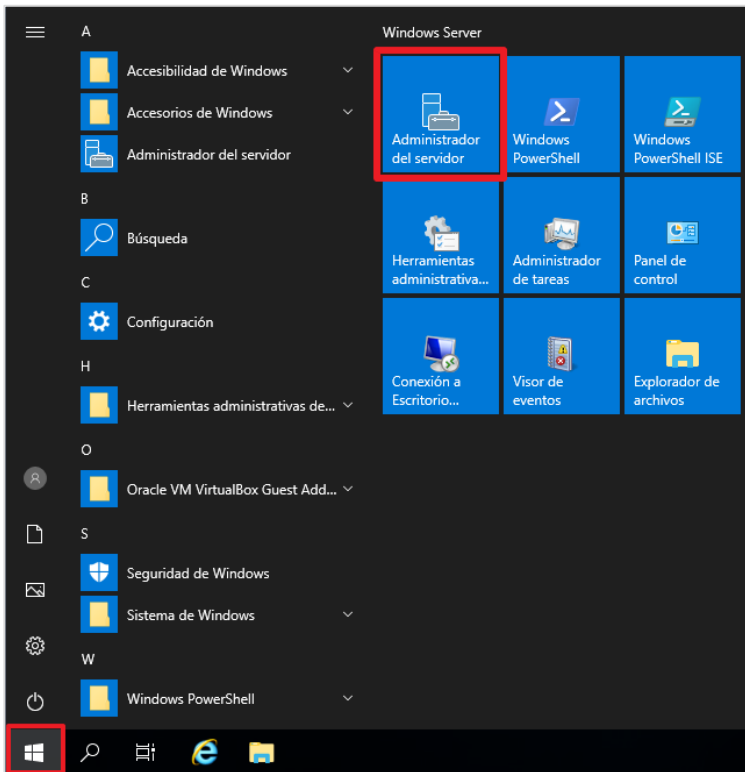
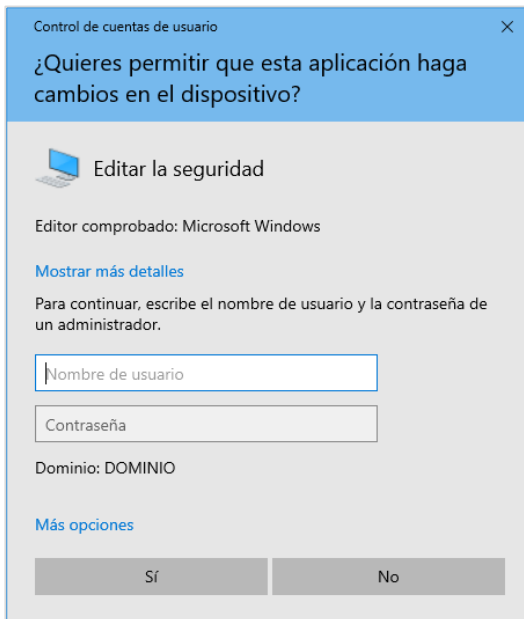
Asignar este derecho de usuario puede suponer un riesgo para la seguridad. Como no existe una forma de saber con certeza si un usuario está haciendo una copia de seguridad de los datos, robando datos o copiando datos para distribuirlos, solo se debe asignar este derecho a usuarios de confianza.

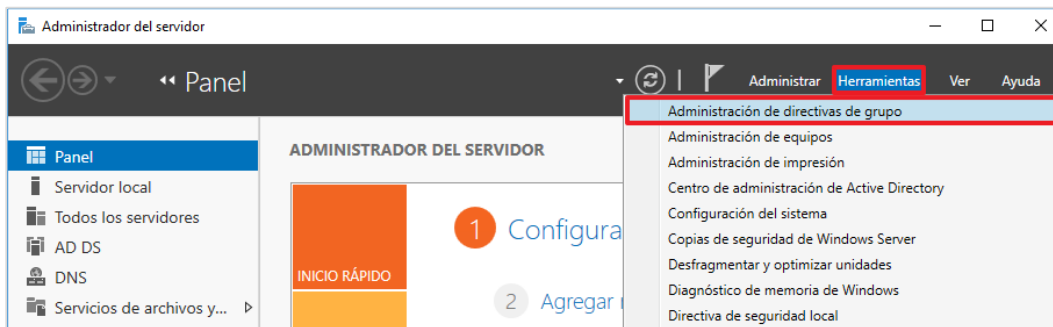
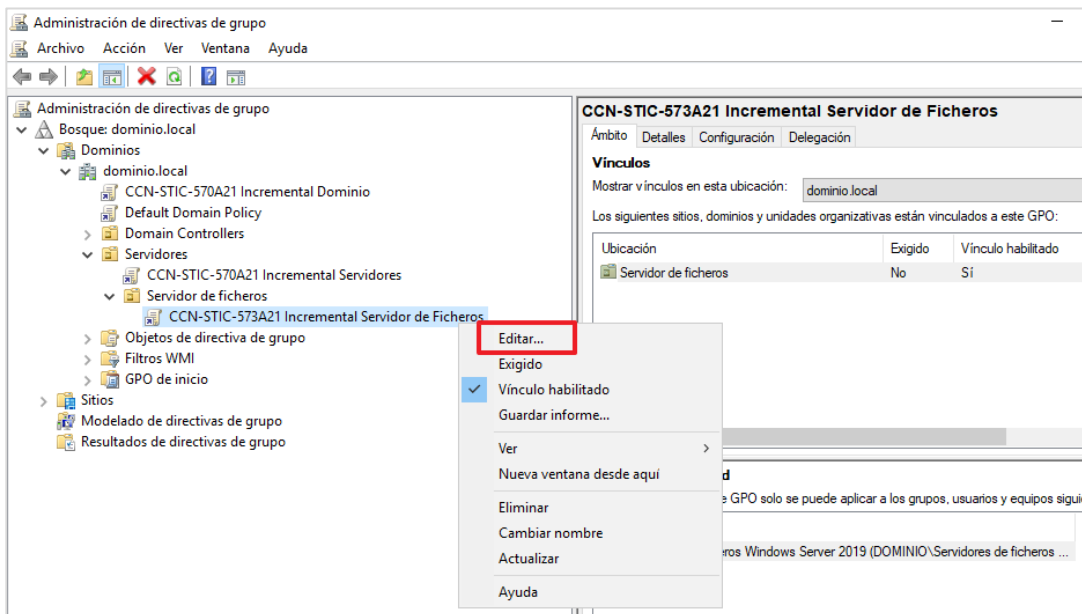
Debido a todo lo expuesto, se debe habilitar “Auditoría: auditar el uso de privilegios de copia de seguridad y restauración”, de manera que se generará un evento de auditoría para cada archivo del que se haga una copia de seguridad o se restaure, ayudando a identificar la cuenta que se usó para restaurar datos accidental o malintencionadamente de forma no autorizada.

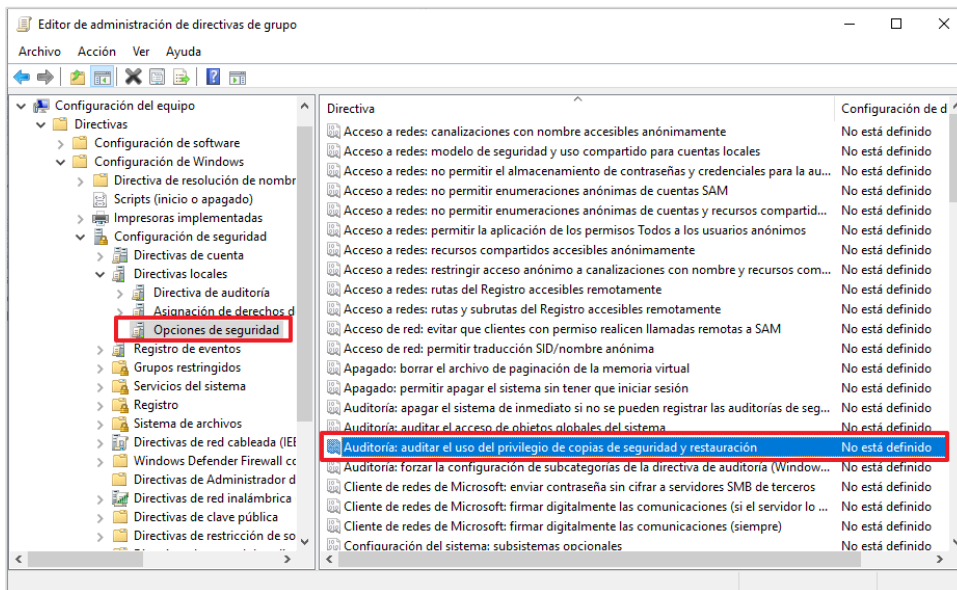
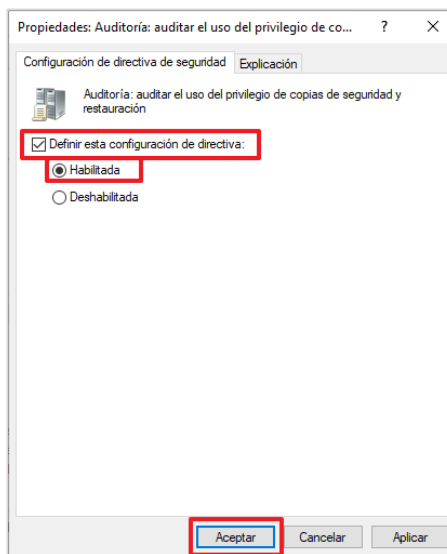
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.6.SEC-FS2]** Se controla quién puede hacer copias de seguridad.

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

Paso	Descripción
113.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 
114.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 

Paso	Descripción
115.	Inicie la consola “Administración de directivas de grupo”. Para ello, pulse sobre el botón “Herramientas → Administración de directivas de grupo”. 
116.	A continuación, despliegue el nodo “Bosque: <<Nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de ficheros”. Nota: En este ejemplo, el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de ficheros”.
117.	Edite la GPO “CCN-STIC-573A21 Incremental Servidor de Ficheros”. 

Paso	Descripción
118.	Expanda el árbol de configuración “Configuración del equipo\ Directivas\Configuración Windows\ Configuración de Seguridad\Directivas locales\Opciones de seguridad” 
119.	Seleccione y habilite la configuración “Auditoría: auditar el uso del privilegio de copias de seguridad y restauración” y seleccione Aceptar para fijar la configuración. 
120.	Cierre la ventana de edición de la GPO

Nota: Habilitar esta configuración de directiva podría generar un gran número de eventos de seguridad, lo que podría hacer que los servidores respondan lentamente y forzar al registro de eventos de seguridad a registrar numerosos eventos de poca importancia. Debido a ello, se recomienda aumentar la capacidad del registro de Seguridad.

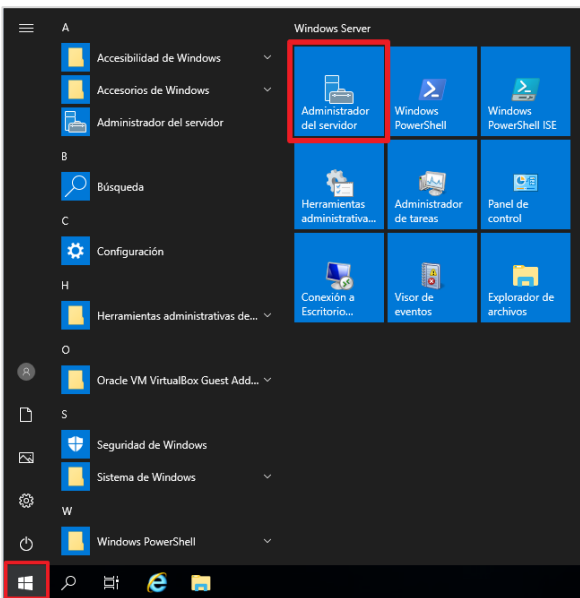
ANEXO A.3.8. AUDITORIA DE ARCHIVOS.

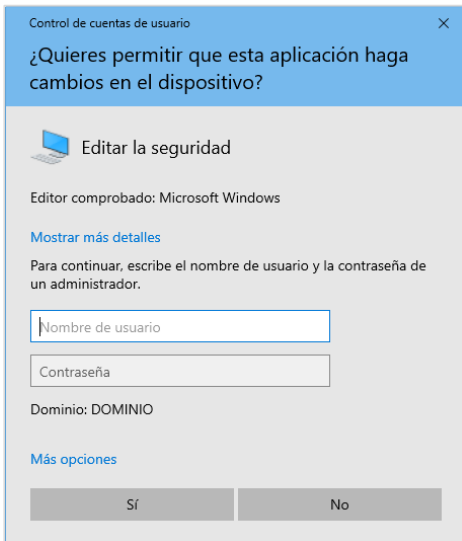
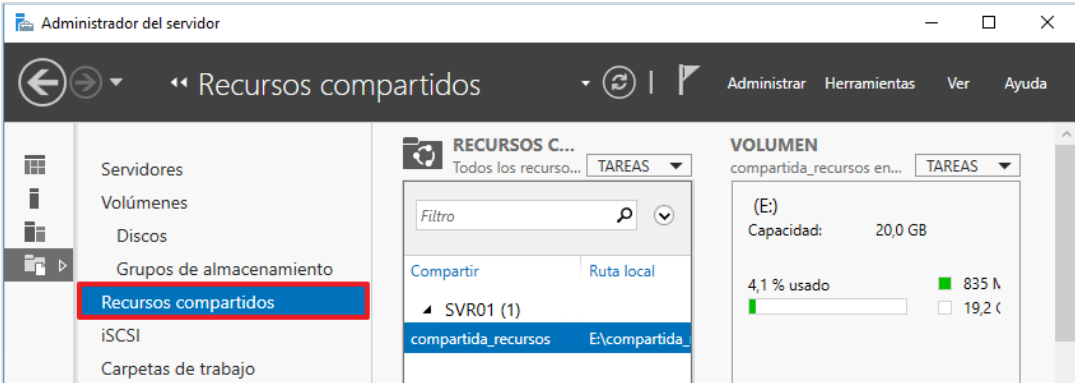
Con la aplicación del perfilado intermedio de ENS sobre el Servidor de ficheros, quedará registrado el uso de los recursos compartidos del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quién realiza la actividad, cuándo y sobre qué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

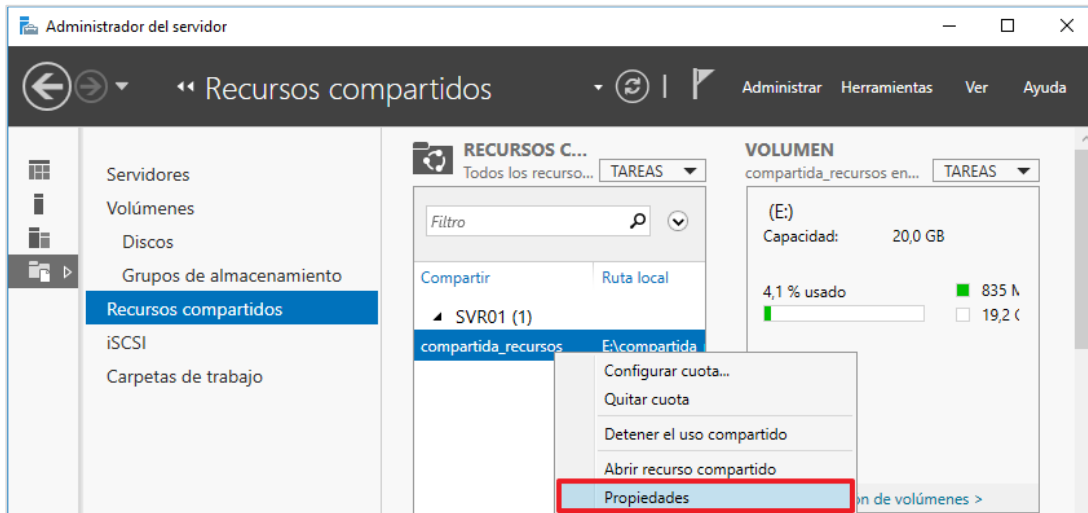
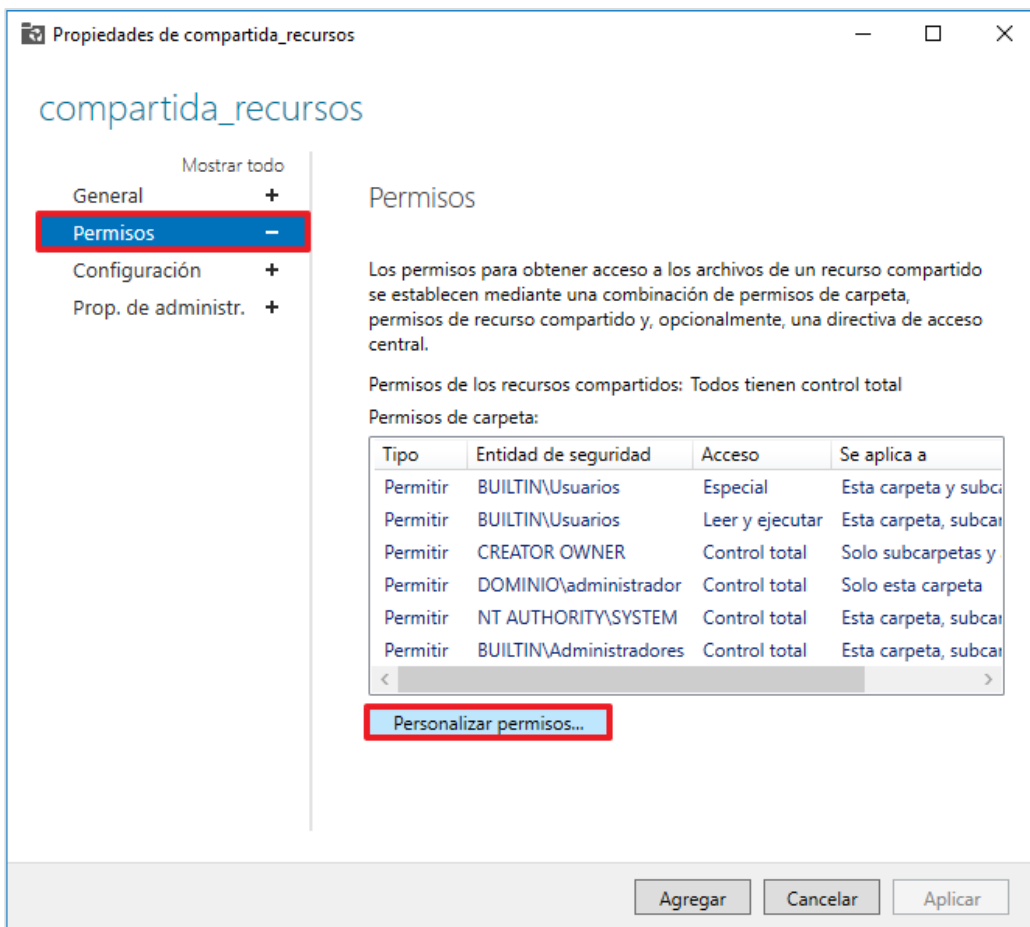
La ubicación de los registros debe ser diferente a la del sistema, además de tener limitado el acceso únicamente a los usuarios autorizados.

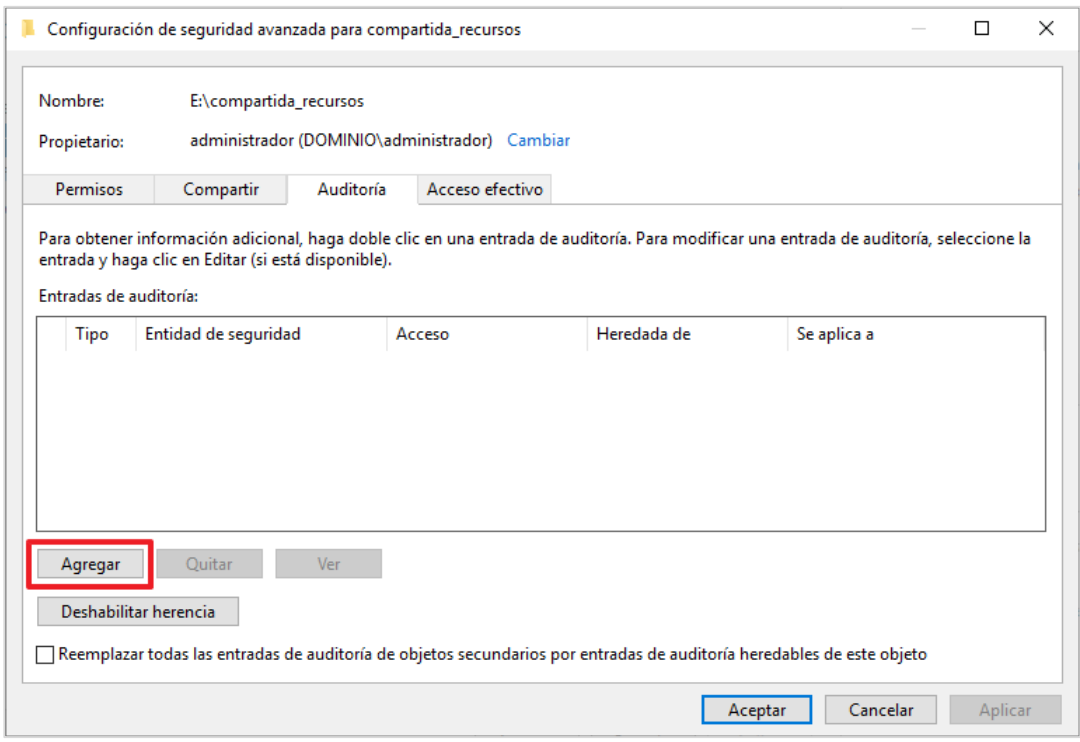
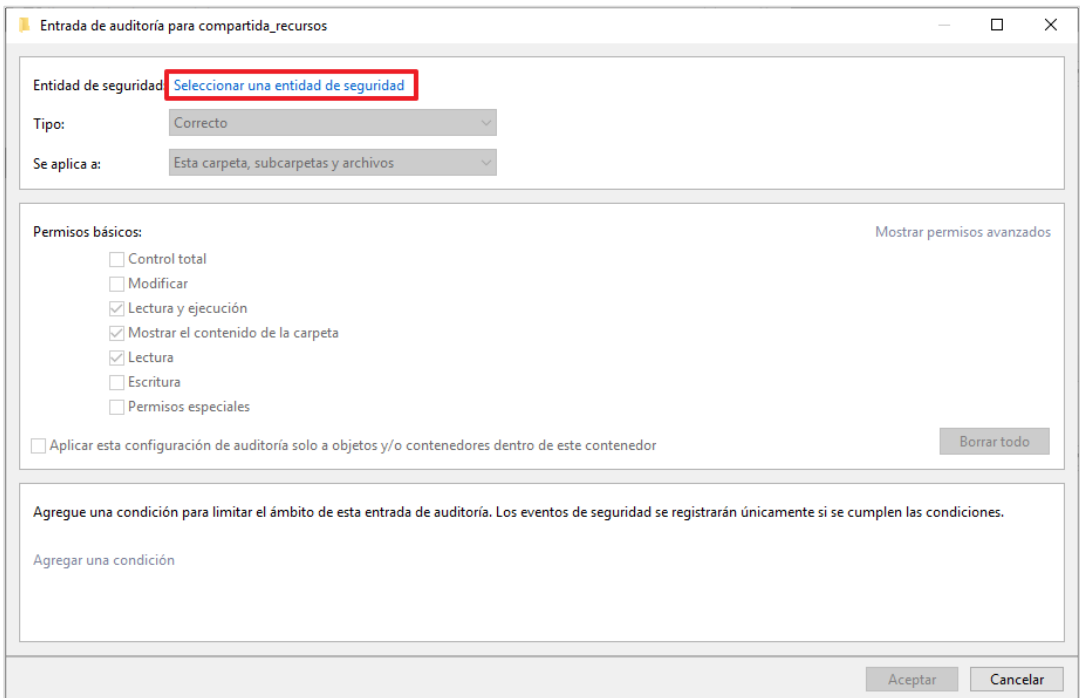
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

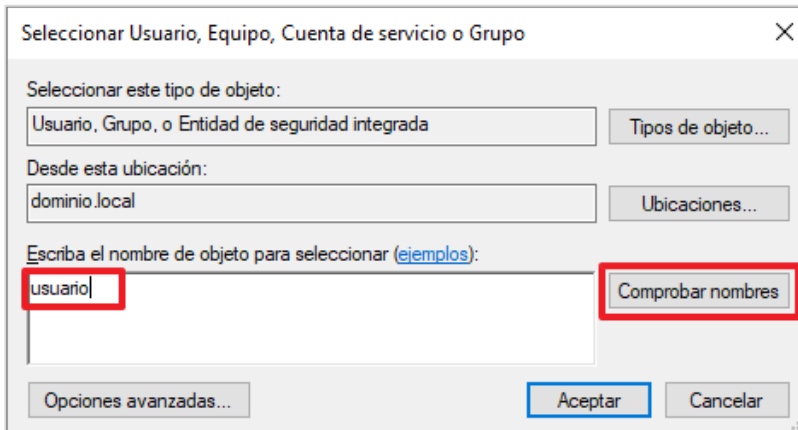
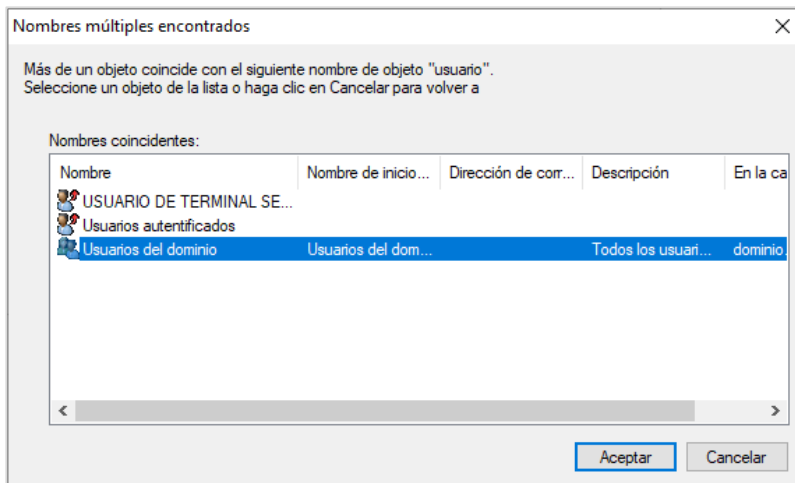
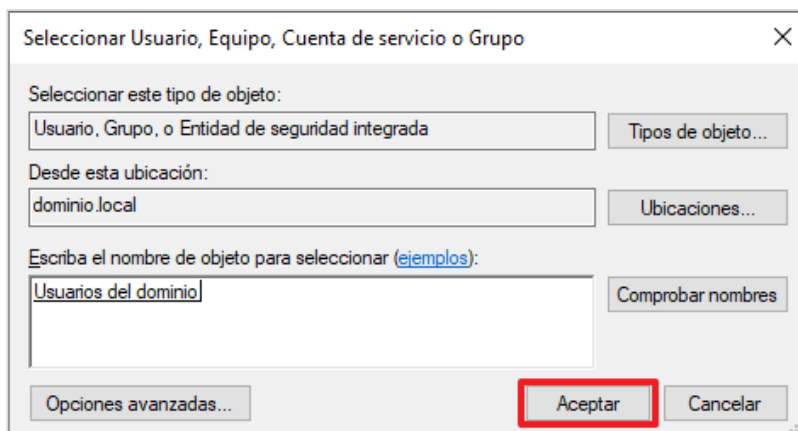
- a) **[A.3.SEC-FS1]** Se encuentra habilitada la auditoría sobre los recursos del servidor.
- b) **[A.3.SEC-FS4]** Se audita el uso de copias de seguridad y restauración.

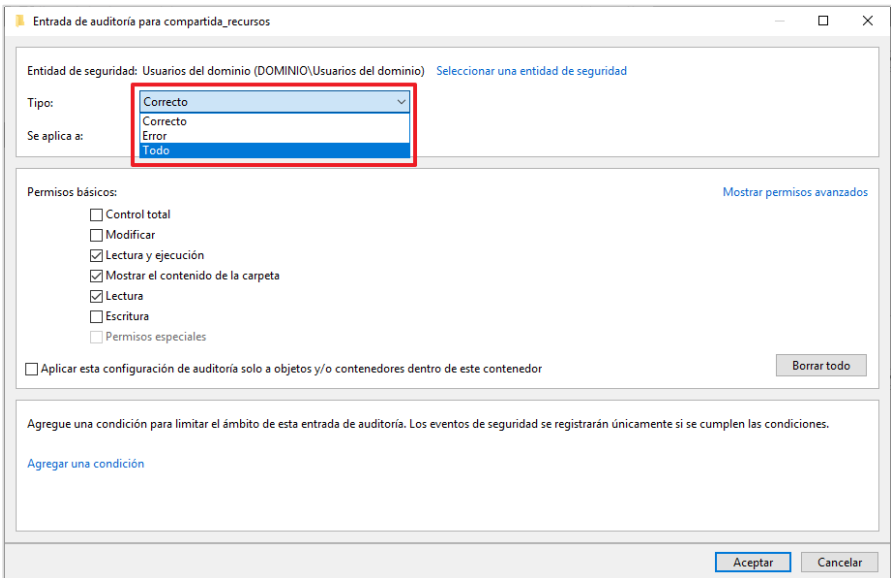
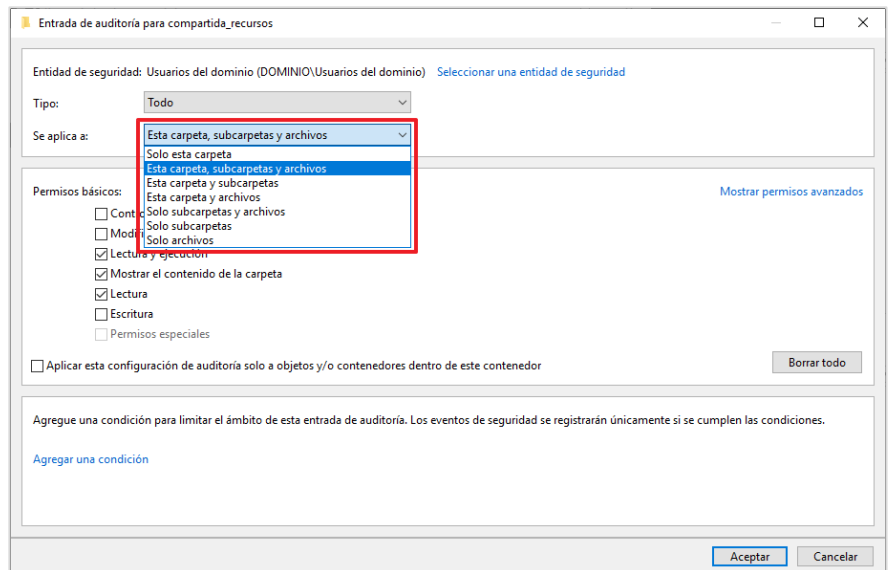
Paso	Descripción
121.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.
122.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 

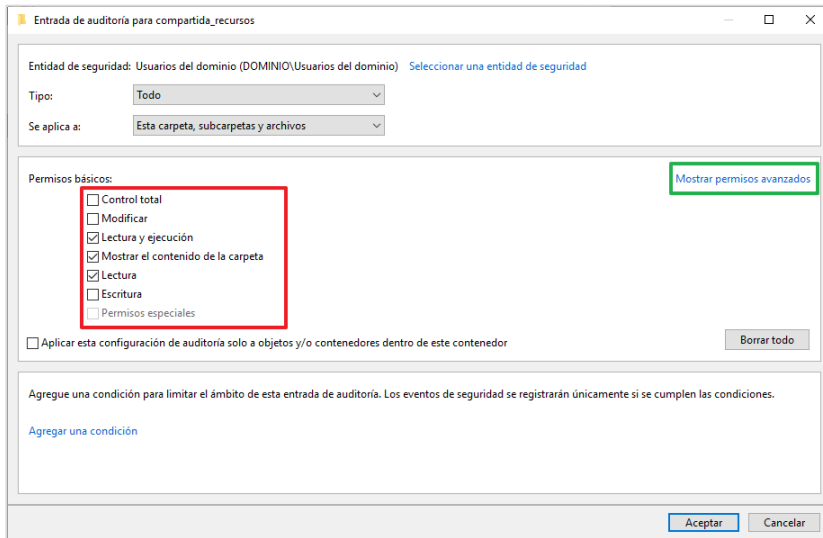
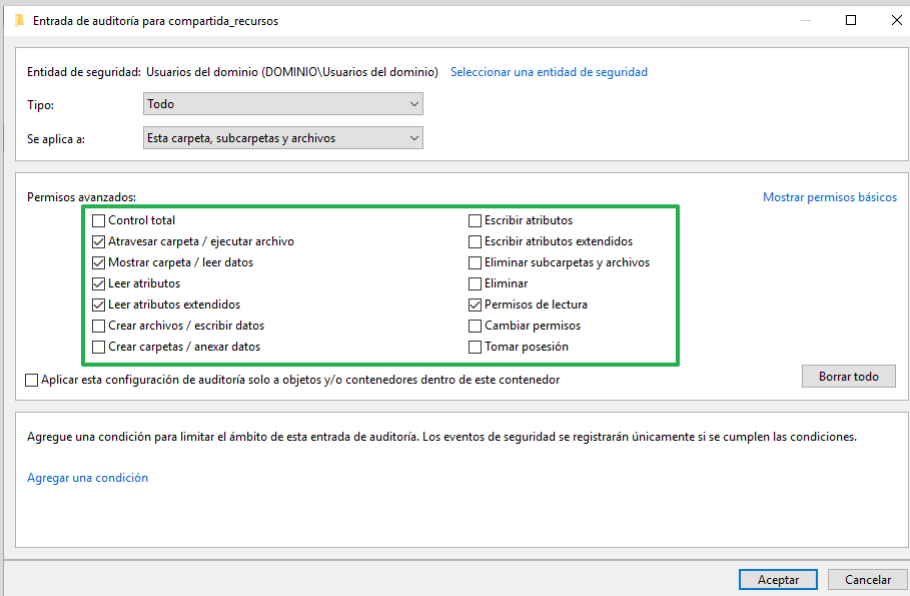
Paso	Descripción
123.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 
124.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
125.	Seleccione la sección “Recursos compartidos”. 

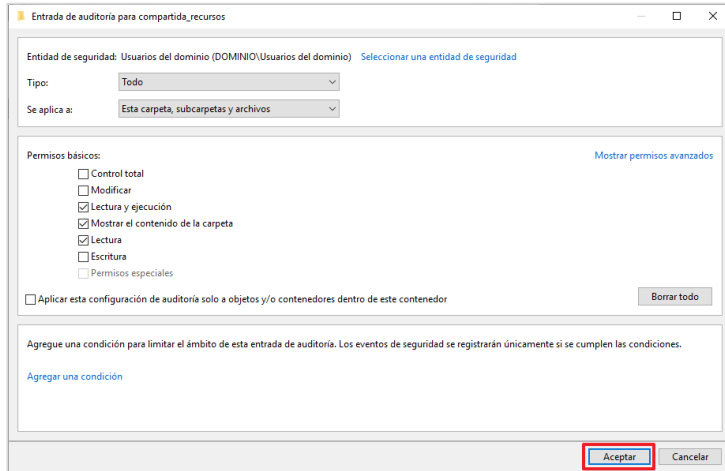
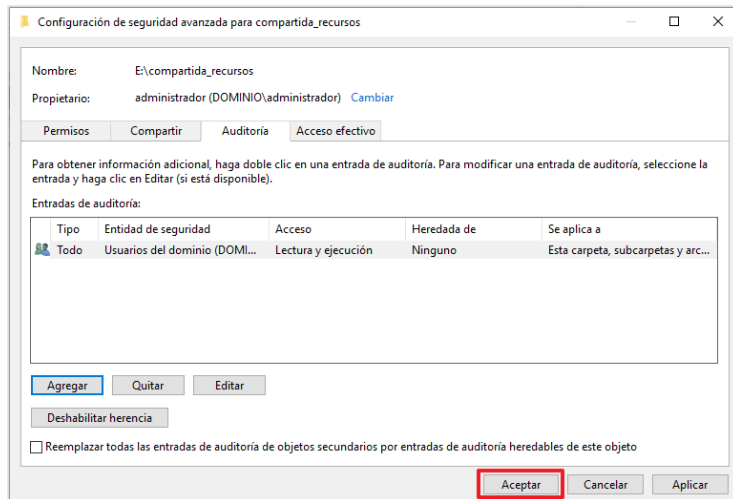
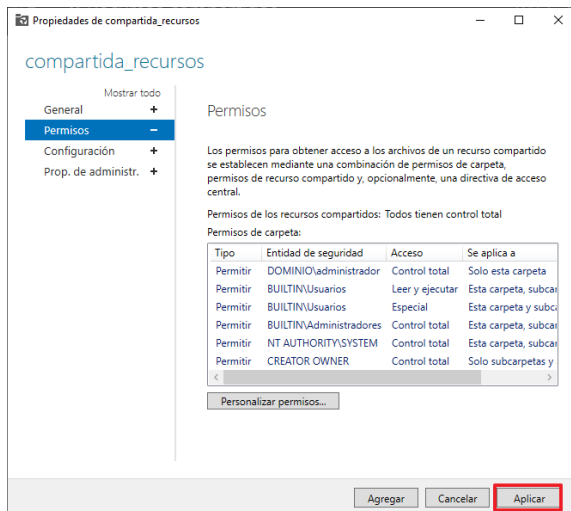
Paso	Descripción
126.	Seleccione, con el botón derecho, el recurso sobre el que desea gestionar la auditoría y pulse la opción “Propiedades”.  Nota: En este ejemplo se selecciona el recurso compartido creado anteriormente “compartida_recursos”.
127.	Acceda a la sección “Permisos” y pulse sobre “Personalizar permisos...”. 

Paso	Descripción
128.	Acceda a la pestaña “Auditoría” y configure ésta acorde a las necesidades de su organización. Por ejemplo, para añadir la auditoria sobre todos los usuarios del Dominio de Windows, pulse en “Agregar”.  The screenshot shows the 'Configuración de seguridad avanzada para compartida_recursos' window. The 'Auditoría' tab is selected. The 'Agregar' button is highlighted with a red rectangle. The window displays the name 'E:\compartida_recursos', the owner 'administrador (DOMINIO\administrador)', and a list of audit entries. Below the list are buttons for 'Agregar', 'Quitar', and 'Ver'. There is also a 'Deshabilitar herencia' button and a checkbox for 'Reemplazar todas las entradas de auditoría de objetos secundarios por entradas de auditoría heredables de este objeto'.
129.	Seleccione el objeto del directorio activo sobre el que quiere auditar haciendo clic sobre “Seleccionar una entidad de seguridad”.  The screenshot shows the 'Entrada de auditoría para compartida_recursos' window. The 'Seleccionar una entidad de seguridad' button is highlighted with a red rectangle. The window displays the 'Entidad de seguridad' field, the 'Tipo' dropdown set to 'Correcto', and the 'Se aplica a' dropdown set to 'Esta carpeta, subcarpetas y archivos'. Below these are the 'Permisos básicos' section with checkboxes for 'Control total', 'Modificar', 'Lectura y ejecución', 'Mostrar el contenido de la carpeta', 'Lectura', 'Escritura', and 'Permisos especiales'. There is also a checkbox for 'Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor' and a 'Borrar todo' button. At the bottom, there is a section for 'Agregar una condición' and 'Aceptar'/'Cancelar' buttons.

Paso	Descripción
130.	Escriba el nombre del grupo o usuario, en este caso, “usuario” y haga clic en “Comprobar nombres” para verificar el grupo/usuario: 
131.	Seleccione el nombre correcto del grupo/usuario a auditar: 
132.	Pulse “Aceptar” para confirmar. 

Paso	Descripción
133.	A continuación, seleccione el nivel de auditoria que desea. 
134.	Seleccione también el nivel de profundidad que necesite: 

Paso	Descripción
135.	Seleccione también los permisos que desea auditar:  Nota: Si requiere mayor nivel de detalle de los permisos a auditar, haga clic en “Mostrar permisos avanzados”. 

Paso	Descripción
136.	Haga clic en “Aceptar” para completar la configuración de la auditoria. 
137.	Haga clic en “Aceptar” una vez complete la configuración de la auditoria. 
138.	Haga clic en “Aplicar” para aplicar la configuración. 
139.	Cierre la ventana de configuración.

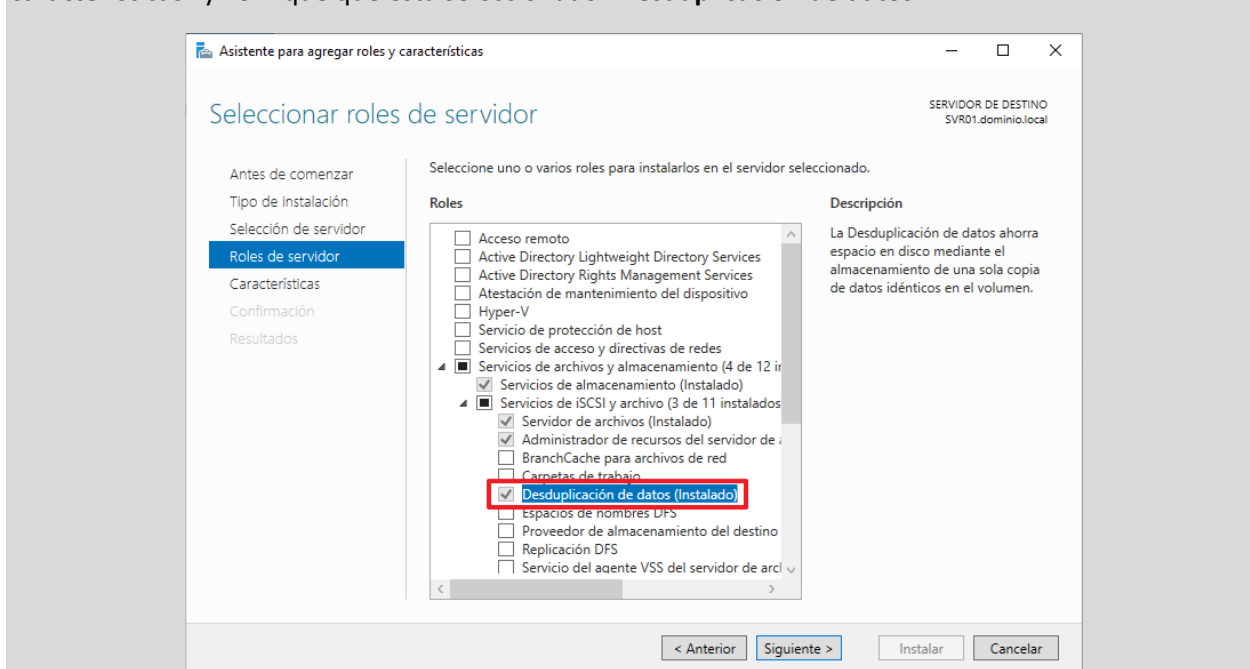
ANEXO A.3.9. ELIMINACIÓN DE DATOS DUPLICADOS.

La eliminación de datos duplicados es una característica que puede ayudar a reducir el impacto de los datos redundantes en los costos de almacenamiento. Cuando está habilitada, optimiza el espacio libre en un volumen mediante el examen de los datos contenidos en él, en busca de partes duplicadas en el volumen, de manera que optimiza redundancias sin poner en peligro la integridad o fidelidad de los datos.

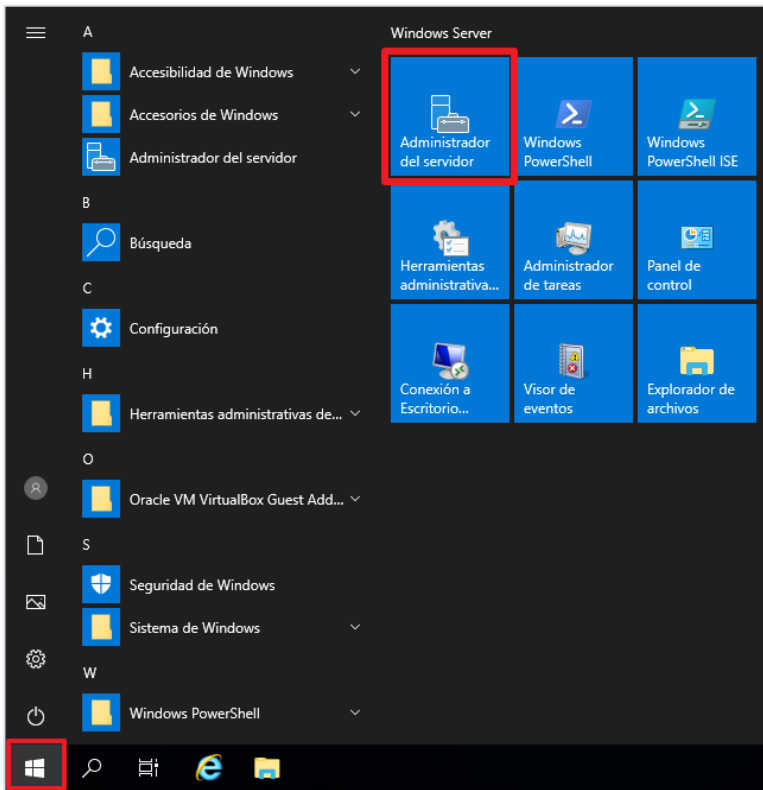
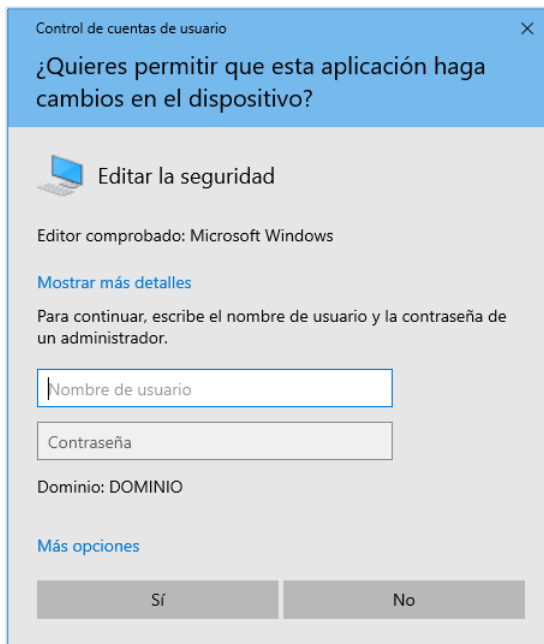
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

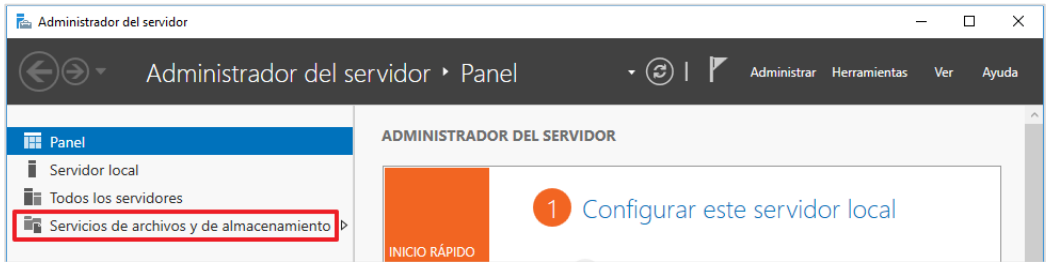
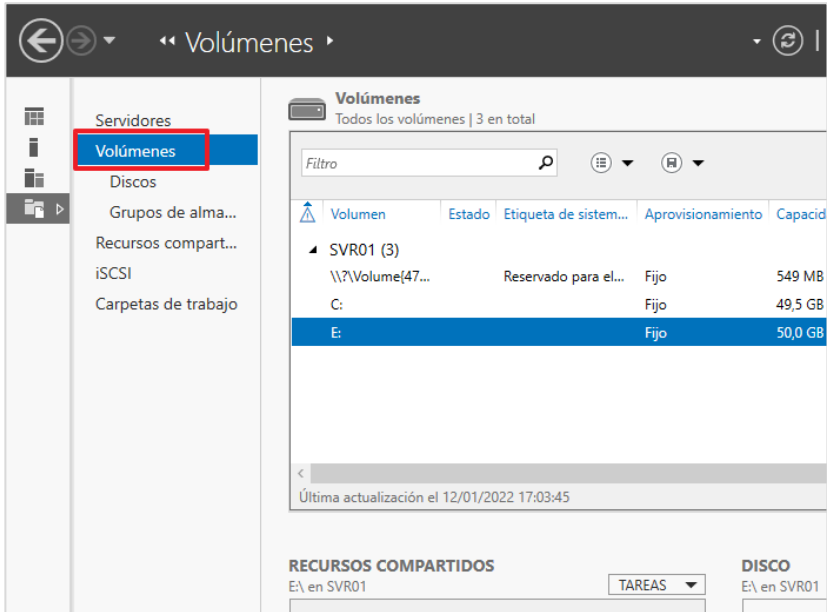
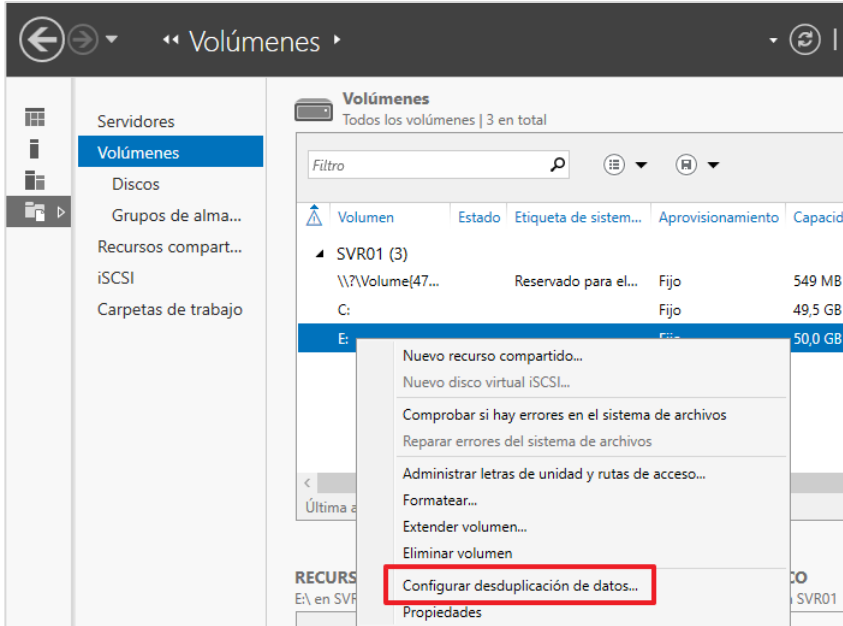
- a) [A.24.SEC-FS3]. Eliminación de datos duplicados.

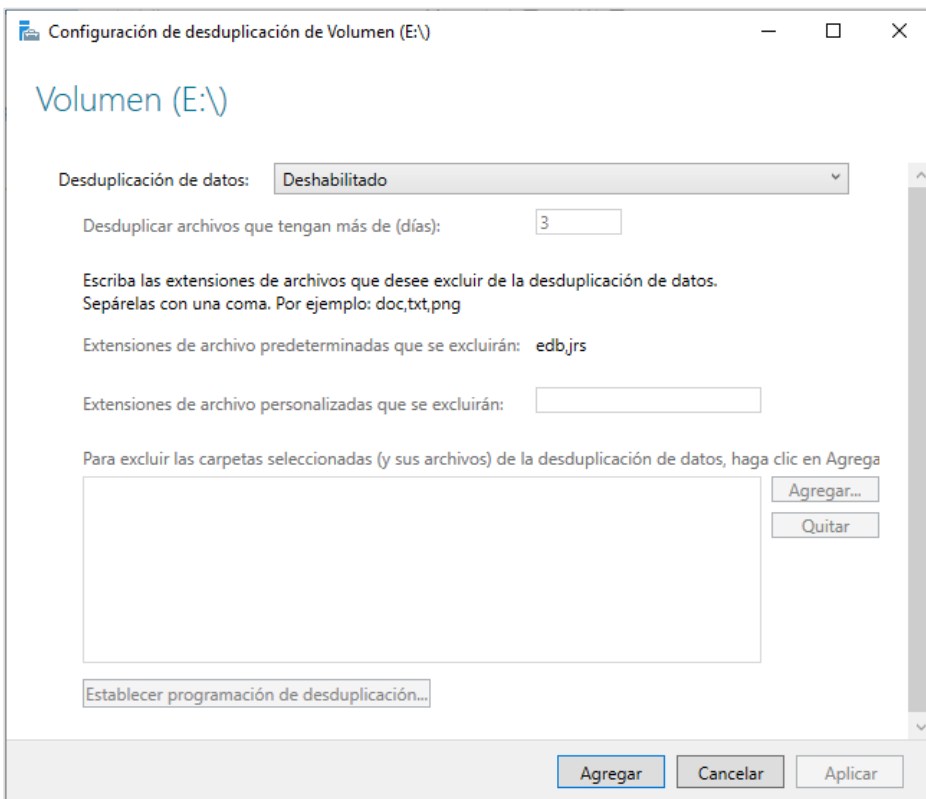
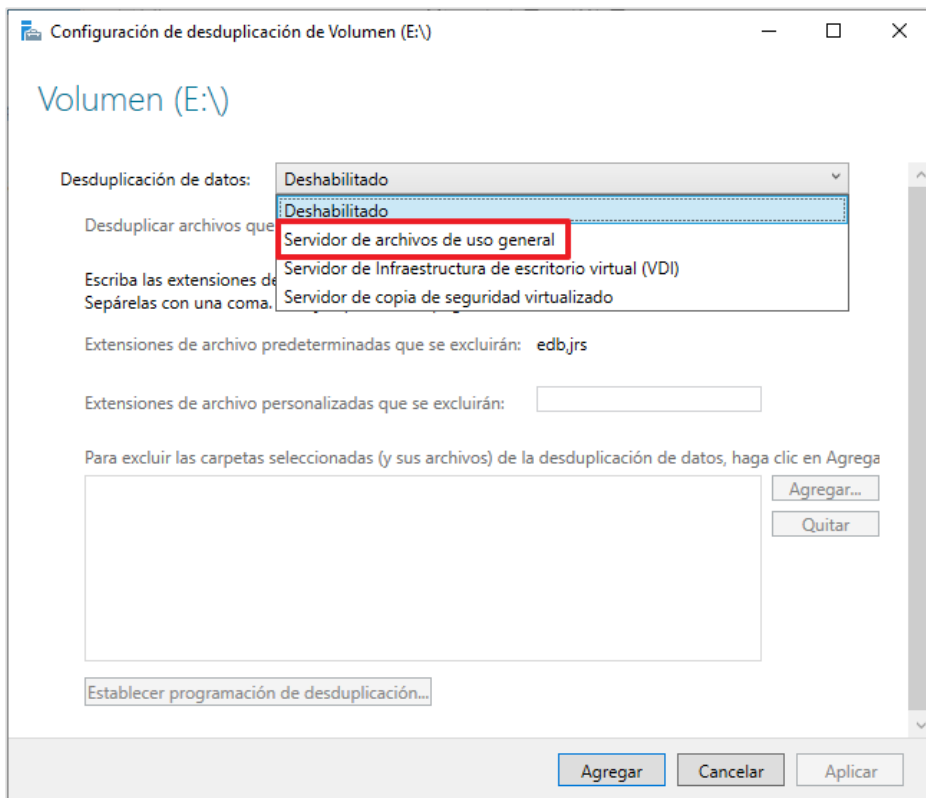
Nota: Antes de activar la eliminación de datos duplicados, verifique que la característica está instalada en el servidor. La característica forma parte del Rol “Servicio de archivos y almacenamiento”, para verificar si está instalado, en el Asistente para agregar roles y características, seleccione “Agregar Roles y características” y verifique que está seleccionado “Desduplicación de datos”.

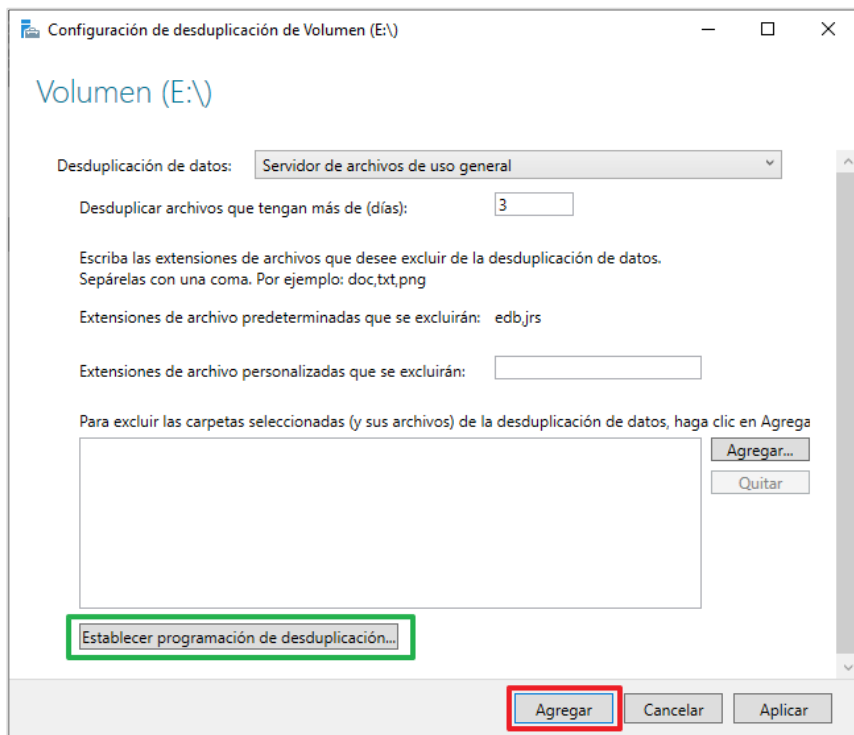
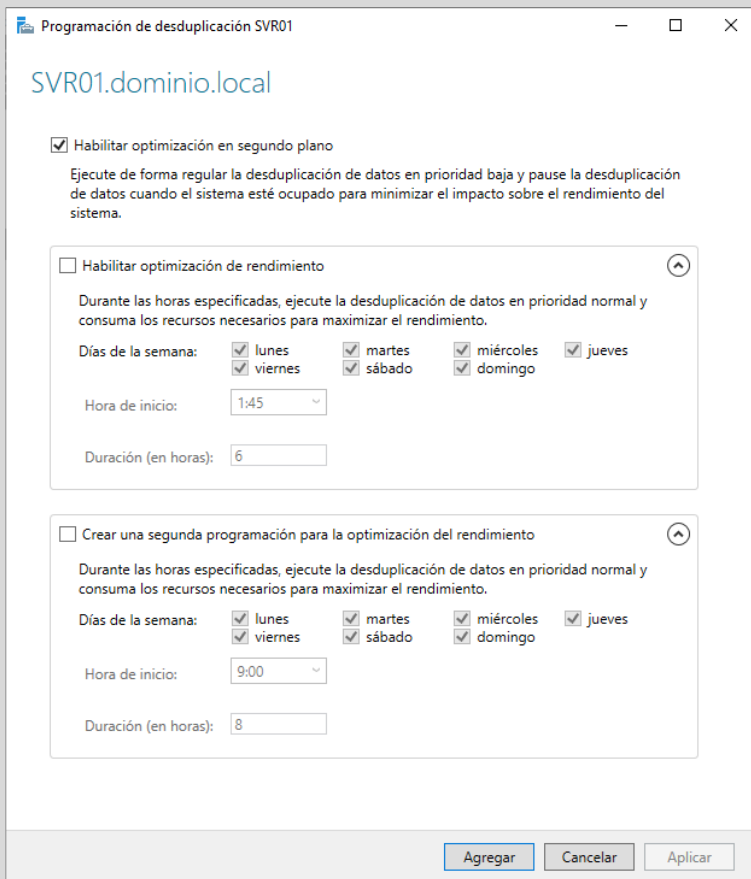


Paso	Descripción
140.	Inicie sesión en el servidor miembro donde tenga instalado el rol “Servidor de ficheros”.  Nota: Inicie sesión con una cuenta que sea Administrador del Servidor.

Paso	Descripción
141.	Abra el “Administrador del servidor”. Para ello, pulse sobre el botón correspondiente en el menú de inicio. 
142.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Proporcione las credenciales adecuadas. 

Paso	Descripción
143.	A continuación, pulse sobre “Servicios de archivos y de almacenamiento”. 
144.	Seleccione “Volúmenes”. 
145.	Haga clic derecho sobre el volumen en el que desea activar la deduplicación de archivos y seleccione “Configurar deduplicación de datos...” 

Paso	Descripción
146.	Se abrirá una ventana de configuración: 
147.	Seleccionar “Servidor de archivos de uso general” 

Paso	Descripción
148.	Pulse en “Agrega” para cerra la configuración.  Nota: Establezca la programación de la deduplicación para adaptarla a sus necesidades: 

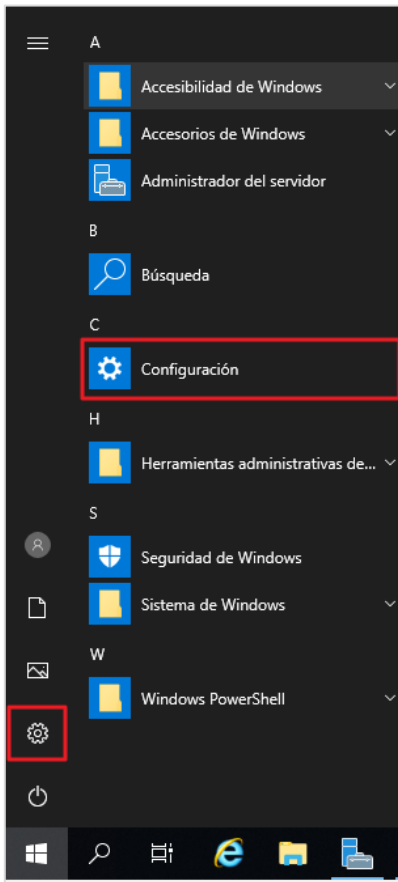
ANEXO A.3.10. MEDIDAS ANTI-RANSOMWARE HABILITADAS.

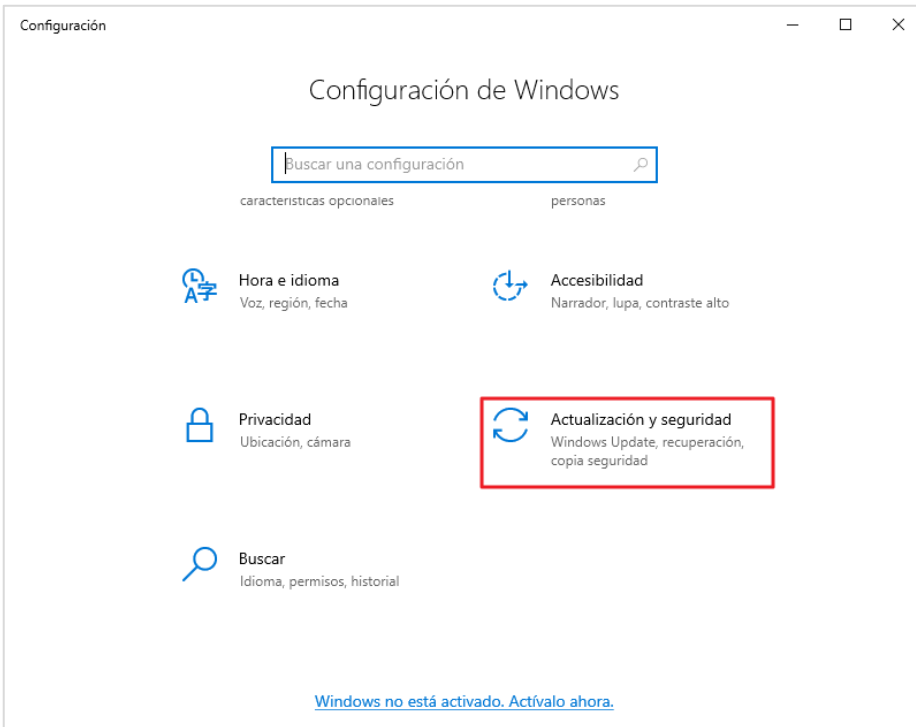
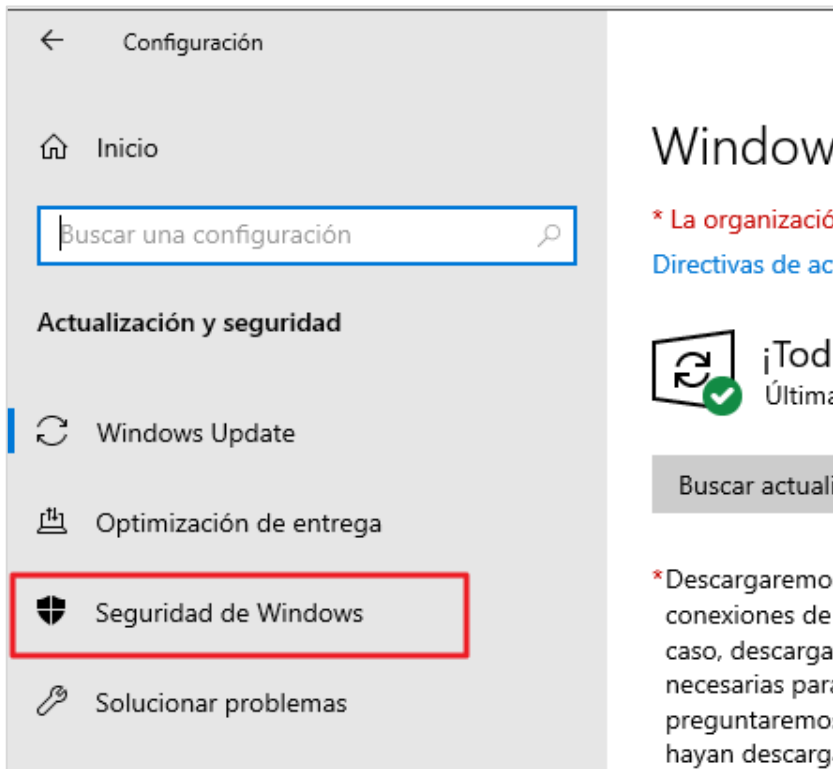
Se dispone de medidas anti-ransomware habilitadas. Si su infraestructura cuenta con un sistema antivirus con dichas funcionalidades, éstas deberán ser habilitadas por los administradores para garantizar la seguridad ante el riesgo de ransomware.

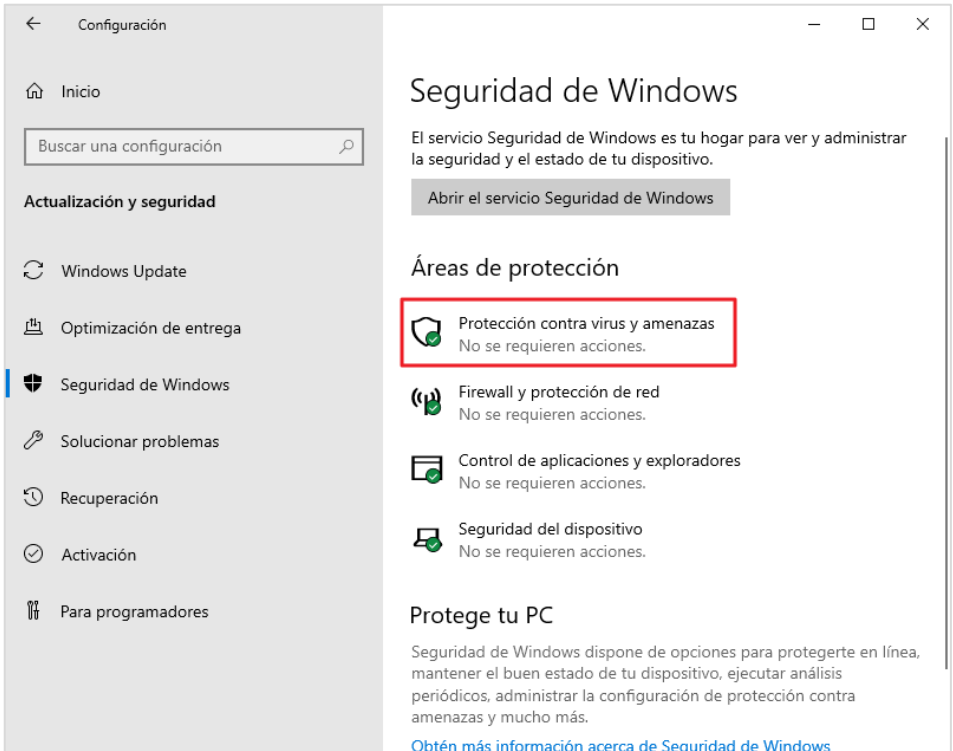
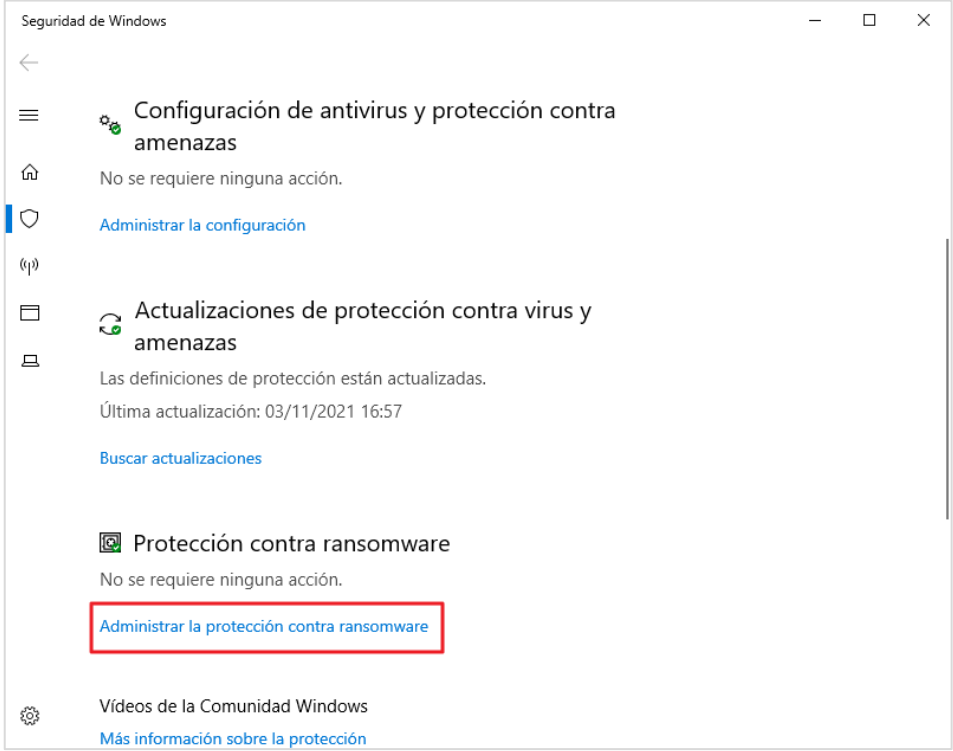
En el caso de no contar con ninguna medida anti-ransomware y si está haciendo uso del antivirus Windows Defender, podrá emplear los siguientes pasos para habilitar esta funcionalidad.

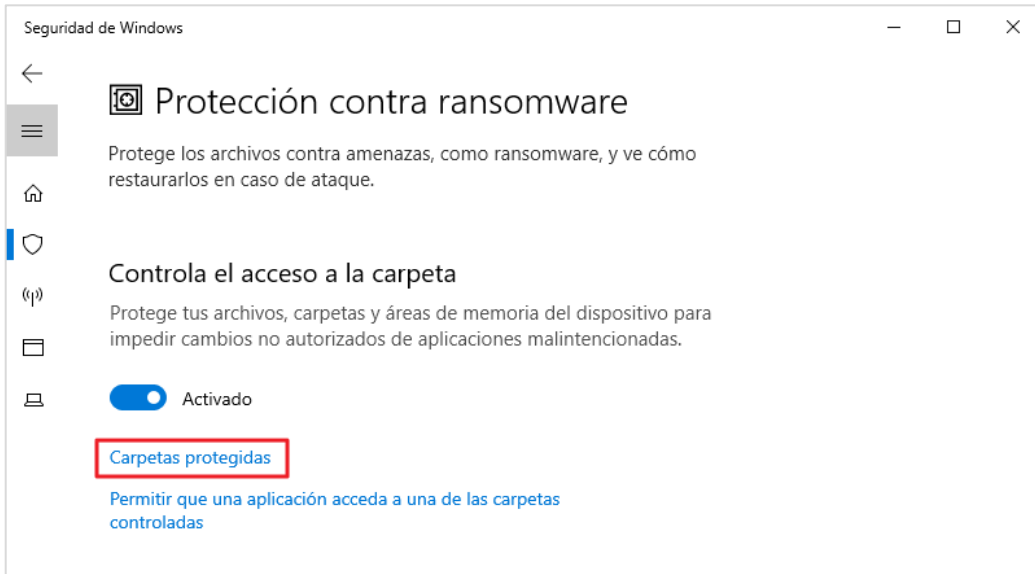
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.13.SEC-FS1]** Se dispone de medidas anti ransomware habilitadas.
- b) **[A.11.SEC-FS1]** Se ha reforzado el uso del protocolo SMB.

Paso	Descripción
149.	Inicie sesión en un servidor del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-573A21.
150.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio o con un usuario con privilegios de administración sobre el servidor.
151.	Ejecute el aplicativo “Configuración” por medio del botón “Inicio → Configuración”.  Nota: La imagen ilustra dos formas de acceder al mismo panel de configuración. Únicamente deberá pulsar sobre una de las dos opciones.

Paso	Descripción
152.	En el menú de Configuración de Windows, localice el apartado “Actualización y seguridad” y acceda al mismo. 
153.	A continuación, pulse sobre “Seguridad de Windows”. 

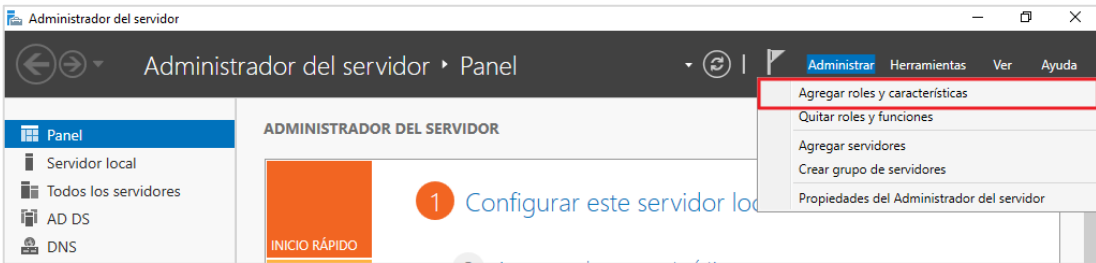
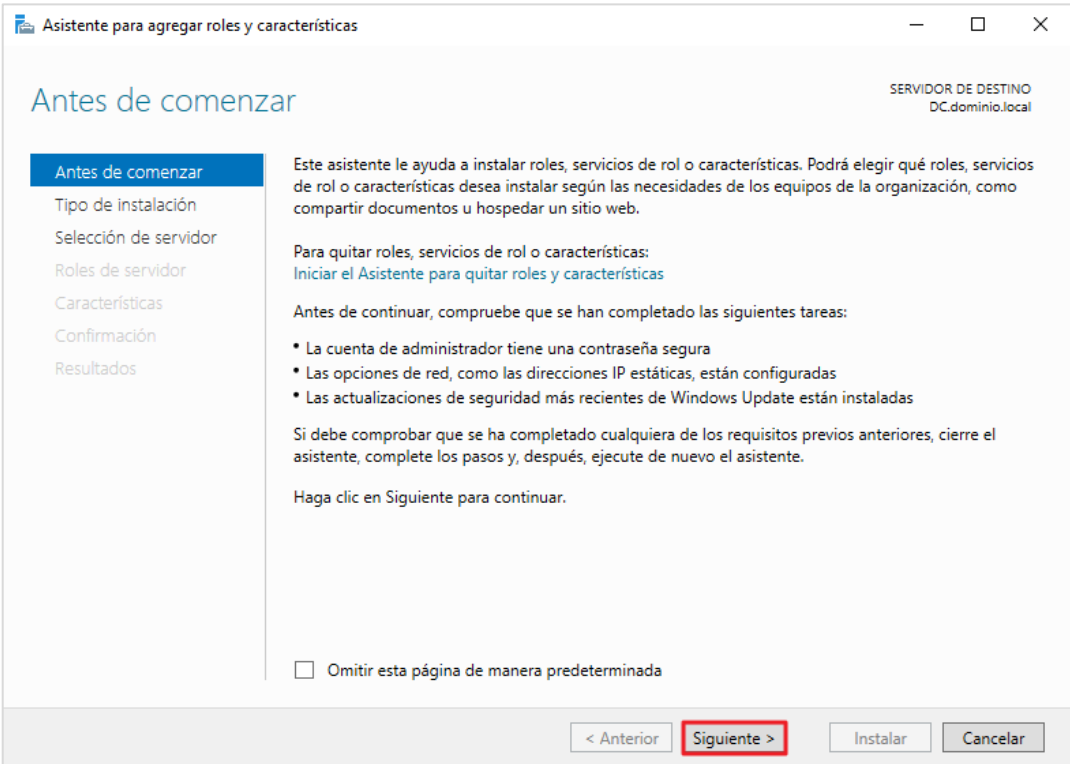
Paso	Descripción
154.	En el nodo de configuración, pulse sobre “Protección contra virus y amenazas” 
155.	Se abrirá el panel de seguridad de Windows con las distintas funciones de Windows Defender. Localice la funcionalidad “Protección contra ransomware” y haga clic sobre “Administrar la protección contra ransomware”. 

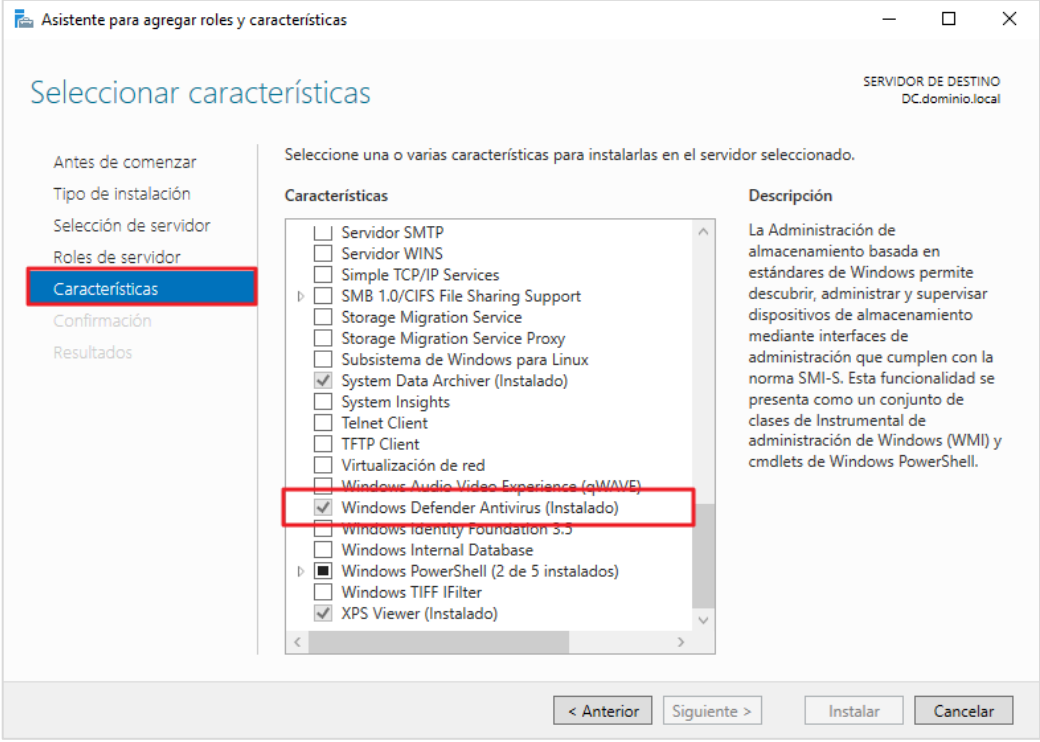
Paso	Descripción
156.	Por defecto, la mayoría de los sistemas mantienen dicha protección desactivada, en este caso, deberá habilitar la funcionalidad pulsando sobre la barra de activación. 
157.	Al habilitar la funcionalidad, se protegen automáticamente ciertas rutas del sistema. Puede gestionar las rutas añadiendo o quitando carpetas desde el apartado “Carpetas protegidas”. 

Adicionalmente, se recomienda que se disponga de un antivirus actualizado.

En el caso de no contar con otro antivirus, Windows Defender estará habilitado como antivirus por defecto en el equipo, para evaluar la activación y estado de dicho elemento deberá realizar los siguientes pasos.

Paso	Descripción
158.	Inicie sesión en un servidor del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-573A21.
159.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
160.	Ejecute el “ Administrador del Servidor ” por medio del botón “Inicio → Administrador del Servidor ”.

Paso	Descripción
161.	Pulse sobre el botón “Administrar” en la esquina superior derecha y sobre el menú desplegable pulse sobre “Agregar roles y características”. 
162.	Se iniciará el asistente para agregar roles y características. Pulse sobre “Siguiente >” hasta llegar al apartado “Características”. 

Paso	Descripción
163.	Sobre el apartado “Características” y utilizando la barra de desplazamiento, localice la característica “Windows Defender Antivirus”. Si en su sistema se encuentra ya instalada dicha característica, aparecerá marcada y no podrá seleccionarla. 
164.	En el caso de haber desinstalado Windows Defender de su sistema, marque la opción anterior y continúe con el asistente para realizar la instalación de Windows Defender sobre Windows Server 2019. Nota: Por defecto, esta característica se encuentra instalada en los servidores con el sistema operativo Windows Server 2019.

ANEXO A.3.11. DISCOS DE DATOS CIFRADOS.

Para cumplir con las configuraciones descritas en el riesgo **A.25.SEC-FS1**, el sistema operativo deberá contar con una característica o software que permita el cifrado de los discos que contienen los datos.

En este ejemplo, se hace uso de la característica nativa de Windows BitLocker. Para habilitar y configurar este software puede guiarse de la siguiente tabla, la cual incluye las directivas a aplicar para una primera configuración de la funcionalidad.

Todas las directivas se encuentran bajo los siguientes nodos de configuración:

- Configuración de equipo → Plantillas administrativas → Componentes de Windows → Cifrado de la unidad BitLocker → Unidades de datos extraíbles
- Configuración de equipo → Plantillas administrativas → Componentes de Windows → Cifrado de la unidad BitLocker → Unidades de datos fijas

Categoría	Directiva	Configuración
[A.25.SEC-FS1] El disco de datos está cifrado.	Elegir cómo se pueden recuperar unidades extraíbles protegidas por BitLocker	Habilitado
	Permitir agente de recuperación de datos.	Habilitado
	Configurar almacenamiento de usuario de la información de recuperación de BitLocker	Permitir contraseña de recuperación de 48 dígitos. Permitir clave de recuperación de 256 bits
	Guardar información de recuperación de BitLocker en AD DS para unidades de datos extraíbles.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades de datos extraíbles.	Deshabilitado
	Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker	Habilitado
	Permitir agente de recuperación de datos.	Habilitado
	Configurar almacenamiento de usuario de la información de recuperación de BitLocker	Permitir contraseña de recuperación de 48 dígitos. Permitir clave de recuperación de 256 bits
	Guardar información de recuperación de BitLocker en AD DS para unidades de datos fijas.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades de datos fijas.	Deshabilitado

